

STATE OF CALIFORNIA
STANDARD AGREEMENT AMENDMENT
 STD. 213 A (Rev 6/03)

CHECK HERE IF ADDITIONAL PAGES ARE ATTACHED

274

Pages

AGREEMENT NUMBER	AMENDMENT NUMBER
5-06-58-22 (DTS 06E1392)	13
REGISTRATION NUMBER	

- This Agreement is entered into between the State Agency and Contractor named below:
 STATE AGENCY'S NAME
California Technology Agency (Formerly Office of the State Chief Information Officer (OCIO))
 CONTRACTOR'S NAME
MCI Network Services, Inc. or MCI Financial Management, Corp. on behalf of MCI Communications Services, Inc d/b/a Verizon Business Services and other authorized Verizon companies
- The term of this Agreement is 1/30/2007 through 1/29/2014
- The maximum amount of this agreement after this amendment is: N/A
- The parties mutually agree to this amendment as follows. All actions noted below are by this reference made a part of the Agreement and incorporated herein: Verizon Business will be providing the State with Managed Security Services for the network environment. Additional Service Agreements (SLAs) have also been provided as part of this amendment to provide service quality assurance for the proposed services.

A. This amendment includes the following changes, Subject CALNET 2, MSA 3 (Verizon Business):

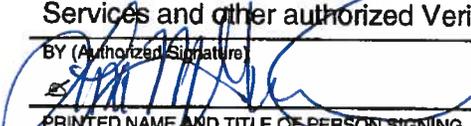
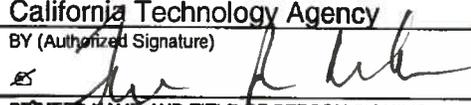
The California Prison Health Care Services Letter of Concurrence (LOC) that was approved by the Office of Technology Services on February 9, 2011, services are included as additional offerings. This amendment includes the following services:

Pursuant to Section 28 Contract Modifications Under RFP DGS-2053, the following Amendments and changes are made to the following Sections and attachments:

Continued on the next page.

This Agreement is effective July 1, 2011 or upon DGS approval, whichever is later.
 All other terms and conditions of the original agreement shall remain the same.

IN WITNESS WHEREOF, this Agreement has been executed by the parties hereto.

CONTRACTOR		CALIFORNIA Department of General Services Use Only	
CONTRACTOR'S NAME (If other than an individual, state whether a corporation, partnership, etc.) <u>MCI Network Services, Inc. or MCI Financial Management, Corp. on behalf of MCI Communications Services, Inc d/b/a Verizon Business Services and other authorized Verizon companies</u>		 GENERAL SERVICES LEGAL SERVICES	
BY (Authorized Signature) 	DATE SIGNED (Do not type) <u>8/24/11</u>		
PRINTED NAME AND TITLE OF PERSON SIGNING <u>Lisa M. Guignard, Director-Pricing/Contract Management</u>		DEPARTMENT OF GENERAL SERVICES PROCUREMENT DIVISION APPROVED BY  DATE <u>8/24/11</u>	
ADDRESS <u>22001 Loudoun County Parkway, Ashburn, VA 20147</u>			
STATE OF CALIFORNIA AGENCY NAME <u>California Technology Agency</u>			
BY (Authorized Signature) 	DATE SIGNED (Do not type) <u>8/10/11</u>	<input type="checkbox"/> Exempt per:	
PRINTED NAME AND TITLE OF PERSON SIGNING <u>Tricia Rodriguez - Manager - Purchasing and Support Services</u>			
ADDRESS <u>P.O. Box 1810, MS Y-18, Rancho Cordova, CA 95741-1810</u>			

Continuation

STD 213A Standard Agreement Amendment 5-06-58-22 (DTS 06E1392) 13

1. 6.3.3.8a Converged Services, IP and Network IP Transport Services – Security Services Attachment 3 has been added to include additional network security requirements, and includes the following offerings:

- Professional Security Services (PSS) additions, pages 1-3
 - Data Protection subheading addition, page 2
 - Data Protection and DLP (Roadmap, Strategy & Implementation) addition, page 2
 - MSS Configuration Support addition, page 3
- Managed Security Services (MSS) heading and description additions, page 4
 - Service Levels to Device Configurations additions, pages 4-27
 - Serviced Device: Firewall heading addition, page 28
 - Firewall Monitoring Only subheading addition, page 28
 - Firewall Monitoring Only Standard to Additional Customer Certificate additions, pages 28-33
 - Firewall Management and Monitoring subheading addition, page 34
 - Firewall Management & Monitoring Standard to Firewall Management & Monitoring High Availability Gigabit Standard additions, pages 34-35
 - Firewall Management and Monitoring Platinum subheading addition, page 36
 - Firewall Management & Monitoring Platinum to Additional Customer Certificate additions, pages 36-39
 - Additional Service Tickets (Apply to All Management and Monitoring Configurations) subheading addition, page 39
 - Regular (1 Service Ticket) to Urgent (8 Service Tickets) additions, pages 39-40
- Serviced Device: Network Intrusion Detection Service (NIDS) subheading addition, page 41
 - Network Intrusion Detection (NIDS) Monitoring Only subheading addition, page 41
 - Network Intrusion Detection (NIDS) Monitoring Only Standard to Network Intrusion Detection (NIDS) Monitoring Only High Availability Gigabit Standard additions, pages 41-42
 - Network Intrusion Detection (NIDS) Monitoring Only Platinum subheading addition, page 43
 - Network Intrusion Detection (NIDS) Monitoring Only Platinum to Additional Customer Certificate additions, pages 43-45
 - Network Intrusion Detection (NIDS) Management and Monitoring subheading addition, page 46
 - Network Intrusion Detection (NIDS) Management and Monitoring Standard to Network Intrusion Detection (NIDS) Management and Monitoring High Availability Gigabit Standard additions, pages 46-47
 - Network Intrusion Detection (NIDS) Management and Monitoring Platinum subheading addition, page 48
 - Network Intrusion Detection (NIDS) Management and Monitoring Platinum to Additional Customer Certificate additions, pages 48-51
 - Additional Service Tickets (Apply to All Management and Monitoring Configurations) subheading addition, page 51
 - Regular (1 Service Ticket) to Urgent (8 Service Tickets) additions, pages 51-53
- Serviced Device: Network Intrusion Prevention Service (NIPS) subheading addition, page 54
 - Network Intrusion Prevention (NIPS) Monitoring Only subheading addition, page 54
 - Network Intrusion Prevention (NIPS) Monitoring Only Standard subheading addition, page 54
 - Network Intrusion Prevention (NIPS) Monitoring Only Standard to Network Intrusion Prevention (NIPS) Monitoring Only High Availability Gigabit Standard additions, pages 54-55
 - Network Intrusion Prevention (NIPS) Monitoring Only Platinum subheading addition, page 56
 - Network Intrusion Prevention (NIPS) Monitoring Only Platinum to Site Set Up Local Event Collector additions, pages 56-57
 - Network Intrusion Prevention (NIPS) Management and Monitoring Service subheading addition, page 58
 - Network Intrusion Prevention (NIPS) Management and Monitoring Standard subheading addition, page 58

- Network Intrusion Prevention (NIPS) Management and Monitoring_Standard to Network Intrusion Prevention (NIPS) Management and Monitoring High Availability Gigabit Standard additions, pages 58-59
- Network Intrusion Prevention (NIPS) Management and Monitoring Platinum subheading addition, page 59
 - Network Intrusion Prevention (NIPS) Management and Monitoring_Platinum to Site Set Up Local Event Collector additions, pages 60-62
- Additional Service Tickets (Apply to All Management and Monitoring Configurations) subheading addition, page 63
 - Regular (1 Service Ticket) to Urgent (8 Service Tickets) additions, pages 63-64
- Serviced Device: Proxy Server subheading and description additions, page 65
 - Proxy Server Monitoring Only subheading addition, page 65
 - Proxy Server Monitoring Only Platinum to Additional Customer Certificate additions, pages 66-67
 - Proxy Server Management and Monitoring subheading and description addition, page 68
 - Proxy Server Management & Monitoring Platinum to Additional Customer Certificate additions, pages 68-71
 - Additional Service Tickets (Apply to All Management and Monitoring Configurations) subheading addition, page 72
 - Regular (1 Service Ticket) to Urgent (8 Service Tickets) additions, pages 72-74
- Serviced Device: Managed Security Event Management (SEM) subheading and description additions, page 75
 - Managed SEM Platform to Managed SEM Platform Site Set-Up Fee(s) additions, pages 76-77
- Applicable Service Level Agreements - Managed Security Service (MSS) addition , page 78
 - Standard Unavailable Device Notification – Monitoring Only, and Management and Monitoring Security Service addition, page 78
 - Standard Health Incident Notification - Monitoring Only, and Management and Monitoring Security Service addition, page 78
 - Standard Active Incident Escalation - Monitoring Only, and Management and Monitoring Security Service addition, page 78
 - Platinum Unavailable Device Notification - Monitoring Only, and Management and Monitoring Security Service addition, page 78
 - Platinum Health Incident Notification - Monitoring Only, and Management and Monitoring Security Service addition, page 78
 - Platinum Active Incident Escalation - Monitoring Only, and Management and Monitoring Security Service addition, page 78
 - Standard Change Request Acceptance – Management and Monitoring addition, page 78
 - Platinum Change Request Acceptance – Management and Monitoring addition, page 78
 - Standard Change Request Implementation – Management and Monitoring addition, page 78
 - Platinum Change Request Implementation – Management and Monitoring addition, page 78

Add Attachment 3 Section 6.3.3.8a (Pages 1-78).

2. 6.3.3.8a Converged Services, IP and Network IP Transport Services – Security Services Attachment 4 has been added to include additional network security requirements, and includes the following offerings:

- Professional Security Services (PSS) additions, page 1
 - Data Protection and DLP (Roadmap, Strategy & Implementation) addition, page 1
 - MSS Configuration Support addition, page 1
- Managed Security Services (MSS) heading addition, page 2
 - Firewall Monitoring Only and Management and Monitoring subheading addition, page 2
 - Firewall Monitoring Only subheading addition, page 2
 - Firewall Monitoring Only Standard to Additional Customer Certificate additions, page 2
 - Firewall Management and Monitoring subheading addition, page 3
 - Firewall Management & Monitoring Standard to Additional Customer Certificate additions, pages 3-4
 - Additional Service Tickets subheading addition, page 4
 - Regular (1 Service Ticket) to Urgent (8 Service Tickets) additions, page 4

- Network Intrusion Detection Service (NIDS) subheading addition, page 5
- Network Intrusion Detection (NIDS) Monitoring Only subheading addition, page 5
 - Network Intrusion Detection (NIDS) Monitoring Only Standard to Additional Customer Certificate additions, pages 5-6
- Network Intrusion Detection (NIDS) Management and Monitoring subheading addition, page 6
 - Network Intrusion Detection (NIDS) Management and Monitoring Standard to Urgent (8 Service Tickets) additions, pages 6-7
- Network Intrusion Prevention Service (NIPS) subheading addition, page 8
- Network Intrusion Prevention Services (NIPS) Monitoring Only subheading addition, page 8
 - Network Intrusion Prevention (NIPS) Monitoring Only Standard to Site Set Up Local Event Collector additions, page 8
- Network Intrusion Prevention Services (NIPS) Management and Monitoring subheading addition, page 9
 - Network Intrusion Prevention (NIPS) Management and Monitoring Standard to Site Set Up Local Event Collector additions, pages 9-10
- Additional Service Tickets subheading addition, page 10
 - Regular (1 Service Ticket) to Urgent (8 Service Tickets) additions, page 10
- Proxy Server subheading addition, page 11
- Proxy Server Monitoring Only subheading addition, page 11
 - Proxy Server Monitoring Only Platinum to Additional Customer Certificate additions, page 11
- Proxy Server Management and Monitoring Service subheading addition, page 11
 - Proxy Server Management & Monitoring Platinum to Additional Customer Certificate additions, pages 11-12
- Additional Service Tickets subheading addition, page 12
 - Regular (1 Service Ticket) to Urgent (8 Service Tickets) additions, page 12
- Managed Security Event Management (SEM) subheading addition, page 13
- Security Event Management (SEM) Platform subheading addition, page 13
 - Managed SEM Platform to Managed SEM Platform Site Set-Up Fee(s) additions, pages 13-14
- Note to Taxes and Surcharges additions, page 15

Add Attachment 4 Section 6.3.3.8a (Pages 1-15).

3. 6.3.4.3 Converged Services, IP Telephony Business Line Services Attachment 3 has been modified to include Managed Wireless LAN (MWLAN) services as follows:

- Managed Wireless LAN (MWLAN) heading and service description additions, pages 24-30
 - MWLAN Controller Full (Small) addition, page 31
 - MWLAN Controller Full (Medium) addition, page 32
 - MWLAN Controller Full (Large) addition, page 33
 - Take Over an Existing MWLAN Controller Device addition, page 34
 - New Device – MWLAN Controller Installation, Configuration and Implementation Support addition, page 35
 - MWLAN Access Point Full addition, page 36
 - Take Over an Existing MWLAN Access Point Device addition, page 37
 - New Device – MWLAN Access Point Installation, Configuration and Implementation Support addition, page 38
 - Managed Power Over Ethernet Mid-Span Device MWLAN Full addition, page 39
 - Take Over an Existing MWLAN Power Over Ethernet Mid-Span Device addition, page 40
 - New Device – MWLAN Power Over Ethernet Mid-Span Device Installation, Configuration and Implementation Support addition, page 41
 - Managed Authentication Appliance MWLAN Full addition, page 42
 - Take Over an Existing MWLAN Authentication Appliance addition, page 43
 - New Device – MWLAN Authentication Appliance Installation, Configuration and Implementation Support addition, page 44
 - Device OS Change addition, page 44
 - MWLAN Intra-building Move (Wireless Device - labor only) addition, page 45
 - MWLAN Move, Inter-building or Across Town (Wireless Device - labor only) addition, page 45
 - MWLAN Exchange (Wireless Device - labor only) addition, page 45

- MWLAN Field Service Technicians (labor only) Normal business hours (M-F, 8 a.m. to 5 p.m.) addition, page 46
- MWLAN Field Service Technicians (labor only) After hours (M-F, 5 p.m. to 8 a.m., including weekends and holidays) addition, page 46
- MWLAN Managed Take Over subheading and Feature additions, page 47
- MWLAN Managed Implementation subheading and Feature additions, pages 48-49
- Applicable Service Level Agreements additions, page 50:
 - Service Availability Percentage - Managed Router and Managed LAN Service correction addition to Section 6.3.4.3, page 50
 - Proactive Notification SLA – Managed Router and Managed LAN Service/WLAN Service addition, page 50
 - Provisioning correction addition to Section 6.3.4.3, page 50
 - Time to Repair (TTR) – Managed Wireless LAN (WLAN) Service addition, page 50

Replace Attachment 3 Section 6.3.4.3 (Pages 1-24) with amended section (Pages 1-50)

4. 6.3.4.3 Converged Services, IP Telephony Business Line Services Attachment 4 has been modified to include Managed Wireless LAN (MWLAN) services as follows:

- Managed Wireless LAN (MWLAN) heading addition, page 7
- MWLAN Controller Full (Small) addition, page 7
- MWLAN Controller Full (Medium) addition, page 7
- MWLAN Controller Full (Large) addition, page 7
- Take Over an Existing MWLAN Controller Device addition, page 7
- New Device – MWLAN Controller Installation, Configuration and Implementation Support addition, page 7
- MWLAN Access Point Full addition, page 7
- Take Over an Existing MWLAN Access Point Device addition, page 7
- New Device – MWLAN Access Point Installation, Configuration and Implementation Support addition, page 7
- Managed Power Over Ethernet Mid-Span Device MWLAN Full addition, page 7
- Take Over an Existing MWLAN Power Over Ethernet Mid-Span Device addition, page 7
- New Device – MWLAN Power Over Ethernet Mid-Span Device Installation, Configuration and Implementation Support addition, page 8
- Managed Authentication Appliance MWLAN Full addition, page 8
- Take Over an Existing MWLAN Authentication Appliance addition, page 8
- New Device – MWLAN Authentication Appliance Installation, Configuration and Implementation Support addition, page 8
- Device OS Change addition, page 8
- MWLAN Intra-building Move (Wireless Device - labor only) addition, page 8
- MWLAN Move, Inter-building or Across Town (Wireless Device - labor only) addition, page 8
- MWLAN Exchange (Wireless Device - labor only) addition, page 8
- MWLAN Field Service Technicians (labor only) Normal business hours (M-F, 8 a.m. to 5 p.m.) addition, page 9
- MWLAN Field Service Technicians (labor only) After hours (M-F, 5 p.m. to 8 a.m., including weekends and holidays) addition, page 9
- MWLAN Managed Take Over subheading and Feature additions, page 9
- MWLAN Managed Implementation subheading and Feature additions, page 9

Replace Attachment 4 Section 6.3.4.3 (Pages 1-7) with amended section (Pages 1-10)

5. 6.3.6.1 Converged Services, Managed IP Video Conference Services Attachment 3 has been modified to include Video Conferencing Management services as follows:

- Video Conferencing Management Services subheading and service description additions, pages 14-16
- Video Conferencing subheading addition, page 17
- Video Conferencing Endpoints: Desktop/Rooms subheading addition, page 17
 - Video Conferencing Codec addition, page 17

- Immersive Video Conferencing Endpoints: Room subheading addition, page 17
 - Immersive Video Conferencing room, small tier, 1 screen addition, page 17
 - Immersive Video Conferencing room, large tier, 3 screens addition, page 17
- Video Conferencing Transition Services service description additions, pages 18-19
- Video Conferencing - Transition Services subheading addition, page 20
 - Design Phase Video Conferencing Environment addition, pages 20-21
 - Move under Management addition, pages 22-23
 - Move under Management – Immersive Video Conferencing addition, pages 24-25
 - Documentation of Managed Take-Over of an Existing Video Conferencing Environment addition, pages 26-27
 - MCD Activities for Video Conferencing Environment addition, page 28
 - Risk & Stability Assessment of Video Conferencing Environment addition, page 29
 - Capacity Planning of Video Conferencing Environment addition, pages 30-31
 - Custom Solution Development for Video Conferencing Environment addition, pages 32-35

Replace Attachment 3 Section 6.3.6.1 (Pages 1-15) with amended section (Pages 1-35)

6. 6.3.6.1 Converged Services, Managed IP Video Conference Service Attachment 4 has been modified to include Video Conferencing Management services as follows:

- Video Conferencing Management Services subheading addition, page 5
- Video Conferencing Endpoints: Desktop/Rooms subheading addition, page 5
 - Video Conferencing Codec addition, page 5
- Immersive Video Conferencing Endpoints: Room subheading addition, page 5
 - Immersive Video Conferencing room, small tier, 1 screen addition, page 5
 - Immersive Video Conferencing room, large tier, 3 screens addition, page 5
- Video Conferencing Transition Services subheading addition, page 6
 - Design Phase Video Conferencing Environment addition, page 6
 - Move under Management addition, page 6
 - Move under Management – Immersive Video Conferencing addition, page 6
 - Documentation of Managed Take-Over of an Existing Video Conferencing Environment addition, page 6
 - MCD Activities for Video Conferencing Environment addition, page 6
 - Risk & Stability Assessment of Video Conferencing Environment addition, page 6
 - Capacity Planning of Video Conferencing Environment addition, page 6
 - Custom Solution Development for Video Conferencing Environment addition, page 6

Replace Attachment 4 Section 6.3.6.1 (1-4) with amended section (1-7)

7. MSA 3 Service Level Agreements have been modified to include WLAN and Security Services, and updates for consistency as follows:

- DTS/ONS changed to OTech/STND, pages 328-374
- 6.3.14.2.1 General Requirements (M), second bullet-first line, addition of “or service”, page 338
- 6.3.14.2.13.1 Proactive Notification SLA –Managed Router and Managed LAN Service – addition of WLAN Service to title; and Converged Services, IP and Network IP Transport – Managed WLAN Service addition, page 363
- 6.3.14.2.14 Provisioning – addition of Converged Services, IP and Network IP Transport – Managed WLAN Service, page 365
- 6.3.14.2.17 Time to Repair (TTR) – Major section number changed to 6.3.14.2.16, page 368-a
- 6.3.14.2.18 Time to Repair (TTR) – Minor section number changed to 6.3.14.2.17, page 368-b
- 6.3.14.2.18 Time to Repair (TTR) – Managed Wireless LAN (WLAN) Service addition, page 368-c
- 6.3.14.2.19 a Standard Unavailable Device Notification – Monitoring Only and Management and Monitoring Security Service addition, page 368-e
- 6.3.14.2.19 b Standard Health Incident Notification – Monitoring Only, and Management and Monitoring Security Service addition, page 368-f

- 6.3.14.2.19 c Standard Active Incident Escalation – Monitoring Only, and Management and Monitoring Security Service addition, pages 368-g - 368-h
- 6.3.14.2.19 d Platinum Unavailable Device Notification – Monitoring Only, and Management and Monitoring Security Service addition, page 368-i – 368-j
- 6.3.14.2.19 e Platinum Health Incident Notification - Monitoring Only, and Management and Monitoring Security Service addition, page 368-k
- 6.3.14.2.19 f Platinum Active Incident Escalation - Monitoring Only, and Management and Monitoring Security Service addition, page 368-l
- 6.3.14.2.19 g Standard Change Request Acceptance – Management and Monitoring addition, page 368-m
- 6.3.14.2.19 h Platinum Change Request Acceptance - Management and Monitoring addition, page 368-n
- 6.3.14.2.19 i Standard Change Request Implementation - Management and Monitoring addition, page 368-o
- 6.3.14.2.19 j Platinum Change Request Implementation - Management and Monitoring addition, page 368-p

Replace Attachment 4 Section 6.3.328 (Pages 328-374) with amended section (Pages 328-368; pages 368a-368p; and pages 369-376)

8. Section 6.3 Internet Protocol Services – MODULE 3, Table of Contents was modified to reflect the pagination changes in the MSA 3 Service Level Agreements.

Replace Attachment 3 Section 6.3 Table of Contents (Pages 6.3-i – 6.3.vi) with amended section (Pages 6.3.i – 6.3.vi)

B. Signature authority for the Office of the State Chief Information Officer (OCIO) has changed to the California Technology Agency per Chapter 404, Statutes of 2010, AB 2408 effective January 1, 2011.

C. Amendment Summary:

- **What is this amendment about?**

- 1) Add Managed Security Services (MSS) for the network environment.
- 2) Additional Service Level Agreements (SLA's) for MSS
- 3) Administrative corrections

- **Why is the contract being amended?**

This amendment is being submitted to augment the existing CALNET 2 services by adding Managed Security Services (MSS) for the network environment. These new services will provide additional support to State agencies, such as California Prison Health Care System. In addition the amendment also includes new Service Level Agreements and Administrative corrections.

- **What is the reason/purpose for the amendment?**

- 1) To augment existing network services by providing Managed Security Services (MSS) for the network environment
- 2) To add the necessary SLAs for the new services.
- 3) Administrative corrections

6.3.3.8a Converged Services, IP and Network IP Transport Services – Security Services Attachment 3

Service Identifier: IP and Network IP Transport Service

Description of the Service: IP Transport services that support Voice, Video and Data. IP transport may include, at a minimum: DSL, DS0, DS1, DS3, Fractional DS3, Ethernet, or a combination to augment geographic coverage or bandwidth. IP transport supports, at a minimum:

- Hosted IP Centrex (HIPC) Services 6.3.4
- IP Contact Center Applications 6.3.5
- IP Communication Applications – Other Services 6.3.6

Availability: Nationwide. International locations are available on an ICB basis.

Unless noted separately in Attachment 4, services include the following elements: planning, applicable design, engineering, testing, and applicable service level agreements.

Professional Security Services (PSS):

Verizon's Professional Security Services (PSS) takes a business-driven approach to information security - looking to ascertain your organization's individual risk profile prior to making recommendations on security controls. This approach reveals where your organization may be disproportionately devoting too many resources on the protection of certain assets. It also sets the stage for the adoption of a security management program that is congruent to the mission of your organization. Verizon's PSS gives you the intelligence-driven capacity to assess risk, manage threats, help address compliance requirements, and reduce complexity—all in the context of your organization's extended enterprise.

The customer must have the required levels of access, interviewees and documentation available upon the pre-determined dates. If interviewees are unavailable or documentation is not provided, the quality of the final deliverables may be affected. The customer will make all systems to be tested available throughout the duration of the testing period. Systems to be tested will have normal operating throughput. Verizon will try to honor the customer's requests regarding the assignment of our personnel to the project. However, Verizon reserves the right to determine the assignment of personnel. Verizon may provide additional details within the purchase order documentation.

Verizon's PSS offerings are divided into the following practice areas to include Threat & Vulnerability Management, Identity & Access Management and Governance Risk & Compliance.

6.3.3.8a Converged Services, IP and Network IP Transport Services – Security Services Attachment 3

All PSS hours quoted in this section are for Normal Working Hours. Any work performed out of normal working hours will need to be reviewed in advance and may carry a premium charge.

Feature Name	Feature Identifier	Feature Description	Feature Limits or Compatibility Restrictions
Data Protection			
Data Protection and DLP (Roadmap, Strategy & Implementation)	PSSV1425	Identify Customer's existing and anticipated business requirements associated with encryption, key management, and/or Data Loss Prevention (DLP). Assess the current state and recommend steps Customer should consider taking to address its current and future needs to identify, monitor, and protect data in use (e.g., endpoint actions), data in motion (e.g., network actions), and data at rest (e.g., data storage). This supplementary service may be purchased in unit increments as small as 1 with no maximum limit. Each increment includes a maximum of 1 personnel day, not to exceed 8 hours of work delivered by a consultant with more than 2 years of experience in the IT	

6.3.3.8a Converged Services, IP and Network IP Transport Services – Security Services Attachment 3

Feature Name	Feature Identifier	Feature Description	Feature Limits or Compatibility Restrictions
		and security area.	
MSS Configuration Support			
MSS Configuration Support	PSSV1427	Services to assist customers with the design and on-boarding of Vz Managed Security Services and service elements. This service is provided on an as needed basis to complement customer resources. This supplementary service may be purchased in unit increments as small as 1 with no maximum limit. Each increment includes a maximum of 1 personnel day, not to exceed 8 hours of work delivered by a consultant with more than 2 years of experience in the IT and security area.	

Managed Security Services (MSS):

Managed Security Services, Premises-based, runs on the Verizon Managed Security Platform and provides a full range of security services to address the customer's most vital security needs. The broad service offering can be purchased as either Monitoring Only or Management and Monitoring Service Types on a wide array of Serviced Devices.

The serviced devices supported under this contract cover the more critical security areas in the customer environment. Devices supported include:

- Firewall (FW)
- Network Intrusion Detection (NIDS)
- Network Intrusion Prevention Services (NIPS)
- Proxy Server
- Managed SEM Platform (SEM)

Verizon security service, whether Monitor Only or Management and Monitoring Service Types can be provided in various Service Levels and Device Configurations. Not all levels and configurations are available for each security device. The Service Levels are designed to meet the broad set of requirements for each type of device and each customer, to provide the optimal security service. Following are the various Service Levels and Device Configurations available:

Service Levels

- Standard is the basic service level and provides industry-standard event definitions, event reporting and email contact with the Security Operations Center (SOC)
- Platinum is a more customized service level providing customer-specific SEAM policy, reporting and alternative contact methods with greater frequency and speed of response.

Device Configurations

- Gigabit provides support for handling devices with Gigabit throughput
- High Availability service is available for devices in a fail-over or load-balancing configuration.
- High Availability Gigabit provides service for Gigabit devices in a fail-over load-balancing configuration.

Not every service level and configuration is offered for each device type, and so the following matrix defines the available configuration options.

6.3.3.8a Converged Services, IP and Network IP Transport Services – Security Services Attachment 3

SERVICE AVAILABILITY MATRIX

Services	Service Type		Service Levels		Device Configuration			
	Monitoring Only	Management and Monitoring	Standard	Platinum	Basic	High Availability	Gigabit	HA + Gigabit
Firewall (FW)	x	x	x	x	x	x	x	x
Network Intrusion Detection System (NIDS)	x	x	x	x	x	x	x	x
Network Intrusion Prevention System (NIPS)	x	x	x	x	x	x	x	x
Proxy Server	x	x		x	x	x		
Add-ons: AS, AV, Content Filtering		x		x	x			
Managed SEM (SEM)	x	x						

Verizon provides these services only on Verizon Business certified hardware platforms. These MSS services exclude Verizon providing the customer premise security devices or device configuration. At the time the customer signs up for the Monitoring Only, or Management and Monitoring service, a Customer Service Manager (CSM) will be assigned to the customer to assist in implementation of the service. The CSM will work with the customer representative(s) to develop a detailed project plan to cover the implementation and activation of the service. During this process, the customer's security design, network and covered devices will be reviewed, documented and configured for inclusion in the service. Given the tremendous variability in project scope, complexity, and number, type and vendor for devices to be covered in this process, the interval necessary to complete the provisioning process varies significantly.

Service Types

Monitoring Only

Monitor Only Service provides a broad range of security services including: Device Availability, Health Monitoring, Threat Analysis, Security Incident Handling, and Service & Security Incident Reporting, which are defined below in greater detail. Verizon provides 24-hour remote monitoring of customer provided security device(s) via a three-tier architecture. Security log data is captured by a hardened Local Event Collector (LEC) device (provided by Verizon with this service) and is sent to our Security Management Center (SMC).

The SMC is where Security logs and alerts are analyzed, correlated, normalized, and classified by our proprietary State and Event Analysis Management (SEAM). SEAM policy is either set to a default configuration or customized based upon level of service (Standard vs. Platinum). From our Security Operations Center (SOC), Verizon then interprets and escalates to you for remediation, as required. Through our Security Dashboard, you get a near-real-time view of your company's security posture and the effectiveness of your security device at every level.

Revised: MSA 3 Amendment No. 13 - 6.3.3.8a Converged Services, IP and Network IP Transport Services – Security Services

6.3.3.8a Converged Services, IP and Network IP Transport Services – Security Services Attachment 3

Monitoring Only offers are generally available in High Availability, Gigabit, and High Availability for Gigabit devices and most are offered in two levels, Standard and Platinum.

Verizon Monitoring Only service provides the following:

1. Device Availability Monitoring

- Verizon establishes a life signal time-out period (e.g., of (2) minutes) for monitoring the availability of a Serviced Device. During monitoring, Verizon can adapt the time-out period to minimize the number of false alerts.
- Verizon monitors the availability of the Serviced Device 24x7 by sending a life signal (a “ping”) once every life signal time-out period.
- If the Serviced Device does not respond three (3) out of five (5) consecutive life signals Verizon assumes it is unavailable.
- When Verizon establishes that a Serviced Device is unavailable, it will contact you within the time agreed in the Service Level Agreement. If Verizon has the information available, it will also send an Availability Report with a first technical assessment.
- These are the contacts and escalation parameters for the Availability Report:

	Interaction	Reporting
Channel	Cf. Service Level	Security Dashboard
Type	Availability Report	Statistics
Reference Time	SMC Time Stamp	SMC Time Stamp
Response Time	Cf. Service Level	Refresh Rate
Contact Person	1° Primary incident contact 2° Secondary incident contact	Authorized users
Escalation	1° Primary escalation contact 2° Secondary escalation contact	

- Verizon is not responsible for the availability monitoring of the devices serviced by the Serviced Device (i.e. the Subordinate Devices).

2. Device Health Monitoring

- Verizon will work with you to define one or more health thresholds for monitoring the health of a Serviced Device. Thresholds are usually set by Verizon at the default levels suggested by the vendor (e.g., 90%). Device

6.3.3.8a Converged Services, IP and Network IP Transport Services – Security Services Attachment 3

thresholds can be viewed and changed by an authorized Customer representative on the web portal. As a precondition to perform such monitoring, Verizon requires access to the Serviced Device in a manner that allows measuring the health parameters reported on by the Serviced Device.

- Verizon monitors the health of the Serviced Device 24x7 by measuring a number of health parameters once every ten (10) minutes. Conditional upon the reporting capability of the Serviced Device, these health parameters include one or more of the following: CPU usage, Memory usage, Disk usage, Swap usage and Network usage.
- If the Serviced Device exceeds a health threshold, Verizon will create a health incident.
- When Verizon creates a health incident, it will contact you within the time agreed to in the Service Level Agreement. If Verizon has the information available, it will also send a Health Report with a first technical assessment.
- These are the contacts and escalation parameters for the Health Report:

	Interaction	Reporting
Channel	Cf. Service Level	Security Dashboard
Type	Health Report	Statistics
Reference Time	SMC Time Stamp	SMC Time Stamp
Response Time	Cf. Service Level	Refresh Rate
Contact Person	1° Primary incident contact 2° Secondary incident contact	Authorized users
Escalation	1° Primary escalation contact 2° Secondary escalation contact	

- Verizon is not responsible for the health monitoring of the devices serviced by the Serviced Device (i.e. the Subordinate Devices).

3. Threat Analysis

The Threat Analysis is based on the logs, events, and reports produced by a Serviced Device or received from devices serviced by that Serviced Device (i.e. the Subordinate Devices), as available.

The results of the Threat Analysis are reported on the Security Dashboard in real-time or periodically. They can also be used for escalating Threats

6.3.3.8a Converged Services, IP and Network IP Transport Services – Security Services Attachment 3

and Incidents in real-time.

Event Collection

- Verizon will, if agreed, enable the Serviced Device to collect Events from the devices that it services (i.e. the Subordinate Devices). Verizon is not responsible to manage the transport of Events from these Subordinate Devices.
- You are responsible to procure one (1) or more Local Event Collectors that Verizon can use to collect Events from the Serviced Devices, and send them over to the SMC. We will jointly agree upon the number of Local Event Collectors used.
- For certain types of Serviced Devices, a Log Transport Agent must run on the Serviced Device to enable the transport of the Event logs generated by the Serviced Device to the Local Event Collector and/or SMC. You are responsible to install and maintain the functioning of the Log Transport Agent, including updating the Log Transport Agent as per any reasonable instructions from time to time given by Verizon. Verizon will provide you with a copy of the Log Transport Agent to be installed and install instructions or direct you to a download/instruction page.

Event Analysis

- Verizon analyzes, 24/7, the Events collected and produced by the Serviced Device. The analysis starts when the Events reach the SMC. All Events are labeled with a sequence number to identify them and to track their status.
- Verizon evaluates the severity of the Event, and classifies it according to the latest Service Context and SEAM policy, into one of the following categories:

Event classification	Level	Conditions
Insufficient Info	L0	Verizon has not enough information to assess the Event. Verizon will ask you for additional details.
Harmful Attack	L1	(i) The Event comes from a device on the inside of the Internet perimeter, and, (ii) The <u>Event</u> points to an attack (attempt) that may result in damage or unauthorized access to a device or application, and, (iii) The cause of the <u>Event</u> may render your infrastructure vulnerable or compromised.

6.3.3.8a Converged Services, IP and Network IP Transport Services – Security Services Attachment 3

Event classification	Level	Conditions
Harmless Attack	L2	(i) The Event comes from a device on the inside of the Internet perimeter, and, (ii) The Event points to a known attack (attempt), and, (iii) Your infrastructure is not considered vulnerable or compromised based on the current Service Context.
False Positive	L4	The Event is falsely triggered by a device on the inside of the Internet perimeter. Such a false positive is caused by: <ul style="list-style-type: none"> • Poor detection code or signatures that do not discriminate well between normal and malicious activity for this Incident. • Devices that show characteristics similar to those of malicious activities.
Forensics	L3	The Event comes from a device on the outside of the Internet perimeter. It is only collected for future forensic analysis.
Off-line Analysis	L5	This level is used during the first phase of a deployment, or after major changes in the network (such as adding or removing a server or Serviced Device, moving a Serviced Device, changing security policies and Rule Sets, installing major signature updates or major software upgrades, implementing an <i>Urgent Change Request</i> , or, replacing a Serviced Device). These Events will only be logged without real time analysis.

- The Security Dashboard shows statistics on Events, not the Events individually.

Incident Creation and Correlation

- Verizon will correlate and aggregate related Events into Incidents.
- Events may appear harmless when they are seen in isolation. However, when they are combined with information from other Events or from the context, a more harmful pattern may appear. Examples of Incidents that may be detected are port scanning, spoofing attempts, exploits of configuration Vulnerabilities, penetration tests, multi-component, and blended worms.

6.3.3.8a Converged Services, IP and Network IP Transport Services – Security Services Attachment 3

- Events are combined with information from other Events to detect segmenting, fragmenting, de-synchronization and other methods applied by hackers, viruses, and worms. Events may also be compared with the Service Context, the output from scanning tools, and Watch Lists.
- Verizon may reclassify Events that were false negatives, and include these in Incidents.
- The ability to correlate and aggregate depends on the level of provided information on the systems that are reachable from the Serviced Device. This information will be configured in the SEAM policy.
- Verizon classifies Incidents into one of the following four (4) categories:

Incident classification	Conditions
Insufficient Info	One or more of the associated Events were classified as Insufficient Info
Harmful Attack	(i) One or more associated Events come from a device on the inside of the Internet perimeter, and, (ii) The Incident is identified as an attack (attempt) that may result in damage or unauthorized access to a device or application, or as an e-mail attachment suspected to be infected by a virus, and, (iii) The cause of the Incident may render your infrastructure vulnerable or compromised.
Harmless Attack	(i) One or more associated Events come from a device on the inside of the Internet perimeter, and, (ii) The Incident is identified as a known attack (attempt) or reconnaissance effort, and, (iii) Your infrastructure is not considered vulnerable or compromised based on the Service Context.
False Positive	The Incident is falsely triggered.

- Individual Incidents, statistics on Incidents, and statistics on Events associated with Incidents are reported on the Security Dashboard

SEAM Policy Update

- Verizon publishes the SEAM policy on the Security Dashboard. It is defined in the SEAM Event Classification Policy Language (“ECPL”).
- The SEAM policy is owned and managed by Verizon.
- Verizon may change the SEAM policy:
 - After an Insufficient Info Incident has been reclassified.

6.3.3.8a Converged Services, IP and Network IP Transport Services – Security Services Attachment 3

- If Verizon sees, or is notified of, a massive attack or a virus/worm outbreak with the risk of flooding.
- If Verizon notes flooding. Flooding may occur as a result of wiring changes, new subnets, or new applications with new protocols within your infrastructure.
- If Verizon thinks that changes to the Service Context may influence a Rule Set. Such changes may include adding, removing, or moving servers, adding new applications or web servers, changing Rule Sets in nearby devices.

4. Security Incident Handling

Incident Handling

- An Incident created during the Threat Analysis starts with status Open.
- During its handling of an Incident, Verizon will change the status of the Incident. Each time a status is changed, a SMC Time Stamp is added. These are the possible statuses of an Incident:

Incident status	Conditions
Open	The Incident has been created by the SEAM engine or by Verizon. Verizon will further examine it.
Active	Verizon has started examining the Incident; the investigation is not yet finished.
Escalated	The <u>Incident</u> has been escalated because: <ul style="list-style-type: none">▪ It concerns a real threat (a Harmful Attack Incident), or,▪ Verizon needs extra information to classify it (an Insufficient Info Incident).
Closed	The Incident has been fully processed by Verizon. It does not require any further action; actions to mitigate, contain, or resolve the risks have been started.

Incident Escalation

- Verizon escalates Insufficient Info or Harmful Attack Incidents. Verizon does not escalate Harmless Attack or False Positive Incidents.
- For Insufficient Info or Harmful Attack Incidents, Verizon examines (if it has enough information):
 - The target of the Incident, and its characteristics
 - If available, the packet dump of the attack to see if it concerns an exploit or a Vulnerability scan
 - If such an attack could be successful on the target and what the impact would be

6.3.3.8a Converged Services, IP and Network IP Transport Services – Security Services Attachment 3

- The best way to mitigate the attack
- The profile of the attackers (based on the attack pattern), to get an idea of their intentions
- For Insufficient Info or Harmful Attack Incidents: when an Incident is created at the SMC, Verizon sends you a Basic Incident Report within the time defined in the Service Level Agreement. A Basic Incident Report contains:
 - The identity of the affected Serviced Device and its location
 - The timestamp in UTC of the Incident
 - Source information, when the Incident does not represent a range of sources
 - Destination information, when the Incident does not represent a range of destinations
 - Threat Signature information; if applicable: Threat Signature ID, name and description
 - Packet dump, if obtainable from the Serviced Device using the existing infrastructure
- For an Insufficient Info Incident: and based upon the additional information you provided, Verizon reclassifies the Incident as Harmful Attack, Harmless Attack or False Positive.
- For Harmful Attack Incidents: after the first escalation, Verizon draws up an Extended Incident Report containing additionally to what is available in the Basic Incident Report:
 - First level analysis of the Incident and related Events
 - Impact on the infrastructure, if known
 - Recommended actions
 - Change Requests to the SEAM policy or device Rule Set, when applicable

Insufficient Info Incident

- Verizon escalates an Insufficient Info Incident to you in the time defined in the Service Level Agreement after Verizon created the Incident. At the same time, it changes the status to Escalated. Next, Verizon waits for the necessary information to reclassify the Incident and to take the necessary actions.
- Verizon does not escalate an Incident as Insufficient Info if it sees that a previously escalated Incident had the same cause. Verizon will reclassify such Incidents in line with the first Incident.
- The quality of Verizon's classification and the number of Incidents escalated as an Insufficient Info Incident depends on the quality and

6.3.3.8a Converged Services, IP and Network IP Transport Services – Security Services Attachment 3

completeness of the information that Verizon receives on the environment of the Serviced Device.

- You are responsible for closing the escalated Incident. This means that you must give Verizon the missing information, so that it can take action and change the status to Closed. Actions that may be necessary are, for example, update the inventory of infrastructure or change the SEAM policy or the Rule Set of the device.
- If you do not provide the missing information in forty-eight (48) hours, Verizon may send a reminder or may change anytime thereafter the status of the Incident to Closed.

Harmful Attack Incident

- Verizon escalates a Harmful Attack Incident to you in the time defined in the Service Level Agreement after Verizon created the Incident. At the same time, it changes the status to Escalated.
- If the Incident is not a reclassification of an Insufficient Info Incident, Verizon will try to trace the identity of the attacking IP addresses or user IDs. Verizon will also ask you to verify the integrity of the (application) servers.
- To block the attack, Verizon may:
 - Implement an Emergency Rule Set Change, if Verizon manages the device that can block the attack.
 - Advise you to implement a Rule Set change, if Verizon does not manage the device that can block the attack.
- In the latter case, you are responsible for bringing the escalated issue to closure and for repairing the integrity of the affected applications and infrastructure. And you should inform Verizon of your actions, so that Verizon can update its inventory of the infrastructure and the SEAM policy, and so that it can set the Incident status to Closed.

5. Service & Security Incident Reporting

Security Dashboard

- You have 24x7 access to the Security Dashboard.
- The information on the Security Dashboard is updated regularly. Each type of information has its specific Refresh Rate.
- The Security Dashboard reports security information on devices and agents, individually and aggregated. You can consult, if applicable:
 - An analysis of the availability of the Serviced Devices, including comments on downtimes during the last 24 hours.
 - A list of Incidents classified per location, device, status, and level

6.3.3.8a Converged Services, IP and Network IP Transport Services – Security Services Attachment 3

- A list of information for each Incident, including associated Events and the signatures that triggered the Events.
- A query builder for searching Events and Incidents
- An overview of connections for the past day, week, or month
- Most frequent sources, destinations, and ports with blocked packets.
- Port scans and spoofing attempts
- A list of planned Security Upgrades
- The status of Change Requests
- Each authorized user requires one (1) unique Verizon Customer Certificate.
- The OG Services include five (5) Verizon Customer Certificates irrespective of the number of subscriptions, unless otherwise agreed in writing. The set up of an additional authorized user, and its associated Verizon Customer Certificate, consumes two (2) Service Tickets.

Management Report

- Every month, Verizon will generate a Management Report and make it available on the Security Dashboard.
- The Management Report shows:
 - A status of the open Change Requests and Security Upgrades
 - A summary of all Incidents of the past period
 - A closure report of all Harmful Attack and Insufficient Info Incidents, and management-level interpretation of the Incidents
 - Most frequent sources, destinations, and ports of blocked packets
 - An overview of all planned and implemented Change Requests, Rule Set updates, and Security Upgrades of the past period
 - Requests For Information from Verizon concerning your network or to clarify irregularities in the Threat analysis of the past period
- The Management Report covers all your sites and devices subscribed to the OG Service. You can order additional Management Reports, e.g. a separate report per site. These will be charged separately.

Problem Ticket

- The Customer Service Desk (“CSD”) accepts Problem Tickets on the Serviced Devices or the OG Services 24x7.
- The CSD can be reached via e-mail or telephone (with Platinum service).

6.3.3.8a Converged Services, IP and Network IP Transport Services – Security Services Attachment 3

- Verizon will only give support to staff that is authorized by your company and that you have registered in the Service Context.
- To help you solve your problem, Verizon needs correct and detailed information:
 - The name of the caller, telephone number, e-mail address, and company name
 - A detailed description of the problem, including steps to reproduce it
 - Error codes, messages, log files, output of diagnostic tools
 - Changes made to the configuration/policy/rules before you detected the problem
 - The impact on the business
 - The availability of back-ups and roll-back procedures
- Verizon will assign a unique Call ID and a Severity Level to every support request that it accepts. The Severity Level is based on your information and on the impact of the problem on your environment.

Problem severity	Level	Conditions
Severity 1	S1	An error causes the Serviced Device or OG Services to fail. Normal day-to-day business is not possible, e.g. system failure, an inaccessible or inoperable production system.
Severity 2	S2	An error significantly affects the functions of the Serviced Device or OG Services and prevents normal day-to-day business. Or an error occurs in a high-risk environment, e.g. an error in one line of a high-availability setup.
Severity 3	S3	An isolated error impacts the functions of the Serviced Device; there is no important impact on the day-to-day business. Or an error occurs that significantly affects the Serviced Device or OG Services, but a Work-around exists.
Severity 4	S4	A benign error occurs, or an improvement is asked. There are no problems with the Serviced Device or OG Services, and there is no immediate impact on the production environment.

6.3.3.8a Converged Services, IP and Network IP Transport Services – Security Services Attachment 3

- For Severity 1 and 2 problems, you and Verizon will both assign a dedicated contact person.
- Severity 3 or 4 problems may be resolved in the next revision or upgrade of the software.
- Verizon will report on the status of a problem with status reports.
- When Verizon starts working on the problem, it will send you an initial status report. The initial status report will include:
 - The Call ID and Severity Level, used in all further calls and e-mails on this problem
 - A description of the problem
 - The status of the investigations
- You may ask for extra status reports by e-mail. Verizon will respond as soon as possible, by return e-mail.
- Verizon will support you, but not the end users of your services, or any other customers of yours.
- Verizon has the right to refuse requests that:
 - Concern general system maintenance
 - Are made by end users of your services
 - Concern installing new devices or software, stripping and hardening, and applying patches or upgrades
 - Would involve giving you implicit training
 - Would involve giving you implicit consultancy
 - Would involve a redesign of your infrastructure
- When Verizon believes that it has given you all information to resolve the problem, it will close the Call ID five (5) Business Days after it has sent the information.
- When a problem is resolved, or when its Severity is lowered to a level that does not require further immediate action, Verizon will inform you.
- If you do not answer a request for information, or a request to perform tasks or to provide Verizon with output:
 - After one (1) Business Day, a Severity 1 or 2 problem will be lowered one level
 - After five (5) Business Days, Verizon may close the Call ID

Request For Information

- The CSD accepts Request For Information enquiries on the OG Services and the Serviced Devices 24x7.
- The CSD can be reached via mail or telephone (with Platinum service). During the telephone call or via e-mail, you receive a Call ID. This Call ID

Revised: MSA 3 Amendment No. 13 - 6.3.3.8a Converged Services, IP and Network IP Transport Services – Security Services

6.3.3.8a Converged Services, IP and Network IP Transport Services – Security Services Attachment 3

must be used in all further calls and e-mails on this Request For Information.

- Any question on what is not directly available on the Security Dashboard or requiring a more detailed analysis compared to what is available on the incident reports, will not be considered as a regular Request For Information. Verizon may charge these requests separately at its then current standard or otherwise agreed upon rates. Examples of such requests are extended retrieval requests and specific forensics reports.

Data Availability and Retention

- Incidents stored in the SMC database, in a Verizon proprietary format, are kept for one (1) year, unless otherwise agreed in writing.
- Data on raw events will be kept for 90 days for Standard service or one (1) year with Platinum service. Moreover, this data can be made available on request up to one (1) month after the Services Agreement has ended. Verizon can also delete these data following mutually agreed procedures.
- Data can be retrieved via the Security Dashboard and following these parameters:

	Interaction	Reporting
Channel	E-mail and Security Dashboard	Security Dashboard
Type	Data Available via appropriate storage medium Confirmed Data Destruction	Ticket Status
Reference Time	Timestamp of the request in Security Dashboard	Timestamp of the request in Security Dashboard
Response Time	N/A	Refresh Rate

- The amount of data to receive per Serviced Device and per month must not exceed ten (10) Gigabytes. Verizon may charge you separately its then current standard or otherwise agreed upon fees for any amount of data received from a Serviced Device during a month exceeding ten (10) Gigabytes.

Availability of SMC Equipment

- The availability of critical SMC equipment is defined to be 99.0% for Standard service or 99.5% for Platinum service for a period of one (1) month.
- The availability calculation specifically excludes:

Revised: MSA 3 Amendment No. 13 - 6.3.3.8a Converged Services, IP and Network IP Transport Services – Security Services

6.3.3.8a Converged Services, IP and Network IP Transport Services – Security Services Attachment 3

- The periods of scheduled and mutually agreed maintenance
- Outages due to your failure to comply with this Service Description
- Cases of force majeure or other events beyond our reasonable control
- Emergency Maintenance

Limitations

Verizon provides this service only on Verizon Business certified hardware platforms. These services exclude Verizon providing the customer premise security devices or device configuration. Verizon offers industry leading monitoring service but cannot guarantee this service to be impenetrable. Although Verizon will catch most threats, Verizon does not guarantee every threat will be detected.

Management and Monitoring

Management and Monitoring Service provides all the same services as Monitoring Only including: Device Availability, Health Monitoring, Threat Analysis, Security Incident Handling, and Service and Security Incident Reporting. In addition, Management service provides Device Health Management including Device Troubleshooting, Hardware Maintenance and Device Restoration. Management service also provides Device Maintenance including Software Maintenance, and Device Security Management, all services that are incremental to the Monitoring Only services detailed in the previous section.

As with Monitoring Only service, Verizon provides 24-hour remote monitoring of customer provided Device(s) via a three-tier architecture. Security log data is captured by a hardened Local Event Collector (LEC) device (provided by Verizon with this service) and is sent to our Security Management Center (SMC).

The SMC is where logs and alerts are analyzed, correlated, normalized, and classified by our proprietary State and Event Analysis Machine (SEAM). SEAM policy is either set to a default configuration or customized based upon level of service (Standard vs. Platinum) as designated in the descriptions below. From our Security Operations Center (SOC), we then interpret and escalate to you for remediation, as required. In addition to the core functions provided by our monitoring service, we also proactively manage your security devices and remotely operate and maintain your platform, operating system, and software. This includes remote installation of security patches, hot fixes, service packs, and vendor product updates. In addition to these essential capabilities, we also perform the rule set change management function on customer provided Device(s) under our management and, with each customer-requested change, assess the risk associated with that change before completing the change in the time specified. Verizon Business also ensures that by managing your rule sets

Revised: MSA 3 Amendment No. 13 - 6.3.3.8a Converged Services, IP and Network IP Transport Services – Security Services

6.3.3.8a Converged Services, IP and Network IP Transport Services – Security Services Attachment 3

and policy backups a device can be remotely restored. Through our Security Dashboard, you get a near-real-time view of your company's security posture and the effectiveness of your Device at every level—from the big-picture view all the way down to the details of an individual security incident.

In order to deliver Security Management and Monitoring service on the Device(s), we only perform device configuration for the Device to be Monitored and Managed to work with SMC and LEC. Site Set Up Local Event Collector charge is not charged for subsequent Device(s) unless another LEC is required.

Verizon requires access to the Serviced Device in a manner that allows measuring the health parameters reported on by the Serviced Device. For Out of Band Management, the Customer is required to provide the 1MB and Modem. In-band Management would apply for existing customer connection to VzB Private IP (PIP) or Internet connection.

Management and Monitoring offers are generally available in High Availability, Gigabit, and High Availability for Gigabit devices and most are offered in two levels, Standard and Platinum.

Verizon Management and Monitoring service provides the following list of services. All the descriptions from the Monitoring Only section above apply to the Management and Monitoring services. **Only those services that are exclusive to Management and Monitoring, and therefore incremental to Monitoring Only services, are detailed in this section.**

1. Device Availability Monitoring

2. **Health Monitoring** - Management adds the following to the Health Monitoring services provided by Monitoring Only:

Device Troubleshooting

- Verizon will try to discover the cause of an unavailability of a Serviced Device with remote problem diagnosis.
- If Verizon thinks the problem is inherent to the Serviced Device and Verizon manages the maintenance contract for the Serviced Device, Verizon will escalate it to the manufacturer or vendor.
- Verizon is not responsible for problem diagnosis of the devices serviced by the Serviced Device (i.e. the Subordinate Devices).

Hardware Maintenance

- If Verizon experiences performance problems with the Serviced Device, it may recommend hardware upgrades.

6.3.3.8a Converged Services, IP and Network IP Transport Services – Security Services Attachment 3

- If Verizon detects a hardware failure, it may escalate the problem to the vendor or the manufacturer of the Serviced Device.
- In both cases, Verizon will contact you.
- Any upgrade or replacement of the hardware, due to failures, new demands, or performance problems, must be jointly coordinated.
- If you manage the maintenance contract of the equipment, you must also organize any on-site servicing of the hardware.
- If Verizon manages the maintenance contract for you, Verizon will coordinate the on-site servicing of the hardware.
- An escalation to the manufacturer or vendor, followed by a hardware replacement or maintenance, will follow the terms and conditions, and the service level of the equipment manufacturer/vendor and its Return Material Authorization (RMA).
- You must not return a Serviced Device, or parts of it, to the manufacturer without Verizon's agreement.

Device Restoration

- You are responsible for restoring the Serviced Device from the full back-up that you have made. You will also restore the connection between the Serviced Device and the SMC.
- If it is not possible to restore the Serviced Device from the full back-up, Verizon may try to restore the Serviced Device with its own copies.
- Verizon and you will together test the Serviced Device and its connection to the SMC.
- Verizon is not responsible for restoring the communication between the Serviced Device and the devices serviced by that Serviced Device (i.e. the Subordinate Devices).

3. Threat Analysis

4. Security Incident Handling

5. Device Maintenance (exclusive to Management service)

Software Maintenance

- Verizon is continuously on the lookout for new Security Upgrades for the Serviced Devices. New Security Upgrades are checked for their effect and impact. If you and Verizon approve a Security Upgrade, Verizon will plan to install it for the next Maintenance Window, as agreed.
- The number of Maintenance Windows you can define in the Service Context is not limited.

6.3.3.8a Converged Services, IP and Network IP Transport Services – Security Services Attachment 3

- If, according to Verizon, the Threat is critical, you will receive a notification on the ready for deployment status of the Security Upgrade within 24 hours.

	Interaction
Channel	E-mail
Type	Ready for deployment notification
Reference Time	SMC Time Stamp
Response Time	NTE 24 hour_Service_Levels
Contact Person	Primary incident contact + Secondary incident contact

- If Verizon does not manage the maintenance contract of the Serviced Device, you should send Verizon any Security Upgrades that you receive from the manufacturer, as soon as possible. Failing that, Verizon cannot install the Security Upgrades.
- Verizon will install the Security Upgrades remotely. During such a remote installation, you will be expected to assist Verizon with expertise on the operating system, the application, and any tool running on the Serviced Device.
- If a remote installation is not possible or practicable, Verizon can install the Security Upgrades on-site. It will do so at the applicable rates.
- Verizon reports on the installation of Security Upgrades by e-mail:

	Reporting
Channel	E-mail
Type	Confirmation of the installation
Reference Time	SMC Time Stamp
Response Time	After the installation
Contact Person	Primary incident contact + Secondary incident contact

- Other upgrades or replacements, such as end-of-life replacements of a Serviced Device, are not included but can be planned and carried out by Verizon as a separate project at the applicable rates.

6.3.3.8a Converged Services, IP and Network IP Transport Services – Security Services Attachment 3

- Verizon will inform you if the manufacturer announces the end-of-life of a Serviced Device.
- Verizon is not responsible for maintaining devices serviced by the Serviced Device (i.e. the Subordinate Devices).

Device Back-Up

- Verizon will back up the configuration files and the Rule Set of the Serviced Device.
- This back-up will be needed to return to a previous version if updates do not have the desired result.
- Verizon will keep a copy of the operating system, the application, and all installed upgrades of the Serviced Device.
- These copies will be needed to reinstall the Serviced Device if full back-ups are corrupted or not available.
- You are responsible for regularly making a full back-up of the Serviced Device and the devices serviced by the Serviced Device (i.e. the Subordinate Devices) where possible.

1. Device Security Management (exclusive to Management service)

Configuration Management

- Verizon will help to maintain the configuration of a Serviced Device in line with new Threats and changes in the environment.
- If you want to change the configuration of a Serviced Device, you must make a request using the Change Request procedures.
- Verizon will implement configuration changes during a Maintenance Window it has agreed with you.
- Verizon is not responsible for the configuration management of the devices serviced by the Serviced Device (i.e. the Subordinate Devices).

Rule Set Management

- Verizon and you will approve jointly the initial device Rule Set during the Service Commencement Procedure.
- You may request changes to the Rule Set of a Service Device. Verizon will evaluate, prepare and implement changes to the Rule Set of a Serviced Device
- You will remain the owner of the Rule Set.

6.3.3.8a Converged Services, IP and Network IP Transport Services – Security Services Attachment 3

Change Management Process

- Only staff that is authorized by your company and that you have registered in the Service Context can submit or approve Change Requests.
- Change Requests must be submitted in the Security Dashboard. The Security Dashboard is a web client that, to the best of our knowledge, has not experienced a customer affecting service interruption. However, a toll free number is provided to each customer during service activation to enable authorized customer contacts to contact the SOC to provide a Change Request should the Security Dashboard not be available.
- We assign a unique Change Request number to each Change Request properly submitted. You must use this number in all communication on this Change Request.
- A Change Requests is either a:
 - Regular Change Request that is a planned change to the topology of your infrastructure or security policy that will be implemented during a Maintenance Window.
 - Fast-Track Change Request that is a planned or unplanned change that meets the constraints specified, and that will be implemented within days.
 - Urgent Change Request that is an unplanned change that meets the constraints specified, that you want implemented as soon as reasonably possible.
- Each Change Request implemented will consume a number of Service Tickets, depending on its category, as specified herein.
- Before implementing a Change Request, Verizon may ask you for extra confirmation and authorization. Verizon will send a confirmation request to the person who has submitted the Change Request, and to his/her management.
- A Change Request has a status in each point of its lifecycle. When the status changes, a time stamp in UTC is attached.
- These are the statuses:

Status	Conditions
Open	The Change Request has been received by Verizon
Accepted for review	The Change Request conforms to the criteria and is waiting for a second-level review
Accepted	The Change Request has been accepted for implementation by Verizon
Escalated	The Change Request has been escalated by Verizon to you because it is not clear or because it may have unexpected security or availability implications

Revised: MSA 3 Amendment No. 13 - 6.3.3.8a Converged Services, IP and Network IP Transport Services – Security Services

6.3.3.8a Converged Services, IP and Network IP Transport Services – Security Services Attachment 3

Discarded	The Change Request has been rejected by Verizon
Requiring your validation	The Change Request has been implemented by Verizon and is waiting for your validation feedback which you are expected to provide within 2 Business Days after implementation.
Closed	The Change Request is closed after your validation or after 2 Business Days (whichever comes first).

- You can track the progress of the Change Requests on the Security Dashboard.
- Next to the normal reconfigurations, a major configuration change may be needed. Such a change will be implemented as a separate project for which Verizon may charge separately at its then current standard or otherwise agreed upon rates.
- A configuration change is major when it involves:
 - More than ten (10) changes to a Rule Set simultaneously
 - Changes to the IP addresses of a Serviced Device
 - Activation of a cross-device function on Serviced Devices
 - A redesign of the infrastructure
 - Introducing a device or application in the infrastructure
 - Activating a previously unused function on a Serviced Device
 - Changes estimated to require more time than available in a Maintenance Window
- Verizon will start the propagation of Rule Set updates to the devices serviced by the Serviced Device (i.e. the Subordinate Devices).
- Verizon is however not responsible for the actual propagation of the Rule Set updates to those Subordinate Devices.
- Verizon will maintain a maximum of five (5) users or user groups for authenticating towards the Serviced Device.
- You should provide an external authentication server if the number of users or user groups exceeds five (5). Monitoring and managing such external authentication server is outside the scope of the OG Services.
- Verizon may discard Change Requests not properly submitted on the Security Dashboard (e.g. in case the Change Request has not been submitted on the Security Dashboard or in case the Change Request information submitted is ambiguous or otherwise insufficiently clear to determine the nature of the requested change). Exceptions will be made if the Security Dashboard is unavailable.

Regular Change Request

- Verizon will analyze a Regular Change Request (“RCR”) and give feedback within the time defined in the Service Level Agreement.

6.3.3.8a Converged Services, IP and Network IP Transport Services – Security Services Attachment 3

- A Change Request is accepted as a Regular Change Request if one of these holds:
 - It meets all criteria for Urgent or Fast-track Change Requests
 - It concerns a change to the application software
 - It concerns changes to operating system settings, except for changes to IP addresses
- Verizon will implement accepted Regular Change Requests in one of the next Maintenance Windows specified in the Service Context. The minimum time between submitting a Regular Change Request and its implementation is 48 hours.

Fast-Track Change Request

- Verizon will analyze a Fast-track Change Request (“FCR”) and give feedback within the time defined in the Service Level Agreement. Verizon may request a second-level review of the Change Request.
- A request can be a Fast-Track Change Request if one of these holds:
 - It concerns changes to existing rules or the creation of new rules and/or objects in the Rule Set of a Serviced Device and, maximum three (3) Serviced Devices are involved.
 - It concerns creating new hosts in the policy; the host is part of a subnet that is already accessible and configured on the Serviced Device.
 - It concerns allowing or disallowing traffic between existing hosts.
- Examples of requests that will not be accepted as Fast-Track Change Requests for blocking Serviced Devices:
 - Changes to the Virtual Private Network (“VPN”) configuration of objects
 - Change to the Network Address Translation (“NAT”) configuration of rules or objects
 - Device policy changes on multiple Serviced Devices
 - Changes to anti-spoofing settings
 - Routing changes
 - Additions of interfaces to the Serviced Device
- Verizon will implement accepted Fast-Track Change Requests within the time defined in the Service Level Agreement.

Urgent Change Request

- Verizon will analyze an Urgent Change Request (“UCR”) and give feedback within the time defined in the Service Level Agreement.
- During the analysis and implementation of an Urgent Change Request, you will:

6.3.3.8a Converged Services, IP and Network IP Transport Services – Security Services Attachment 3

- Ensure that the request is internally approved.
- Ensure that the data supplied to Verizon are detailed enough to allow Verizon to analyze the request on time.
- Ensure that an authorized person is available by telephone to further clarify the Urgent Change Request.
- Confirm the decisions taken during phone calls with Secure E-mail.
- A request can be an Urgent Change Request if:
 - It concerns changes to existing rules or the creation of new rules and/or objects in the Rule Set of one (1) Serviced Device.
 - It clearly specifies the required configuration setting and its new value.
- Examples of such clearly defined change requests are:
 - Changes to mailer tables if the exact entries are specified
 - Changes to a routing table if the exact entries are specified
- As you allow less time for Verizon to analyze and mitigate potential availability or security risks associated with your change request, the implementation of an Urgent Change Request carries a higher degree of risk, which you accept by submitting such request.
- Verizon will implement accepted Urgent Change Requests within the time defined in the Service Level Agreement.

Emergency Change Request

- Verizon may implement Emergency Change Requests, such as changing the device Rule Set or disabling Threat Signatures. This may be the case, for example:
 - After Verizon witnesses or is notified of a massive attack or of a virus/worm outbreak with the risk of flooding.
 - After Verizon notes flooding that may be caused by changes in the topology of your infrastructure (rewiring, adding new subnets, new applications with new protocols...).
 - If changes to the Service Context submitted to Verizon are believed to influence a Rule Set. Such changes may include adding, removing, or moving servers, adding new applications or web servers, changes to Rule Sets in adjacent devices.
- Verizon is authorized to make changes to the device Rule Set and to disable Threat Signatures in emergencies, after your approval, and according to the procedures for Urgent Change Requests.

2. Service & Security Incident Reporting

Service Level Definitions

- **Standard Service** provides all the features listed above for both the Monitored and Managed and Monitored devices. State and Event Analysis Machine (SEAM) Policy is not customized. Events Verizon deems a significant risk are stored and labeled with a sequence number to identify them and to track their status. In addition to the Dashboard, only email is used as a method of contact from the Security Operations Center (SOC) to customer. Verizon may provide additional details within the purchase order documentation.
- **Platinum Service** provides all the features listed above for both the Monitored and Managed and Monitored devices, however with Platinum service, SEAM Policy is customized to fit the customer's security needs. Event Analysis includes all the features for Standard except all events, not only those Verizon deems a significant risk, are labeled with a sequence number to identify them and to track their status. Phone, in addition to email, is a method of contact from the SOC to customer and vice versa

Device Configurations

- Basic Service is for standard devices in a basic configuration.
- High Availability Service is per pair of Security Devices in a fail-over or load-balancing configuration. High Availability service is to provide a level of redundancy of the device in case the primary device fails and/or load-balancing when the customer has the required CPE engineered solution. This service is only available on security device platforms supporting High Availability.
- Gigabit Service is for those Security Devices handling gigabit throughput.
- High Availability + Gigabit Service is for those Security Devices handling gigabit throughput in a fail-over or load-balancing configuration. High Availability service is to provide a level of redundancy of the device in case the primary device fails and/or load-balancing when the customer has the required CPE engineered solution.

6.3.3.8a Converged Services, IP and Network IP Transport Services – Security Services Attachment 3

Serviced Device: Firewall

Security services for Firewall devices are available in all configurations: Monitor Only and Management and Monitor; Standard and Platinum; High Availability (HA); Gigabit; and High Availability for Gigabit devices. The service descriptions, and requirements and limitations, for each of the configurations as reviewed above apply for this service. Verizon may provide additional details within the purchase order documentation for all Firewall Security Services.

Firewall Monitoring Only

Monitor Only features include: Device Availability & Health Monitoring, Threat Analysis, Security Incident Handling, and Service & Security Incident Reporting.

Feature Name	Feature Identifier	Feature Description	Feature Limits or Compatibility Restrictions
<p>Firewall Monitoring Only Standard</p>	<p>FRWL0001</p>	<p>Firewall Monitoring Only Standard provides all the Monitoring Only and Standard features and attributes described above. State and Event Analysis Machine (SEAM) Policy is not customized. Events Verizon deems a significant risk are stored and labeled with a sequence number to identify them and to track their status. In addition to the Dashboard, only email is used as a method of contact from the Security Operations Center (SOC) to customer.</p>	<p>Requires the following Feature Identifier if order is for the first managed security device at the location:</p> <p>FRWL0010</p>

6.3.3.8a Converged Services, IP and Network IP Transport Services – Security Services Attachment 3

Feature Name	Feature Identifier	Feature Description	Feature Limits or Compatibility Restrictions
Firewall Monitoring Only Gigabit Standard	FRWL0002	This service provides all the features of Firewall Monitoring Only Standard Service for those firewalls handling gigabit throughput. All other Standard attributes and restrictions apply.	Requires the following Feature Identifier if order is for the first managed security device at the location: FRWL0010
Firewall Monitoring Only High Availability Standard	FRWL0003	This service provides all the features of Firewall Monitoring Only Standard service per pair of Firewalls devices in a fail-over or load-balancing configuration. High Availability service is to provide a level of redundancy of the firewall in case the primary firewall fails and/or load-balancing when the customer has the required CPE engineered solution. This service is only available on Firewall platforms supporting High Availability. All other Standard attributes and restrictions apply	Requires the following Feature Identifier if order is for the first managed security device at the location: FRWL0010

6.3.3.8a Converged Services, IP and Network IP Transport Services – Security Services Attachment 3

Feature Name	Feature Identifier	Feature Description	Feature Limits or Compatibility Restrictions
Firewall Monitoring Only High Availability Gigabit Standard	FRWL0004	This service provides all the features of Firewall Monitoring Only Standard Service for those firewalls handling gigabit throughput and service per pair of Firewalls devices in a fail-over or load-balancing configuration. High Availability service is to provide a level of redundancy of the firewall in case the primary firewall fails and/or load -balancing when the customer has the required CPE engineered solution. All other Standard features and restrictions apply.	Requires the following Feature Identifier if order is for the first managed security device at the location: FRWL0010

6.3.3.8a Converged Services, IP and Network IP Transport Services – Security Services Attachment 3

Feature Name	Feature Identifier	Feature Description	Feature Limits or Compatibility Restrictions
Firewall Monitoring Only Platinum	FRWL0005	Firewall Monitoring Only Platinum provides all the features listed under Firewall Monitoring. SEAM Policy is customized to fit the customer's security needs. Event Analysis includes all the features for Standard except all events, not only those Verizon deems a significant risk, are labeled with a sequence number to identify them and to track their status. Phone is a method of contact from the SOC to customer and vice versa in addition to the Dashboard. Data on raw events defined as harmful by the customer will be kept for one (1) year. Moreover, this data can be made available on request up to one (1) month after the Service has been terminated. Verizon provides a review between the customer and a security Customer Service Manager (CSM) once a month.	Requires the following Feature Identifier if order is for the first managed security device at the location: FRWL0010
Firewall Monitoring Only Gigabit Platinum	FRWL0006	This service provides all the features of Firewall Monitoring Only Platinum Service for those firewalls handling gigabit throughput. All other Platinum features and restrictions apply.	Requires the following Feature Identifier if order is for the first managed security device at the location: FRWL0010

6.3.3.8a Converged Services, IP and Network IP Transport Services – Security Services Attachment 3

Feature Name	Feature Identifier	Feature Description	Feature Limits or Compatibility Restrictions
Firewall Monitoring Only High Availability Platinum	FRWL0007	This service provides all the features of Firewall Monitoring Only Platinum service per pair of Firewalls devices in a fail-over or load-balancing configuration. High Availability service is to provide a level of redundancy of the firewall in case the primary firewall fails and/or load- balancing when the customer has the required CPE engineered solution. This service is only available on Firewall platforms supporting High Availability. All other Platinum features and restrictions apply.	Requires the following Feature Identifier if order is for the first managed security device at the location: FRWL0010
Firewall Monitoring Only High Availability Gigabit Platinum	FRWL0008	This service provides all the features of Firewall Monitoring Only Platinum Service for those firewalls handling gigabit throughput per pair of Firewalls devices in a fail-over or load-balancing configuration. All other Platinum features and restrictions apply.	Requires the following Feature Identifier if order is for the first managed security device at the location: FRWL0010
Site Set Up Local Event Collector	FRWL0010	Site Set Up fee is charged for each Local Event Collector (LEC) per location. This fee covers placement of a local event collector and is dependent on the architectural solution design per customer.	Required for first managed security device on site.

6.3.3.8a Converged Services, IP and Network IP Transport Services – Security Services Attachment 3

Feature Name	Feature Identifier	Feature Description	Feature Limits or Compatibility Restrictions
Additional Customer Certificate	FRWL0011	All Firewall Monitoring MSS services require authorized Customer Certificates for user access authorization. Five (5) Customer Certificates are included in the price of all Monitored MSS services. Additional Customer Certificates are available for each additional user access.	

6.3.3.8a Converged Services, IP and Network IP Transport Services – Security Services Attachment 3

Firewall Management and Monitoring

Management and Monitoring services include: Device Availability Monitoring, Health Monitoring, Device Troubleshooting, Threat Analysis, Security Incident Handling, Device Maintenance, Device Security Management, Service & Security Incident Reporting.

Feature Name	Feature Identifier	Feature Description	Feature Limits or Compatibility Restrictions
Firewall Management & Monitoring Standard	FRWL0013	Firewall Management and Monitoring Standard provides all the features listed above for Management & Monitoring Standard. State and Event Analysis Machine (SEAM) Policy is not customized. Events Verizon deems a significant risk are stored and labeled with a sequence number to identify them and to track their status. In addition to the Dashboard, only email is used as a method of contact from the SOC to customer. Standard service will allow up to 1 Regular Change, 1 Fast-Track and 0 Urgent monthly Change Request. Additional Change Request will incur charges identified as Regular, Fast-Track, and Urgent.	Requires the following Feature Identifier if order is for the first managed security device at the location: FRWL0022
Firewall Management & Monitoring Gigabit Standard	FRWL0014	This service provides all the features of Standard Firewall Management and Monitoring Service for Firewalls handling gigabit throughput. All other Standard features and restrictions apply.	Requires the following Feature Identifier if order is for the first managed security device at the location: FRWL0022

6.3.3.8a Converged Services, IP and Network IP Transport Services – Security Services Attachment 3

Feature Name	Feature Identifier	Feature Description	Feature Limits or Compatibility Restrictions
Firewall Management & Monitoring High Availability Standard	FRWL0015	This service provides all the Firewall Management and Monitoring Standard features per pair of Firewalls devices in a fail-over or load-balancing configuration. High Availability service is to provide a level of redundancy of the firewall in case the primary firewall fails and/or load-balancing when the customer has the required CPE engineered solution. All other Standard features and restrictions apply.	Requires the following Feature Identifier if order is for the first managed security device at the location: FRWL0022
Firewall Management & Monitoring High Availability Gigabit Standard	FRWL0016	This service provides all the features of Firewall Management and Monitoring Standard Service for those firewalls handling gigabit throughput per pair of Firewall devices in a fail-over or load-balancing configuration. All other Standard features and restrictions apply.	Requires the following Feature Identifier if order is for the first managed security device at the location: FRWL0022

6.3.3.8a Converged Services, IP and Network IP Transport Services – Security Services Attachment 3

Feature Name	Feature Identifier	Feature Description	Feature Limits or Compatibility Restrictions
Firewall Management and Monitoring Platinum			
Firewall Management & Monitoring Platinum	FRWL0017	<p>Firewall Management and Monitoring Platinum provides all the features listed under Firewall Management and Monitoring with the following features: SEAM Policy is customized to fit the customers security needs. Event Analysis includes all the features for Standard except all events, not only those Verizon deems a significant risk, are labeled with a sequence number to identify them and to track their status. Phone is a method of contact from the SOC to customer and vice versa in addition to the Dashboard. Data on raw events defined as harmful by the customer will be kept for one (1) year. Moreover, this data can be made available on request up to one (1) month after the Service has been terminated. To perform firewall upgrades, customer can define an unlimited number of Maintenance Windows necessary to perform these upgrades. Verizon provides a review between the customer and a security Customer Service Manager (CSM) once a month. Platinum service will allow up to unlimited Regular Change, 1 Fast-</p>	<p>Requires the following Feature Identifier if order is for the first managed security device at the location:</p> <p>FRWL0022</p>

6.3.3.8a Converged Services, IP and Network IP Transport Services – Security Services Attachment 3

Feature Name	Feature Identifier	Feature Description	Feature Limits or Compatibility Restrictions
		Track and 1 Urgent monthly Change Request. Additional Change Request will incur charges identified as Fast-Track, and Urgent. All other Platinum features and restrictions apply.	
Firewall Management & Monitoring Gigabit Platinum	FRWL0018	This service provides all the features of Firewall Management and Monitoring Platinum Service for those firewalls handling gigabit throughput. All other Platinum features and restrictions apply.	Requires the following Feature Identifier if order is for the first managed security device at the location: FRWL0022
Firewall Management & Monitoring High Availability Platinum	FRWL0019	This service provides all the features of Verizon Firewall Management and Monitoring Platinum service per pair of Firewalls devices in a fail-over or load-balancing configuration. High Availability service is to provide a level of redundancy of the firewall in case the primary firewall fails and/or load balancing when the customer has the required CPE engineered solution. This service is only available on Firewall platforms supporting High Availability. All other Platinum features and restrictions apply.	Requires the following Feature Identifier if order is for the first managed security device at the location: FRWL0022

6.3.3.8a Converged Services, IP and Network IP Transport Services – Security Services Attachment 3

Feature Name	Feature Identifier	Feature Description	Feature Limits or Compatibility Restrictions
Firewall Management & Monitoring High Availability Gigabit Platinum	FRWL0020	This service provides all the features of Firewall Management and Monitoring Platinum Service for those Firewall devices handling gigabit throughput per pair of Firewall devices in a fail-over or load balancing configuration. High Availability service is to provide a level of redundancy of the Firewall device in case the primary Firewall device fails and/or load balancing when the customer has the required CPE engineered solution. This service is only available on Firewall platforms supporting High Availability. All other Platinum features and restrictions apply.	Requires the following Feature Identifier if order is for the first managed security device at the location: FRWL0022
Site Set Up Local Event Collector	FRWL0022	Site Set Up fee is charged for each Local Event Collector (LEC) per location. This fee covers placement of a local event collector and is dependent on the architectural solution design per customer.	.Required for first managed security device on site.

6.3.3.8a Converged Services, IP and Network IP Transport Services – Security Services Attachment 3

Feature Name	Feature Identifier	Feature Description	Feature Limits or Compatibility Restrictions
Additional Customer Certificate	FRWL0023	All Firewall Management and Monitoring MSS services require authorized Customer Certificates for user access authorization. Five (5) Customer Certificates are included in the price of all Management and Monitored MSS services. Additional Customer Certificates are available for each additional user access.	
Additional Service Tickets (Apply to All Management and Monitoring Configurations):			
Regular (1 Service Ticket)	FRWL0025	A Regular Change Request includes but is not limited to changes to the application software and/or changes to operating system settings (except for changes to IP addresses). Verizon will implement accepted Regular Change Requests on the next Maintenance Window agreed upon with the customer when setting up the service.	

6.3.3.8a Converged Services, IP and Network IP Transport Services – Security Services Attachment 3

Feature Name	Feature Identifier	Feature Description	Feature Limits or Compatibility Restrictions
Fast-track (4 Service Tickets)	FRWL0026	<p>Fast-Track Change Request includes:</p> <ul style="list-style-type: none"> • Changes to existing rules or the creation of new rules and/or objects in the Rule Set of a Serviced Device and, maximum three (3) Serviced Devices are involved. • Creation of new hosts in the policy; the host is part of a subnet that is already accessible and configured on the Serviced Device. • Allowing or disallowing traffic between existing hosts. <p>Fast-Track Change Request does not include changes to the Virtual Private Network (“VPN”) configuration, change to the Network Address Translation (“NAT”) configuration of rules or objects, device policy changes on multiple Serviced Devices, changes to anti-spoofing settings, routing changes, or additions of interfaces to the Serviced Device.</p>	
Urgent (8 Service Tickets)	FRWL0027	<p>Urgent Change Request includes changes to existing rules or the creation of new rules and/or objects in the Rule Set of one (1) Serviced Device, and clearly specified required configuration setting and its new value.</p>	

6.3.3.8a Converged Services, IP and Network IP Transport Services – Security Services Attachment 3

Serviced Device: Network Intrusion Detection Service (NIDS)

Security service for Network Intrusion Detection (NIDS) devices are available in all configurations: Monitor Only; Management and Monitor; Standard and Platinum; High Availability (HA); Gigabit; and High Availability for Gigabit devices. The service descriptions and requirements and limitations as reviewed above apply for this service. Verizon may provide additional details within the purchase order documentation for all NIDS Security Services.

Network Intrusion Detection (NIDS) Monitoring Only

Monitor only features include: Device Availability & Health Monitoring, Threat Analysis, Security Incident Handling, and Service & Security Incident Reporting.

Feature Name	Feature Identifier	Feature Description	Feature Limits or Compatibility Restrictions
Network Intrusion Detection (NIDS) Monitoring Only Standard	NIDS0001	NIDS Monitoring Only Standard provides all the Monitoring Only and Standard features and attributes described above. State and Event Analysis Machine (SEAM) Policy is not customized. Events Verizon deems a significant risk are stored and labeled with a sequence number to identify them and to track their status. In addition to the Dashboard, only email is used as a method of contact from the Security Operations Center (SOC) to customer.	Requires the following Feature Identifier if order is for the first managed security device at the location: NIDS0009
Network Intrusion Detection (NIDS) Monitoring Only Gigabit Standard	NIDS0002	This service provides all the features of Network Intrusion Detection (NIDS) Monitoring Only Standard service for those NIDS devices handling gigabit throughput. All other Standard attributes and restrictions apply.	Requires the following Feature Identifier if order is for the first managed security device at the location: NIDS0009

6.3.3.8a Converged Services, IP and Network IP Transport Services – Security Services Attachment 3

Feature Name	Feature Identifier	Feature Description	Feature Limits or Compatibility Restrictions
<p>Network Intrusion Detection (NIDS) Monitoring Only High Availability Standard</p>	<p>NIDS0003</p>	<p>This service provides all the features of NIDS Monitoring Only Standard service per pair of NIDS devices in a fail-over or load balancing configuration. High Availability service is to provide a level of redundancy of the NIDS in case the primary NIDS fails and/or load balancing when the customer has the required CPE engineered solution. This service is only available on NIDS platforms supporting High Availability. All other Standard attributes and restrictions apply.</p>	<p>Requires the following Feature Identifier if order is for the first managed security device at the location:</p> <p>NIDS0009</p>
<p>Network Intrusion Detection (NIDS) Monitoring Only High Availability Gigabit Standard</p>	<p>NIDS0004</p>	<p>This service provides all the features of Network Intrusion Detection (NIDS) Monitoring Only Standard Service for those NIDS devices handling gigabit throughput and per pair of NIDS devices in a fail-over or load balancing configuration. High Availability service is to provide a level of redundancy of the NIDS in case the primary NIDS fails and/or load balancing when the customer has the required CPE engineered solution. All other Standard features and restrictions apply.</p>	<p>Requires the following Feature Identifier if order is for the first managed security device at the location:</p> <p>NIDS0009</p>

6.3.3.8a Converged Services, IP and Network IP Transport Services – Security Services Attachment 3

Feature Name	Feature Identifier	Feature Description	Feature Limits or Compatibility Restrictions
Network Intrusion Detection (NIDS) Monitoring Only Platinum			
Network Intrusion Detection (NIDS) Monitoring Only Platinum	NIDS0005	NIDS Monitoring Only Platinum provides all the features listed under NIDS Monitoring. SEAM Policy is customized to fit the customer's security needs. Event Analysis includes all the features for Standard except all events, not only those Verizon deems a significant risk, are labeled with a sequence number to identify them and to track their status. Phone is a method of contact from the SOC to customer and vice versa in addition to the Dashboard. Data on raw events defined as harmful by the customer will be kept for one (1) year. Moreover, this data can be made available on request up to one (1) month after the Service has been terminated. Verizon provides a review between the customer and a security Customer Service Manager (CSM) once a month.	Requires the following Feature Identifier if order is for the first managed security device at the location: NIDS0009
Network Intrusion Detection (NIDS) Monitoring Only Gigabit Platinum	NIDS0006	This service provides all the features of NIDS Monitoring Only Platinum Service for those NIDS handling gigabit throughput. All other Platinum features and restrictions apply.	Requires the following Feature Identifier if order is for the first managed security device at the location: NIDS0009

6.3.3.8a Converged Services, IP and Network IP Transport Services – Security Services Attachment 3

Feature Name	Feature Identifier	Feature Description	Feature Limits or Compatibility Restrictions
Network Intrusion Detection (NIDS) Monitoring Only High Availability Platinum	NIDS0007	This service provides all the features of NIDS Monitoring Only Platinum service per pair of NIDS devices in a fail-over or load balancing configuration. High Availability service is to provide a level of redundancy of the NIDS in case the primary NIDS fails and/or load balancing when the customer has the required CPE engineered solution. This service is only available on NIDS platforms supporting High Availability. All other Platinum features and restrictions apply.	Requires the following Feature Identifier if order is for the first managed security device at the location: NIDS0009
Network Intrusion Detection (NIDS) Monitoring Only High Availability Gigabit Platinum	NIDS0008	This service provides all the features of NIDS Monitoring Only Platinum Service for those NIDS handling gigabit throughput per pair of NIDS devices in a fail-over or load balancing configuration. All other Platinum features and restrictions apply.	Requires the following Feature Identifier if order is for the first managed security device at the location: NIDS0009
Site Set Up Local Event Collector	NIDS0009	Site Set Up fee is charged for each Local Event Collector (LEC) per location. This fee covers placement of a local event collector and is dependent on the architectural solution design per customer.	Required for first managed security device on site.

6.3.3.8a Converged Services, IP and Network IP Transport Services – Security Services Attachment 3

Feature Name	Feature Identifier	Feature Description	Feature Limits or Compatibility Restrictions
Additional Customer Certificate	NIDS0010	All NIDS Monitoring MSS services require authorized Customer Certificates for user access authorization. Five (5) Customer Certificates are included in the price of all Monitored MSS services. Additional Customer Certificates are available for each additional user access.	

Network Intrusion Detection (NIDS) Management and Monitoring:

Management and Monitoring services include: Device Availability Monitoring, Health Monitoring, Device Troubleshooting, Hardware Maintenance, Threat Analysis. Security Incident Handling, Device Maintenance, Device Security Management, and Service & Security Incident Reporting.

Feature Name	Feature Identifier	Feature Description	Feature Limits or Compatibility Restrictions
<p>Network Intrusion Detection (NIDS) Management and Monitoring Standard</p>	<p>NIDS0011</p>	<p>NIDS Management and Monitoring Standard provides all the features listed above for NIDS Management & Monitoring. State and Event Analysis Machine (SEAM) Policy is not customized. Events Verizon deems a significant risk are stored and labeled with a sequence number to identify them and to track their status. In addition to the Dashboard, only email is used as a method of contact from the SOC to customer. Standard service will allow up to 1 Regular Change, 1 Fast-Track and 0 Urgent monthly Change Request. Additional Change Request will incur charges identified as Regular, Fast-Track, and Urgent.</p>	<p>Requires the following Feature Identifier if order is for the first managed security device at the location:</p> <p>NIDS0019</p>
<p>Network Intrusion Detection (NIDS) Management and Monitoring Gigabit Standard</p>	<p>NIDS0012</p>	<p>This service provides all the features of Standard NIDS Management and Monitoring Service for those NIDS devices handling gigabit throughput. All other Standard features and restrictions apply.</p>	<p>Requires the following Feature Identifier if order is for the first managed security device at the location:</p> <p>NIDS0019</p>

6.3.3.8a Converged Services, IP and Network IP Transport Services – Security Services Attachment 3

Feature Name	Feature Identifier	Feature Description	Feature Limits or Compatibility Restrictions
Network Intrusion Detection (NIDS) Management and Monitoring High Availability Standard	NIDS0013	This service provides all the NIDS Management and Monitoring Standard features per pair of NIDS devices in a fail-over or load balancing configuration. High Availability service is to provide a level of redundancy of the NIDS in case the primary NIDS fails and/or load balancing when the customer has the required CPE engineered solution. All other Standard features and restrictions apply.	Requires the following Feature Identifier if order is for the first managed security device at the location: NIDS0019
Network Intrusion Detection (NIDS) Management and Monitoring High Availability Gigabit Standard	NIDS0014	This service provides all the features of NIDS Management and Monitoring Standard Service for those NIDS devices handling gigabit throughput per pair of NIDS devices in a fail-over or load balancing configuration. All other Standard features and restrictions apply.	Requires the following Feature Identifier if order is for the first managed security device at the location: NIDS0019

6.3.3.8a Converged Services, IP and Network IP Transport Services – Security Services Attachment 3

Feature Name	Feature Identifier	Feature Description	Feature Limits or Compatibility Restrictions
Network Intrusion Detection (NIDS) Management and Monitoring Platinum			
Network Intrusion Detection (NIDS) Management and Monitoring Platinum	NIDS0015	<p>NIDS Management and Monitoring Platinum provides all the features listed under NIDS Management and Monitoring with the following features: SEAM Policy is customized to fit the customers security needs. Event Analysis includes all the features for Standard except all events, not only those Verizon deems a significant risk, are labeled with a sequence number to identify them and to track their status. Phone is a method of contact from the SOC to customer and vice versa in addition to the Dashboard. Data on raw events defined as harmful by the customer will be kept for one (1) year. Moreover, this data can be made available on request up to one (1) month after the Service has been terminated. To perform NIDS upgrades, customer can define an unlimited number of Maintenance Windows necessary to perform these upgrades. Verizon provides a review between the customer and a security Customer Service Manager (CSM) once a month. Platinum service will allow up to unlimited Regular Change, 1 Fast-</p>	<p>Requires the following Feature Identifier if order is for the first managed security device at the location:</p> <p>NIDS0019</p>

6.3.3.8a Converged Services, IP and Network IP Transport Services – Security Services Attachment 3

Feature Name	Feature Identifier	Feature Description	Feature Limits or Compatibility Restrictions
		Track and 1 Urgent monthly Change Request. Additional Change Request will incur charges identified as Fast-Track, and Urgent. Verizon may provide additional details within the purchase order	
Network Intrusion Detection (NIDS) Management and Monitoring Gigabit Platinum	NIDS0016	This service provides all the features of NIDS Management and Monitoring Platinum Service for those NIDS devices handling gigabit throughput. All other Platinum features and restrictions apply.	Requires the following Feature Identifier if order is for the first managed security device at the location: NIDS0019
Network Intrusion Detection (NIDS) Management and Monitoring High Availability Platinum	NIDS0017	This service provides all the features of Verizon NIDS Management and Monitoring Platinum service per pair of NIDS devices in a fail-over or load balancing configuration. High Availability service is to provide a level of redundancy of the NIDS in case the primary NIDS fails and/or load balancing when the customer has the required CPE engineered solution. This service is only available on NIDS platforms supporting High Availability. All other Platinum features and restrictions apply.	Requires the following Feature Identifier if order is for the first managed security device at the location: NIDS0019

6.3.3.8a Converged Services, IP and Network IP Transport Services – Security Services Attachment 3

Feature Name	Feature Identifier	Feature Description	Feature Limits or Compatibility Restrictions
<p>Network Intrusion Detection (NIDS) Management and Monitoring High Availability Gigabit Platinum</p>	<p>NIDS0018</p>	<p>This service provides all the features of NIDS Management and Monitoring Platinum Service for those NIDS devices handling gigabit throughput per pair of NIDS devices in a fail-over or load balancing configuration. High Availability service is to provide a level of redundancy of the NIDS device in case the primary NIDS device fails and/or load balancing when the customer has the required CPE engineered solution. This service is only available on NIDS platforms supporting High Availability. All other Platinum features and restrictions apply.</p>	<p>Requires the following Feature Identifier if order is for the first managed security device at the location:</p> <p>NIDS0019</p>
<p>Site Set Up Local Event Collector</p>	<p>FRWL0019</p>	<p>Site Set Up fee is charged for each Local Event Collector (LEC) per location. This fee covers placement of a local event collector and is dependent on the architectural solution design per customer.</p>	<p>Required for first managed security device on site.</p>

6.3.3.8a Converged Services, IP and Network IP Transport Services – Security Services Attachment 3

Feature Name	Feature Identifier	Feature Description	Feature Limits or Compatibility Restrictions
Additional Customer Certificate	NIDS0020	All Intrusion Detection Management and Monitoring MSS services require authorized Customer Certificates for user access authorization. Five (5) Customer Certificates are included in the price of all Management and Monitored MSS services. Additional Customer Certificates are available for each additional user access.	
Additional Service Tickets (Apply to All Management and Monitoring Configurations):			
Regular (1 Service Ticket)	NIDT0001	A Regular Change Request includes but is not limited to changes to the application software and changes to operating system settings (except for changes to IP addresses). Verizon will implement accepted Regular Change Requests on the next Maintenance Window agreed upon with the customer when setting up the service.	

6.3.3.8a Converged Services, IP and Network IP Transport Services – Security Services Attachment 3

Feature Name	Feature Identifier	Feature Description	Feature Limits or Compatibility Restrictions
<p>Fast-track (4 Service Tickets)</p>	<p>NIDT0004</p>	<p>Fast-Track Change Request includes:</p> <ul style="list-style-type: none"> • Changes to existing rules or the creation of new rules and/or objects in the Rule Set of a Serviced Device and, maximum three (3) Serviced Devices are involved. • Creation of new hosts in the policy; the host is part of a subnet that is already accessible and configured on the Serviced Device. • Allowing or disallowing traffic between existing hosts. <p>Fast-Track Change Request does not include changes to the Virtual Private Network (“VPN”) configuration, change to the Network Address Translation (“NAT”) configuration of rules or objects, device policy changes on multiple Serviced Devices, changes to anti-spoofing settings, routing changes, or additions of interfaces to the Serviced Device.</p>	

6.3.3.8a Converged Services, IP and Network IP Transport Services – Security Services Attachment 3

Feature Name	Feature Identifier	Feature Description	Feature Limits or Compatibility Restrictions
Urgent (8 Service Tickets)	NIDT0008	Urgent Change Request includes changes to existing rules or the creation of new rules and/or objects in the Rule Set of one (1) Serviced Device, and clearly specified required configuration setting and its new value.	

Serviced Device: Network Intrusion Prevention Service (NIPS)

Security service for Network Intrusion Prevention (NIPS) devices are available in all configurations: Monitor Only, Management and Monitor; Standard and Platinum; High Availability (HA); Gigabit; High Availability for Gigabit devices. The service descriptions and requirements and limitations as reviewed above apply for this service. Verizon may provide additional details within the purchase order documentation for all NIPS Security Services.

Network Intrusion Prevention (NIPS) Monitoring Only

Monitor only features include: Device Availability & Health Monitoring, Threat Analysis, Security Incident Handling, and Service & Security Incident Reporting.

Feature Name	Feature Identifier	Feature Description	Feature Limits or Compatibility Restrictions
Network Intrusion Prevention (NIPS) Monitoring Only Standard			
Network Intrusion Prevention (NIPS) Monitoring Only Standard	NIPS0001	Network Intrusion Prevention Monitoring Only Standard provides all the Monitoring Only and Standard features and attributes described above. State and Event Analysis Management (SEAM) Policy is not customized. Events Verizon deems a significant risk are stored and labeled with a sequence number to identify them and to track their status. In addition to the Dashboard, only email is used as a method of contact from the Security Operations Center (SOC) to customer.	Requires the following Feature Identifier if order is for the first managed security device at the location: NIPS0009
Network Intrusion Prevention (NIPS) Monitoring Only Gigabit Standard	NIPS0002	This service provides all the features of NIPS Monitoring Only Standard Service for those NIPS devices handling gigabit throughput. All other Standard attributes and restrictions apply.	Requires the following Feature Identifier if order is for the first managed security device at the location: NIPS0009

6.3.3.8a Converged Services, IP and Network IP Transport Services – Security Services Attachment 3

Feature Name	Feature Identifier	Feature Description	Feature Limits or Compatibility Restrictions
Network Intrusion Prevention (NIPS) Monitoring Only High Availability Standard	NIPS0003	This service provides all the features of NIPS Monitoring Only Standard service per pair of NIPS devices in a fail-over or load balancing configuration. High Availability service is to provide a level of redundancy of the NIPS in case the primary NIPS fails and/or load balancing when the customer has the required CPE engineered solution. This service is only available on NIPS platforms supporting High Availability. All other Standard attributes and restrictions apply.	Requires the following Feature Identifier if order is for the first managed security device at the location: NIPS0009
Network Intrusion Prevention (NIPS) Monitoring Only High Availability Gigabit Standard	NIPS0004	This service provides all the features of NIPS Monitoring Only Standard Service for those NIPS devices handling gigabit throughput and service per pair of NIPS devices in a fail-over or load balancing configuration. High Availability service is to provide a level of redundancy of the NIPS in case the primary NIPS fails and/or load balancing when the customer has the required CPE engineered solution. All other Standard features and restrictions apply.	Requires the following Feature Identifier if order is for the first managed security device at the location: NIPS0009

6.3.3.8a Converged Services, IP and Network IP Transport Services – Security Services Attachment 3

Feature Name	Feature Identifier	Feature Description	Feature Limits or Compatibility Restrictions
Network Intrusion Prevention (NIPS) Monitoring Only Platinum			
Network Intrusion Prevention (NIPS) Monitoring Only Platinum	NIPS0005	NIPS Monitoring Only Platinum provides all the features listed under NIPS Monitoring. SEAM Policy is customized to fit the customer's security needs. Event Analysis includes all the features for Standard except all events, not only those Verizon deems a significant risk, are labeled with a sequence number to identify them and to track their status. Phone is a method of contact from the SOC to customer and vice versa in addition to the Dashboard. Data on raw events defined as harmful by the customer will be kept for one (1) year. Moreover, this data can be made available on request up to one (1) month after the Service has been terminated. Verizon provides a review between the customer and a security Customer Service Manager (CSM) once a month.	Requires the following Feature Identifier if order is for the first managed security device at the location: NIPS0009
Network Intrusion Prevention (NIPS) Monitoring Only Gigabit Platinum	NIPS0006	This service provides all the features of NIPS Monitoring Only Platinum Service for those NIPS devices handling gigabit throughput. All other Platinum features and restrictions apply.	Requires the following Feature Identifier if order is for the first managed security device at the location: NIPS0009

6.3.3.8a Converged Services, IP and Network IP Transport Services – Security Services Attachment 3

Feature Name	Feature Identifier	Feature Description	Feature Limits or Compatibility Restrictions
Network Intrusion Prevention (NIPS) Monitoring Only High Availability Platinum	NIPS0007	This service provides all the features of NIPS Monitoring Only Platinum service per pair of NIPS devices in a fail-over or load balancing configuration. High Availability service is to provide a level of redundancy of the NIPS in case the primary NIPS fails and/or load balancing when the customer has the required CPE engineered solution. This service is only available on NIPS platforms supporting High Availability. All other Platinum features and restrictions apply.	Requires the following Feature Identifier if order is for the first managed security device at the location: NIPS0009
Network Intrusion Prevention (NIPS) Monitoring Only High Availability Gigabit Platinum	NIPS0008	This service provides all the features of NIPS Monitoring Only Platinum Service for those NIPS devices handling gigabit throughput per pair of NIPS devices in a fail-over or load balancing configuration. All other Platinum features and restrictions apply.	Requires the following Feature Identifier if order is for the first managed security device at the location: NIPS0009
Site Set Up Local Event Collector	NIPS0009	Site Set Up fee is charged for each Local Event Collector (LEC) per location. This fee covers placement of a local event collector and is dependent on the architectural solution design per customer.	Required for first managed security device on site.

6.3.3.8a Converged Services, IP and Network IP Transport Services – Security Services Attachment 3

Network Intrusion Prevention (NIPS) Management and Monitoring Service

Management and Monitoring services include: Device Availability Monitoring, Health Monitoring, Device Troubleshooting, Threat Analysis. Security Incident Handling, Device Maintenance, Device Security Management, Service & Security Incident Reporting.

Feature Name	Feature Identifier	Feature Description	Feature Limits or Compatibility Restrictions
Network Intrusion Prevention (NIPS) Management and Monitoring Standard			
Network Intrusion Prevention (NIPS) Management and Monitoring Standard	NIPS0012	NIPS Management and Monitoring Standard provides all the features listed above for Management & Monitoring Standard. State and Event Analysis Machine (SEAM) Policy is not customized. Events Verizon deems a significant risk are stored and labeled with a sequence number to identify them and to track their status. In addition to the Dashboard, only email is used as a method of contact from the SOC to customer. Standard service will allow up to 1 Regular Change, 1 Fast-Track and 0 Urgent monthly Change Request. Additional Change Request will incur charges identified as Regular, Fast-Track, and Urgent.	Requires the following Feature Identifier if order is for the first managed security device at the location: NIPS0020

6.3.3.8a Converged Services, IP and Network IP Transport Services – Security
 Services Attachment 3

Feature Name	Feature Identifier	Feature Description	Feature Limits or Compatibility Restrictions
Network Intrusion Prevention (NIPS) Management and Monitoring Gigabit Standard	NIPS0013	This service provides all the features of Standard NIPS Management and Monitoring Service for those NIPS devices handling gigabit throughput. All other Standard features and restrictions apply.	Requires the following Feature Identifier if order is for the first managed security device at the location: NIPS0020
Network Intrusion Prevention (NIPS) Management and Monitoring High Availability Standard	NIPS0014	This service provides all the NIPS Management and Monitoring Standard features per pair of NIPS devices in a fail-over or load balancing configuration. High Availability service is to provide a level of redundancy of the NIPS in case the primary NIPS fails and/or load balancing when the customer has the required CPE engineered solution. All other Standard features and restrictions apply.	Requires the following Feature Identifier if order is for the first managed security device at the location: NIPS0020
Network Intrusion Prevention (NIPS) Management and Monitoring High Availability Gigabit Standard	NIPS0015	This service provides all the features of NIPS Management and Monitoring Standard Service for those NIPS devices handling gigabit throughput per pair of NIPS devices in a fail-over or load balancing configuration. All other Standard features and restrictions apply.	Requires the following Feature Identifier if order is for the first managed security device at the location: NIPS0020
Network Intrusion Prevention (NIPS) Management and Monitoring Platinum			

6.3.3.8a Converged Services, IP and Network IP Transport Services – Security Services Attachment 3

Feature Name	Feature Identifier	Feature Description	Feature Limits or Compatibility Restrictions
<p>Network Intrusion Prevention (NIPS) Management and Monitoring Platinum</p>	<p>NIPS0016</p>	<p>NIPS Management and Monitoring Platinum provides all the features listed under NIPS Management and Monitoring with the following features: SEAM Policy is customized to fit the customers security needs. Event Analysis includes all the features for Standard except all events, not only those Verizon deems a significant risk, are labeled with a sequence number to identify them and to track their status. Phone is a method of contact from the SOC to customer and vice versa in addition to the Dashboard. Data on raw events defined as harmful by the customer will be kept for one (1) year. Moreover, this data can be made available on request up to one (1) month after the Service has been terminated. To perform NIPS upgrades, customer can define an unlimited number of Maintenance Windows necessary to perform these upgrades. Verizon provides a review between the customer and a security Customer Service Manager (CSM) once a month. Platinum service will allow up to unlimited Regular Change, 1 Fast-Track and 1 Urgent monthly</p>	<p>Requires the following Feature Identifier if order is for the first managed security device at the location:</p> <p>NIPS0020</p>

6.3.3.8a Converged Services, IP and Network IP Transport Services – Security Services Attachment 3

Feature Name	Feature Identifier	Feature Description	Feature Limits or Compatibility Restrictions
		Change Request. Additional Change Request will incur charges identified as Fast-Track, and Urgent. All other Platinum features and restrictions apply.	
Network Intrusion Prevention (NIPS) Management and Monitoring Gigabit Platinum	NIPS0017	This service provides all the features of NIPS Management and Monitoring Platinum Service for those NIPS devices handling gigabit throughput. All other Platinum features and restrictions apply.	Requires the following Feature Identifier if order is for the first managed security device at the location: NIPS0020
Network Intrusion Prevention (NIPS) Management and Monitoring High Availability Platinum	NIPS0018	This service provides all the features of Verizon NIPS Management and Monitoring Platinum service per pair of NIPS devices in a fail-over or load balancing configuration. High Availability service is to provide a level of redundancy of the NIPS in case the primary NIPS fails and/or load balancing when the customer has the required CPE engineered solution. This service is only available on NIPS platforms supporting High Availability. All other Platinum features and restrictions apply.	Requires the following Feature Identifier if order is for the first managed security device at the location: NIPS0020

6.3.3.8a Converged Services, IP and Network IP Transport Services – Security Services Attachment 3

Feature Name	Feature Identifier	Feature Description	Feature Limits or Compatibility Restrictions
<p>Network Intrusion Prevention (NIPS) Management and Monitoring High Availability Gigabit Platinum</p>	<p>NIPS0019</p>	<p>This service provides all the features of NIPS Management and Monitoring Platinum Service for those NIPS devices handling gigabit throughput per pair of NIPS devices in a fail-over or load balancing configuration. High Availability service is to provide a level of redundancy of the NIPS device in case the primary NIPS device fails and/or load balancing when the customer has the required CPE engineered solution. This service is only available on NIPS platforms supporting High Availability. All other Platinum features and restrictions apply.</p>	<p>Requires the following Feature Identifier if order is for the first managed security device at the location:</p> <p>NIPS0020</p>
<p>Site Set Up Local Event Collector</p>	<p>NIPS0020</p>	<p>Site Set Up fee is charged for each Local Event Collector (LEC) per location. This fee covers placement of a local event collector and is dependent on the architectural solution design per customer.</p>	<p>Required for first managed security device on site.</p>

6.3.3.8a Converged Services, IP and Network IP Transport Services – Security Services Attachment 3

Feature Name	Feature Identifier	Feature Description	Feature Limits or Compatibility Restrictions
Additional Service Tickets (Apply to All Management and Monitoring Configurations)			
Regular (1 Service Ticket)	NIPT0001	A Regular Change Request includes but is not limited to changes to the application software and/or changes to operating system settings (except for changes to IP addresses). Verizon will implement accepted Regular Change Requests on the next Maintenance Window agreed upon with the customer when setting up the service.	
Fast-track (4 Service Tickets)	NIPT0004	<p>Fast-Track Change Requests are limited to the following:</p> <ul style="list-style-type: none"> • Changes to existing rules or the creation of new rules and/or objects in the Rule Set of a Serviced Device and, maximum three (3) Serviced Devices are involved. • Creation of new hosts in the policy; the host is part of a subnet that is already accessible and configured on the Serviced Device. • Allowing or disallowing traffic between existing hosts. <p>Fast-Track Change Request does not include changes to the Virtual Private Network (“VPN”) configuration,</p>	

6.3.3.8a Converged Services, IP and Network IP Transport Services – Security Services Attachment 3

Feature Name	Feature Identifier	Feature Description	Feature Limits or Compatibility Restrictions
		<p>change to the Network Address Translation (“NAT”) configuration of rules or objects, device policy changes on multiple Serviced Devices, changes to anti-spoofing settings, routing changes, or additions of interfaces to the Serviced Device.</p> <p>Urgent Change Request are limited to changes to existing rules or the creation of new rules and/or objects in the Rule Set of one (1) Serviced Device, and clearly specified required configuration setting and its new value.</p>	
<p>Urgent (8 Service Tickets) -</p>	<p>NIPT0008</p>	<p>Urgent Change Request are limited to changes to existing rules or the creation of new rules and/or objects in the Rule Set of one (1) Serviced Device, and clearly specified required configuration setting and its new value.</p>	

6.3.3.8a Converged Services, IP and Network IP Transport Services – Security Services Attachment 3

Serviced Device: Proxy Server

Security service for Proxy Server devices are available in the following configurations: Monitor Only, Management and Monitor, Platinum, and High Availability (HA)

Proxy service is not available in Standard, Gigabit and High Availability for Gigabit devices.

The service descriptions, and requirements and limitations for each of the configurations as reviewed above apply. Verizon may provide additional details within the purchase order documentation to contract for all Proxy Server Security Services.

Proxy Server Monitoring Only

Monitor only features include: Device Availability & Health Monitoring, Threat Analysis, Security Incident Handling, and Service & Security Incident Reporting.

6.3.3.8a Converged Services, IP and Network IP Transport Services – Security Services Attachment 3

Feature Name	Feature Identifier	Feature Description	Feature Limits or Compatibility Restrictions
<p>Proxy Server Monitoring Only Platinum</p>	<p>PRXY0009</p>	<p>Proxy Server Monitoring Only Platinum provides all the features listed under Proxy Server Monitoring. SEAM Policy is customized to fit the customer's security needs. Event Analysis includes all the features for Standard except all events, not only those Verizon deems a significant risk, are labeled with a sequence number to identify them and to track their status. Phone is a method of contact from the SOC to customer and vice versa in addition to the Dashboard. Data on raw events defined as harmful by the customer will be kept for one (1) year. Moreover, this data can be made available on request up to one (1) month after the Service has been terminated. Verizon provides a review between the customer and a security Customer Service Manager (CSM) once a month.</p>	<p>Requires the following Feature Identifier if order is for the first managed security device at the location:</p> <p>PRXY0011</p>

6.3.3.8a Converged Services, IP and Network IP Transport Services – Security Services Attachment 3

Feature Name	Feature Identifier	Feature Description	Feature Limits or Compatibility Restrictions
Proxy Server Monitoring Only High Availability Platinum	PRXY0010	This service provides all the features of Proxy Server Monitoring Only Platinum service per pair of Proxy Server devices in a fail-over or load balancing configuration. High Availability service is to provide a level of redundancy of the Proxy Server in case the primary Proxy Server fails and/or load balancing when the customer has the required CPE engineered solution. This service is only available on Proxy Server platforms supporting High Availability. All other Platinum features and restrictions apply.	Requires the following Feature Identifier if order is for the first managed security device at the location: PRXY0011
Site Set Up Local Event Collector	PRXY0011	Site Set Up fee is charged for each Local Event Collector (LEC) per location. This fee covers placement of a local event collector and is dependent on the architectural solution design per customer.	Required for first managed security device on site.
Additional Customer Certificate	PRXY0012	All Proxy Server Monitoring MSS services require authorized Customer Certificates for user access authorization. Five (5) Customer Certificates are included in the price of all Monitored MSS services. Additional Customer Certificates are available for each additional user access.	

6.3.3.8a Converged Services, IP and Network IP Transport Services – Security Services Attachment 3

Feature Name	Feature Identifier	Feature Description	Feature Limits or Compatibility Restrictions
<p>Proxy Server Management and Monitoring Management and Monitoring services include: Device Availability Monitoring, Health Monitoring, Device Troubleshooting, Threat Analysis. Security Incident Handling, Device Maintenance, Device Security Management, Service & Security Incident Reporting.</p>			
<p>Proxy Server Management & Monitoring Platinum</p>	<p>PRXY0022</p>	<p>Proxy Server Management and Monitoring Platinum provides all the features listed under Proxy Server Management and Monitoring with the following features: SEAM Policy is customized to fit the customers security needs. Event Analysis includes all the features for Standard except all events, not only those Verizon deems a significant risk, are labeled with a sequence number to identify them and to track their status. Phone is a method of contact from the SOC to customer and vice versa in addition to the Dashboard. Data on raw events defined as harmful by the customer will be kept for one (1) year. Moreover, this data can be made available on request up to one (1) month after the Service has been terminated. To perform SSL VPN upgrades, customer can define an unlimited number of Maintenance Windows necessary to perform these upgrades. Verizon provides a review between the customer and a security Customer Service Manager (CSM) once a</p>	<p>Requires the following Feature Identifier if order is for the first managed security device at the location: PRXY0024</p>

6.3.3.8a Converged Services, IP and Network IP Transport Services – Security Services Attachment 3

Feature Name	Feature Identifier	Feature Description	Feature Limits or Compatibility Restrictions
		<p>month. Platinum service will allow up to unlimited Regular Change, 1 Fast-Track and 1 Urgent monthly Change Request. Additional Change Request will incur charges identified as Fast-Track, and Urgent. All other Platinum features and restrictions apply.</p>	
<p>Proxy Server Management & Monitoring High Availability Platinum</p>	<p>PRXY0023</p>	<p>This service provides all the features of Verizon Proxy Server Management and Monitoring Platinum service per pair of Proxy Server devices in a fail-over or load balancing configuration. High Availability service is to provide a level of redundancy of the Proxy Server in case the primary Proxy Server fails and/or load balancing when the customer has the required CPE engineered solution. This service is only available on Proxy Server platforms supporting High Availability. All other Platinum features and restrictions apply.</p>	<p>Requires the following Feature Identifier if order is for the first managed security device at the location:</p> <p>PRXY0024</p>

6.3.3.8a Converged Services, IP and Network IP Transport Services – Security Services Attachment 3

Feature Name	Feature Identifier	Feature Description	Feature Limits or Compatibility Restrictions
<p>Proxy Server Management Manage & Monitoring Anti-spam Add-on Platinum</p>	<p>PRXY0016</p>	<p>Proxy Server Management and Monitoring Anti-Spam Add-on Platinum provides Management and Monitoring service for Anti-Spam to a device enabled with Anti-Spam. This service provides the same level of Management and Monitoring of the Anti-Spam as the Proxy Server Monitoring Only Platinum. All services provided under Proxy Server Management and Monitoring Platinum are transitioned to the device's Anti-Spam capability.</p>	<p>Requires the following Feature Identifier if order is for the first managed security device at the location:</p> <p>PRXY0024</p>
<p>Proxy Server Management & Monitoring Anti-virus Add-on Platinum</p>	<p>PRXY0017</p>	<p>Proxy Server Management and Monitoring Anti-Virus Add-on Platinum provides Management and Monitoring service for Anti-Virus to a device enabled with Anti-virus. This service provides the same level of Management and Monitoring of the Anti-Virus as the Proxy Server Monitoring Only Platinum. All services provided under Proxy Server Management and Monitoring Platinum are transitioned to the device's Anti-Virus capability.</p>	<p>Requires the following Feature Identifier if order is for the first managed security device at the location:</p> <p>PRXY0024</p>

6.3.3.8a Converged Services, IP and Network IP Transport Services – Security Services Attachment 3

Feature Name	Feature Identifier	Feature Description	Feature Limits or Compatibility Restrictions
Proxy Server Management & Monitoring Content Filtering Add-on Platinum	PRXY0018	Proxy Server Management and Monitoring Content Filtering Add-on Platinum provides Management and Monitoring service for Content Filtering to a Proxy Server security device enabled with Content Filtering. This service provides the same level of Management and Monitoring of the Proxy Server Content Filtering as the Proxy Server Monitoring Only Platinum. All services provided under Proxy Server Management and Monitoring Platinum are transitioned to the device's Content Filtering capability.	Requires the following Feature Identifier if order is for the first managed security device at the location: PRXY0024
Site Set Up Local Event Collector	PRXY0024	Site Set Up fee is charged for each Local Event Collector (LEC) per location. This fee covers placement of a local event collector and is dependent on the architectural solution design per customer.	Required for first managed security device on site.
Additional Customer Certificate	PRXY0025	All Proxy Server Management and Monitoring MSS services require authorized Customer Certificates for user access authorization. Five (5) Customer Certificates are included in the price of all Management and Monitored MSS services. Additional Customer Certificates are available for each additional user access.	

6.3.3.8a Converged Services, IP and Network IP Transport Services – Security Services Attachment 3

Feature Name	Feature Identifier	Feature Description	Feature Limits or Compatibility Restrictions
Additional Service Tickets (Apply to All Management and Monitoring Configurations)			
Regular (1 Service Ticket)	PRXT0001	A Regular Change Request includes but is not limited to changes to the application software and/or changes to operating system settings (except for changes to IP addresses). Verizon will implement accepted Regular Change Requests on the next Maintenance Window agreed upon with the customer when setting up the service.	

6.3.3.8a Converged Services, IP and Network IP Transport Services – Security Services Attachment 3

Feature Name	Feature Identifier	Feature Description	Feature Limits or Compatibility Restrictions
Fast-track (4 Service Tickets)	PRXT0004	<p>Fast-Track Change Requests are limited to the following:</p> <ul style="list-style-type: none"> • Changes to existing rules or the creation of new rules and/or objects in the Rule Set of a Serviced Device and a maximum three (3) Serviced Devices are involved. • Creation of new hosts in the policy; the host is part of a subnet that is already accessible and configured on the Serviced Device. • Allowing or disallowing traffic between existing hosts. <p>Fast-Track Change Requests do not include changes to the Virtual Private Network (“VPN”) configuration, change to the Network Address Translation (“NAT”) configuration of rules or objects, device policy changes on multiple Serviced Devices, changes to anti-spoofing settings, routing changes, or additions of interfaces to the Serviced Device.</p>	

6.3.3.8a Converged Services, IP and Network IP Transport Services – Security Services Attachment 3

Feature Name	Feature Identifier	Feature Description	Feature Limits or Compatibility Restrictions
Urgent (8 Service Tickets)	PRXT0008	Urgent Change Requests are limited to changes to existing rules or the creation of new rules and/or objects in the Rule Set of one (1) Serviced Device and must clearly specify required configuration setting and its new value.	

Serviced Device: Managed Security Event Management (SEM)

Managed SEM is included with Verizon's Managed Security Service (MSS) portfolio of services. This Managed SEM service is exclusively for Organizations that need Verizon to manage their customer-owned SEM system(s) and thus the service and fees are incremental to the Verizon Managed Security Service fees in the Managed Services section.

Security services for SEM provides Management and Monitoring for the SEM platform. While device services in this section are limited to Monitoring Only features.

Option: The CALNET service provides Management and Monitoring as described below, but Verizon can offer Monitoring Only for SEM platform and subordinate devices.

Verizon may provide additional details within the purchase order documentation for all MSEM Security Services.

Managed SEM Management and Monitoring

The SEM Management tool and Serviced Devices are Monitored under this MSS offer. The SEM Serviced Devices that depend on the SEM Management tool are not managed by Verizon under this offer.

Verizon offers the following Managed SEM services:

Monitoring Services:

- Availability and Health Monitoring of the SEM tool
- Availability and Health Monitoring of the Serviced Devices
- Threat Analysis and Active Incident Handling of the events and incidents generated by the SEM tool

Management Services:

- Proactive Device Maintenance of the SEM tool
- Device Security Management of the SEM tool

Optional: Management of the Serviced Devices behind the SEM tool. This service can be offered for those devices that are part of the Verizon MSS portfolio but pricing is not included here in this submission for this optional service.

Reporting Services:

- Access to Security Dashboard
- To be confirmed and depending on the SEM tool: access to compliance reports generated by the SEM tool

6.3.3.8a Converged Services, IP and Network IP Transport Services – Security Services Attachment 3

Feature Name	Feature Identifier	Feature Description	Feature Limits or Compatibility Restrictions
Managed SEM Platform	OLGM0001	Managed SEM Platform is a one-time and monthly fee required to manage the customer-provided SEM platform	Required for first managed security device on site. OLGP0000
Managed SEM, Type 1: NIDS/NIPS, mainframe, enterprise application, policy manager, vulnerability scanner, wireless access controller set-up	OLGM0002	Managed SEM, Type 1: is a monthly fee per device.	Requires the following Feature Identifier: OLGM0001
Managed SEM, Type 2: Firewall, web application firewall, router, proxy, gateway av, ssl vpn, identity management server, Content Filtering, switch	OLGM0003	Managed SEM, Type 2: is a monthly fee per device.	Requires the following Feature Identifier: OLGM0001
Managed SEM, Type 3: HIPS/HIDS on server, operating system, database server, web server, application server	OLGM0004	Managed SEM, Type 3: is a monthly fee per service running on a server	Requires the following Feature Identifier: OLGM0001

6.3.3.8a Converged Services, IP and Network IP Transport Services – Security Services Attachment 3

Feature Name	Feature Identifier	Feature Description	Feature Limits or Compatibility Restrictions
Managed SEM, Type 4: Personal av, personal fw, HIPS/HIDS on laptop, up to 100 clients	OLGM0005	Managed SEM, Type 4: is a monthly fee per device (for up to 100 clients)	Requires the following Feature Identifier: OLGM0001
Managed SEM, Type 4: Personal av, personal fw, HIPS/HIDS on laptop, 101 to 250 clients	OLGM0006	Managed SEM, Type 4: is a monthly fee per device (for 101 to 250 clients)	Requires the following Feature Identifier: OLGM0001
Managed SEM, Type 4: Personal av, personal fw, HIPS/HIDS on laptop, 251 to 1000 clients	OLGM0007	Managed SEM, Type 4: is a monthly fee per device (for 251 to 1,000 clients)	Requires the following Feature Identifier: OLGM0001
Managed SEM, Type 4: Personal av, personal fw, HIPS/HIDS on laptop, 1001 to 5000 clients	OLGM0008	Managed SEM, Type 4: is a monthly fee per device (for 1,001 to 5,000 clients)	Requires the following Feature Identifier: OLGM0001
Managed SEM Platform Site Set-Up Fee(s)	OLGP0000	MANAGED SEM Platform Site Set-Up Fee is a one-time NRC required per platform site for implementing and initiating customer-provided MSEM service	Required for first managed security device on site.

6.3.3.8a Converged Services, IP and Network IP Transport Services – Security Services Attachment 3

Applicable Service Level Agreements - Managed Security Service (MSS):

- Standard Unavailable Device Notification – Monitoring Only, and Management and Monitoring Security Service
- Standard Health Incident Notification - Monitoring Only, and Management and Monitoring Security Service
- Standard Active Incident Escalation - Monitoring Only, and Management and Monitoring Security Service
- Platinum Unavailable Device Notification - Monitoring Only, and Management and Monitoring Security Service
- Platinum Health Incident Notification - Monitoring Only, and Management and Monitoring Security Service
- Platinum Active Incident Escalation - Monitoring Only, and Management and Monitoring Security Service.
- Standard Change Request Acceptance – Management and Monitoring
- Platinum Change Request Acceptance – Management and Monitoring
- Standard Change Request Implementation – Management and Monitoring
- Platinum Change Request Implementation – Management and Monitoring

6.3.3.8a Converged Services, IP and Network IP Transport Services – Security Services Attachment 4

Service Identifier: IP and Network IP Transport Services

The pricing includes the following elements: planning, applicable design, engineering, testing, wiring, termination, and applicable service level agreements.

Professional Security Services (PSS):

Feature Name	Feature Identifier	Unit of Measure	Unit Non - Recurring	Unit Recurring	Change Charges
Data Protection and DLP (Roadmap, Strategy & Implementation)	PSSV1425	Per Day (up to 8 hours, NWH)	\$1,600	N/A	N/A
MSS Configuration Support	PSSV1427	Per Day (up to 8 hours, NWH)	\$1,480	N/A	N/A

6.3.3.8a Converged Services, IP and Network IP Transport Services – Security Services Attachment 4

Managed Security Services (MSS):

Firewall Monitoring Only and Firewall Management and Monitoring

Feature Name	Feature Identifier	Unit of Measure	Unit Non – Recurring	Unit Recurring	Change Charges
Firewall Monitoring Only					
Firewall Monitoring Only Standard	FRWL0001	Per Device	\$500	\$383	N/A
Firewall Monitoring Only Gigabit Standard	FRWL0002	Per Device	\$500	\$459	N/A
Firewall Monitoring Only High Availability Standard	FRWL0003	Per Device	\$500	\$479	N/A
Firewall Monitoring Only High Availability Gigabit Standard	FRWL0004	Per Device	\$500	\$575	N/A
Firewall Monitoring Only Platinum	FRWL0005	Per Device	\$500	\$791	N/A
Firewall Monitoring Only Gigabit Platinum	FRWL0006	Per Device	\$500	\$952	N/A
Firewall Monitoring Only High Availability Platinum	FRWL0007	Per Device	\$500	\$989	N/A
Firewall Monitoring Only High Availability Gigabit Platinum	FRWL0008	Per Device	\$500	\$1,191	N/A
Site Set Up Local Event Collector	FRWL0010	Per Site Per LEC	\$2,500	N/A	N/A
Additional Customer Certificate	FRWL0011	Per Certificate	\$125	N/A	N/A

6.3.3.8a Converged Services, IP and Network IP Transport Services – Security Services Attachment 4

Feature Name	Feature Identifier	Unit of Measure	Unit Non – Recurring	Unit Recurring	Change Charges
Firewall Management and Monitoring					
Firewall Management & Monitoring Standard	FRWL0013	Per Device	\$500	\$500	N/A
Firewall Management & Monitoring Gigabit Standard	FRWL0014	Per Device	\$500	\$600	N/A
Firewall Management & Monitoring High Availability Standard	FRWL0015	Per Device	\$500	\$700	N/A
Firewall Management & Monitoring High Availability Gigabit Standard	FRWL0016	Per Device	\$500	\$845	N/A
Firewall Management & Monitoring Platinum	FRWL0017	Per Device	\$500	\$1,080	N/A
Firewall Management & Monitoring Gigabit Platinum	FRWL0018	Per Device	\$500	\$1,268	N/A
Firewall Management & Monitoring High Availability Platinum	FRWL0019	Per Device	\$500	\$1,530	N/A
Firewall Management & Monitoring High Availability Gigabit Platinum	FRWL0020	Per Device	\$500	\$1,795	N/A
Site Set Up LEC	FRWL0022	Per Site Per LEC	\$2,500	N/A	N/A

6.3.3.8a Converged Services, IP and Network IP Transport Services – Security Services Attachment 4

Feature Name	Feature Identifier	Unit of Measure	Unit Non – Recurring	Unit Recurring	Change Charges
Additional Customer Certificate	FRWL0023	Per Certificate	\$125	N/A	N/A
Additional Service Tickets					
Regular (1 Service Ticket)	FRWL0025	Per Occurrence	\$75.00	N/A	N/A
Fast-track (4 Service Tickets)	FRWL0026	Per Occurrence	\$125.00	N/A	N/A
Urgent (8 Service Tickets)	FRWL0027	Per Occurrence	\$200.00	N/A	N/A

6.3.3.8a Converged Services, IP and Network IP Transport Services – Security Services Attachment 4

Network Intrusion Detection Service (NIDS)

Feature Name	Feature Identifier	Unit of Measure	Unit Non – Recurring	Unit Recurring	Change Charges
Network Intrusion Detection (NIDS) Monitoring Only					
Network Intrusion Detection (NIDS) Monitoring Only Standard	NIDS0001	Per Device	\$500.00	\$434.00	N/A
Network Intrusion Detection (NIDS) Monitoring Only Gigabit Standard	NIDS0002	Per Device	\$500.00	\$527.00	N/A
Network Intrusion Detection (NIDS) Monitoring Only High Availability Standard	NIDS0003	Per Device	\$500.00	\$542.00	N/A
Network Intrusion Detection (NIDS) Monitoring Only High Availability Gigabit Standard	NIDS0004	Per Device	\$500.00	\$660.000	N/A
Network Intrusion Detection (NIDS) Monitoring Only Platinum	NIDS0005	Per Device	\$500.00	\$1,335.00	N/A
Network Intrusion Detection (NIDS) Monitoring Only Gigabit Platinum	NIDS0006	Per Device	\$500.00	\$1,607.00	N/A
Network Intrusion Detection (NIDS) Monitoring Only High Availability Platinum	NIDS0007	Per Device	\$500	\$1,472	N/A
Network Intrusion Detection (NIDS) Monitoring Only High Availability Gigabit Platinum	NIDS0008	Per Device	\$500	\$1,772	N/A
Site Set Up Local Event Collector	NIDS0009	Per Site Per LEC	\$2,500	N/A	N/A

6.3.3.8a Converged Services, IP and Network IP Transport Services – Security Services Attachment 4

Feature Name	Feature Identifier	Unit of Measure	Unit Non – Recurring	Unit Recurring	Change Charges
Additional Customer Certificate	NIDS0010	Per Certificate	\$125	N/A	N/A
Network Intrusion Detection (NIDS) Management and Monitoring					
Network Intrusion Detection (NIDS) Management and Monitoring Standard	NIDS0011	Per Device	\$500	\$550	N/A
Network Intrusion Detection (NIDS) Management and Monitoring Gigabit Standard	NIDS0012	Per Device	\$500	\$660	N/A
Network Intrusion Detection (NIDS) Management and Monitoring High Availability Standard	NIDS0013	Per Device	\$500	\$770	N/A
Network Intrusion Detection (NIDS) Management and Monitoring High Availability Gigabit Standard	NIDS0014	Per Device	\$500	\$924	N/A
Network Intrusion Detection (NIDS) Management and Monitoring Platinum	NIDS0015	Per Device	\$500	\$1,200	N/A
Network Intrusion Detection (NIDS) Management and Monitoring Gigabit Platinum	NIDS0016	Per Device	\$500	\$1,340	N/A
Network Intrusion Detection (NIDS) Management and Monitoring High Availability Platinum	NIDS0017	Per Device	\$500	\$1,680	N/A

Revised: MSA 3 Amendment No. 13 - 6.3.3.8a Converged Services, IP and Network IP Transport Services – Security Services

6.3.3.8a Converged Services, IP and Network IP Transport Services – Security Services Attachment 4

Feature Name	Feature Identifier	Unit of Measure	Unit Non – Recurring	Unit Recurring	Change Charges
Network Intrusion Detection (NIDS) Management and Monitoring High Availability Gigabit Platinum	NIDS0018	Per Device	\$500	\$2,016	N/A
Site Set Up - First Device	NIDS0019	Per Site Per LEC	\$2,500	N/A	N/A
Additional Customer Certificate	NIDS0020	Per Certificate	\$125	N/A	N/A
Regular (1 Service Ticket)	NIDT0001	Per Occurrence	\$75.00	N/A	N/A
Fast-track (4 Service Tickets)	NIDT0002	Per Occurrence	\$125.00	N/A	N/A
Urgent (8 Service Tickets)	NIDT0003	Per Occurrence	\$200.00	N/A	N/A

6.3.3.8a Converged Services, IP and Network IP Transport Services – Security Services Attachment 4

Network Intrusion Prevention Service (NIPS)

Feature Name	Feature Identifier	Unit of Measure	Unit Non – Recurring	Unit Recurring	Change Charges
Network Intrusion Prevention Services (NIPS) Monitoring Only					
Network Intrusion Prevention (NIPS) Monitoring Only Standard	NIPS0001	Per Device	\$500	\$442	N/A
Network Intrusion Prevention (NIPS) Monitoring Only Gigabit Standard	NIPS0002	Per Device	\$500	\$536	N/A
Network Intrusion Prevention (NIPS) Monitoring Only High Availability Standard	NIPS0003	Per Device	\$500	\$553	N/A
Network Intrusion Prevention (NIPS) Monitoring Only High Availability Gigabit Standard	NIPS0004	Per Device	\$500	\$670	N/A
Network Intrusion Prevention (NIPS) Monitoring Only Platinum	NIPS0005	Per Device	\$500	\$1,369	N/A
Network Intrusion Prevention (NIPS) Monitoring Only Gigabit Platinum	NIPS0006	Per Device	\$500	\$1,641	N/A
Network Intrusion Prevention (NIPS) Monitoring Only High Availability Platinum	NIPS0007	Per Device	\$500	\$1,912	N/A
Network Intrusion Prevention (NIPS) Monitoring Only High Availability Gigabit Platinum	NIPS0008	Per Device	\$500	\$2,292	N/A
Site Set Up Local Event Collector	NIPS0009	Per Site Per LEC	\$2,500	N/A	N/A

Revised: MSA 3 Amendment No. 13 - 6.3.3.8a Converged Services, IP and Network IP Transport Services – Security Services

6.3.3.8a Converged Services, IP and Network IP Transport Services – Security Services Attachment 4

Feature Name	Feature Identifier	Unit of Measure	Unit Non – Recurring	Unit Recurring	Change Charges
Network Intrusion Prevention Services (NIPS) Management and Monitoring					
Network Intrusion Prevention (NIPS) Management and Monitoring Standard	NIPS0012	Per Device	\$500	\$612	N/A
Network Intrusion Prevention (NIPS) Management and Monitoring Gigabit Standard	NIPS0013	Per Device	\$500	\$740	N/A
Network Intrusion Prevention (NIPS) Management and Monitoring High Availability Standard	NIPS0014	Per Device	\$500	\$857	N/A
Network Intrusion Prevention (NIPS) Management and Monitoring High Availability Gigabit Standard	NIPS0015	Per Device	\$500	\$1,035	N/A
Network Intrusion Prevention (NIPS) Management and Monitoring Platinum	NIPS0016	Per Device	\$500	\$1,640	N/A
Network Intrusion Prevention (NIPS) Management and Monitoring Gigabit Platinum	NIPS0017	Per Device	\$500	\$1,964	N/A
Network Intrusion Prevention (NIPS) Management and Monitoring High Availability Platinum	NIPS0018	Per Device	\$500	\$2,567	N/A

6.3.3.8a Converged Services, IP and Network IP Transport Services – Security Services Attachment 4

Feature Name	Feature Identifier	Unit of Measure	Unit Non – Recurring	Unit Recurring	Change Charges
Network Intrusion Prevention (NIPS) Management and Monitoring High Availability Gigabit Platinum	NIPS0019	Per Device	\$500	\$3,072	N/A
Site Set Up Local Event Collector	NIPS0020	Per Site Per LEC	\$2,500	N/A	N/A
Additional Service Tickets					
Regular (1 Service Ticket)	NIPT0001	Per Occurrence	\$75	N/A	
Fast-track (4 Service Tickets)	NIPT0004	Per Occurrence	\$125	N/A	
Urgent (8 Service Tickets)	NIPT0008	Per Occurrence	\$200	N/A	

6.3.3.8a Converged Services, IP and Network IP Transport Services – Security Services Attachment 4

Proxy Server

Feature Name	Feature Identifier	Unit of Measure	Unit Non – Recurring	Unit Recurring	Change Charges
Proxy Server Monitoring Only					
Proxy Server Monitoring Only Platinum	PRXY0009	Per Device	\$500	\$876	N/A
Proxy Server Monitoring Only High Availability Platinum	PRXY0010	Per Device	\$500	\$1,095	N/A
Site Set Up Local Event Collector	PRXY0011	Per Site	\$2,500	N/A	N/A
Additional Customer Certificate	PRXY0012	Per Device	\$125	N/A	N/A
Proxy Server Management and Monitoring Service					
Proxy Server Management & Monitoring Platinum	PRXY0022	Per Device	\$500	\$1,018	N/A
Proxy Server Management & Monitoring High Availability Platinum	PRXY0023	Per Device	\$500	\$1,425	N/A
Proxy Server Management Manage & Monitoring Anti-spam Add-on Platinum	PRXY0016	Per Device	\$500	\$505	N/A
Proxy Server Management & Monitoring Anti-virus Add-on Platinum	PRXY0017	Per Device	\$500	\$505	N/A
Proxy Server Management & Monitoring Content Filtering Add-on Platinum	PRXY0018	Per Device	\$500	\$505	N/A

6.3.3.8a Converged Services, IP and Network IP Transport Services – Security Services Attachment 4

Feature Name	Feature Identifier	Unit of Measure	Unit Non – Recurring	Unit Recurring	Change Charges
Site Set Up Local Event Collector	PRXY0024	Per Site	\$2,500	N/A	N/A
Additional Customer Certificate	PRXY0025	Per Device	\$125	N/A	N/A
Additional Service Tickets					
Regular (1 Service Ticket)	PRXT0001	Per Device	\$75.00	N/A	N/A
Fast-track (4 Service Tickets)	PRXT0004	Per Device	\$125.00	N/A	N/A
Urgent (8 Service Tickets)	PRXT0008	Per Device	\$200.00	N/A	N/A

6.3.3.8a Converged Services, IP and Network IP Transport Services – Security Services Attachment 4

Managed Security Event Management (SEM)

Feature Name	Feature Identifier	Unit of Measure	Unit Non – Recurring	Unit Recurring	Change Charges
Security Event Management (SEM) Platform					
Managed SEM Platform	OLGM0001	Per platform	\$1,557	\$1,557	NA
Managed SEM, Type 1: NIDS/NIPS, mainframe, enterprise application, policy manager, vulnerability scanner, wireless access controller set-up	OLGM0002	Per device	\$250	\$324	NA
Managed SEM, Type 2: Firewall, web application firewall, router, proxy, gateway av, ssl vpn, identity management server, Content Filtering, switch	OLGM0003	Per device	\$250	\$259	NA
Managed SEM, Type 3: HIPS/HIDS on server, operating system, database server, web server, application server	OLGM0004	Per server	\$50	\$32	NA
Managed SEM, Type 4: Personal av, personal fw, HIPS/HIDS on laptop, up to 100 clients	OLGM0005	Per group of clients	\$1,000	\$649	NA

6.3.3.8a Converged Services, IP and Network IP Transport Services – Security Services Attachment 4

Feature Name	Feature Identifier	Unit of Measure	Unit Non – Recurring	Unit Recurring	Change Charges
Managed SEM, Type 4: Personal av, personal fw, HIPS/HIDS on laptop, 101 to 250 clients	OLGM0006	Per group of clients	\$1,500	\$1,167	NA
Managed SEM, Type 4: Personal av, personal fw, HIPS/HIDS on laptop, 251 to 1000 clients	OLGM0007	Per group of clients	\$2,500	\$2,270	NA
Managed SEM, Type 4: Personal av, personal fw, HIPS/HIDS on laptop, 1001 to 5000 clients	OLGM0008	Per group of clients	\$3,500	\$3,243	NA
Managed SEM Platform Site Set-Up Fee(s)	OLGP0000	Per site	\$3,000.00	N/A	N/A

6.3.3.8a Converged Services, IP and Network IP Transport Services – Security Services Attachment 4

Note:

Taxes and Surcharges

The following taxes and/or surcharges may apply. See CALNET II Exhibit 5A - Tax Determination Matrix, Module 3 specific detail.

CA Sales Tax
CA City Utility Users Tax
CA 9-1-1 Surcharge
CA Universal Lifeline Surcharge
CA Relay Service and Communications Device Fund Surcharge
Teleconnect Fund Surcharge
CA PUC Fee
AD Valorem Surcharge
California High Cost Fund
Federal Universal Service Fee/Charge
Regulatory Charge
Administrative Charge

6.3.4.3 Converged Services, IP Telephony Business Line Services Attachment 3

Service Identifier: Converged Services, IP Telephony Business Line Service - Hosted IP Centrex (HIPC)

Description of the Service: Verizon’s Converged Services, Hosted IP Centrex (HIPC) Service is available to CALNET II customers throughout the entire State of California. The HIPC Service is deployed in geographically diverse locations throughout the US to provide redundancy and survivability. While the service is available throughout the country, HIPC is designed to deliver service to the entire state of California.

Unless noted separately in Attachment 4, services include the following elements: planning, applicable design, engineering, testing, and applicable service level agreements.

Feature Name	Feature Identifier	Feature Description	Feature Limits or Compatibility Restrictions
<p>Converged Service, IP Telephony Business Line Service – Hosted IP Centrex (HIPC)</p>	<p>CSBL0000</p>	<p>Hosted IP Centrex (HIPC) Line, including the following features:</p> <ul style="list-style-type: none"> Call Transfer Call Park Call Pickup Conference Call Hold Call Forward – Busy Don’t Answer Call Forward – All Calls Hunt Groups Multi Line Appearance Speed Dial Redial Message Waiting Indicator Auto Attendant Four-digit extension dialing 	<p>Requires Site Survey by Verizon prior to submission of order under the provisions of the Managed Project Work SLA. Provisioning timeframes will be established under the provisions of Managed Project Work.</p>

6.3.4.3 Converged Services, IP Telephony Business Line Services Attachment 3

Feature Name	Feature Identifier	Feature Description	Feature Limits or Compatibility Restrictions
		<p>Conference Bridge Caller ID Group Pickup Web Directory Directory Phone Display 900 Blocking</p> <p>Additional Included Features:</p> <ul style="list-style-type: none"> • Alternate Numbers • Anonymous Call Rejection • Authentication • Blind Call Transfer • Call Blast Personal • Call Forwarding-Multi Phone • Call Forwarding-No Answer • Call Forwarding Selective • Call Notify • Call Pickup-Directed with Barge-In • Call Return • Call Screening • Call Waiting • Calling Line ID Blocking 	

6.3.4.3 Converged Services, IP Telephony Business Line Services Attachment 3

Feature Name	Feature Identifier	Feature Description	Feature Limits or Compatibility Restrictions
		<ul style="list-style-type: none"> • Calling Line ID Blocking per Call • Cancel Call Waiting/Call Waiting per Call • Communication Manager • Distinctive Alert/Ringing • Do Not Disturb • Find Me • Flash Call Hold • LDAP Directory Integration • Loudspeaker Paging • Multi-path Forwarding • Music on Hold • Outbound Caller ID • Outlook Integration • Personalized Name Recording • Phone List Group • Phone List Personal • Phone List Call Log • Priority Alert/Ringing • Private Dial Plans 	

6.3.4.3 Converged Services, IP Telephony Business Line Services Attachment 3

Feature Name	Feature Identifier	Feature Description	Feature Limits or Compatibility Restrictions
		<ul style="list-style-type: none"> • PS/ALI • Ring Splash • Selective Call Acceptance • Selective Call Rejection • Selective Call Appearance • Selective Call Rejection • Telephony User Interface 	
Off-Net Toll	CSOF0000	Verizon HIPC service routes call traffic off of the IP network within the 50 United States, the District of Columbia, the Virgin Islands, and Puerto Rico. This is accomplished using PSTN gateways hosted within the network, further enabling the converged VoIP service.	
Off-Net Toll Free	CSOF0000	The Hosted Standalone IP Telephony service allows CALNET II customers to receive off-net toll free calls from the 50 United States, the District of Columbia, the Virgin Islands, and Puerto Rico.	

6.3.4.3 Converged Services, IP Telephony Business Line Services Attachment 3

Feature Name	Feature Identifier	Feature Description	Feature Limits or Compatibility Restrictions
Additional Line Appearances	IAAP0000	Provides additional Line Appearance for multi-line phones.	
Account Codes	IACD0000	Enables the tracking of calls made outside of the location by prompting subscribers for an account code.	
Attendant Console	IACN0000	The web-based Attendant Console enables a subscriber (e.g., receptionist) to monitor a configurable set of subscribers. All must be built under the same location as the Attendant. The Attendant Console graphically displays subscribers status (busy, idle, do not disturb), as well as detailed call information. The Attendant Console window is integrated with the Communication Manager, thereby enabling the attendant to perform functions such as click-to-transfer or click-to-dial.	

6.3.4.3 Converged Services, IP Telephony Business Line Services Attachment 3

Feature Name	Feature Identifier	Feature Description	Feature Limits or Compatibility Restrictions
Authorization Codes	IATC0000	Prompts subscribers for an authorization code when making calls outside of the location. Calls will not be connected unless a valid code is entered.	
Block of DID Numbers	IDID0000	Block of 20 DID numbers	
Virtual FX (per line)	IVFX0000	Inbound Only: CALNET II customers can use Virtual FX as an inbound-only application using Direct Inward Dialing (DID) to set up one or more virtual locations and permanently forward incoming calls to another physical hub location. This means that a CALNET II customer may have local DIDs in a variety of cities but have one central location where all of those incoming calls are terminated.	

6.3.4.3 Converged Services, IP Telephony Business Line Services Attachment 3

Feature Name	Feature Identifier	Feature Description	Feature Limits or Compatibility Restrictions
<p>Auto Attendant (per instance)</p>	<p>IAPI0000</p>	<p>The Auto Attendant serves as an automated receptionist that answers the phone and provides a personalized message to callers with options for connecting to the operator, dialing by name or extension, or connecting to up to six configurable extensions (e.g., 1 = Marketing, 2 = Sales, etc.). Configuration via the Verizon Customer Center Administrator Dashboard web interface also allows for hours of operation to be modified, with different options available for hours that the company is open or closed.</p>	

6.3.4.3 Converged Services, IP Telephony Business Line Services Attachment 3

Feature Name	Feature Identifier	Feature Description	Feature Limits or Compatibility Restrictions
Remote Office	IROF0000	<p>Enables subscribers to access and use their VoIP service from any end point, on-net or off-net (e.g., home office, mobile phone). This service is especially useful for teleworkers and mobile workers, as it enables them to use all of their Communication Manager features while working remotely (e.g., extension dialing, transfers, conference calls, Outlook Integration, directories, etc.). In addition, since calls are still originated from VoIP, the service provides an easy mechanism for separating personal and business phone expenses, as well as keeping alternate phone numbers private. This service must be set-up by the administrator.</p>	

6.3.4.3 Converged Services, IP Telephony Business Line Services Attachment 3

IP Network Transport Management (Switch):

Feature Name	Feature Identifier	Feature Description	Feature Limits or Compatibility Restrictions
<p>Management (Switch / Hub) - Managed LAN Monitor & Notify (Small)</p>	<p>MLMN0001</p>	<p>Managed Services LAN Monitor & Notify allows Verizon Business to be responsible to clear logical and physical issues with the access and/or the Verizon network. With Monitor and Notify, the customer retains responsibility to resolve logical and/or physical issues with the CPE. Switches must be certified by VzB MNS. VzB PIP network will provide inband management. This service requires Feature ID of either MTOI0001 or MII00002.</p>	<p>Hardware must not be identified as End of Life by the manufacturer.</p>

6.3.4.3 Converged Services, IP Telephony Business Line Services Attachment 3

Feature Name	Feature Identifier	Feature Description	Feature Limits or Compatibility Restrictions
Management (Switch /Hub) - Managed LAN Monitor & Notify (Medium)	MLMN0002	Managed Services LAN Monitor & Notify allows Verizon Business to be responsible to clear logical and physical issues with the access and/or the Verizon network. With Monitor and Notify, the customer retains responsibility to resolve logical and/or physical issues with the CPE. Switches must be certified by VzB MNS. VzB PIP network will provide inband management. This service requires Feature ID of either MTOI0001 or MIIO0002.	Hardware must not be identified as End of Life by the manufacturer.

6.3.4.3 Converged Services, IP Telephony Business Line Services Attachment 3

Feature Name	Feature Identifier	Feature Description	Feature Limits or Compatibility Restrictions
<p>Management (Switch /Hub) - Managed LAN Monitor & Notify (Large)</p>	<p>MLMN0003</p>	<p>Managed Services LAN Monitor & Notify allows Verizon Business to be responsible to clear logical and physical issues with the access and/or the Verizon network. With Monitor and Notify, the customer retains responsibility to resolve logical and/or physical issues with the CPE. Switches must be certified by VzB MNS. VzB PIP network will provide inband management. This service requires Feature ID of either MTOI0001 or MII00002.</p>	<p>Hardware must not be identified as End of Life by the manufacturer.</p>

6.3.4.3 Converged Services, IP Telephony Business Line Services Attachment 3

Feature Name	Feature Identifier	Feature Description	Feature Limits or Compatibility Restrictions
<p>Management (Switch /Hub) - Managed LAN Physical (Small)</p>	<p>MLPH0001</p>	<p>Managed Services LAN Physical allows Verizon Business to be responsible to clear logical and physical issues with the access and/or the Verizon network. Isolate and resolve physical fault conditions with the CPE. With Physical Mgmt, the customer retains the responsibility to resolve logical issues with the CPE. Switch must be certified by VzB MNS. Customer must have a manufacture certified maintenance agreement in place for this service. An Out of Band Modem & Modem Line are required from the customer. This service requires Feature ID of either MTOI0001 or MIIO0002.</p>	<p>Hardware must not be identified as End of Life by the manufacturer.</p>

6.3.4.3 Converged Services, IP Telephony Business Line Services Attachment 3

Feature Name	Feature Identifier	Feature Description	Feature Limits or Compatibility Restrictions
<p>Management (Switch /Hub) - Managed LAN Physical (Medium)</p>	<p>MLPH0002</p>	<p>Managed Services LAN Physical allows Verizon Business to be responsible to clear logical and physical issues with the access and/or the Verizon network. Isolate and resolve physical fault conditions with the CPE. With Physical Mgmt, the customer retains the responsibility to resolve logical issues with the CPE. Switch must be certified by VzB MNS. Customer must have a manufacture certified maintenance agreement in place for this service. An Out of Band Modem & Modem Line are required from the customer. This service requires Feature ID of either MTOI0001 or MII0002.</p>	<p>Hardware must not be identified as End of Life by the manufacturer.</p>

6.3.4.3 Converged Services, IP Telephony Business Line Services Attachment 3

Feature Name	Feature Identifier	Feature Description	Feature Limits or Compatibility Restrictions
<p>Management (Switch /Hub) - Managed LAN Physical (Large)</p>	<p>MLPH0003</p>	<p>Managed Services LAN Physical allows Verizon Business to be responsible to clear logical and physical issues with the access and/or the Verizon network. Isolate and resolve physical fault conditions with the CPE. With Physical Mgmt, the customer retains the responsibility to resolve logical issues with the CPE. Switch must be certified by VzB MNS. Customer must have a manufacture certified maintenance agreement in place for this service. An Out of Band Modem & Modem Line are required from the customer. This service requires Feature ID of either MTOI0001 or MII00002.</p>	<p>Hardware must not be identified as End of Life by the manufacturer.</p>

6.3.4.3 Converged Services, IP Telephony Business Line Services Attachment 3

Feature Name	Feature Identifier	Feature Description	Feature Limits or Compatibility Restrictions
<p>Management (Switch /Hub) - Managed LAN Full (Small)</p>	<p>MLFL0001</p>	<p>Managed Services LAN Full allows Verizon Business to be responsible to clear logical and physical issues with the access and/or the Verizon network. Resolve both logical and physical fault conditions that occur with the CPE. Switch must be certified by VzB MNS. Customer must have a manufacture certified maintenance agreement in place for this service. An Out of Band Modem & Modem Line are required from the customer. VzB will work to clear the fault condition remotely or by dispatching someone to the site. This service requires Feature ID of either MTOI0001 or MIIO0002.</p>	<p>Hardware must not be identified as End of Life by the manufacturer.</p>

6.3.4.3 Converged Services, IP Telephony Business Line Services Attachment 3

Feature Name	Feature Identifier	Feature Description	Feature Limits or Compatibility Restrictions
<p>Management (Switch /Hub) - Managed LAN Full (Medium)</p>	<p>MLFL0002</p>	<p>Managed Services LAN Full allows Verizon Business to be responsible to clear logical and physical issues with the access and/or the Verizon network. Resolve both logical and physical fault conditions that occur with the CPE. Switch must be certified by VzB MNS. Customer must have a manufacture certified maintenance agreement in place for this service. An Out of Band Modem & Modem Line are required from the customer. VzB will work to clear the fault condition remotely or by dispatching someone to the site. This service requires Feature ID of either MTOI0001 or MII00002.</p>	<p>Hardware must not be identified as End of Life by the manufacturer.</p>

6.3.4.3 Converged Services, IP Telephony Business Line Services Attachment 3

Feature Name	Feature Identifier	Feature Description	Feature Limits or Compatibility Restrictions
Management (Switch /Hub) - Managed LAN Full (Large)	MLFL0003	Managed Services LAN Full allows Verizon Business to be responsible to clear logical and physical issues with the access and/or the Verizon network. Resolve both logical and physical fault conditions that occur with the CPE. Switch must be certified by VzB MNS. Customer must have a manufacture certified maintenance agreement in place for this service. An Out of Band Modem & Modem Line are required from the customer. VzB will work to clear the fault condition remotely or by dispatching someone to the site. This service requires Feature ID of either MTOI0001 or MIIO0002.	Hardware must not be identified as End of Life by the manufacturer.
Takeover of Existing Device - Management Takeover of Switch	MTOI0001	This applies to Management (Switch/Hub) of Monitor & Notify, Physical and Full (Small, Medium and Large).	
New Device - Switch Installation requiring initial configuration and implementation support	MIIO0002	This applies to Management (Switch/Hub) of Monitor & Notify, Physical and Full (Small, Medium and Large).	

6.3.4.3 Converged Services, IP Telephony Business Line Services Attachment 3

Feature Name	Feature Identifier	Feature Description	Feature Limits or Compatibility Restrictions
Management (Switch /Hub) - Threshold Reporting	THRE0000	Verizon Business Notifies Managed Network Service engineers of performance exceptions, including enhanced latency, discards, traffic shaping, and more. A total of 11 thresholds are included.	
Management (Switch /Hub) - Order Expedite	OEXP0000	Request to activate switch in 15 days or less (Not Including Circuit).	
Management (Switch /Hub) - New Implementation Rescheduling	RSCH0000	Management (Switch/ Hub) New Implementation Rescheduling is an additional charge to reschedule Switch / Hub within less than 48 hours (2 calendar days) of original scheduled installation date. If Switch / Hub is rescheduled before 48 hours then no additional charge shall apply.	
Management (Switch /Hub) - After-Hours Premium Charge (M-F, 5 p.m. to 8 a.m., including weekends and holidays)	PREM0000	Managed (Switch/Hub) After Hours Premium Charge is a one site charge for standby support at the NOC during non-business hour installations. This charge is in addition to the normal business installation charge.	

6.3.4.3 Converged Services, IP Telephony Business Line Services Attachment 3

Optional Change Management provides additional change management support for items customers are not likely to encounter on a daily basis. Optional Change Management items are charged on a per-incident basis (NRC), and are available to customers that subscribe to 6.3.4.3 Converged Services, IP Telephony Business Line Services. These are enhanced features and a subset of the 6.3.4.3 Converged Services, IP Telephony Business Line Services.

Optional Change Management Activities:

Feature Name	Feature Identifier	Feature Description	Feature Limits or Compatibility Restrictions
Management (Switch /Hub) - LAN Dynamic Host Configuration Protocol (DHCP) IP Helper Add / Modify / Delete	LDFM0000	Switch configuration to Add / Modify / Delete Dynamic Host Configuration Protocol (DHCP) IP Helper Add / Modify / Delete. Available for Full Mgmt Only.	Remote configuration activity on the Switch/Hub
Management (Switch /Hub) - IP Address / Subnet Mask – Add / Modify / Delete	IAFM0000	IP Network Address /Subnet Mask - Add / Modify / Delete. Available for Full Mgmt Only.	Remote configuration activity on the Switch/Hub
Management (Switch /Hub) - Hostname change	HCFM0000	Switch configuration changes to change router host name WAN and LAN. Available for Full Mgmt Only.	Remote configuration activity on the Switch/Hub
Management (Switch /Hub) - VLAN – Add / Delete	VLFM0000	Add or remove a new VLAN to existing managed switch. Available for Full Mgmt Only.	Remote configuration activity on the Switch/Hub
Management (Switch /Hub) - Trunking Configuration – Add / Delete	TCFM0000	Enable or Disable ISL or 802.1Q trunking between two switches and configure DTP mode. Available for Full Mgmt Only.	Remote configuration activity on the Switch/Hub

6.3.4.3 Converged Services, IP Telephony Business Line Services Attachment 3

Feature Name	Feature Identifier	Feature Description	Feature Limits or Compatibility Restrictions
Management (Switch /Hub) - Spanning Tree – Add / Delete	STFM0000	Enable or Delete Spanning Tree Protocol (STP), configure port priority/VLAN priority, configure port costs, configure root switch. Available for Full Mgmt Only.	Remote configuration activity on the Switch/Hub
Management (Switch /Hub) - Storm Control – Add / Delete	SCFM0000	Enable or Delete broadcast, multicast, or unicast traffic storm control on the interface and configure the traffic storm control level. Available for Full Mgmt Only.	Remote configuration activity on the Switch/Hub
Management (Switch /Hub) - Ether Channel – Add / Delete	ECFM0000	Configure the EtherChannel on the switch port and set its EtherChannel mode or Delete EtherChannel on the switch port. Available for Full Mgmt Only.	Remote configuration activity on the Switch/Hub
Management (Switch /Hub) – UniDirectional Link Detection (UDLD) Configuration – Add / Delete	UCFM0000	Enable or Delete Unidirectional Link Detection (UDLD) protocol on a specific LAN port. Available for Full Mgmt Only.	Remote configuration activity on the Switch/Hub
Management (Switch /Hub) - Multicast Configuration – Add / Delete	MCFM0000	Enable/Delete or configure Internet Group Management Protocol (IGMP) snooping, GARP Multicast Registration Protocol (GMRP), or RGMP. Available for Full Mgmt Only.	Remote configuration activity on the Switch/Hub

6.3.4.3 Converged Services, IP Telephony Business Line Services Attachment 3

Feature Name	Feature Identifier	Feature Description	Feature Limits or Compatibility Restrictions
Management (Switch /Hub) – VLAN Trunk Protocol (VTP) Configuration – Add / Modify / Delete	VTPC0000	Enable VLAN Trunking Protocol (VTP); set mode, password, and pruning. Available for Full Mgmt Only.	Remote configuration activity on the Switch/Hub
<p>In lieu of the optional change management per occurrence services described above, customers have the option to utilize the established hourly rate. Labor charges will commence upon arrival at customer site. Only the highest single NRC will be charged per device. Feature ID's are MEMU0000, DOFM0000, IBSM0001, HRDU0001, LNIB0000, LERS0001, DDON0000, LAFT0000.</p>			
Management (Switch - labor only) - Memory Upgrade	MEMU0000	Dispatch of a technician to the premises to perform Add or swap to an upgraded memory (flash or DRAM). This includes additional remote management and configuration services. Available for Full Mgmt Only.	
Management (Switch - labor only) Switch IOS Change Support New Features	DOFM0000	Dispatch of a technician to the premises to perform Changes the IOS on the router for new feature requirements. This includes additional remote management and configuration services. Available for Full Mgmt Only.	

6.3.4.3 Converged Services, IP Telephony Business Line Services Attachment 3

Feature Name	Feature Identifier	Feature Description	Feature Limits or Compatibility Restrictions
Management (Switch - labor only) Intra-building Move	IBSM0001	Dispatch of a technician to the premises to perform In-building move of existing switch – using same circuit and no design impact. Done during normal business hours. This includes additional remote management and configuration services. Available for Full Mgmt Only.	
Management (Switch - labor only) Hardware Module Upgrade	HRDU0001	Dispatch of a technician to the premises to perform Add or swap a component to upgrade a module. This includes additional remote management and configuration services. Available for Full Mgmt Only.	
Management (Switch - labor only) Switch Move, Inter-building or Across Town	LNIB0000	Request to reschedule a router activation within 48 hours.	
Management (Switch-labor only) Switch Exchange	LERS0001	Dispatch of a technician to the premises to perform Across town is within 30 miles of original circuit, same switch but new circuit, done during normal business hours. This includes additional remote management and configuration services. Available for Full Mgmt Only.	

6.3.4.3 Converged Services, IP Telephony Business Line Services Attachment 3

Feature Name	Feature Identifier	Feature Description	Feature Limits or Compatibility Restrictions
Management (Switch) Field Service Technicians (labor only) - Normal business hours (M-F, 8 a.m. to 5 p.m.).	DDON0000	Management Field Service Technicians hourly rate during normal business hours (M-F, 8 a.m. to 5 p.m.). Dispatches a technician to perform on-site managed services on a time basis at the level of journeyman.	
Management (Switch) Field Service Technicians (labor only) – After hours (M-F, 5 p.m. to 8 a.m., including weekends and holidays).	LAFT0000	Management Field Service Technicians hourly rate after hours (M-F, 5 p.m. to 8 a.m., including weekends and holidays) dispatches a technician to perform on-site managed services on a time basis at the level of journeyman.	

Managed Wireless LAN (MWLAN)

MWLAN services provide ongoing 24x7 remote management support for customer Wireless LAN environments to keep them Secure, Highly Available and Performing at High Service Levels. Managed Services are delivered using an ITIL-based service model and include Technical Account Management and Proactive Engineering support. When Customer Wireless LAN's are supported by Verizon's Wireless LAN Management Services, Verizon provides the added benefit of an end-to-end view and SLA's for the Customer's Wireless LAN that includes:

- Time to Repair
- Managed Service Installation (Provisioning)
- Proactive Outage Notification

MWLAN services is a best effort service. The service features a robust Customer Portal with real-time dashboard for Application and Transaction status.

The MWLAN service must be associated with at least one Managed LAN site and the MWLAN management level must be at the same level or below the Managed LAN management level for the same site. Service does not include major upgrades. Hardware must not be identified as End of Life by the manufacturer.

MWLAN services provide a multistep deployment and management offering, including a pre-deployment evaluation of the customer site and usage plans, the creation and validation of a WLAN schematic, and a review of security and authentication policies. Verizon has Wireless Engineering and Assessment services which are required for preparing the Customer Wireless LAN for Managed Services. Please review the list of Supported Technologies for important feature limitations on technology scope.

Managed Wireless LAN (MWLAN) - Service Activation

Verizon has two service activation options are available for Managed Wireless LAN:

1. Managed Implementation – for new networks and devices
2. Managed Take Over – for existing networks and devices

Custom engineering services may be required for MWLAN takeover or implementation for large or complex Customer wireless environments. The MWLAN service must be associated with at least one Managed LAN site and the MWLAN management level must be at the same level or below the Managed LAN management level for the same site. The service does not include major upgrades and hardware must not be identified as End of Life by the manufacturer. Customer will be charged a service charge for all issues discovered with Full Management that result in an Verizon technician being

6.3.4.3 Converged Services, IP Telephony Business Line Services Attachment 3

dispatched that are due to the act or omission of Customer including, but not limited to, faulty in house wiring.

Managed Implementation

This option applies when a new network is required to meet the customer's requirements.

The Design process considers the customer's business requirements and technology needs in order to create a solution to meet current and future business needs. This includes:

- The collection of system, application and end-user requirements
- The creation of a detailed logical and physical design plan for transport and equipment
- Implementation of the overall project plan

The Implementation process consists of the activities required to deliver the network solution and to bring the network under management. Verizon Business performs the overall project management function for timely and efficient network activation. This includes:

- Order validation and acceptance for Managed Wireless LAN Service (and Managed WAN or Managed Services Complete, if required)
- Site readiness to include site survey (if required), dispatch and tracking
- CPE coordination for timely staging and configuration of devices
- Scheduling and confirming physical and out-of-band connectivity (Note out-of-band connectivity is required for every managed Wireless LAN Controller)
- Network / Site installation and acceptance
- Hand-off operational network to the Managed Services Operations center
- Static IP addresses are required for every Wireless LAN Controller and Wireless Access Point. Customers may be required to change the IP addresses of the managed devices in order to allow Verizon to assume management.

Managed Implementation Design Engineering Tasks

- Create Statement of Requirements
 - Network addressing
 - Routing protocol requirements
 - Redundancy/availability requirements
 - Scalability requirements
 - Remote access requirements
 - Implementation requirements
- Validate MSO compliancy
- Establish and confirm management connectivity (i.e., Management PVC for MSO visibility)

6.3.4.3 Converged Services, IP Telephony Business Line Services Attachment 3

- Review IP addressing scheme for MSO compliance. Customer may be required to alter the IP addressing of the managed wireless LAN devices so as to avoid overlapping with existing customer managed devices.
- Customer Design Document
 - Physical and logical topology
 - Detailed IP routing protocol design
 - Security
 - Hardware and software requirements
 - Quality of Service requirements (if needed)
 - Redundancy and backup, and remote access requirements
 - Remote access

MWLAN Certified CPE

For new implementations, all devices must be certified by Managed Network Solutions Operations (MNSO) for use with the service. The term "certified" means that:

- A device is fully qualified for use with the MWLAN service
- Standard pricing applies for this device
- This list will be updated on a regular basis

Note: Select Cisco and Aruba Networks equipment is certified for use with Verizon MWLAN. Hardware must not be identified as End of Life by the manufacturer. The customer may select self-sparing of access points in lieu of a maintenance agreement. Access point self-sparing option must be approved by MNSO.

Managed Take Over

This option applies when the customer wants Verizon Business to take an existing network or solution under management. Verizon Business will perform a design review exercise for customers with existing networks. This non-intrusive process is accomplished by:

- Customer interviews
- Customer-provided network diagrams
- Site-specific information

At the completion of the design review effort, Verizon Business will provide the customer with the feedback on what changes to the customer network are necessary, before it can be accepted for management. These changes may result in one-time charges to the customer that will be in addition to those listed in their service agreement. As part of the implementation process, the customer may elect to have Verizon Business affect these changes at additional onetime costs, do it themselves, or use a third party.

The Service Delivery process consists of all the activities required to bring the network under management. Verizon Business performs the overall

6.3.4.3 Converged Services, IP Telephony Business Line Services Attachment 3

project management function for efficient network activation. These activities will include Verizon Business to:

- Create a customer design document and overall project plan to bring the network under management
- Execute the necessary changes to bring the network under management
- Confirm site readiness
- Coordinate CPE for timely staging and configuration of devices (if required)
- Hand-off operational network to the Managed Services Operations center

Managed Take over Design Engineering Tasks

The planning and service delivery functions performed by the Managed Services Delivery organization associated with Managed Take Over.

- Identify network and CPE assets including network and router configurations
- Validate MSO compliancy
- Document physical and logical topology
- Network addressing and routing protocol design
- Security requirements
- Creates Statement of Requirement/Customer Design Document
- Review IP addressing scheme for MSO compliance
- Establish and confirm management connectivity (i.e., Management PVC for MSO visibility)

MWLAN - CPE Managed Take Over Guidelines

In order to bring an existing customer solution under management, Verizon Business will analyze the customer's current network and CPE assets against Verizon Business's baseline requirements. The following points highlight the key baseline criteria used to evaluate the CPE that will be brought under management as part of the Managed Take Over process.

- The customer network should be running standard WLAN feature sets.
- The wireless LAN equipment must be listed on the Managed Network Services Certified Device List.
- Verizon Business will confirm if the devices will continue to be supported by the manufacturer over the next two years.
- Wireless LAN Controllers must be operating a General Deployment (GD) version of the operating system.
- Verizon Business will confirm if the operating system of the wireless LAN has been upgraded in the past two years.
- Customer will allow Verizon Business to manage the maintenance contract for the customer-premised equipment.
- The wireless LAN equipment is currently configured, deployed, and operational within the customer's network.

Note: Hardware must not be identified as End of Life by the manufacturer.

Change Management

Change Management broadly defines the logical and physical activities performed by Verizon Business to ensure the Customer MWLAN solution keeps pace with their changing needs and requirements. Standard change management activities are included in the MWLAN monthly recurring charge. All other change management activities are custom and are quoted on an individual case basis.

The following table details the different change management activities and pricing:

Standard Change Management Activities	Charge
Wireless LAN Security - Modify	Included in MRC
Wireless LAN Authentication - Modify	Included in MRC
Wireless Access Point - Modify	Included in MRC
Protocol/Feature Modify	Included in MRC
DHCP Configuration - Modify	Included in MRC
IOS Emergency Upgrade	Included in MRC
IP Address/Subnet Mask Changes	Included in MRC
Switch VLAN Changes - Modify	Included in MRC
Switch Spanning Tree Configuration Modify	Included in MRC
Filters/Access-Lists - Modify	Included in MRC
Management Access List - Modify	Included in MRC

Optional Change Management provides additional change management support for items customers are not likely to encounter on a daily basis. Optional Change Management items are charged on a per-incident basis (NRC), and are available to customers that subscribe to 6.3.3.8 Converged Services, IP and Network IP Transport Services. These are enhanced features and a subset of the 6.3.3.8 Converged Services, IP and Network IP Transport Services.

Configuration Back Up

Verizon Business will back up the customer's Wireless LAN Controller configuration on a weekly basis. This allows quick recovery when a hardware replacement is made and provides accurate record keeping when performing configuration changes on the customer network. As part of the network acceptance process, all managed devices will have a copy of the most current

6.3.4.3 Converged Services, IP Telephony Business Line Services Attachment 3 configuration backed up on a weekly basis.

MWLAN – Custom Design Elements

The following custom activities may be required as part of Managed Implementation Design Engineering or Managed Take over Design Engineering:

- **Wireless Quality of Service** – Some Quality of Service features could be supported to make the WLAN Quality of Service “aware”. True QoS cannot be realized on the wireless side of the customer’s LAN environment.
- **Voice over Wireless LAN** – Verizon provides custom VoWLAN solutions for secure, reliable, scalable platform for all of voice, video, and data services.
- **Exterior Wireless Bridges/Access Points** – Verizon has custom solutions to meet customer needs for implementing and managing exterior wireless environments.
- **WLAN Physical Network Modifications** – Verizon will dispatch technician(s) to the premises to perform adds, moves and changes of Customer wireless network and equipment. This includes additional remote management and configuration services as required.

Customer Responsibilities

1. **Information and Access Requests.** Upon request, Customer will provide information to Verizon, its subcontractors or its designated point of contact (“Verizon or its Designees”) that is reasonably necessary or useful for Verizon to perform its obligations. In addition, upon request Customer will provide Verizon or its Designees with access to Customer facilities, installation sites, and equipment as reasonably necessary or useful for Verizon to perform its obligations hereunder.
2. **Licenses.** Customer will obtain any necessary permits, licenses, variances, and/or other authorizations required by state and local jurisdictions for installation and operation of the CPE on Customer’s premises or where the jurisdiction requires Customer to obtain the permit, license, variance and/or authorization.
3. **Building Space.** Where applicable, Customer will provide adequate building space, circuitry, facility wiring, temperature, humidity, and power to comply with the standards established by the manufacturer of the CPE for proper installation and operation of the Managed Service.
4. **IP Addresses.** Verizon reserves the right to use secondary IP addressing if Customer is using unregistered IP address space. If Customer will not allow secondary IP addressing, Customer agrees to pay reasonable costs for a dedicated management domain or an IP proxy hardware solution. Additionally, Verizon reserves the right to use border gateway protocol (“BGP”) routing for the management permanent virtual circuits (“PVCs”) used to access and monitor Customer’s Network.

6.3.4.3 Converged Services, IP Telephony Business Line Services Attachment 3

5. **Out of Band Access.** ("OOB") access is required for all Managed WLAN Full Management. Customer will provide at their cost either a Port Terminal Server or dedicated, analog telephone connection or indirect cable access for use by each OOB modem for troubleshooting. Managed WLAN OOB access is in addition to any Managed WAN OOB access.
6. **Supported Devices.** Only Verizon certified devices will be supported and must be an approved Verizon design as outlined in Customer's Statement of Requirements.

Reports. All copies of any reports, recommendations, documentation, Customer Portal printouts, or other materials in any media form provided to Customer by Verizon hereunder will be treated as Verizon Confidential Information.

Services Disclaimer. Verizon makes no warranties, guarantees, or representations, express, or implied, that (i) the services provided pursuant to this service will protect Customer's network from intrusions, viruses, trojan horses, worms, time bombs, cancelbots or other similar harmful or destructive programming routines; (ii) any security threats and vulnerabilities to Customer's network will be prevented or detected; or (iii) the performance by Verizon of any services will render Customer's systems invulnerable to security breaches.

6.3.4.3 Converged Services, IP Telephony Business Line Services Attachment 3

Feature Name	Feature Identifier	Feature Description	Feature Limits or Compatibility Restrictions
<p>MWLAN Controller Full (Small)</p>	<p>MGSM0000</p>	<p>MWLAN Controller Full (Small) (wireless controllers that control 1-25 access points) allows Verizon to be responsible to clear logical and physical issues with the network access LAN devices including patches, IOS releases, upgrades and other remediation plans. Controller must be certified by Verizon MNSO to be eligible for this service. Customer must have a manufacture certified maintenance agreement in place for this service. A modem line with either an Out of Band Modem or a Port Terminal Server is required from the customer. Verizon will work to clear the fault condition remotely or by dispatching someone to the site. This service requires Feature ID of either TWLN0000 or NDWC0000. Implementation of this service requires Wireless LAN Engineering Assessment.</p>	<p>Requires one of the following Feature Identifiers have been completed by Verizon for this device:</p> <p>TWLN0000 NDWC0000</p>

6.3.4.3 Converged Services, IP Telephony Business Line Services Attachment 3

Feature Name	Feature Identifier	Feature Description	Feature Limits or Compatibility Restrictions
<p>MWLAN Controller Full (Medium)</p>	<p>MWMD0000</p>	<p>MWLAN Controller Full (Medium) (wireless controllers that allow 26-50 access points) allows Verizon to be responsible to clear logical and physical issues with the network access LAN devices including patches, IOS releases, upgrades and other remediation plans. Controller must be certified by Verizon MNSO to be eligible for this service. Customer must have a manufacture certified maintenance agreement in place for this service. A Modem Line with either an Out of Band Modem or a Port Terminal Server is required from the customer. Verizon will work to clear the fault condition remotely or by dispatching someone to the site. This service requires Feature ID of either TWLN0000 or NDWC0000. Implementation of this service requires Wireless LAN Engineering Assessment.</p>	<p>Requires one of the following Feature Identifiers have been completed by Verizon for this device:</p> <p>TWLN0000 NDWC0000</p>

6.3.4.3 Converged Services, IP Telephony Business Line Services Attachment 3

Feature Name	Feature Identifier	Feature Description	Feature Limits or Compatibility Restrictions
<p>MWLAN Controller Full (Large)</p>	<p>MWLG0000</p>	<p>MWLAN Controller Full (Large) (wireless controllers that control 51 or more access points) allows Verizon to be responsible to clear logical and physical issues with the network access LAN devices including patches, IOS releases, upgrades and other remediation plans. Controller must be certified by Verizon MNSO to eligible for this service. Customer must have a manufacture certified maintenance agreement in place for this service. A Modem Line with either an Out of Band Modem or a Port Terminal Server is required from the customer. Verizon will work to clear the fault condition remotely or by dispatching someone to the site. This service requires Feature ID of either TWLN0000 or NDWC0000. Implementation of this service requires Wireless LAN Engineering Assessment.</p>	<p>Requires one of the following Feature Identifiers have been completed by Verizon for this device:</p> <p>TWLN0000 NDWC0000</p>

6.3.4.3 Converged Services, IP Telephony Business Line Services Attachment 3

Feature Name	Feature Identifier	Feature Description	Feature Limits or Compatibility Restrictions
<p>Take Over an Existing MWLAN Controller Device</p>	<p>TWLN0000</p>	<p>This applies to the Full Management of Wireless Controllers (Small, Medium and Large). With Managed Take-Over, Verizon reviews, optimizes and takes over management of a Customer's existing network. All network data must be provided by the Customer, including, but not limited to, Customer interviews, Customer-provided network diagrams, and site-specific information. Verizon will provide Managed Take-Over Service in accordance with a separate SOR that contains appropriate terms and conditions agreed upon by the parties. The SOR provides i) the inventory of the Customer's network; ii) identifies any physical / logical activities required to bring the network under management by Verizon, and iii) identifies any associated costs to Customer to upgrade the network necessary to bring the network under management.</p>	

6.3.4.3 Converged Services, IP Telephony Business Line Services Attachment 3

Feature Name	Feature Identifier	Feature Description	Feature Limits or Compatibility Restrictions
<p>New Device – MWLAN Controller Installation, Configuration and Implementation Support</p>	<p>NDWC0000</p>	<p>This applies to the Full Management of Wireless Controllers (Small, Medium and Large). Managed Implementation brings a new Customer Managed WAN network online after the Customer's requirements have been gathered and the design activities have been completed. Verizon provides support for the planning, system engineering and overall project management of a new network. Verizon will provide Managed Implementation Service in accordance with a SOR that contains appropriate terms and conditions agreed upon by the parties.</p>	

6.3.4.3 Converged Services, IP Telephony Business Line Services Attachment 3

Feature Name	Feature Identifier	Feature Description	Feature Limits or Compatibility Restrictions
<p>MWLAN Access Point Full</p>	<p>MAPW0000</p>	<p>MWLAN services Full allows Verizon to be responsible to clear logical and physical issues with the network access LAN devices including patches, IOS releases, upgrades and other remediation plans. Access Point(s) must be certified by Verizon MNSO to be eligible for this service. Verizon will work to clear the fault condition remotely or by dispatching someone to the site. This service requires Feature ID of either TWLP000 or NDWA0000. Implementation of this service requires Wireless LAN Engineering Assessment.</p>	<p>Requires one of the following Feature Identifiers have been completed by Verizon for this device:</p> <p>TWLP0000 NDWA0000</p>

6.3.4.3 Converged Services, IP Telephony Business Line Services Attachment 3

Feature Name	Feature Identifier	Feature Description	Feature Limits or Compatibility Restrictions
<p>Take Over an Existing MWLAN Access Point Device</p>	<p>TWLP0000</p>	<p>This applies to the Full Management of Wireless Access Point. With Managed Take-Over, Verizon reviews, optimizes and takes over management of a Customer's existing network. All network data must be provided by the Customer, including, but not limited to, Customer interviews, Customer-provided network diagrams, and site-specific information. Verizon will provide Managed Take-Over Service in accordance with a separate SOR that contains appropriate terms and conditions agreed upon by the parties. The SOR provides i) the inventory of the Customer's network; ii) identifies any physical / logical activities required to bring the network under management by Verizon, and iii) identifies any associated costs to Customer to upgrade the network necessary to bring the network under management.</p>	

6.3.4.3 Converged Services, IP Telephony Business Line Services Attachment 3

Feature Name	Feature Identifier	Feature Description	Feature Limits or Compatibility Restrictions
<p>New Device – MWLAN Access Point Installation, Configuration and Implementation Support</p>	<p>NDWA0000</p>	<p>This applies to the Full Management of Wireless Access Point. Managed Implementation brings a new Customer Managed WAN network online after the Customer's requirements have been gathered and the design activities have been completed. Verizon provides support for the planning, system engineering and overall project management of a new network. Verizon will provide Managed Implementation Service in accordance with a SOR that contains appropriate terms and conditions agreed upon by the parties.</p>	

6.3.4.3 Converged Services, IP Telephony Business Line Services Attachment 3

Feature Name	Feature Identifier	Feature Description	Feature Limits or Compatibility Restrictions
<p>Managed Power Over Ethernet Mid-Span Device MWLAN Full</p>	<p>MPWE0000</p>	<p>MWLAN services Full allows Verizon to be responsible to clear logical and physical issues with the network access LAN devices including patches, IOS releases, upgrades and other remediation plans. Controller must be certified by Verizon MNSO to be eligible for this service. Customer must have a manufacture certified maintenance agreement in place for this service. Verizon will work to clear the fault condition remotely or by dispatching someone to the site. This service requires Feature ID of either TWPO000 or NDWP0000. Implementation of this service requires Wireless LAN Engineering Assessment.</p>	<p>Requires one of the following Feature Identifiers have been completed by Verizon for this device:</p> <p>TWPO0000 NDWP0000</p>

6.3.4.3 Converged Services, IP Telephony Business Line Services Attachment 3

Feature Name	Feature Identifier	Feature Description	Feature Limits or Compatibility Restrictions
<p>Take Over an Existing MWLAN Power Over Ethernet Mid-Span Device</p>	<p>TWPO0000</p>	<p>This applies to the Full Management of Wireless Power Over Ethernet Mid-Span Device. With Managed Take-Over, Verizon reviews, optimizes and takes over management of a Customer's existing network. All network data must be provided by the Customer, including, but not limited to, Customer interviews, Customer-provided network diagrams, and site-specific information. Verizon will provide Managed Take-Over Service in accordance with a separate SOR that contains appropriate terms and conditions agreed upon by the parties. The SOR provides i) the inventory of the Customer's network; ii) identifies any physical / logical activities required to bring the network under management by Verizon, and iii) identifies any associated costs to Customer to upgrade the network necessary to bring the network under management.</p>	

6.3.4.3 Converged Services, IP Telephony Business Line Services Attachment 3

Feature Name	Feature Identifier	Feature Description	Feature Limits or Compatibility Restrictions
<p>New Device – MWLAN Power Over Ethernet Mid-Span Device Installation, Configuration and Implementation Support</p>	<p>NDWP0000</p>	<p>This applies to the Full Management of Wireless Power Over Ethernet Mid-Span Device. Managed Implementation brings a new Customer Managed WAN network online after the Customer's requirements have been gathered and the design activities have been completed. Verizon provides support for the planning, system engineering and overall project management of a new network. Verizon will provide Managed Implementation Service in accordance with a SOR that contains appropriate terms and conditions agreed upon by the parties.</p>	

6.3.4.3 Converged Services, IP Telephony Business Line Services Attachment 3

Feature Name	Feature Identifier	Feature Description	Feature Limits or Compatibility Restrictions
<p>Managed Authentication Appliance MWLAN Full</p>	<p>MAPF0000</p>	<p>MWLAN Services Full allows Verizon to be responsible to clear logical and physical issues with the network access LAN devices including patches, IOS releases, upgrades and other remediation plans. Controller must be certified by Verizon MNSO to be eligible for this service. Customer must have a manufacture certified maintenance agreement in place for this service. Verizon will work to clear the fault condition remotely or by dispatching someone to the site. This service requires Feature ID of either TWAA000 or NDWS0000. Implementation of this service requires Wireless LAN Engineering Assessment.</p>	<p>Requires one of the following Feature Identifiers have been completed by Verizon for this device:</p> <p>TWAA0000 NDWS0000</p>

6.3.4.3 Converged Services, IP Telephony Business Line Services Attachment 3

Feature Name	Feature Identifier	Feature Description	Feature Limits or Compatibility Restrictions
<p>Take Over an Existing MWLAN Authentication Appliance</p>	<p>TWAA0000</p>	<p>This applies to the Full Management of Wireless Authentication Appliance. With Managed Take-Over, Verizon reviews, optimizes and takes over management of a Customer's existing network. All network data must be provided by the Customer, including, but not limited to, Customer interviews, Customer-provided network diagrams, and site-specific information. Verizon will provide Managed Take-Over Service in accordance with a separate SOR that contains appropriate terms and conditions agreed upon by the parties. The SOR provides i) the inventory of the Customer's network; ii) identifies any physical / logical activities required to bring the network under management by Verizon, and iii) identifies any associated costs to Customer to upgrade the network necessary to bring the network under management.</p>	

6.3.4.3 Converged Services, IP Telephony Business Line Services Attachment 3

Feature Name	Feature Identifier	Feature Description	Feature Limits or Compatibility Restrictions
<p>New Device – MWLAN Authentication Appliance Installation, Configuration and Implementation Support</p>	<p>NDWS0000</p>	<p>This applies to the Full Management of Wireless Authentication Appliance. Managed Implementation brings a new Customer MWLAN network online after the Customer's requirements have been gathered and the design activities have been completed. Verizon provides support for the planning, system engineering and overall project management of a new network. Verizon will provide Managed Implementation Service in accordance with a SOR that contains appropriate terms and conditions agreed upon by the parties.</p>	
<p>Device OS Change</p>	<p>MWLN1101</p>	<p>This service applies to operating system changes to wireless controllers.</p>	<p>Device must be currently under Verizon management.</p>

6.3.4.3 Converged Services, IP Telephony Business Line Services Attachment 3

Feature Name	Feature Identifier	Feature Description	Feature Limits or Compatibility Restrictions
MWLAN Intra-building Move (Wireless Device - labor only)	MWLN1201	Dispatch of a technician to the premises to perform In-building move of existing wireless device – using same circuit and no design impact. Done during normal business hours. This includes additional remote management and configuration services. Available for Full Management Only.	Device must be currently under Verizon management.
MWLAN Move, Inter-building or Across Town (Wireless Device - labor only)	MWLN1202	Dispatch of a technician to the premises to perform across town is within 30 miles of original circuit, same wireless device but new circuit, done during normal business hours. This includes additional remote management and configuration services. Available for Full Management Only.	Device must be currently under Verizon management.
MWLAN Exchange (Wireless Device - labor only)	MWLN1203	MWLAN Exchange dispatches a technician to the premises to perform Substitute one wireless device for another at an existing site. This includes additional remote management and configuration services. Available for Full Management Only.	

6.3.4.3 Converged Services, IP Telephony Business Line Services Attachment 3

Feature Name	Feature Identifier	Feature Description	Feature Limits or Compatibility Restrictions
MWLAN Field Service Technicians (labor only) Normal business hours (M-F, 8 a.m. to 5 p.m.)	MWLN1204	Management Field Service Technicians hourly rate during Normal business hours (M-F, 8 a.m. to 5 p.m.). Dispatches a technician to perform on-site managed services on a time basis at the level of journeyman.	
MWLAN Field Service Technicians (labor only) After hours (M-F, 5 p.m. to 8 a.m., including weekends and holidays)	MWLN1205	Management Field Service Technicians hourly rate After hours (M-F, 5 p.m. to 8 am, including weekends and holidays) dispatches a technician to perform on-site managed services on a time basis at the level of journeyman.	

6.3.4.3 Converged Services, IP Telephony Business Line Services Attachment 3

Feature Name	Feature Identifier	Feature Description	Feature Limits or Compatibility Restrictions
MWLAN Managed Take Over:			
MWLAN Managed Take Over	MWLN1301	<p>The planning and service delivery functions performed by the Managed Services Delivery organization associated with Managed Take Over.</p> <ul style="list-style-type: none"> • Identify network and CPE assets including network and router configurations • Validate MSO compliancy • Document physical and logical topology • Network addressing and routing protocol design • Security requirements • Creates Statement of Requirement/Customer Design Document • Review IP addressing scheme for MSO compliance • Establish and confirm management connectivity (i.e., Management PVC for MSO visibility) 	

6.3.4.3 Converged Services, IP Telephony Business Line Services Attachment 3

Feature Name	Feature Identifier	Feature Description	Feature Limits or Compatibility Restrictions
MWLAN Managed Implementation:			
MWLAN Managed Implementation	MWLN1401	<p>The Design process considers the customer's business requirements and technology needs in order to create a solution to meet current and future business needs. This includes:</p> <ul style="list-style-type: none"> • The collection of system, application and end-user requirements • The creation of a detailed logical and physical design plan for transport and equipment • Implementation of the overall project plan <p>The Implementation process consists of the activities required to deliver the network solution and to bring the network under management. Verizon Business performs the overall project management function for timely and efficient network activation. This includes:</p> <ul style="list-style-type: none"> • Order validation and acceptance for Managed Wireless LAN Service (and Managed WAN or Managed Services Complete, if required) • Site readiness 	

6.3.4.3 Converged Services, IP Telephony Business Line Services Attachment 3

Feature Name	Feature Identifier	Feature Description	Feature Limits or Compatibility Restrictions
		<p>to include site survey (if required), dispatch and tracking</p> <ul style="list-style-type: none"> • CPE <p>coordination for timely staging and configuration of devices</p> <ul style="list-style-type: none"> • Scheduling and confirming physical and out-of-band connectivity (Note out-of-band connectivity is required for every managed Wireless LAN Controller) • Network / Site installation and acceptance • Hand-off operational network to the Managed Services Operations center • Static IP addresses are required for every Wireless LAN Controller and Wireless Access Point. Customers may be required to change the IP addresses of the managed devices in order to allow Verizon to assume management. 	

6.3.4.3 Converged Services, IP Telephony Business Line Services Attachment 3

Applicable Service Level Agreements:

- Service Availability Percentage
- Service Availability Percentage – Managed Router and Managed LAN Service
- Catastrophic Outage 1
- Catastrophic Outage 2
- Catastrophic Outage 3
- One-Way Transmission Delay
- Jitter
- Packet Loss
- Excessive Outage
- Notification
- Proactive Notification SLA – Managed Router and Managed LAN Service/WLAN Service
- Provisioning
- Time to Repair (TTR) – Managed Wireless LAN (WLAN) Service
- Response Duration from Receipt of Order
- Administrative Service Level Agreements

6.3.4.3 Converged Services, IP Telephony Business Line Services Attachment 4

Service Identifier: Converged Services, IP Telephony Business Line Service - Hosted IP Centrex (HIPC)

The pricing includes the following elements: planning, applicable design, engineering, testing, and applicable service level agreements.

Feature Name	Feature Identifier	Unit of Measure	Unit Non - Recurring	Unit Recurring	Change Charges
Converged Services, IP Telephony Business Line Service	CSBL0000	Per Subscriber	\$0.00	\$9.86	\$0.00
Off-Net Toll	CSOF0000	Per Minute	\$0.00	\$0.00	\$0.00
Off-Net Toll Free	CSOF0000	Per Minute	\$0.00	\$0.0247	\$0.00
Additional Line Appearances	IAAP0000	Per Appearance	\$0.00	\$3.38	\$0.00
Account Codes	IACD0000	Per Group	\$0.00	\$6.80	\$0.00
Attendant Console	IACN0000	Per Configured User	\$0.00	\$12.75	\$0.00
Authorization Codes	IATC0000	Per Group	\$0.00	\$6.80	\$0.00
Block of DID Numbers	IDID0000	Per Block of 20	\$0.00	\$5.31	\$0.00
Virtual FX	IVFX0000	Per FX Line	\$0.00	\$4.05	\$0.00
Auto Attendant	IAPI0000	Per Instance	\$0.00	\$18.70	\$0.00
Remote Office	IROF0000	Per Configured User	\$0.00	\$7.20	\$0.00

6.3.4.3 Converged Services, IP Telephony Business Line Services Attachment 4

IP Network Transport Management (Switch):

Feature Name	Feature Identifier	Unit of Measure	Unit Non - Recurring	Unit Recurring	Change Charges
Management (Switch / Hub) - Managed LAN Monitor & Notify (Small)	MLMN0001	Per Month	N/A	\$23.40	N/A
Management (Switch /Hub) - Managed LAN Monitor & Notify (Medium)	MLMN0002	Per Month	N/A	\$23.40	N/A
Management (Switch /Hub) - Managed LAN Monitor & Notify (Large)	MLMN0003	Per Month	N/A	\$23.40	N/A
Management (Switch /Hub) - Managed LAN Physical (Small)	MLPH0001	Per Month	N/A	\$31.50	N/A
Management (Switch /Hub) - Managed LAN Physical (Medium)	MLPH0002	Per Month	N/A	\$41.40	N/A
Management (Switch /Hub) - Managed LAN Physical (Large)	MLPH0003	Per Month	N/A	\$73.80	N/A
Management (Switch /Hub) - Managed LAN Full (Small)	MLFL0001	Per Month	N/A	\$39.60	N/A
Management (Switch /Hub) - Managed LAN Full (Medium)	MLFL0002	Per Month	N/A	\$51.30	N/A
Management (Switch /Hub) - Managed LAN Full (Large)	MLFL0003	Per Month	N/A	\$93.60	N/A
Takeover of Existing Device - Management Takeover of Switch	MTOI0001	Per Month	\$350	N/A	N/A
New Device - Switch Installation requiring initial configuration and implementation support	MIIO0002	Per Month	\$350	N/A	N/A
Management (Switch /Hub) - Threshold Reporting	THRE0000	Per Device Per Month	N/A	\$5.40	N/A

6.3.4.3 Converged Services, IP Telephony Business Line Services Attachment 4

Feature Name	Feature Identifier	Unit of Measure	Unit Non - Recurring	Unit Recurring	Change Charges
Management (Switch /Hub) - Order Expedite	OEXP0000	Per Order	\$935.00	N/A	N/A
Management (Switch /Hub) - New Implementation Rescheduling	RSCH0000	Per Site	\$300	N/A	N/A
Management (Switch /Hub) - After-Hours Premium Charge (M-F, 5 p.m. to 8 a.m., including weekends and holidays)	PREM0000	Per Occurrence	\$600	N/A	N/A

6.3.4.3 Converged Services, IP Telephony Business Line Services Attachment 4

Optional Change Management provides additional change management support for items customers are not likely to encounter on a daily basis. Optional Change Management items are charged on a per-incident basis (NRC), and are available to customers that subscribe to 6.3.4.3 Converged Services, IP Telephony Business Line Services. These are enhanced features and a subset of the 6.3.4.3 Converged Services, IP Telephony Business Line Services.

Optional Change Management Activities:

Feature Name	Feature Identifier	Unit of Measure	Unit Non - Recurring	Unit Recurring	Change Charges
Management (Switch /Hub) - LAN Dynamic Host Configuration Protocol (DHCP) IP Helper Add / Modify / Delete	LDFM0000	Per Occurrence	N/A	N/A	\$42.50
Management (Switch /Hub) - IP Address / Subnet Mask – Add / Modify / Delete	IAFM0000	Per Occurrence	N/A	N/A	\$42.50
Management (Switch /Hub) - Hostname change	HCFM0000	Per Occurrence	N/A	N/A	\$42.50
Management (Switch /Hub) - VLAN – Add / Delete	VLFM0000	Per Occurrence	N/A	N/A	\$42.50
Management (Switch /Hub) - Trunking Configuration – Add / Delete	TCFM0000	Per Occurrence	N/A	N/A	\$42.50
Management (Switch /Hub) - Spanning Tree – Add / Delete	STFM0000	Per Occurrence	N/A	N/A	\$42.50
Management (Switch /Hub) - Storm Control – Add / Delete	SCFM0000	Per Occurrence	N/A	N/A	\$42.50

6.3.4.3 Converged Services, IP Telephony Business Line Services Attachment 4

Feature Name	Feature Identifier	Unit of Measure	Unit Non - Recurring	Unit Recurring	Change Charges
Management (Switch /Hub) - Ether Channel - Add / Delete	ECFM0000	Per Occurrence	N/A	N/A	\$42.50
Management (Switch /Hub) - UniDirectional Link Detection (UDLD) Configuration - Add / Delete	UCFM0000	Per Occurrence	N/A	N/A	\$42.50
Management (Switch /Hub) - Multicast Configuration - Add / Delete	MCFM0000	Per Occurrence	N/A	N/A	\$42.50
Management (Switch /Hub) - VLAN Trunk Protocol (VTP) Configuration - Add / Modify / Delete	VTPC0000	Per Occurrence	N/A	N/A	\$42.50
<p>In lieu of the optional change management per occurrence services described above, customers have the option to utilize the established hourly rate. Labor charges will commence upon arrival at customer site. Only the highest single NRC will be charged per device. Feature ID's are MEMU0000, DOFM0000, IBSM0001, HRDU0001, LNIB0000, LERS0001, DDON0000, LAFT0000.</p>					
Management (Switch - labor only) - Memory Upgrade	MEMU0000	Per Occurrence	\$350	\$0.00	\$0.00
Management (Switch - labor only) Switch IOS Change Support New Features	DOFM0000	Per Occurrence	\$350	\$0.00	\$0.00
Management (Switch - labor only) Intra-building Move	IBSM0001	Per Occurrence	\$350	\$0.00	\$0.00
Management (Switch - labor only) Hardware Module Upgrade	HRDU0001	Per Occurrence	\$350	\$0.00	\$0.00

6.3.4.3 Converged Services, IP Telephony Business Line Services Attachment 4

Feature Name	Feature Identifier	Unit of Measure	Unit Non - Recurring	Unit Recurring	Change Charges
Management (Switch - labor only) Switch Move, Inter-building or Across Town	LNIB0000	Per Occurrence	\$600	\$0.00	\$0.00
Management (Switch - labor only) Switch Exchange	LERS0001	Per Occurrence	\$350	\$0.00	\$0.00
Management (Switch) Field Service Technicians (labor only) - Normal business hours (M-F, 8 a.m. to 5 p.m.).	DDON0000	Per Hour	\$135	\$0.00	\$0.00
Management (Switch) Field Service Technicians (labor only) – After hours (M-F, 5 p.m. to 8 a.m., including weekends and holidays).	LAFT0000	Per Hour	\$170	\$0.00	\$0.00

6.3.4.3 Converged Services, IP Telephony Business Line Services Attachment 4

Managed Wireless LAN (MWLAN)

Feature Name	Feature Identifier	Unit of Measure	Unit Non – Recurring	Unit Recurring	Change Charges
MWLAN Controller Full (Small)	MGSM0000	Per Device	N/A	\$120.00	NA
MWLAN Controller Full (Medium)	MWMD0000	Per Device	N/A	\$200.00	NA
MWLAN Controller Full (Large)	MWLG0000	Per Device	N/A	\$335.00	NA
Take Over an Existing MWLAN Controller Device	TWLN0000	Per Device	\$550.00	N/A	NA
New Device – MWLAN Controller Installation, Configuration and Implementation Support	NDWC0000	Per Device	\$550.00	N/A	NA
MWLAN Access Point Full	MAPW0000	Per Device	N/A	\$25.00	NA
Take Over an Existing MWLAN Access Point Device	TWLP0000	Per Device	\$150.00	N/A	NA
New Device – MWLAN Access Point Installation, Configuration and Implementation Support	NDWA0000	Per Device	\$150.00	N/A	NA
Managed Power Over Ethernet Mid-Span Device MWLAN Full	MPWE0000	Per Device	N/A	\$30.00	NA
Take Over an Existing MWLAN Power Over Ethernet Mid-Span Device	TWPO0000	Per Device	\$150.00	N/A	NA

6.3.4.3 Converged Services, IP Telephony Business Line Services Attachment 4

Feature Name	Feature Identifier	Unit of Measure	Unit Non – Recurring	Unit Recurring	Change Charges
New Device – MWLAN Power Over Ethernet Mid-Span Device Installation, Configuration and Implementation Support	NDWP0000	Per Device	\$150.00	N/A	NA
Managed Authentication Appliance MWLAN Full	MAPF0000	Per Device	N/A	\$80.00	NA
Take Over an Existing MWLAN Authentication Appliance	TWAA0000	Per Device	\$200.00	N/A	NA
New Device – MWLAN Authentication Appliance Installation, Configuration and Implementation Support	NDWS0000	Per Device	\$200.00	N/A	NA
Device OS Change	MWLN1101	Per Occurrence	\$30.00	N/A	NA
MWLAN Intra-building Move (Wireless Device - labor only)	MWLN1201	Per Occurrence	\$350.00	N/A	NA
MWLAN Move, Inter-building or Across Town (Wireless Device - labor only)	MWLN1202	Per Occurrence	\$600.00	N/A	NA
MWLAN Exchange (Wireless Device - labor only)	MWLN1203	Per Occurrence	\$350.00	N/A	NA

6.3.4.3 Converged Services, IP Telephony Business Line Services Attachment 4

Feature Name	Feature Identifier	Unit of Measure	Unit Non – Recurring	Unit Recurring	Change Charges
MWLAN Field Service Technicians (labor only) Normal business hours (M-F, 8 a.m. to 5 p.m.)	MWLN1204	Per Hour	\$135.00	N/A	NA
MWLAN Field Service Technicians (labor only) After hours (M-F, 5 p.m. to 8 a.m., including weekends and holidays)	MWLN1205	Per Hour	\$170.00	N/A	NA
MWLAN Managed Take Over					
MWLAN Managed Take Over	MWLN1301	ICB	ICB	N/A	NA
MWLAN Managed Implementation					
MWLAN Managed Implementation	MWLN1401	ICB	ICB	N/A	NA

6.3.4.3 Converged Services, IP Telephony Business Line Services Attachment 4

Note:

Taxes and Surcharges

The following taxes and/or surcharges may apply. See CALNET II Exhibit 5A - Tax Determination Matrix, Module 3 specific detail.

CA Sales Tax
CA City Utility Users Tax
CA 9-1-1 Surcharge
CA Universal Lifeline Surcharge
CA Relay Service and Communications Device Fund Surcharge
Teleconnect Fund Surcharge
CA PUC Fee
AD Valorem Surcharge
California High Cost Fund
Federal Universal Service Fee/Charge
Regulatory Charge
Administrative Charge

6.3.6.1 Converged Services, Managed IP Video Conferencing Services
Attachment 3

Service Identifier: IP Network Based Managed IP Video Conference Service

Description of the Service: IP Network Based Managed IP Video Conference service provides multiple simultaneous connections and the necessary protocol conversions for connecting dissimilar open standards based equipment. Video conferencing solutions provided are open Standards based as set by the ITU and IETF. Verizon's video conferencing services are available throughout the U.S.

Availability: Statewide. Domestic locations are available on an ICB basis.

Unless noted separately in Attachment 4, services include the following elements: planning, applicable design, engineering, testing, training and applicable service level agreements.

Feature Name	Feature Identifier	Feature Description	Feature Limits or Compatibility Restrictions
IP Video - Standard Session Support	ISSS0000	Verizon provides Standard Session Support by having a Conferencing Attendant greet each caller; assist participants in connecting, perform a roll call of all participants and notify the conference leader when all participants are present. At the completion of the roll call, the Conferencing Specialist will disconnect from the call. If technical assistance is needed during the conference, the Customer can contact a Conferencing Attendant for	

6.3.6.1 Converged Services, Managed IP Video Conferencing Services
Attachment 3

Feature Name	Feature Identifier	Feature Description	Feature Limits or Compatibility Restrictions
		assistance. Standard Session Support with a connection at 384k.	
IP Video - Enhanced Session Support	IESS0000	Verizon provides Enhanced Session Support by having a Conferencing Attendant greet each caller, assist participants in connecting, perform a roll call of all participants, and notify the conference leader when all participants are present. At the completion of the roll call, the Conferencing Attendant shall remain online and provide technical assistance until the end of the conference.	
IP Video - Session Support Cancellation Fee	ISCF0000	Cancellation less than 1 hour prior to scheduled conference is the Session Support Cancellation Fee.	
IP Video - Network MCU Services (Port)	IMCU0000	Verizon provides MCU services that allow for a single session IP based video and audio conferencing in a multipoint	

6.3.6.1 Converged Services, Managed IP Video Conferencing Services
Attachment 3

Feature Name	Feature Identifier	Feature Description	Feature Limits or Compatibility Restrictions
		arrangement. This is accomplished through a centralized system of provider based equipment and software. The Network MCU Service is up to 384k connection.	
-Enhanced Network MCU Services (Port-512KB)	IMCU0512	Enhanced Network MCU Services (512kbps) allow for a single session IP based video and audio conferencing in a multipoint arrangement. This is accomplished through a centralized system of provider based equipment and software at 512kbps. The Enhanced Network MCU Service is from 512k to 768k connection.	
IP Video - MCU Cascading Services (Port)	ICAS0000	MCU Cascading Services allows for distributed videoconferencing arrangements utilizing a combination of customer owned and network based MCUs. The MCU Cascading Service is up to 384k connection.	

6.3.6.1 Converged Services, Managed IP Video Conferencing Services
Attachment 3

Feature Name	Feature Identifier	Feature Description	Feature Limits or Compatibility Restrictions
IP Video - Enhanced MCU Cascading Services (512KB Port)	ICAS0512	Enhanced MCU Cascading Services (512kbps) allows for distributed videoconferencing arrangements utilizing a combination of customer owned and network based MCUs at 512kbps. The MCU Cascading Service is from 512k up to 768k connections.	
IP Video - Gateway Services	IGYS0000	Gateway Services allows for the interconnection of IP based videoconference sessions with ISDN based videoconferencing sessions connecting via the PSTN. This is accomplished through use of a specific number to call where parties can join. The MCU Cascading Service is up to 384k connection.	
IP Video - Enhanced Gateway Services (512KB)	IGYS0512	Enhanced Gateway Services allows for the interconnection of IP based videoconference sessions with ISDN based	

6.3.6.1 Converged Services, Managed IP Video Conferencing Services
Attachment 3

Feature Name	Feature Identifier	Feature Description	Feature Limits or Compatibility Restrictions
		videoconferencing sessions connecting via the PSTN. This is accomplished through use of a specific number to call where parties can join. The MCU Cascading Service is from 512k up to 768k connections.	
IP Video - Transcoding Services	ITRN0000	Transcoding Service enables a participant to take part in a conference even though they communicate via unlike compression methods or dissimilar codec speeds. Converts the Customer's codec algorithm or speed to match with the other participants in the videoconference.	
IP Video - Conferencing Scheduling Services	ICSS0000	Conference Scheduling Services is a network wide scheduling of video/audio conferencing sessions shall be available through any combination of web-based, e-mail or phone initiated methods.	

6.3.6.1 Converged Services, Managed IP Video Conferencing Services
Attachment 3

Feature Name	Feature Identifier	Feature Description	Feature Limits or Compatibility Restrictions
IP Video - Enhanced Session Power	ISPP0000	Verizon supports Enhanced Session PowerPoint Pushes. Verizon supports H.239 standard for document sharing, or the customer can use Verizon's Net Conferencing solution in conjunction with the video. The H.239 feature enables both video and graphical data to be transmitted over a single network connection and displayed in the video conference simultaneously using a single monitor, using the H.239 industry standard protocol.	
IP Video - Enhanced Session Content Manipulation	ISCM0000	Verizon supports Enhanced Session Content Manipulation. Verizon supports H.239 standard for document sharing, or the customer can use Verizon's Net Conferencing solution in conjunction with the video. The H.239 feature enables both video and graphical data to be transmitted over a	

6.3.6.1 Converged Services, Managed IP Video Conferencing Services
Attachment 3

Feature Name	Feature Identifier	Feature Description	Feature Limits or Compatibility Restrictions
		single network connection and displayed in the video conference simultaneously using a single monitor, using the H.239 industry standard protocol.	
IP Video - Enhanced Session Q&A Moderation	ISQA0000	Enhanced Session Q & A Moderation is supported in Verizon's Premier Level service. When using Verizon's Premier Level service, Verizon's video coordinators will moderate a formal Q & A.	
IP Video - Connection speed of 1.5Mbps	ICSP0015	Verizon supports connection speed of 1.5 Mbps on the conferencing video bridges.	

6.3.6.1 Converged Services, Managed IP Video Conferencing Services
Attachment 3

Additional options available to Verizon IP Video end-users, not required for above IP Video Services:

Feature Name	Feature Identifier	Feature Description	Feature Limits or Compatibility Restrictions
Domestic IP Video Conferencing Service up to 768KB	IPVC0768	Verizon provides Domestic IP Video Conferencing Service by having a Conferencing Attendant greet each caller; assist participants in connecting, perform a roll call of all participants and notify the conference leader when all participants are present. At the completion of the roll call, the Conferencing Specialist will disconnect from the call. If technical assistance is needed during the conference, the Customer can contact a Conferencing Attendant for assistance.	

6.3.6.1 Converged Services, Managed IP Video Conferencing Services
Attachment 3

Feature Name	Feature Identifier	Feature Description	Feature Limits or Compatibility Restrictions
Domestic IP Video Conferencing Service up to T1	IPVC1544	Verizon provides Standard Session Support by having a Conferencing Attendant greet each caller; assist participants in connecting, perform a roll call of all participants and notify the conference leader when all participants are present. At the completion of the roll call, the Conferencing Specialist will disconnect from the call. If technical assistance is needed during the conference, the Customer can contact a Conferencing Attendant for assistance.	
Domestic IP Video Conferencing Service over 512k - Additional Per Call Per Minute Charge Premier Level	VCPC0000	Verizon provides Domestic IP Video Conferencing Service on an additional per call per minute charge for premier level video conferencing basis.	

6.3.6.1 Converged Services, Managed IP Video Conferencing Services
Attachment 3

Feature Name	Feature Identifier	Feature Description	Feature Limits or Compatibility Restrictions
-Translations Services	VCTS0000	Verizon offers many options for video conferencing, including translation services in multiple languages. Verizon uses a third party for translation and interpretation service.	
-Instant Video	VCIV0000	Instant Videoconferencing is a subscription-based service that provides the flexibility to conduct an unattended, reservationless videoconference for up to six participants, in any combination of video and audio participants, at any time. The subscriber is provided a unique dial-in number, host and participant passcodes, which can be used over and over again. Instant Videoconferencing enables participants to connect at speeds up to 384Kbps via ISDN or IP.	

6.3.6.1 Converged Services, Managed IP Video Conferencing Services
Attachment 3

Feature Name	Feature Identifier	Feature Description	Feature Limits or Compatibility Restrictions
-IP Access Dial-Out Charge	ADOC0000	A Verizon operator can dial-out to participant Video systems to start a call, upon request.	
-IP Video Endpoint Start Up Charge	See Below	When establishing new IP Video Service with Verizon, a Start-up Charge may apply.	
IP Video Endpoint Start Up Charge per IP Video Endpoint	IPSU0001	Per Endpoint	
IP Video Endpoint Start Up Charge per-customer	IPSU0002	Per User	
-IP Encryption Feature Charge (up to 384KB)	IPER0384	When requesting encryption the optional IP Video service, up to 384k, a Feature Charge may apply	
IP Encryption Instant (up to 384K)	IPEI0384		
-Flat Rate IP Video	IPFV0000	Flat Rate IP Video allows users to purchase unlimited IP Video Conferencing Services for one flat rate charge.	

6.3.6.1 Converged Services, Managed IP Video Conferencing Services
Attachment 3

Feature Name	Feature Identifier	Feature Description	Feature Limits or Compatibility Restrictions
IP Video Recording - File Download	IPVR0001	This service provides recording services from the Verizon Business MCU bridge during Video Conference sessions. Video Recording provided via self-service file download of the recorded session. Download media will be ".asf" files, which are playable in Windows Media Player. The session is stored for 30 days for download on this service.	
IP Video Recording - CD/DVD Copy	IPVR0002	This service provides recording services from the VzB MCU bridge during Video Conference sessions. Video Recording provided via Hard Media CD/DVD Copy. Hard media will be ".asf" files, which are playable in Windows Media Player. The session is stored for 30 days to order CD/DVD.	

6.3.6.1 Converged Services, Managed IP Video Conferencing Services
Attachment 3

Applicable Service Level Agreements:

- Service Availability Percentage
- Excessive Outage
- Notification
- Provisioning
- Response Duration from Receipt of Order

Video Conferencing Management Services:

Video Conferencing Management Services offers a comprehensive approach to creating and executing a Video Conferencing strategy that can improve the way you use existing technologies, the way your people communicate, and the way you manage technology costs.

Customer provides all Video Conferencing hardware, (servers, gateways, end-points and all required components), hardware maintenance contracts, software licensing, and software support contracts. Management is remote management only.

All devices must be certified by Verizon for use with the Video Conferencing Management service. The term "certified" means that a device is fully qualified for use with the Video Conferencing Management service and that standard pricing applies for this device

Video Conferencing Management

Verizon Business Video Conferencing Management Services provides customers a comprehensive set of support services to meet their expectations for a high quality, simple to use, collaboration experience.

Customer provided Video Conferencing environment consists of hardware, hardware maintenance contracts, software licensing, and software support contracts. . Customer is responsible for acquiring hardware and licenses, keeping the licenses current, maintaining the appropriate licensing quantities for the devices under management, and managing hardware and software support contracts.

Customers must maintain an agreement for Verizon provided Private IP (PIP) service that supports the required bandwidth to support Video Conferencing Management Services. Specific configurations will need to be used to ensure quality of service; such configurations will be worked through during the implementation process.

Video Conferencing Management Service requires the VNOC have login access to the customer's immersive video devices via a dedicated connection at the customer end point. This connection must be continuously available and encrypted. Reporting requires login access to customer bridging devices, if applicable. Incident management and change management requires login access to the endpoints and premise based bridges, if applicable. Video Conferencing system must be certified by Verizon Managed Services.

6.3.6.1 Converged Services, Managed IP Video Conferencing Services
Attachment 3

Support for Video Conferencing and Immersive Video Conferencing (High Definition Video Conferencing such as Telemedicine) includes the following:

Single Support Organization - Video Network Operations Center (VNOC) provides a single contact organization for all immersive support services.

Multi-Language Support - Multi-language support is available.

Scheduling via Phone - Customers may establish a reservation by contacting the VNOC operator. Operator will need to know the time of call and endpoint locations. The operator may need to check the availability of the end-point with a customer scheduling system. If not, the operator will be able to confirm the reservation while on the phone, and then send an email confirmation to the leader. If there is a conflict, the operator will offer alternative times.

Scheduling via Web Portal - Customers may establish a reservation using the web portal.

Customer will need to complete a request with the time of call and endpoint locations. After the request is submitted, the leader will receive an email confirming the meeting. If there is a conflict, the organizer will receive a phone call with other meeting options.

Ad Hoc Calls (not scheduled) - Ad hoc calls enable the user to initiate a call without a reservation. However, the endpoint must be in the company directory or the user must obtain the E.164 address (room phone number).

One Button Call Launching - The end-user can launch the call by either touching the highlighted listed reservation displayed on the LED screen of the room console or simply hitting the dial button (configured by customer). The actual key may be different for a particular customer but the experience is the same. The end-user touches a single button to launch the call. System must support this feature.

One Button Call Support - The VNOC is available for questions/problems during a call, touch a designated 'livedesk' soft button on the LED screen (configured by customer) AND contacting the VNOC before or after a call.

Incident Support - VNOC provides in-call phone support and troubleshooting assistance. VNOC is accessed via the one-button push for help on the console.

Incident Management - Provides proactive monitoring, fault isolation and troubleshooting of customer's immersive video solution. Potential failures are identified and calls are either uninterrupted or quickly restored resulting in minimal downtime.

6.3.6.1 Converged Services, Managed IP Video Conferencing Services Attachment 3

Problem Management - Verizon's Problem Management team will proactively capture global system performance and error data, perform root cause and trend analysis, document recommended remediation and resolution procedures, work with the Incident Management team to implement preventive procedures and monitor problem resolutions to prevent recurring errors.

Call Level Reporting - Verizon can provide Call Level Reporting based on call detail records (CDR) delivered from all system endpoints. System must support this CDR feature. Reports for each room can include: 1.) Usage Overview – total hours of use for reporting period; total # of calls for reporting period; total hours of use for reporting period and 2.) Usage Statistics – total monthly scheduled conferences; total multi-point calls by month; total point to point calls per month; total conferences per day by room type.

Diagnostics - The support desk will isolate problems and if the problem is determined to be an equipment failure, will inform the customer so that they may take further action (e.g. contact equipment vendor for maintenance support).

6.3.6.1 Converged Services, Managed IP Video Conferencing Services
Attachment 3

Video Conferencing

Feature Name	Feature Identifier	Feature Description	Feature Limits or Compatibility Restrictions
Video Conferencing Endpoints: Desktop/Rooms			
Video Conferencing Codec	TLCN1901	Remote IP Application Management of video conferencing codec	Requires the following Feature Identifier be completed by Verizon in advance of Move Under Management: TLCN1801
Immersive Video Conferencing Endpoints: Room			
Immersive Video Conferencing room, small tier, 1 screen	TLCN2001	Remote IP Application Management of immersive video conferencing codec, small tier, 1 screen	Requires the following Feature Identifier be completed by Verizon in advance of Move Under Management: TLCN1802
Immersive Video Conferencing room, large tier, 3 screens	TLCN2002	Remote IP Application Management of immersive video conferencing codecs, large tier, 3 screens	Requires the following Feature Identifier be completed by Verizon in advance of Move Under Management: TLCN1802

Video Conferencing Transition Services

Transition services provide one-time engagements for a managed take-over of a customer's existing Video Conferencing environment, or the design, customer build and move under management of a new Video Conferencing environment. Once these infrastructures are moved under management, the Video Conferencing Managed Services are available for ongoing remote support. Moves, changes, and deletes, and additions to existing environments are also considered as transition services. Additionally, Verizon offers one-time optional projects for assessing Video Conferencing environments for Risks and Stability, providing a Capacity Planning report, or other Custom Solution Development.

Transition Services - Design Phase Video Conferencing Environment

Transition Services for the Design Phase of a new Video Conferencing environment deployment are the first step of a three-step process of design, build and move under management for deploying a new environment.

Customer Build Phase

The Build Phase of a new Video Conferencing environment deployment are the second step of a three-step process of design, customer build, and move under management for deploying a new environment. Customer Build Phase is not a service provided by Verizon. The customer is responsible for all equipment procurement, physical construction, equipment build activities and ensuring that the environment has been built to meet equipment manufacturer and Verizon design specifications. Customer is also responsible for delivery of as-built drawings detailing any design modifications, and a finalized bill of materials. Verizon will participate in final test activities to ensure the environment is ready for Verizon management, but the customer is responsible for resolving all issues and deficiencies identified during testing.

Transition Services – Move Under Management Phase

Transition Services for the Move Under Management Phase of a new environment deployment is the third step of a three-step process of design, build and move under management for deploying a new environment. For an existing environment, this is the second step in the documentation, move under management process.

Transition Services - Documentation of Managed Take-Over of an Existing Video Conferencing Environment:

Transition Services for a Managed Take-Over of an existing environment consist of a Documentation phase and a Move under Management phase.

Development of as-built documentation is a required part of a managed take-over of an existing Video Conferencing environment. This step must be completed before the move under management phase can begin. The document

6.3.6.1 Converged Services, Managed IP Video Conferencing Services Attachment 3

is similar to the output from the build phase for new infrastructures.

Transition Services – MCD Activities

The service provides on-going changes to the customer's environment per customer requests. (Incremental Video Conferencing Application Device adds are handled separately as a build and move under management.) Moves of devices or applications that are outside of the building they are originally housed may require Custom Solution Development.

Transition Services: Optional Managed Projects

Risk and Stability Assessment for a Video Conferencing Environment:

Transition Services for Risk and Stability Assessment for a Video Conferencing environment are stand-alone projects for assessing an existing Customer environment without regard to who built it or how it was built.

Capacity Planning for a Video Conferencing Environment:

Transition Services for Capacity Planning for a Video Conferencing environment are stand-alone projects for assessing an environment without regard to who built it or how it was built.

Custom Solution Development:

Develops a Custom Solution from high level requirements for the purpose of generating budgeting information, high level solution requirements, high level design, high level pricing, and a high level proposal for (i) implementation and (ii) management of new Customer environments. This service assists Customers with turning ideas into actionable solutions, with a tables and diagrams of the required Environment components along with pricing information. This service can be leveraged for budgeting and planning new application and environment deployments.

Video Conferencing - Transition Services

Feature Name	Feature Identifier	Feature Description	Feature Limits or Compatibility Restrictions
<p>Design Phase Video Conferencing Environment</p>	<p>TLCN1101</p>	<p>Transition Services for the Design Phase of a new infrastructure deployment are the first step of a three-step process of design, build and move under management for deploying a new environment.</p> <p>This transition service includes:</p> <ol style="list-style-type: none"> 1) Document Business and Technical Requirements 2) Infrastructure Architecture Diagram(s) 3) Logical and Physical Network Designs 4) Summary of Risks and Mitigations for the Design 5) High Level Bill of Materials (make, model, version and basic specifications for each server, infrastructure software, network device, etc) 	

6.3.6.1 Converged Services, Managed IP Video Conferencing Services
Attachment 3

Feature Name	Feature Identifier	Feature Description	Feature Limits or Compatibility Restrictions
		<p>6) List of requirements for Management Services</p> <p>7) Limits to scope of incremental moves, adds, changes, and deletes: The design document shall state what constitutes an incremental change or addition to an existing environment, and the limits to the extension of an existing structure, for example maximum number of endpoints, users, and throughput, above and beyond which a new, separate one-time Design, Build, and Move under Management will be required.</p>	

6.3.6.1 Converged Services, Managed IP Video Conferencing Services
Attachment 3

Feature Name	Feature Identifier	Feature Description	Feature Limits or Compatibility Restrictions
Move under Management	TLCN1801	<p>Transition Services for the Move Under Management Phase of a new infrastructure deployment is the third step of a three-step process of design, build and move under management for deploying a new environment. For an existing environment, this is the second step in the documentation, move under management process. This transition service includes:</p> <ol style="list-style-type: none"> 1. Installation and functional testing of Verizon tools 2. Creation of Request for Monitoring (RFM) forms 3. Implementation and testing of monitoring templates 4. Testing of Infrastructure failover mechanisms 5. Testing of backup / restore capability 	<p>This is a required service for each codec either built new or existing for which Verizon will provide on-going management. This is a fixed fee charge per instance.</p> <p>Requires the following Feature Identifier be completed by Verizon in advance of Move Under Management:</p> <p>TLCN1103 or the customer complete the Customer Build Phase including resolution of all issues and discrepancy identified during testing with Verizon.</p>

6.3.6.1 Converged Services, Managed IP Video Conferencing Services
Attachment 3

Feature Name	Feature Identifier	Feature Description	Feature Limits or Compatibility Restrictions
		<p>(where applicable)</p> <ol style="list-style-type: none"> 6. Establish contact, notification and escalation procedures 7. Baseline Critical Application Functionality and Performance for the Managed Services phase 8. Create the Operations Run-book for Verizon Operations 9. Knowledge Transfer to Verizon Operations 10. Operations launch readiness checklist 11. Hand over the environment to Verizon Operations 	

6.3.6.1 Converged Services, Managed IP Video Conferencing Services
Attachment 3

Feature Name	Feature Identifier	Feature Description	Feature Limits or Compatibility Restrictions
<p>Move under Management – Immersive Video Conferencing</p>	<p>TLCN1802</p>	<p>Transition Services for the Move Under Management Phase of a new infrastructure deployment is the third step of a three-step process of design, build and move under management for deploying a new environment. For an existing environment, this is the second step in the documentation, move under management process. This transition service includes:</p> <ol style="list-style-type: none"> 1. Installation and functional testing of Verizon tools 2. Creation of Request for Monitoring (RFM) forms 3. Implementation and testing of monitoring templates 4. Testing of Infrastructure failover mechanisms 5. Testing of backup / restore capability 	<p>This is a required service for each immersive video system either built new or existing for which Verizon will provide on-going management. This is a fixed fee charge per instance.</p> <p>Requires the following Feature Identifier be completed by Verizon in advance of Move Under Management:</p> <p>TLCN1103 or the customer complete the Customer Build Phase including resolution of all issues and discrepancy identified during testing with Verizon.</p>

6.3.6.1 Converged Services, Managed IP Video Conferencing Services
Attachment 3

Feature Name	Feature Identifier	Feature Description	Feature Limits or Compatibility Restrictions
		<p>(where applicable)</p> <ol style="list-style-type: none"> 6. Establish contact, notification and escalation procedures 7. Baseline Critical Application Functionality and Performance for the Managed Services phase 8. Create the Operations Run-book for Verizon Operations 9. Knowledge Transfer to Verizon Operations 10. Operations launch readiness checklist 11. Hand over the environment to Verizon Operations 	

6.3.6.1 Converged Services, Managed IP Video Conferencing Services
Attachment 3

Feature Name	Feature Identifier	Feature Description	Feature Limits or Compatibility Restrictions
<p>Documentation of Managed Take-Over of an Existing Video Conferencing Environment</p>	<p>TLCN1103</p>	<p>Development of as-built documentation is a required part of a managed take-over of an existing video conferencing infrastructure. This step must be completed before the move under management phase can begin. The outputs from the assessment include:</p> <ol style="list-style-type: none"> 1) Development of as-built documentation 2) Document Business and Technical Requirements 3) Infrastructure Architecture Diagram(s) 4) Logical and Physical Network Designs 5) Summary of Risks and Mitigations 6) List of requirements for Management Services 7) Limits to scope of incremental moves, adds, changes, and deletes: The assessment 	

6.3.6.1 Converged Services, Managed IP Video Conferencing Services
Attachment 3

Feature Name	Feature Identifier	Feature Description	Feature Limits or Compatibility Restrictions
		<p>document shall state what constitutes an incremental change or addition to an existing environment, and the limits to the extension of an existing structure, for example maximum number of codecs, users, and throughput, above and beyond which a new, separate one-time Design, Build, and Move under Management will be required.</p>	

6.3.6.1 Converged Services, Managed IP Video Conferencing Services
Attachment 3

Feature Name	Feature Identifier	Feature Description	Feature Limits or Compatibility Restrictions
MCD Activities for Video Conferencing Environment	TLCN1104	The service provides on-going moves, changes and deletes to the customer's environment per customer requests. These activities are defined and limited as provided in the Design or Managed Take-Over assessment. Moves of codecs or devices that are outside of the building they are originally housed may require Custom Solution Development.	Requires that the effected codec or device be currently under Verizon management.

6.3.6.1 Converged Services, Managed IP Video Conferencing Services
Attachment 3

Feature Name	Feature Identifier	Feature Description	Feature Limits or Compatibility Restrictions
Risk & Stability Assessment of Video Conferencing Environment	TLCN1105	Transition Services for Risk and Stability Assessment for a Video Conferencing environment is a stand-alone project for assessing an existing Customer environment without regard to who built it or how it was built. This infrastructure-oriented project service includes: <ol style="list-style-type: none"> 1) Document Business and Technical Requirements 2) Basic Systems and Environment Discovery 3) Infrastructure Architecture Diagram 4) Logical Network Diagram 5) Prioritized list of Infrastructure Management Security, Performance and Stability Risks with Recommendations for Mitigation 	

6.3.6.1 Converged Services, Managed IP Video Conferencing Services
Attachment 3

Feature Name	Feature Identifier	Feature Description	Feature Limits or Compatibility Restrictions
Capacity Planning of Video Conferencing Environment	TLCN1106	<p>Transition Services for Capacity Planning for a Server</p> <p>Infrastructure is a stand-alone project for assessing an environment without regard to who built it or how it was built. This infrastructure-oriented project service includes:</p> <ol style="list-style-type: none"> 1) Document Business and Technical Requirements 2) Infrastructure Architecture Diagram 3) Document historical performance and utilization data on the existing Infrastructure 4) Document historical business performance data 5) Document future business projections 6) Analyze the historical data to establish correlations between the technical and 	

6.3.6.1 Converged Services, Managed IP Video Conferencing Services
Attachment 3

Feature Name	Feature Identifier	Feature Description	Feature Limits or Compatibility Restrictions
		<p>business information</p> <p>7) Model future business projections against the correlated data</p> <p>8) Summary of Analysis and Recommendations (including rationale for recommendations)</p> <p>Note: Verizon assumes that some historical technical data is available, or can be easily derived about the Infrastructure.</p>	

6.3.6.1 Converged Services, Managed IP Video Conferencing Services
Attachment 3

Feature Name	Feature Identifier	Feature Description	Feature Limits or Compatibility Restrictions
<p>Custom Solution Development for Video Conferencing Environment</p>	<p>TLCN1107</p>	<p>Develops a Custom Solution from high level requirements for the purpose of generating budgeting information, high level solution requirements, high level design, high level pricing, and a high level proposal for (i) implementation and (ii) management of new Customer Infrastructure environments. This service assists Customers with turning ideas into actionable solutions, with a tables and diagrams of the required Infrastructure components along with pricing information. This service can be leveraged for budgeting and planning new application and infrastructure deployments. This service includes:</p> <ol style="list-style-type: none"> 1) Gathering high level business and technical requirements 2) Evaluating 	

6.3.6.1 Converged Services, Managed IP Video Conferencing Services
Attachment 3

Feature Name	Feature Identifier	Feature Description	Feature Limits or Compatibility Restrictions
		<p>technology stack for Verizon tools or custom tool development requirements</p> <p>3) Evaluating technology stack for applicable Service Level Agreements</p> <p>4) Evaluating customer requirements for various aspects of Service Delivery</p> <p>5) Creating diagram and element table(s) of the Customer System (Customer System is defined as the hardware and software owned, licensed or leased by the customer, or under the control of the customer for which Verizon has agreed to provide IT Services as set forth in the details included with a Purchase Order)</p>	

6.3.6.1 Converged Services, Managed IP Video Conferencing Services
Attachment 3

Feature Name	Feature Identifier	Feature Description	Feature Limits or Compatibility Restrictions
		<p>6) Creating proposal documentation for Project Services and Managed Services The Deliverable/Proposal will include:</p> <ul style="list-style-type: none"> a) Service Descriptions for the Design, Build and Implementation Project Services b) Service Descriptions for the Managed Services, c) Summary of Service Pricing Information and Terms d) Diagrams and element tables of the Customer System e) (optional scope) Bill of Materials list for required Hardware, Software and OEM Support Services f) (optional scope) Budgetary Pricing Information for 	

6.3.6.1 Converged Services, Managed IP Video Conferencing Services
Attachment 3

Feature Name	Feature Identifier	Feature Description	Feature Limits or Compatibility Restrictions
		required Hardware, Software and OEM Support Services g) (optional scope) Summary of required Hosting Services h) (optional scope) Pricing Information for required Management Services.	

6.3.6.1 Converged Services, Managed IP Video Conferencing Services Attachment 4

Service Identifier: IP Network Based Managed IP Video Conference Service

The pricing includes the following elements: planning, applicable design, engineering, testing, training and applicable service level agreements.

Feature Name	Feature Identifier	Unit of Measure	Unit Non – Recurring	Unit Recurring	Change Charges
IP Video - Standard Session Support	ISSS0000	Per Minute	\$0.00	\$0.6120	\$0.00
IP Video - Enhanced Session Support	IESS0000	Per Minute	\$0.00	\$0.6120	\$0.00
IP Video - Session Support Cancellation fee	ISCF0000	Per Session	\$0.00	\$0.00	\$0.00
IP Video - Network MCU Services (Port)	IMCU0000	Per Minute	\$0.00	\$0.6120	\$0.00
Enhanced Network MCU Services (Port) (512kbps)	IMCU0512	Per Minute	\$0.00	\$0.9350	\$0.00
IP Video - MCU Cascading Services (Port)	ICAS0000	Per Minute	\$0.00	\$0.6120	\$0.00
IP Video - Enhanced MCU Cascading Service (Port) (512kbps)	ICAS0512	Per Minute	\$0.00	\$0.9350	\$0.00
IP Video - Gateway Services	IGYS0000	Per Minute	\$0.00	\$0.6120	\$0.00
IP Video - Enhanced Gateway Services (512kbps)	IGYS0512	Per Minute	\$0.00	\$0.9350	\$0.00
IP Video - Transcoding Services per session	ITRN0000	Per Session	\$0.00	\$0.6375	\$0.00

Revised: MSA 3 Amendment No. 13 - 6.3.6.1 Converged Services, Managed IP Video Conferencing Services

6.3.6.1 Converged Services, Managed IP Video Conferencing Services Attachment 4

Feature Name	Feature Identifier	Unit of Measure	Unit Non – Recurring	Unit Recurring	Change Charges
IP Video - Conference Scheduling Services	ICSS0000	Per Room/Per Month	\$100.00	\$0.00	\$0.00
IP Video - Enhanced Session Powerpoint Pushes	ISPP0000	Per Minute	\$0.00	\$0.00	\$0.00
IP Video - Enhanced Session Content Manipulation	ISCM0000	Per Minute	\$0.00	\$0.00	\$0.00
IP Video - Enhanced Session Q&A Moderation	ISQA0000	Per Minute	\$0.00	\$0.00	\$0.00
IP Video - Connection speed of 1.5Mbps	ICSP0015	Per Minute	\$0.00	\$1.3600	\$0.00

6.3.6.1 Converged Services, Managed IP Video Conferencing Services Attachment 4

Additional options available to Verizon IP Video end-users:

Feature Name	Feature Identifier	Unit of Measure	Unit Non – Recurring	Unit Recurring	Change Charges
Domestic IP Video Conferencing Service up to 768KB	IPVC0768	Per Minute	\$0.00	\$1.1220	\$0.00
Domestic IP Video Conferencing Service up to T1	IPVC1544	Per Minute	\$0.00	\$1.6830	\$0.00
Domestic IP Video Conferencing Service - Additional per call per minute charge for Premier Level Video Conferencing	VCPC0000	Per Minute	\$0.00	\$1.2750	\$0.00
Translation Services	VCTS0000	Per Minute	\$0.00	\$1.2070	\$0.00
Instant Video	VCIV0000	Per Minute	\$0.00	\$0.6800	\$0.00
IP Access Dial-Out Charge	ADOC0000	Per Endpoint	\$0.00	\$21.25	\$0.00
IP Video Endpoint Start Up Charge	See Below		See Below	See Below	See Below
IP Video Endpoint Start Up Charge per IP Video Endpoint	IPSU0001	Per Endpoint	\$0.00	\$0.00	\$0.00
Or	Or	Or	Or	Or	Or
IP Video Endpoint Start Up Charge per-customer	IPSU0002	Per User	\$0.00	\$0.00	\$0.00
IP Encryption Reserved (up to 384K)	IPER0384	Per Minute/Per Endpoint	\$0.00	\$0.0425	\$0.00
IP Encryption Instant (up to 384K)	IPEI0384	Per Minute/Per Endpoint	\$0.00	\$0.0425	\$0.00
Flat Rate IP Video	IPFV0000	Per User	ICB	ICB	ICB

Revised: MSA 3 Amendment No. 13 - 6.3.6.1 Converged Services, Managed IP Video Conferencing Services

6.3.6.1 Converged Services, Managed IP Video Conferencing Services Attachment 4

Feature Name	Feature Identifier	Unit of Measure	Unit Non – Recurring	Unit Recurring	Change Charges
IP Video Recording - File Download	IPVR0001	Per Occurrence	\$85.00	N/A	N/A
IP Video Recording - CD/DVD Copy	IPVR0002	Per Occurrence	\$144.50	N/A	N/A

6.3.6.1 Converged Services, Managed IP Video Conferencing Services Attachment 4

Video Conferencing Management Services

Feature Name	Feature Identifier	Unit of Measure	Unit Non – Recurring	Unit Recurring	Change Charges
Video Conferencing Endpoints: Desktop/Rooms					
Video Conferencing Codec	TLCN1901	Per codec	N/A	\$1,375.00	See TLCN1104
Immersive Video Conferencing Endpoints: Room					
Immersive Video Conferencing room, small tier, 1 screen	TLCN2001	Per 1-screen room	N/A	\$1,875.00	See TLCN1104
Immersive Video Conferencing room, large tier, 3 screens	TLCN2002	Per 3-screen room	N/A	\$5,625.00	See TLCN1104

6.3.6.1 Converged Services, Managed IP Video Conferencing Services Attachment 4

Video Conferencing Transition Services

Feature Name	Feature Identifier	Unit of Measure	Unit Non – Recurring	Unit Recurring	Change Charges
Design Phase Video Conferencing Environment	TLCN1101	Per codec	\$8,478.00	N/A	N/A
Move under Management	TLCN1801	Per codec	\$3,000.00	N/A	N/A
Move under Management – Immersive Video Conferencing	TLCN1802	Per Immersive Video System	\$3,000.00	N/A	N/A
Documentation of Managed Take-Over of an Existing Video Conferencing Environment	TLCN1103	Per codec	\$5,299.00	N/A	N/A
MCD Activities for Video Conferencing Environment	TLCN1104	Per codec	\$1,696.00	N/A	N/A
Risk & Stability Assessment of Video Conferencing Environment	TLCN1105	Per codec	\$5,299.00	N/A	N/A
Capacity Planning of Video Conferencing Environment	TLCN1106	Per codec	\$5,299.00	N/A	N/A
Custom Solution Development for Video Conferencing Environment	TLCN1107	Per codec	\$15,896.00	N/A	N/A

6.3.6.1 Converged Services, Managed IP Video Conferencing Services Attachment 4

Taxes and Surcharges

The following taxes and/or surcharges may apply. See CALNET II Exhibit 5A - Tax Determination Matrix, Module 3 specific detail.

CA Sales Tax
CA City Utility Users Tax
CA 9-1-1 Surcharge
CA Universal Lifeline Surcharge
CA Relay Service and Communications Device Fund Surcharge
Teleconnect Fund Surcharge
CA PUC Fee
AD Valorem Surcharge
California High Cost Fund
Federal Universal Service Fee/Charge
Regulatory Charge
Administrative Charge

- Restoration measures, time and date of restoration.
- Provide an Executive Summary root cause analysis report at STND’s request. Information for this report shall include the following:
 - High-level event summary
 - Impact to the State customers
 - Timeline of events
 - Discussion/outage issues
 - Mitigation plan/path forward

6.3.14 SERVICE LEVEL AGREEMENTS (SLA) (M)

6.3.14.1 Service Level Agreement Overview (M)

The intent of this section is to provide the Contract Customers, OTech/STND and the Contractor with Requirements that define and assist in the management of the Service Level Agreements (SLA). This section identifies and explains the required SLAs for the IP services identified in this RFP Module. The SLAs shall be categorized as Network, or Administrative in nature. The intent of this section is to define performance objectives and measurement processes.

In the event a Bidder proposes a service that has been designated as Desirable, the Bidder must meet or exceed the associated SLAs as described in this Section.

The Bidder must identify their associated SLAs for unsolicited services.

The SLAs in the network category shall each consist of the following components: services, definition, measurement process, objective(s), immediate rights and remedies, and monthly rights and remedies. All applicable services are listed in each SLA.

Network Service Level Agreement Format

<u>Services</u>	<u>SLA Name</u>
[List of all applicable services]	<p>Definition [Definition or description of the SLA]</p> <p>Measurement Process [Instructions on how to measure network performance in order to determine compliance]</p>

	<p>Objective (s) [Defines the performance goal/parameters for each SLA. The objective(s) may be different than the technical Requirements found in Sections 6.3.2-6.3.6.2 et. al..]</p> <p>Immediate Rights and Remedies [Allows immediate action by OTech/STND and the Customer (e.g., OTech/STND Escalation), and/or rebates which are applied to their monthly invoices on a per occurrence basis (e.g., TTR).]</p> <p>Monthly Rights and Remedies [Applicable to SLAS that require accumulation of statistics over a period of time or multiple trouble tickets (e.g., availability). Note: the Off Ramp process is included in this component]</p>
--	---

The SLAs in the Administrative category shall each consist of the following components: tools, reports and applications, objective(s), measurement process, OTech/STND rights and remedies, and Customer rights and remedies.

Administrative Service Level Agreement Format

<u>Administrative Tools, Reports and Applications</u>	<u>SLA Name</u>
<p>[List of all applicable tools, reports and application]</p>	<p>Definition [Define or describe the SLA]</p> <p>Measurement Process [Instruct how to measure or derive the objectives]</p> <p>Objective (s) [Define Contractor program performance objectives]</p> <p>OTech/STND Rights and Remedies [Identifies actions to be taken by OTech/STND or rebates from Contractor when the objectives are not met]</p> <p>Customer Rights and Remedies [Identifies actions to be taken by the Customers or rebates from Contractor when the objectives are not met]</p>

Bidder understands the Requirement and shall meet or exceed it? Yes No

Reference: document _____

location _____ page _____ paragraph _____

Description:

Verizon understands and will comply with this requirement as specified. Verizon recognizes that this section will provide the Contract (CALNET II) Customers, OTech/STND and Verizon with requirements that define and will assist in the management of the Service Level Agreements (SLAs), and this section identifies and explains the required SLAs for the IP services identified in this RFP Module. Verizon understands that the SLAs shall be categorized as Network or Administrative in nature. The intent of this section is to define performance objectives and measurement processes. Verizon understands that in the event that a propose service, that has been designated as Desirable, or Unsolicited service submitted in this response, Verizon will be required to meet or exceed the associated SLAs as described in this Section.

Verizon agrees to Network Service Level Agreement Format proposed by OTech/STND, consisting of the following components: services, definition, measurement process, objective(s), immediate rights and remedies, and monthly rights and remedies.

6.3.14.1.1 Technical Requirements versus SLA (M)

This section shall distinguish between technical Requirements and the SLA objectives. Sections 6.3.2 to 6.3.6.2 identify the technical Requirements for each service. These Requirements are the minimum parameters each Bidder must meet in order for their Bid to qualify for award. Upon award the committed technical Requirements will be maintained throughout the remainder of the Contract.

Committed SLA objectives are minimum Requirements, which the Contractor shall be held accountable for all rights and remedies accordingly.

Bidder understands the Requirement and shall meet or exceed it? Yes No

Reference: document _____

location _____ page _____ paragraph _____

Description:

Verizon understands and will comply with this requirement as specified. Verizon is in agreement that Sections 6.3.2 to 6.3.6.2 identify the technical requirements for each service and

that these requirements are the minimum parameters Verizon must meet, in order to qualify for an award.

Verizon agrees that upon award, it commits to the technical requirements for the term of the CALNET II Contract.

6.3.14.1.2 Two Methods Of Outage Reporting: Customer Or Contractor (M)

There are two methods in which outages may be identified and outage durations derived: Customer reported or Contractor reported.

The first method results from a Customer reporting service trouble to the Contractor's Customer Service Center. Customer reported trouble tickets track service failures or quality of service issues.

In the second method of outage reporting, the Contractor shall open a ticket as a result of network alarms or identification of a service failure in the backbone (i.e., Cat 2 or 3). In each instance a trouble ticket shall be assigned and monitored until service is restored.

Bidder understands the Requirement and shall meet or exceed it? Yes No

Reference: document _____

location _____ page _____ paragraph _____

Description:

Verizon understands and will comply with this requirement as specified.

Verizon recognizes that there are two methods in which outages may be identified and outage durations derived, these are Customer reported or Verizon reported.

The first method results from a Customer reporting service trouble to the Verizon's Customer Service Center. Customer reported trouble tickets track service failures or quality of service issues.

In the second method of outage reporting, Verizon opens a ticket as a result of network alarms or identification of a service failure in the backbone (i.e., Cat 2 or 3). In each instance a trouble ticket shall be assigned and monitored until service is restored.

The first method is a result of a CALNET II Customer reporting service trouble by contacting Verizon's Customer Service Center or via the CALNET II Customer Web Portal.

The second method of outage reporting is when Verizon identifies service failures in the backbone (i.e. CAT 2 or 3) or as a result of network alarms.

In either case, Verizon will assign a trouble ticket to the failure and monitor the outage until restoration of service is completed.

Verizon's first and most important task will be to correctly notify the proper personnel so that corrective remediation can be started in an expeditious manner. Notification of outages should be flexible and concise. Contact by e-mail, fax, page, Web portal and telephone may be used to provide up-to-date trouble resolution information. Likewise, the creation of the trouble tickets should start the remedial process with prioritization, regular updates, and escalation as required.

Verizon will proactively monitor network components in the proposed CALNET II network. Verizon can also provide STND (and agencies, if required) the capability to review network monitoring activities. This capability has the extensive functionality described below and can be offered to STND and its customers in a read-only mode.

Verizon also offers an optional proactive monitoring service which would monitor designated CPE (end site routers and LAN-based components), firewalls, servers, and applications. The proactive querying of such devices can vary and would be based on the critical nature of the components. Monitoring will be IP-based using certified MIBs and SNMP standard interfaces.

Proactive monitoring, whether implemented for network components or for customer equipment and/or applications, can provide significant benefits, especially by facilitating timely restoration when faults actually occur.

Proactive monitoring can be implemented to measure various network performance activities. Thresholds can be set throughout the network and even at a customer's remote sites to enable reporting on different service level measurements. Verizon is proud of its automated and integrated proactive monitoring systems and requests that STND carefully review the functional capabilities it proposes in this response.

MNS System Architecture (IMPACT)

Verizon will utilize its Integrated Management Platform for Advanced Communications Technologies (IMPACT) system, which is a real-time, state-of-the-art monitoring and control system. The system is composed of a modular software and hardware design to accommodate expansion of network operations and monitoring. Information is processed and stored using object technology, XML data modeling and incorporates industry standards such as ITUT M.3100. The system notifies operations personnel, in real time, of transport, switching, data, IP, and hosted services problems occurring in Verizon's network.

IMPACT provides increased supervision of the network through a highly flexible, distributed design with survivable system implementation, which incorporates the best-of-breed, off-the-shelf technologies integrated within a sophisticated "manager of managers" architecture.

IMPACT utilizes a state-of-the-art communications bus architecture for distributed system component communications and an IP-based internal telemetry network for access to network equipment. This telemetry network utilizes ATM routed networking to maintain high availability and reliability of network management connectivity.

IMPACT provides a competitive advantage in the telecommunications marketplace by offering a high performance distributed monitoring system capable of rapid detection and location of network faults and outages. IMPACT helps to lower operational costs through automated integration with network construction and provisioning systems to help to ensure new and existing network equipment and services are managed efficiently.

IMPACT Functions

- Network fault and performance data collection
- Fault correlation, filtering and reduction
- Alarm presentation
- Performance monitoring
- Command/Control
- Trouble ticket integration
- Field technician information integration
- On-line help facilities
- Flexible/survivable system configuration
- Current and historical data reporting
- Color, graphic operator stations

Operator Interface

The IMPACT GUI is based on the latest industry technology utilizing JAVA for platform independence and XML for information exchange between client and server. The GUI enables access to the network management platform from any desktop station capable of supporting a JAVA Virtual Machine.

The mouse-driven user interface provides the ability to monitor network events, ranging from network-wide to station-specific – from one workstation. Work flow support is provided to enable operations personnel to relate multiple network-reported faults to consolidated events. These events can relate to maintenance activities, new installs, or actual network outages. The work flow support enables consolidated trouble ticketing and subsequent tracking of these events from time of occurrence through repair and verification. Automation features enable repetitive network conditions to be handled by the system, thereby freeing network operators to focus on more complex tasks.

Color is used to convey the status of events in the network along with graphical depictions of network topology. For example, critical conditions or service-affecting alarms are shown in red, minor alarm conditions in yellow and normal conditions in blue. Narrative alarm text messages are also available for viewing.

Primary Protocols Supported

- TL-1
- SNMP
- CMIP/CMISE(Q3)
- Vendor Proprietary

Network Technologies Supported

- Fiber Systems - OC-192, OC-148, OC-12, OC-3 (e.g. Nortel, Fujitsu, Pirelli, Lucent, Ciena)
- Digital Cross Connects (e.g., Alcatel, Tellabs, DSC, Marconi)
- Voice Switches, Signaling Elements, Intelligent Network Devices (e.g., Nortel, DSC, Ericsson, Lucent)
- Data and IP Routers (e.g., Cisco, Lucent, Nortel, Newbridge)
- Mid-Range Servers (e.g., SUN, HP, IBM)

Integrated Network Management Technologies

- HP's Openview (TeMIP)
- System Management ARTS Service Assurance Manager
- Micromuse NetCool
- SystemEdge (probes)
- Open's NerveCenter
- Orillion's O' Vista
- QLink (business process automation)
- ILOG Rules (fault reduction and correlation)

Integrated Testing System (ITS)

Verizon's proposed Integrated Testing System (ITS) provides an intelligent, integrated circuit and element testing architecture. ITS will provide the State with an integrated software solution to be used by customer care and operations centers to install circuits and provide fault isolation for customer-reported problems. ITS provides sophisticated interfaces to network elements (DXCs, Switches, Test Heads, DSL equipment, etc.) and Verizon back end systems. ITS also provides automation for flow through provisioning by automatically performing tests on newly installed circuits.

ITS primarily supports the following types of testing:

- DS1 testing
- Fault isolation features such as Alarms, Performance data, access to switches for feature data
- Automated testing of non HyperLink circuits
- HDSL (High Digital Subscriber Line)
- XDSL (Digital Subscriber Line) testing
- DS0, FT1 and VF testing across the networks
- Frame Relay Integration
- Smart Circuits (CSU/DSU) – This reaches into the customer site to retrieve Frame Relay statistics from the customer's perspective
- Enhances trouble ticketing interface
- Automatic testing of DS0 circuits upon trouble ticket creation
- Performs periodic testing (routine) of switched network DS0 circuits, IMTs (Intermachine trunks), FGs (feature groups), and direct circuits to customer facilities. The reports are available to the field switch sites and to the Switch Performance Automated Trunk Routine Group (ATR). ATR provides the capability to sample test 100 percent of the circuits in the network within a twenty one-day period

IMPACT Architecture

IMPACT is an integrated management platform that will support the services provided by Verizon. IMPACT interfaces with various Element Management and Network Management Systems to provide a unified view of network problems to the user community. Additionally, IMPACT makes available many features that allow users to be more productive in their daily tasks, such as workflow, ticketing, topology information, task automation, command interaction capabilities, as well as interfaces to several internal systems for maintenance activities, outage notifications, and contact information. The IMPACT architecture consists of three functional tiers and is illustrated below.

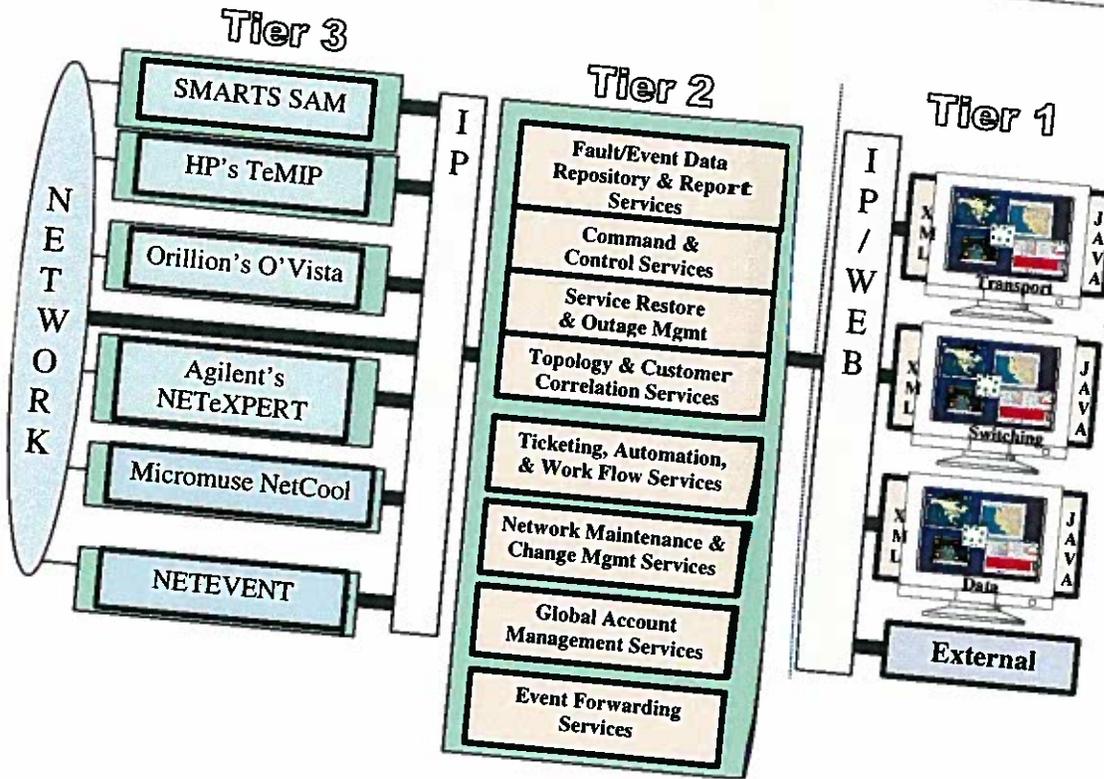


Figure 6.3.14.1.2-1. IMPACT Architecture

Tier 1

Tier 1 of the IMPACT architecture provides the user interface and consists of 100 percent JAVA GUIs that are used to interact with the alarms, tickets, and workflow events that exist within the system. Tier 1 also has the ability to call Web links directly to both Tier 3 systems and other business processes, which can provide access to detailed information and business functions when needed.

Tier 2

Tier 2 is the heart of the architecture and functions as a “manager of managers” that incorporates business logic supporting network management activities. It enables the integration of network reported fault indications from the Tier 3 systems and provides value-added common business process features, thus enabling efficient service restoration and equipment repair tracking. This tier of the architecture provides the following services:

- **Fault/Event Data Repository and Reporting Services**
 - Stores the alarms and events and all associated data
 - Provides user reporting capabilities
- **Command and Control Services**
 - Provides the ability to interact with managed elements in the network
- **Service Restoration and Outage Management**
 - Provides automatic service restoration for some network types
 - Provides an interface into the outage tracking and notification systems
- **Topology and Customer Correlation Services**
 - Provides an interface to several external databases for accurate and timely topology and customer correlation to events being generated in the network
- **Ticketing, Automation, and Work Flow Services**
 - Provides an interface to the standard trouble ticketing system
 - Provides workflow services to events created within the system, such as status tracking and clear correlation
 - Provides automation capabilities, thus resulting in more efficient operation centers
- **Network Maintenance and Change Management Services**
 - Provides an interface to track network equipment maintenance to shield the operations centers from alarms that are generated from known maintenance activities
- **Event Forwarding Services**
 - Provides the ability to forward alarms out of IMPACT to external systems that may need this information.

Tier 3

Tier 3 is the collection of network and element management platforms that provide direct management of network elements. All Tier 3 systems communicate to the Tier 2 manager of managers, thus utilizing a common XML-based information exchange model and CORBA communications bus architecture. Tier 3 systems are expected to provide the following basic services to Tier 2:

- Highly reliable fault and performance data collection
- Command and Control of network elements
- Alarm reduction (root cause analysis)
- Common CORBA XML interface to Tier 2
- Tier3-Tier2 Synchronization

Some examples of vendor-provided Tier 3 systems interfacing to IMPACT today are HP's OV-TeMIP, Agilent's NetExpert, Micromuse's NetCool, and Open's NerveCenter.

6.3.14.2 Network Service Level Agreements (M)

SLAs have been established for various aspects of the network Requirements of this Module 3. The Network SLAs address the performance and delivery of services as described throughout this RFP Section 6.3.

6.3.14.2.1 General Requirements (M)

The following general Requirements are applicable to the Network SLAs:

- The total rights and remedies for failure to satisfy a single service SLA for any given month shall not exceed the sum of 100 percent of the Total Monthly Recurring Cost (TMRC) plus 2 days of the AMUC
- If the circuit or service fails to meet one or more of the performance objectives, only the largest monthly Rights and Remedies for all performance objectives not met will be credited to the customer.
- If a tool fails to meet its objectives, the tool rights and remedies will apply. If the tool provides reports, only the rights and remedies for the tool will apply.
- To the extent that Contractor offers additional or more advantageous rights and/or remedies to Customers for similar services offered through tariffs, online service guides, or other programs, the State shall be entitled to exercise the rights and/or remedies therein
- For subcontracted local services from other ILECs or CLECs, the Contractor shall provide the State or Customer, at a minimum, the same service level agreements provided to Contractor by each

subcontractor Copies of all Service Level Agreements between Subcontractors and the awarded Contractor shall be provided to OTech/STND for all services

- When the Contractor provides Facilities based services directly to the Customer in other ILEC's or CLEC's territories, the rights and remedies for service outages for those services are as set forth in Sections 6.3.14.2.3 through 6.3.14.2.15
- The election by OTech/STND of any remedy covered by this Contract shall not exclude or limit OTech/STND's or any Customer's rights and remedies otherwise available within the Contract or at law or equity
- The Contractor shall act as the single point of contact coordinating all entities to meet the State's needs for ordering/provisioning, maintenance, restoration and resolution of service issues or that of their Affiliates, subsidiaries, subcontractors or resellers under this Contract
- Bidders may provide SLAs for proposed unsolicited services in the description field below

Bidder understands the Requirement and shall meet or exceed it? Yes No

Reference: document _____

location _____ page _____ paragraph _____

Description:

Verizon understands and will comply with this requirement as specified.

6.3.14.2.2 Trouble Ticket Stop Clock Conditions (M)

Stop Clock criteria includes the following: (Note: in this section, the term "End-User" includes End-Users and Customers, whichever is applicable.)

9. Periods when a restoration or testing effort is delayed at the specific request of the End-User. The Stop Clock condition shall exist during the period the Contractor was delayed, provided that reasonable and documented efforts are made to contact the End-User during the applicable Stop Clock period.
10. Time after a service has been restored, but End-User request

ticket be kept open for observation. If the service is later determined by the End-User to not have been restored, the Stop Clock shall continue until the time the End-User notifies the Contractor that the service has not been restored.

11. Time after a service has been restored, but End-User is not available to verify that the service is working. If the service is later determined by the End-User to not have been restored, the Stop Clock shall apply only for the time period between Contractor's reasonable attempt to notify the End-User that Contractor believes the service has been restored and the time the End-User notifies the Contractor that the service has not been restored.
12. Restoration cannot be achieved because the problem has been isolated to wiring that is not maintained by Contractor, or any of its subsidiaries, subcontractors, or Affiliates.
13. Trouble caused by a power problem outside of the responsibility of the Contractor. This does not apply to the power Requirements necessary to support dial tone to IP phones.
14. Lack of building entrance Facilities or conduit structure that are the End-User's responsibility to provide.
15. The following contact/access problems, provided that Contractor makes reasonable efforts to contact End-User during the applicable stop clock period:
 - a. Access necessary to correct the problem is not available because access has not been arranged by site contact or End-User representative
 - b. Site contact refuses access to technician who displays proper identification
 - c. Insufficient or incorrect site contact information which prevents access, provided that Contractor takes reasonable steps to notify End-User of the improper contact information and takes reasonable steps to obtain the correct information.
 - d. Site has limited hours of business that directly impacts the Contractor's ability to resolve the problem.
 - e. If it is determined later that the cause of the problem was not at the site in question, then the Stop Clock shall not apply.
16. Any problem or delay to the extent caused by End-User's staff that prevents or delays Contractor's resolution of the problem.

In such event, Contractor shall make a reasonable request to End-User staff to correct the problem or delay.

17. End-User applications that interfere with repair of the trouble.
18. Repair/replacement of CPE not provided by Contractor if the problem has reasonably been isolated to the CPE.
19. Failure of the trouble ticket originator or responsible End-User to return a call from Contractor's technician for on-line close-out of trouble tickets after the service has been restored as long as Contractor can provide Documentation substantiating message from Contractor's technician.
20. An outage directly related to any properly performed scheduled maintenance or upgrade. Any such stop clock condition shall not extend beyond the scheduled period of the maintenance or upgrade. SLAs will apply for any maintenance caused outage beyond the scheduled maintenance period. Outages occurring during a scheduled maintenance or upgrade period and not caused by the scheduled maintenance shall not be subject to this paragraph 12 stop clock criteria.
21. Any problem or delay caused by a third party not under the control of Contractor, not reasonably preventable by Contractor, including, at a minimum, cable cuts not caused by the Contractor. Contractor's Affiliates, subsidiaries, or subcontractors shall be deemed to be under the control of Contractor with respect to the Equipment, services, or Facilities to be provided under this Contract.
22. Force Majeure events, as defined in the terms and conditions of the Contract (Appendix B, Section 21).

Bidder understands the Requirement and shall meet or exceed it? Yes No

Reference: document _____

location _____ page _____ paragraph _____

Description:

Verizon understands and will comply with this requirement as specified.

6.3.14.2.3 Service Availability Percentage (M)

Services	Availability Percentage
Hosted Standalone IP Telephony Business Line Services	<p>Definition</p> <p>The monthly availability percentage equals the Scheduled Uptime per month less Unavailable Time divided by Scheduled Uptime per month multiplied by 100 per service ID. Scheduled uptime is based on 7x24x number of days in the month.</p>
Hosted Standalone IP Telephony Voice Mail Services	<p>Measurement Process</p>
Hosted Standalone IP Telephony Audio Conferencing (includes WebEx)	<p>The monthly Availability percentage shall be based on the accumulative total of all outage durations for each port number/service ID, per calendar month. All outage durations applied to other SLAs, which result in a remedy, will be excluded from the monthly accumulative total.</p>
Converged Services, IP and IP Network Transport – Multicast Service	<p>Objectives</p> <p>99.2 percent</p>
Converged Services, Secure Gateway Services – Universal Port	<p>Immediate Rights and Remedies</p> <p>End-User Escalation Process</p> <p>OTech/STND Escalation Process</p>
Converged Services, IP and Network IP Transport Services – Additional Router IOS Encryption Option	<p>Monthly Rights and Remedies</p> <p>First month to fail to meet the SLA objective shall result in a 15 percent rebate of the TMRC and 2 days of the Average Monthly Usage Cost (AMUC).</p>
Converged Services, IP Telephony Business Line Services	<p>Next consecutive month to fail to meet the SLA objective shall result in a 25 percent rebate of TMRC and 2 days of the AMUC.</p>
Converged Services, Internet Dedicated Access (IDA) Service	<p>Each additional consecutive month to fail to meet the SLA objective shall result in a 50 percent rebate of the TMRC, and 2 days of the AMUC.</p>
Converged Services, IP Flexible T1 Service	
Converged Services, IP Telephony Voice Mail Services	

Services	Availability Percentage
Converged Services, Managed IP Audio Conferencing (includes WebEx)	
Converged Services, Managed IP Video Conference Services	
Converged Services, Unified Messaging	

Bidder understands the Requirement and shall meet or exceed it? Yes X No _____

Reference: document _____

location _____ page _____ paragraph _____

Description:

Verizon understands and will comply with this requirement as specified.

6.3.14.2.3.1 Service Availability Percentage (M) – Converged Services, IP and Network IP Transport Services

Services	Availability Percentage
<p>Converged Services, IP and Network IP Transport Services</p>	<p>Definition</p> <p>The monthly availability percentage equals the Scheduled Uptime per month less Unavailable Time divided by Scheduled Uptime per month multiplied by 100 per service ID. Scheduled uptime is based on 7x24x number of days in the month. Service objectives will be based on access facility required to provide the service.</p> <p>Measurement Process</p> <p>The monthly Availability percentage shall be based on the accumulative total of all outage durations for each port number/service ID, per calendar month. All outage durations applied to other SLAs, which result in a remedy, will be excluded from the monthly accumulative total.</p> <p>Objectives</p> <p>DS0 > 99.2 DS1 > 99.5 DS3 > 99.8 OCX > 99.8 Ethernet > 99.5</p> <p>Immediate Rights and Remedies</p> <p>End-User Escalation Process OTech/STND Escalation Process</p> <p>Monthly Rights and Remedies</p> <p>First month to fail to meet the SLA objective shall result in a 15 percent rebate of the TMRC</p> <p>Next consecutive month to fail to meet the SLA objective shall result in a 25 percent rebate of TMRC.</p> <p>Each additional consecutive month to fail to meet the SLA objective shall result in a 50 percent rebate of the TMRC,</p>

6.3.14.2.3.2 Service Availability Percentage (M) - DAN

Services	Availability Percentage
<p>Converged Services, Internet Dedicated Dial IP Access Network (DAN)</p>	<p>Definition</p> <p>The monthly availability percentage equals the Scheduled Uptime per month less Unavailable Time divided by Scheduled Uptime per month multiplied by 100 per service ID. Scheduled uptime is based on 7x24x number of days in the month.</p> <p>Measurement Process</p> <p>The monthly Availability percentage shall be based on the accumulative total of all outage durations for each port number/service ID, per calendar month. All outage durations applied to other SLAs, which result in a remedy, will be excluded from the monthly accumulative total.</p> <p>Objectives</p> <p>85 percent</p> <p>Immediate Rights and Remedies</p> <p>End-User Escalation Process OTech/STND Escalation Process</p> <p>Monthly Rights and Remedies</p> <p>First month to fail to meet the SLA objective shall result in a 15 percent rebate of the TMRC and 2 days of the Average Monthly Usage Cost (AMUC).</p> <p>Next consecutive month to fail to meet the SLA objective shall result in a 25 percent rebate of TMRC and 2 days of the AMUC.</p> <p>Each additional consecutive month to fail to meet the SLA objective shall result in a 50 percent rebate of the TMRC, and 2 days of the AMUC.</p>

6.3.14.2.3.3 Service Availability Percentage (M) – Managed Router and Managed LAN Service

Services	Availability Percentage
<p>Converged Services, IP and Network IP Transport Managed Router Service</p> <p>Converged Services, IP Telephony Business Line Services - Managed LAN Service</p>	<p>Definition</p> <p>Managed Site Availability is based on the total number of minutes in a calendar month during which the Managed Router/LAN Site for Physical Management is available to exchange data divided by the total number of minutes in that month. Sites are considered available whether data is passing through the primary connection or through a back up connection. Physical Management rights and remedies are determined by the type of maintenance coverage as listed in the monthly rights and remedies.</p> <p>Managed Site Availability is based on the total number of minutes in a calendar month during which the Managed Site Router/LAN Site for Full Management is available to exchange data divided by the total number of minutes in that month. Sites are considered available whether data is passing through the primary connection or through a back up connection. Full Management rights and remedies are determined by the type of maintenance coverage as listed in the monthly rights and remedies.</p> <p>For sites located between a sixty (60) and one hundred twenty (120) mile radius from a authorized service center, Next Day monthly rights and remedies apply. Sites beyond a one hundred twenty (120) mile radius from authorized service center have no monthly rights and remedies.</p> <p>An Outage is defined as an unscheduled period in which the Customer Device is interrupted and unavailable for use by Customer for sixty (60) seconds. Or more then 60 cumulative seconds within a 15-minute period measured by Verizon.</p> <p>Measurement Process</p> <p>Availability is the percentage of time that the Customer’s site is available within a given calendar month. Availability only applies to Outages (Router/Switch). Monthly Managed Site Availability (%) = Total Minutes of site Outages per month x 100% number of days in month x 24 hours x 60 Minutes.</p> <p>All outage durations applied to other SLAs, which result in a remedy, will be excluded from the monthly accumulative total.</p> <p>Objectives 99.5%</p> <p>Immediate Rights and Remedies End-User Escalation Process</p>

Services	Availability Percentage																																										
	<p>OTech/STND Escalation Process</p> <p>Monthly Rights and Remedies 24x7 4 Hours Response Maintenance</p> <table border="0"> <thead> <tr> <th>From</th> <th>To</th> <th>Remedy</th> </tr> </thead> <tbody> <tr> <td>99.49%</td> <td>99.00%</td> <td>5%</td> </tr> <tr> <td>98.99%</td> <td>97.00%</td> <td>15%</td> </tr> <tr> <td>96.99%</td> <td>95.00%</td> <td>20%</td> </tr> <tr> <td>94.99%</td> <td>93.00%</td> <td>25%</td> </tr> <tr> <td>92.99%</td> <td>90.00%</td> <td>30%</td> </tr> <tr> <td>Less than 90.00%</td> <td></td> <td>100%</td> </tr> </tbody> </table> <p>Next Day 24x7 24 Hours Response Maintenance</p> <table border="0"> <thead> <tr> <th>From</th> <th>To</th> <th>Remedy</th> </tr> </thead> <tbody> <tr> <td>96.16%</td> <td>95.66</td> <td>5%</td> </tr> <tr> <td>95.67%</td> <td>93.66</td> <td>15%</td> </tr> <tr> <td>93.67%</td> <td>91.66</td> <td>20%</td> </tr> <tr> <td>91.67%</td> <td>89.66</td> <td>25%</td> </tr> <tr> <td>89.67%</td> <td>86.66</td> <td>30%</td> </tr> <tr> <td>Less than 86.67%</td> <td></td> <td>100%</td> </tr> </tbody> </table> <p>Failure to meet the SLA objective shall result in an associated right and remedy percent rebate of the TMRC.</p>	From	To	Remedy	99.49%	99.00%	5%	98.99%	97.00%	15%	96.99%	95.00%	20%	94.99%	93.00%	25%	92.99%	90.00%	30%	Less than 90.00%		100%	From	To	Remedy	96.16%	95.66	5%	95.67%	93.66	15%	93.67%	91.66	20%	91.67%	89.66	25%	89.67%	86.66	30%	Less than 86.67%		100%
From	To	Remedy																																									
99.49%	99.00%	5%																																									
98.99%	97.00%	15%																																									
96.99%	95.00%	20%																																									
94.99%	93.00%	25%																																									
92.99%	90.00%	30%																																									
Less than 90.00%		100%																																									
From	To	Remedy																																									
96.16%	95.66	5%																																									
95.67%	93.66	15%																																									
93.67%	91.66	20%																																									
91.67%	89.66	25%																																									
89.67%	86.66	30%																																									
Less than 86.67%		100%																																									

6.3.14.2.4 Catastrophic Outage 1 (M)

Services	Catastrophic Outage 1
Hosted Standalone IP Telephony Business Line Services	<p>Definition</p> <p>The total loss of two or more services at one address.</p>
Converged Services, IP and Network IP Transport Services	<p>Measurement Process</p>
Converged Services, IP and Network IP Transport – Multicast Service	<p>The outage start shall be determined by the network alarm resulting from the outage-causing event or the opening of a trouble ticket by a Customer, whichever occurs first. The Contractor shall open a trouble ticket and compile a list for each End-User service affected by the common cause. Each End-User service is out of service from the first notification until the Contractor determines the service is restored. Any service reported by End-User/Customer as not having been restored shall have the outage time adjusted to the actual restoration time.</p>
Converged Services, Secure Gateway Services – Universal Port	<p>(7X24)</p>
Converged Services IP, and Network IP Transport Services – Additional Router IOS Encryption Option	<p>Objectives</p> <p>Less than 2 hours;</p>
Converged Services, Internet Dedicated Dial IP Access Network (DAN) Flat Rate	<p>Immediate Rights and Remedies</p> <p>100 percent of the TMRC for each service not meeting the per occurrence objective for a single Cat 1 fault</p>
Converged Services, IP Telephony Business Line Services	<p>End-User Escalation Process</p> <p>OTech/STND Escalation Process</p>
Converged Services, Internet Dedicated Access (IDA) Service	<p>Monthly Rights and Remedies</p> <p>N/A</p>
Converged Services, IP Flexible T1 Service	

Bidder understands the Requirement and shall meet or exceed it? Yes No

Reference: document _____

location _____ page _____ paragraph _____

Description:

Verizon understands and will comply with this requirement as specified.

6.3.14.2.5 Catastrophic Outage 2 (M)

Services	Catastrophic Outage 2
<p>Hosted Standalone IP Telephony Business Line Services</p> <p>Converged Services, IP and Network IP Transport Services</p> <p>Converged Services, Secure Gateway Services – Universal Port</p> <p>Converged Services IP, and Network IP Transport Services – Additional Router IOS Encryption Option</p> <p>Converged Services, Internet Dedicated Dial IP Access Network (DAN) Flat Rate</p> <p>Converged Services, IP Telephony Business Line Services</p> <p>Converged Services, Internet Dedicated Access (IDA) Service</p> <p>Converged Services, IP Flexible T1 Service</p>	<p>Definition</p> <p>A total failure of the Contractor’s (or subcontractor’s or Affiliate’s) network Equipment nearest the End-User locations regardless of where the failure occurs in the network. .</p> <p>Measurement Process</p> <p>The outage duration start shall be determined by the network alarm resulting from the outage-causing event or the opening of a trouble ticket by the Customer, whichever occurs first. Outage duration shall be measured on a per End-User service basis from information recorded from the network Equipment or trouble ticket</p> <p>The Contractor shall open a trouble ticket and compile a list for each service affected by the common cause. Each End-User service is considered out of End-User service from the first notification until the Contractor determines the End-User service is restored. Any End-User service reported by the End-User/Customer as not having been restored shall have the outage time adjusted to the actual restoration time.</p> <p>(7X24)</p> <p>Objectives</p> <p>Less than 30 minutes</p> <p>Immediate Rights and Remedies</p> <p>100 percent of the TMRC for each service not meeting the per occurrence objective for a single Cat 2 fault</p> <p>End-User Escalation Process</p> <p>OTech/STND Escalation Process</p> <p>Monthly Rights and Remedies</p> <p>N/A</p>

Bidder understands the Requirement and shall meet or exceed it? Yes X No

Reference: document _____

location _____ page _____ paragraph _____

Description:

Verizon understands and will comply with this requirement as specified.

6.3.14.2.6 Catastrophic Outage 3 (M)

Services	Catastrophic Outage 3
Hosted Standalone IP Telephony Business Line Services	<p>Definition</p> <p>The total loss of any service type on a network wide basis.</p> <p>Measurement Process</p>
Converged Services, IP and Network IP Transport Services	<p>The outage duration start shall be determined by the network alarm resulting from the outage-causing event or the opening of a trouble ticket by the Customer, whichever occurs first. Outage duration shall be measured on a per End-User service basis from information recorded from the network Equipment or trouble ticket.</p>
Converged Services, Secure Gateway Services – Universal Port	<p>The Contractor shall open a trouble ticket and compile a list for each End-User service affected by the common cause. Each End-User service is out of service from the first notification until the Contractor determines the End-User service is restored. Any service reported by End-User/Customer as not having been restored shall have the outage time adjusted to the actual restoration time.</p>
Converged Services, IP and Network IP Transport Services – Additional Router IOS Encryption Option	<p>(7X24)</p> <p>Objectives</p>
Converged Services, Internet Dedicated Dial IP Access Network (DAN) Flat Rate	<p>Less than 15 minutes</p> <p>Immediate Rights and Remedies</p>
Converged Services, IP Telephony Business Line Services	<p>Senior Management Escalation Process</p> <p>100 percent of the TMRC for each service not meeting the per occurrence objective for a single Cat 3 fault</p> <p>Monthly Rights and Remedies</p>
Converged Services, Internet Dedicated Access (IDA) Service	<p>N/A</p>
Converged Services, IP Flexible T1 Service	

Bidder understands the Requirement and shall meet or exceed it? Yes No

Reference: document _____

location _____ page _____ paragraph _____

Description:

Verizon understands and will comply with this requirement as specified.

6.3.14.2.7 Round Trip Transmission Delay (M)

Services	Round Trip Transmission Delay
<p>Converged Services, IP and Network IP Transport Services</p> <p>Converged Services, IP and Network IP Transport Services – Additional Router IOS Encryption Option</p>	<p>Definition</p> <p>Average round trip transfer delay measured from Contractor's to Customer hand off (CCH) to the remote CCH and back</p> <p>Measurement Process</p> <p>End-User/Customer is responsible for opening a trouble ticket with the Contractor Customer Service Center (helpdesk) when the data transfer delay is below the committed level. OTech/STND shall determine the sample interval, provided that a minimum of 100 pings or more shall constitute test. The problem requires timely verification, consistent with industry Standards (e.g., a protocol analyzer), by the Contractor. Trouble shall be tracked as a Quality of Service (QoS) problem using a special disposition code on the trouble ticket. QoS tickets shall not count in availability or Time to Repair measurements unless and until the End-User reports service as unusable for its intended uses.</p> <p>(7x24)</p> <p>Objectives</p> <p>IP Transport for Converged Services:</p> <p>56Kbps – 1.536Mbps</p> <p>64 byte ping: <120ms</p> <p>1000 byte ping: <400ms</p> <p>1.792Mbps – 40Mbps</p> <p>64 byte ping: <60ms</p> <p>1000 byte ping: <120ms</p> <p>40Mbps and above</p> <p>64 byte ping: <65 ms</p> <p>1000 byte ping: <110 ms</p> <p>Immediate Rights and Remedies</p> <p>15 percent of TMRC per occurrence for the reported service.</p> <p>Next consecutive month to fail to meet the SLA objectives shall result in a 25 percent rebate of TMRC.</p> <p>Each additional consecutive month to fail to meet the SLA objective shall result in a 50 percent rebate of the TMRC.</p> <p>End-User Escalation Process</p> <p>OTech/STND Escalation Process</p>

Services	Round Trip Transmission Delay
	<p>Monthly Rights and Remedies N/A</p>

Bidder understands the Requirement and shall meet or exceed it? Yes No

Reference: document _____

location _____ page _____ paragraph _____

Description:

Verizon understands and will comply with this requirement as specified.

6.3.14.2.8 One-Way Transmission Delay (M)

Services	One-Way Transmission Delay
<p>Hosted Standalone IP Telephony Services</p> <p>Converged Services, IP Telephony Services</p>	<p>Definition</p> <p>Average one-way transfer delay measured from the Contractor to Customer handoff to the remote Contractor to Customer handoff ("CCH to CCH").</p> <p>Measurement Process</p> <p>End-User/Customer is responsible for opening a trouble ticket with the Contractor Customer Service Center (helpdesk) when the data transfer delay fails to meet the committed level. The problem requires timely verification, consistent with industry Standards (e.g., a protocol analyzer), by the Contractor. Trouble shall be tracked as a Quality of Service (QoS) problem using a special disposition code on the trouble ticket. QoS tickets shall not count in availability or Time to Repair measurements unless and until the End-User reports service as unusable for its intended uses.</p> <p>This measurement applies to local loop transport under the control of the Contractor or not under the control of Contractor that do not exceed 70% peak utilization for three consecutive business days.</p> <p>(7x24)</p> <p>Objectives</p> <p>less than 130 ms one way</p>

Services	One-Way Transmission Delay
	<p>Immediate Rights and Remedies</p> <p>15 percent of TMRC per occurrence for the reported service.</p> <p>Next consecutive month to fail to meet the SLA objectives shall result in a 25 percent rebate of TMRC.</p> <p>Each additional consecutive month to fail to meet the SLA objective shall result in a 50 percent rebate of the TMRC.</p> <p>End-User Escalation Process</p> <p>OTech/STND Escalation Process</p> <p>Monthly Rights and Remedies</p> <p>N/A</p>

Bidder understands the Requirement and shall meet or exceed it? Yes X No ___

Reference: document _____

location _____ page _____ paragraph _____

Description:

Verizon understands and will comply with this requirement as specified.

6.3.14.2.9 Jitter (M)

Services	Jitter
<p>Hosted Standalone IP Telephony Business Line Services</p> <p>Converged Services, IP Telephony Business Line Services</p> <p>Converged Services, IP Flexible T1 Service</p>	<p>Definition</p> <p>Variations in transfer delay measured from the CCH to the remote CCH.</p> <p>Measurement Process</p> <p>End-User/Customer is responsible for opening a trouble ticket with the Contractor Customer Service Center (helpdesk) when the jitter exceeds the committed level. The problem requires timely verification, consistent with industry Standards (calculations defined in: IETF RFC 3550 RTP, RFC 3611 RTP), by the Contractor. Trouble shall be tracked as a Quality of Service (QoS) problem using a special disposition code on the trouble ticket. QoS tickets shall not count in availability or Time to Repair measurements unless and until the End-User reports service as unusable for its intended uses.</p> <p>This measurement applies to local loop transport under the control of the Contractor or not under the control of Contractor that do not exceed 70% peak utilization for three consecutive business days (7x24)</p> <p>Objectives</p> <p>Less than 15 ms</p> <p>Immediate Rights and Remedies</p> <p>15 percent of TMRC per occurrence for the reported service.</p> <p>Next consecutive month to fail to meet the SLA objectives shall result in a 25 percent rebate of TMRC.</p> <p>Each additional consecutive month to fail to meet the SLA objective shall result in a 50 percent rebate of the TMRC.</p> <p>End-User Escalation Process</p> <p>OTech/STND Escalation Process</p> <p>Monthly Rights and Remedies</p> <p>N/A</p>

Bidder understands the Requirement and shall meet or exceed it? Yes No

Reference: document _____

location _____ page _____ paragraph _____

Description:

Verizon understands and will comply with this requirement as specified.

6.3.14.2.9.1 Jitter - IDA

Services	Jitter - IDA
<p>Converged Services Internet Dedicated Access (IDA) Service</p>	<p>Definition</p> <p>Also known as delay variation, Jitter is defined as the variation or difference in the end-to-end delay between received packets of an IP or packet stream. Verizon's North American Network jitter performance will not exceed 1 milliseconds between Verizon-designated inter-regional transit backbone network routers Hub Routers in the contiguous U.S..</p> <p>Measurement Process</p> <p>End-User/Customer is responsible for opening a trouble ticket with the Contractor Customer Service Center (helpdesk) when the jitter exceeds the committed level. Trouble shall be tracked as a Quality of Service (QoS) problem using a special disposition code on the trouble ticket. QoS Tickets shall not count in availability measurements unless and until the End-User reports service as unusable for its intended use.</p> <p>Jitter shall be measured by averaging sample measurements taken during a calendar month between Hub Routers The problem requires timely verification, consistent with industry Standards by Verizon Business.</p> <p>(7x24)</p> <p>Objectives</p> <p>1 ms US</p> <p>Immediate Rights and Remedies</p> <p>15 percent of TMRC per occurrence for the reported service.</p> <p>Next consecutive month to fail to meet the SLA objectives shall result in a 25 percent rebate of TMRC.</p> <p>Each additional consecutive month to fail to meet the SLA objective shall result in a 50 percent rebate of the TMRC.</p> <p>End-User Escalation Process</p> <p>OTech/STND Escalation Process</p>

Services	Jitter - IDA
	<p>Monthly Rights and Remedies</p> <p>N/A</p>

6.3.14.2.9.2 Latency - IDA

Services	Latency - IDA
<p>Converged Services Internet Dedicated Access (IDA) Service</p> <p>Converged Services, Internet Dedicated Dial IP Access Network (DAN)</p>	<p>Definition</p> <p>Verizon’s U.S. Latency SLA provides for average round-trip transmissions of 45 milliseconds or less between Verizon-designated inter-regional transit backbone routers (“Hub Routers”) in the contiguous U.S.</p> <p>Verizon’s Transatlantic Latency SLA provides for average round-trip transmissions of 90 milliseconds or less between a Verizon Hub Router in the New York metropolitan area and a Verizon Hub Router in the London metropolitan area.</p> <p>Measurement Process</p> <p>End-User/Customer is responsible for opening a trouble ticket with the Contractor Customer Service Center (helpdesk) when the data transfer delay is below the committed level. Trouble shall be tracked as a Quality of Service (QoS) problem using a special disposition code on the trouble ticket. QoS tickets shall not count in availability or Time to Repair measurements unless and until the End-User reports service as unusable for its intended uses.</p> <p>Latency is calculated by averaging sample measurements taken during a calendar month between VZ Internet Hub Routers. The problem requires timely verification, consistent with industry Standards by Verizon Business.</p> <p>(7x24)</p> <p>Objectives</p> <p>45 ms US</p> <p>90 ms between New York and London</p>

Services	Latency - IDA
	<p>Immediate Rights and Remedies</p> <p>15 percent of TMRC per occurrence for the reported service.</p> <p>Next consecutive month to fail to meet the SLA objectives shall result in a 25 percent rebate of TMRC.</p> <p>Each additional consecutive month to fail to meet the SLA objective shall result in a 50 percent rebate of the TMRC.</p> <p>End-User Escalation Process</p> <p>OTech/STND Escalation Process</p> <p>Monthly Rights and Remedies</p> <p>N/A</p>

6.3.14.2.10 Packet Loss (M)

Services	Packet Loss
<p>Hosted Standalone IP Telephony Business Line Services</p> <p>Converged Services, IP and Network IP Transport Services</p> <p>Converged Services, IP and Network IP Transport Services – Additional Router IOS Encryption Option</p> <p>Converged Services, IP Telephony Business Line Services</p> <p>Converged Services, IP Flexible T1 Service</p>	<p>Definition</p> <p>Packet loss is measured from Contractor’s hand off to Customer at each end of data channel.</p> <p>Measurement Process</p> <p>End-User/Customer is responsible for opening a trouble ticket with the Contractor Customer Service Center (helpdesk) when the data packet loss exceeds the committed level. The problem requires timely verification, consistent with industry Standards (e.g., protocol analyzer), by the Contractor. Trouble shall be tracked as a Quality of Service (QoS) problem using a special disposition code on the trouble ticket. QoS tickets shall not count in availability or Time to Repair measurements unless and until the End-User reports service as unusable for its intended uses.</p> <p>This measurement applies to local loop transport under the control of the Contractor or not under the control of Contractor that do not exceed 70% peak utilization for three consecutive business days (7x24)</p> <p>Objectives</p> <p>0.5 percent maximum packet loss</p>

Services	Packet Loss - IDA
	<p>Measurement Process</p> <p>End-User/Customer is responsible for opening a trouble ticket with the Contractor Customer Service Center (helpdesk) when the data packet loss exceeds the committed level. . Trouble shall be tracked as a Quality of Service (QoS) problem using a special disposition code on the trouble ticket. QoS Tickets shall not count in availability measurements unless and until the End-User reports service as unusable for its intended use.</p> <p>Packet delivery is calculated based on the average of regular periodic measurements taken during a calendar month between Hub Routers. The problem requires timely verification, consistent with industry Standards by Verizon Business.</p> <p>(7x24)</p> <p>Objectives</p> <p>0.5 percent maximum packet loss</p> <p>Immediate Rights and Remedies</p> <p>15 percent of TMRC per occurrence for the reported service.</p> <p>Next consecutive month to fail to meet the SLA objectives shall result in a 25 percent rebate of TMRC.</p> <p>Each additional consecutive month to fail to meet the SLA objective shall result in a 50 percent rebate of the TMRC.</p> <p>End-User Escalation Process</p> <p>OTech/STND Escalation Process</p> <p>Monthly Rights and Remedies</p> <p>N/A</p>

6.3.14.2.11 IP Contact Center Service Outage (M)

Services	IP Contact Center Service Outage
<p>Converged Services, Computer Telephone Integration (CTI) for IP Network Based ACD</p> <p>Converged Services, IP Network Based Automatic Call Distribution (ACD)</p> <p>Converged Services, IP Network Based Interactive Voice Response (IVR) System</p> <ul style="list-style-type: none"> - Open Hosted IVR - IP Hosted Intelligent Contact Routing (HICR) <p>Converged Services, IP Network Based Specialized Call Routing</p>	<p>Definition</p> <p>The loss of an IP Contact Center Service or identified feature at a single End-User location.</p> <p>Measurement Process</p> <p>The outage start shall be determined by either the application alarm/other fault indicator which automatically results in the opening of a trouble ticket by the contractor or the start shall be determined by the opening of a trouble ticket by the Customer, whichever occurs first. The Contractor shall identify each IP Contact Center service/identified feature affected as a result of the outage. Each impacted IP Contact Center service/identified feature shall be considered unavailable from the first notification until the Contractor determines the IP Contact Center service/identified feature is restored. Any IP Contact Center service reported by End-User/Customer as not having been restored shall have the outage time adjusted to the actual restoration time.</p> <p>Monday through Friday 7:00 am to 6:00 pm PST</p> <p>Objectives</p> <p>Less than 4 hours</p> <p>Immediate Rights and Remedies</p> <p>15 percent of the TMRC and 2 days of any applicable average monthly usage costs (AMUC), as defined in the glossary, for each service/identified feature not meeting the per occurrence objective for a single IP Contact Center Service Outage</p> <p>End-User Escalation Process</p> <p>OTech/STND Escalation Process</p> <p>Monthly Rights and Remedies</p> <p>N/A</p>

Bidder understands the Requirement and shall meet or exceed it? Yes X No

Reference: document _____

location _____ page _____ paragraph _____

Description:

Verizon understands and will comply with this requirement as specified.

6.3.14.2.12 Excessive Outage (M)

Services	Excessive Outage
<p>Hosted Standalone IP Telephony Business Line Services</p> <p>Hosted Standalone IP Telephony Voice Mail Services</p> <p>Hosted Standalone IP Telephony Audio Conferencing (includes WebEx)</p> <p>Converged Services, IP and Network IP Transport Services</p> <p>Converged Services, IP and Network IP Transport – Multicast Service</p> <p>Converged Services, Secure Gateway Services – Universal Port</p> <p>Converged Services IP, and Network IP Transport Services – Additional Router IOS Encryption Option</p> <p>Converged Services, Internet Dedicated Dial IP Access Network (DAN)</p> <p>Converged Services, IP Telephony Business Line Services</p> <p>Converged Services, Internet Dedicated Access (IDA) Service</p> <p>Converged Services, IP Flexible T1 Service</p> <p>Converged Services, IP Telephony Voice Mail Services</p>	<p>Definition</p> <p>An Excessive outage shall be defined as a trouble ticket that remains opened with the Contractor on a service, for more than twelve hours.</p> <p>Measurement Process</p> <p>The service is unusable during the time the trouble ticket is reported as opened until restoration of the service, minus stop clock conditions. Any service reported by End-User/Customer as not having been restored shall have the outage time adjusted to the actual restoration time.</p> <p>(7 x 24)</p> <p>Objectives</p> <p>Less than 12 hours</p> <p>Immediate Rights and Remedies</p> <p>Senior Management Escalation</p> <p>Customer may request from Contractor an Excessive Outage restoration briefing.</p> <p>100 percent of the TMRC per occurrence and 2 days of any applicable AMUC-for each service out of service greater than 12 hours.</p> <p>Monthly Rights and Remedies</p> <p>N/A</p>

Services	Excessive Outage
Converged Services, Managed IP Audio Conferencing (includes WebEx) Converged Services, IP Network Based Automatic Call Distribution (ACD) Converged Services, IP Network Based Interactive Voice Response (IVR) System (includes Open Hosted IVR, IP Hosted Intelligent Contact Routing (HICR)) Converged Services, IP Network Based Specialized Call Routing Converged Services, Computer Telephone Integration (CTI) for IP Network Based ACD Converged Services, Managed IP Video Conference Services Converged Services, Unified Messaging	

Bidder understands the Requirement and shall meet or exceed it? Yes X No _____

Reference: document _____
location _____ page _____ paragraph _____

Description:

Verizon understands and will comply with this requirement as specified.

6.3.14.2.13 Notification (M)

Services	Notification
<p>All Services as listed in Module 3</p>	<p>Definition</p> <p>The Contractor notification to OTech/STND in the event of a Catastrophic Outage, network failure, terrorist activity, or threat of natural disaster, which results in a significant loss of telecommunication services to CALNET II End-Users or has the potential to impact services in a general or statewide area.</p> <p>Measurement Process</p> <p>The Contractor shall invoke the notification process for all CAT 1, CAT 2, and CAT 3 Outages or network outages resulting in significant loss of services. The Contractor shall notify OTech/STND via the Contractor's automated notification system.</p> <p>Updates shall be given on the above-mentioned failures via the Contractor's automated notification system which shall include time and date of the updates.</p> <p>Objectives</p> <p>Within 30 minutes of a CAT 1, CAT 2, or CAT 3 failure, the Contractor shall notify general stakeholders (as determined by OTech/STND) via the Contractor's automated notification system.</p> <p>At 60 minute intervals, updates shall be given on the above mentioned failures via the Contractors automated notification system which shall include time and date of the updates.</p> <p>Immediate Rights and Remedies</p> <p>Senior Management Escalation</p> <p>Monthly Rights and Remedies</p> <p>N/A</p>

Bidder understands the Requirement and shall meet or exceed it? Yes X No

Reference: document _____

location _____ page _____ paragraph _____

Description:

Verizon understands and will comply with this requirement as specified.

6.3.14.2.13.1 Proactive Notification SLA – Managed Router and Managed LAN Service/WLAN Service

Services	Proactive Notification
<p>Converged Services, IP and IP Network Transport Managed Router Service</p> <p>Converged Services, IP Telephony Business Line Services - Managed LAN Service</p> <p>Converged Services, IP and Network IP Transport – Managed WLAN Service</p>	<p>Definition The proactive outage notification SLA provides credits if Verizon fails to notify Customer of an Outage by electronic means (e.g., pager or e-mail)</p> <p>An Outage is defined as an unscheduled period in which the Customer Device is interrupted and unavailable for use by Customer for sixty (60) seconds. Or more then 60 cumulative seconds within a 15-minute period measured by Verizon.</p> <p>Measurement Process The outage duration start shall be determined by the first network alarm resulting from the outage-causing event or the opening of a trouble ticket by the Customer, whichever occurs first. Verizon has fifteen (15) minutes to notify Customer’s primary point of contact from the start point of the Notification Period. Verizon is in compliance with the proactive outage notification SLA if the Customer opened the trouble ticket or contacts Verizon within the Notification Period. Verizon will provide the ticket number and an initial status.</p> <p>Objectives 15 Minutes</p> <p>Immediate Rights and Remedies Customer will receive a credit equal to ten percent (10%) of the monthly recurring charge for each Managed Service that was impacted during an Outage that was not properly notified by electronic means (e.g., pager or e-mail).</p> <p>End-User Escalation Process OTech/STND Escalation Process</p> <p>Monthly Rights and Remedies N/A</p>

6.3.14.2.14 Provisioning (M)

Services	Business Days	Provisioning
Hosted Standalone IP Telephony Business Line Services (includes Hosted Standalone IP Telephony Voice Mail functionality and Hosted Standalone IP Telephony Audio Conferencing (includes WebEx) functionality)	Managed Project	Definition Provisioning shall be defined as new service, adds, moves, changes, reconfiguration and retermination, and deletes completed by the Contractor on or before the due dates. Provisioning SLAs are two-fold: Individual Service Order and Monthly Average Percentage by Service Type. Note: Provisioning timelines include extended demarcation, wiring, when appropriate.
Adds, moves, changes, and deletes for Hosted Standalone IP Telephony Voice Services	2 Day	Measurement Process Individual Service Order: Install intervals are based on the intervals provided in the adjacent column or Customer/Contractor negotiated due dates documented on the order form/system.
Hosted Standalone IP Telephony Audio Conferencing (includes WebEx) Scheduling	4 hours	Monthly Average Percentage by Service Type:
Inside Wiring Services	Contracted Service Project Work – Section 6.3.12.1	The sum of all individual service orders meeting the objective in the measurement period divided by the sum of all individual service orders due in the measurement period equals the monthly average. The entire installation on any reconfiguration or retermination fee is refunded to the Customers for all orders that did not complete on time during the month if the monthly objective is not met.
Converged Services, IP and Network IP Transport Services Port Speed: 56K- 1.5Mbps 1..792Mbps-3.3 Mbps 3.3Mbps up	20 days 30 days Managed Project	Objective Individual Order:
Converged Services – IP and Network IP Transport Managed Router Service	45 Business Days	Service/Transport as appropriate provisioned on or before the due date per install order.
Converged Services, IP and Network IP Transport – Multicast Service	Managed Project	Monthly Average percent by Service Type: Greater than 95 percent
Converged Services, Secure Gateway Services – Universal Port	Managed Project	Immediate Rights and Remedies Individual Order:

Services	Business Days	Provisioning
Converged Services, IP and Network IP Transport Services – Additional Router IOS Encryption Option	Managed Project	50 percent of installation fee refunded to Customer for any missed due date. End-User Escalation Process OTech/STND Escalation Process
Converged Services, Internet Dedicated Dial IP Access Network (DAN)	Managed Project	Monthly Rights and Remedies:
Converged Services, IP Telephony Business Line Services (includes Converged Services, IP Telephony Voice Mail functionality and Converged Services, Managed IP Telephony Audio Conferencing (includes WebEx) functionality)	Managed Project	- Monthly Average percent by Service Type: The entire installation fee refunded to Customer for all orders that did not complete on time during the month if the monthly average objective is not met.
Converged Services, IP Telephony Business Line Services – Managed LAN Service	45 Business Days	
Converged Services, IP and Network IP Transport – Managed WLAN Service	45 Business Days (measured from Verizon's acceptance of a complete and accurate order through the date when the service is up and billable at the customer site.)	
Adds, moves, changes, and deletes for Hosted Standalone IP Telephony Voice Services	2 Days	

Services	Business Days	Provisioning
Converged Services, Internet Dedicated Access (IDA) Service T1 port T3 port OC3 and higher	40 Business Days 60 Business Days Managed Project	
Converged Services, IP Flexible T1 Service T1 port T3 port OC3 and higher	40 Business Days 60 Business Days Managed Project	
Converged Services, Managed IP Audio Conferencing (includes WebEx)Scheduling	4 hours	
Converged Services, IP Network Based Automatic Call Distribution (ACD)	Managed Project	
Converged Services, IP Network Based Interactive Voice Response (IVR) System (includes Open Hosted IVR, IP Hosted Intelligent Contact Routing (HICR))	Managed Project	
Converged Services, IP Network Based Specialized Call Routing	Managed Project	
Converged Services, Computer Telephone Integration (CTI) for IP Network Based ACD	Managed Project	
Converged Services, Managed IP Video Conference Services	4 hours	
Converged Services, Unified Messaging	Managed Project	

Services	Business Days	Provisioning
Low Voltage Simple Wiring Services	Contracted Service Project Work – Section 6.3.12.1	
Service Entrance	Contracted Service Project Work – Section 6.3.12.1	
Extended Termination	Contracted Service Project Work – Section 6.3.12.1	
Station Wiring	Contracted Service Project Work – Section 6.3.12.1	
Converged Services, Required Customer Premise Equipment	Managed Project	

Bidder understands the Requirement and shall meet or exceed it? Yes No

Reference: document _____

location _____ page _____ paragraph _____

Description:

Verizon understands and will comply with this requirement as specified.

6.3.14.2.15 Response Duration from Receipt of Order (M)

Services	Response Duration from Receipt of Order
All Services in Module 3	<p>Definition The interval for Contractor response to initial request from Customer when initiating a service request.</p> <p>Measurement Process The Response SLA shall be based on the Customer order submittal date when using either the STD 20 or the ordering system or the date the Contractor responds to the Customer. If the Contractor fails to schedule appointment with the Customer within the objective interval, then the Contractor shall be subject to the rights and remedies below.</p> <p>Objectives Next Business Day for Contractor response to initial request from Customer when initiating a service request.</p> <p>Immediate Rights and Remedies Escalation to Contractor’s Account Manager</p> <p>Monthly Rights and Remedies Review process with OTech/STND</p>

Bidder understands the Requirement and shall meet or exceed it? Yes X No _____

Reference: document _____

location _____ page _____ paragraph _____

Description:

Verizon understands and will comply with this requirement as specified.

6.3.14.2.16 Time To Repair (TTR) – Major

<p>Converged Services, IP and Network IP Transport Services</p>	<p>Definition A Major Fault shall be defined as five (5) or more physical circuit (DS-1 or higher speed) at the same address location affected by a common cause.</p> <p>Measurement Process This Service Level Agreement (SLA) applies to the services listed in the adjacent column. This SLA is based on a trouble ticket outage durations. The circuit or service is unusable during the time the trouble ticket is recorded as opened in the Contractors trouble ticket system minus stop clock conditions. This SLA is applied per occurrence. Trouble reporting shall be 7X24. Any circuits or service reported by End-User/Customer as not having been restored shall have the outage time adjusted to the actual restoration time.</p> <p>Objectives Less than 2 hours</p> <p>Immediate Rights and Remedies Failing to meet the SLA objective shall result in a 25 percent rebate of the TMRC per occurrence. End-User Escalation Process OTech/STND Escalation Process</p> <p>Monthly Rights and Remedies N/A</p>
---	--

6.3.14.2.17 Time To Repair (TTR) - Minor

Services	Time to Repair (TTR)-Minor
<p>Converged Services, IP and Network IP Transport Services</p>	<p>Definition</p> <p>A Minor Fault shall be defined as a trouble ticket opened with the Contractor's helpdesk on the loss of any circuit or service to a single End-User at a site. Service objectives will be based on access facility required to provide the service.</p> <p>Measurement Process</p> <p>This Service Level Agreement (SLA) applies to the services listed in the adjacent column. This SLA is based on a trouble ticket outage durations. The circuit or service is unusable during the time the trouble ticket is recorded as open in the Contractors trouble ticket system minus stop clock conditions. This SLA is applied per occurrence. Trouble reporting shall be 7X24. Any circuits or service reported by End-User/Customer as not having been restored shall have the outage time adjusted to the actual restoration time.</p> <p>Objectives</p> <p>DS0=less than 5 hours DS1=less than 4 hours DS3=less than 2 hours Ethernet=less than 4 hours OCX=less than 3 hours</p> <p>Immediate Rights and Remedies</p> <p>Failing to meet the SLA Objective shall result in a 15 percent rebate of the TMRC per occurrence. End-User Escalation Process OTech/STND Escalation Process</p> <p>Monthly Rights and Remedies N/A</p>

6.3.14.2.18 Time to Repair (TTR) – Managed Wireless LAN (WLAN) Service

Services	Time to Repair
<p>Converged Services, IP and Network IP Transport – Managed WLAN Service</p>	<p>Definition Time to Repair (TTR). TTR is the time to resolve an Outage Trouble Ticket for a Device under management</p> <p>Measurement Process The Customer’s TTR is based on the Outage time per Device for each Outage event. The TTR time starts when a Trouble Ticket is opened by Verizon or the Customer in response to an Outage and concludes with the restoration of Device and the WLAN interface.</p> <p>Where the maintenance contract has been purchased through Verizon Business, trouble tickets opened after 1 PM Pacific Time will be considered to be opened on the next business day. Where the customer purchases maintenance contract directly (through a third party and not from Verizon Business) and Verizon Business manages, trouble tickets opened after 4 PM Pacific Time will be considered to be opened the next business day. Repair & Replacement of CPE Stop-Clock conditions may apply.</p> <p>Business day hours are 8:00 AM to 5:00 PM PT.</p> <p>Device Time To Repair (Hrs.) = Length of Trouble Ticket resolution per Device per Outage incident</p> <p>Objectives By close of business Pacific Time on the next Business Day</p> <p>Immediate Rights and Remedies Customer will receive a credit equal to 5 percent (5%) of the monthly recurring charge for Managed WLAN TMRC for the affected Device.</p> <p>End-User Escalation Process OTech/STND Escalation Process</p> <p>Monthly Rights and Remedies N/A</p>

Page Intentionally Left Blank

6.3.14.2.19 a Standard Unavailable Device Notification – Monitoring Only and Management and Monitoring Security Service

Services	Standard Unavailable Device Notification – Security Services
<p>Monitoring Only, and Management and Monitoring service - Standard</p> <p><u>Applies to these services:</u> Firewalls</p> <p>Network Intrusion Detection System(NIDS)</p> <p>Network Intrusion Prevention System(NIPS)</p> <p>Managed SEM - (SEM tool only)</p>	<p>Definition Unavailable Device Notification is defined as the Service notifying the customer via email the Serviced Device is determined to be unavailable.</p> <p><u>Excludes these services:</u> Proxy Server</p> <p>Measurement Process Verizon monitors the availability of the Serviced Device 24x7 by sending a ping once every 2 minutes. If the Serviced Device does not respond to 3 out of 5 of consecutive pings, Verizon assumes it is unavailable. Once determined the device is unavailable, the event is given an SMC time stamp and a notification is provided to the customer via email. The referenced time is per the Security Management Center (SMC). A time stamp of the Incident creation is recorded at the Verizon SMC taken as reference for measuring the service level. The ending SLA timestamp is when the email notification is sent to the customer. A failure to generate an email notification is equivalent to a notification that took greater than 30 minutes.</p> <p>Objective (s) Not more than 1 missed or late notification for every 10 notification events during the month. The target time to generate the email notification is 30 minutes or less from the time the event is detected.</p> <p><u>Immediate Rights and Remedies</u> Credits will be calculated monthly. One (1) Credit will be remedied for missed SLA. One Device Credit equals the monthly recurring fee for the device divided by the number of days in the month of the event. If a series of cases of unmet target levels arise out of the same event, you will only be entitled to a single service credit. Service credits for any series of cases of unmet target levels will, in aggregate during any month, not exceed 50% of the recurring service fee payable for the affected serviced device during that month. Credit remedy is only available from the first full service month the SLA is effective.</p> <p>End-User Escalation Process OTech/STND Escalation Process</p> <p>Monthly Rights and Remedies This SLA is triggered on an immediate basis. Therefore, Monthly Rights and Remedies do not apply.</p>

6.3.14.2.19 b Standard Health Incident Notification – Monitoring Only, and Management and Monitoring Security Service

Services	Standard Health Incident Notification – Security Services
<p>Monitoring Only, and Management and Monitoring service - Standard</p> <p><u>Applies to these services:</u> Firewalls Network Intrusion Detection System (NIDS) Network Intrusion Prevention System (NIPS) Managed SEM - (SEM tool only)</p>	<p>Definition Health Incident Notification is defined as Notification via email in the event a monitored health parameter (e.g. Device CPU Usage, Memory Usage, Disk Usage, Network Usage) exceeds health threshold.</p> <p><u>Excludes these services:</u> Proxy Server</p> <p>Measurement Process Verizon monitors the health of the Serviced Device 24x7 by measuring a number of health parameters once every ten (10) minutes. In the event a monitored health parameter exceeds health threshold, the event is given an SMC time stamp and a notification is provided to the customer via email. The referenced time is per the Security Management Center (SMC). A time stamp of the Incident creation is recorded at the Verizon SMC taken as reference for measuring the service level. The ending SLA timestamp is when the email notification is sent to the customer. A failure to generate an email notification is equivalent to a notification that took greater than 30 minutes.</p> <p>Objective(s) Not more than 1 missed or late notification for every 10 notification events during the month. The target time to generate the email notification is 30 minutes or less from the time the event is detected.</p> <p>Immediate Rights and Remedies Credits will be calculated monthly. One (1) Credit will be remedied for missed SLA. One Device Credit equals the monthly recurring fee for the device divided by the number of days in the month of the event. If a series of cases of unmet target levels arise out of the same event, you will only be entitled to a single service credit. Service credits for any series of cases of unmet target levels will, in aggregate during any month, not exceed 50% of the recurring service fee payable for the affected serviced device during that month. Credit remedy is only available from the first full service month the SLA is effective.</p> <p>End-User Escalation Process OTech/STND Escalation Process</p> <p>Monthly Rights and Remedies This SLA is triggered on an immediate basis. Therefore, Monthly Rights and Remedies do not apply.</p>

6.3.14.2.19 c Standard Active Incident Escalation – Monitoring Only, and Management and Monitoring Security Service

Services	Standard Active Incident Escalation – Security Services
<p>Monitoring Only, and Management and Monitoring service - Standard</p> <p><u>Applies to these services:</u> Firewalls</p> <p>Network Intrusion Detection System (NIDS)</p> <p>Network Intrusion Prevention System (NIPS)</p> <p>Managed SEM - (SEM tool only)</p>	<p>Definition</p> <p>Active Incident Escalation is when a Harmful Attack Incident or Insufficient Info Incident is escalated via email to the customer.</p> <p>Excludes these services; Proxy Server</p> <p>Measurement Process</p> <p>When an incident is classified as a Harmful Attack Incident, or an Insufficient Info Incident, the Incident is given an SMC time stamp and a notification is provided to the customer via email. The referenced time is per the Security Management Center (SMC). A time stamp of the Incident creation is recorded at the Verizon SMC taken as reference for measuring the service level. The ending SLA timestamp is when the email notification is sent to the customer.</p> <p>Objective(s)</p> <p>Provides the minimum level that the Service needs to achieve in any particular month.</p> <p>Objective Levels for Incident Handling are:</p> <ul style="list-style-type: none"> • Not more than 1 in 100 Harmful Attack Incident notifications took more than 15 minutes but not more than 60 minutes to generate an email notification • Not more than 0 Harmful Attack Incident notifications took more than 60 minutes to generate an email notification • Not more than 5 in 100 Insufficient Info Incident notifications took more than 30 minutes but not more than 120 minutes to generate an email notification • Not more than 0 Insufficient Info Incident notifications took more than 120 minutes to generate an email notification <p>Immediate Rights and Remedies</p> <p>Credits will be calculated monthly. One (1) Credit will be remedied for missed SLA or (2) Credits for Harmful Attack Incident notification beyond 60 minutes. One Device Credit equals the monthly recurring fee for the device divided by the number of days in the month of the event. Credit remedy is only available from the first full service month the SLA is effective. Service credits for any series of cases of unmet target levels will, in aggregate during any month, not exceed 50% of the recurring service fee payable for the affected serviced device during that month.</p> <p>End-User Escalation Process</p> <p>OTech/STND Escalation Process</p>

Services	Standard Active Incident Escalation – Security Services
	Monthly Rights and Remedies This SLA is triggered on an immediate basis. Therefore, Monthly Rights and Remedies do not apply.

6.3.14.2.19 d Platinum Unavailable Device Notification – Monitoring Only, and Management and Monitoring Security Service

Services	Platinum Unavailable Device Notification – Security Services
<p>Monitoring Only, and Management and Monitoring service - Platinum</p> <p><u>Applies to these services:</u> Firewalls</p> <p>Network Intrusion Detection System (NIDS)</p> <p>Network Intrusion Prevention System (NIPS)</p> <p>Managed SEM - (SEM tool only)</p> <p>Proxy Server</p>	<p>Definition Unavailable Device Notification is defined as the Service notifying the customer via email and by phone the Serviced Device is determined to be unavailable.</p> <p>Measurement Process Verizon monitors the availability of the Serviced Device 24x7 by sending a ping once every 2 minutes. If the Serviced Device does not respond to 3 out of 5 of consecutive pings, Verizon assumes it is unavailable. Once determined the device is unavailable, the event is given an SMC time stamp and a notification is provided to the customer via email and phone. The referenced time is per the Security Management Center (SMC). A time stamp of the Incident creation is recorded at the Verizon SMC taken as reference for measuring the service level. The ending SLA timestamp is when the email and phone notification are sent to the customer. A failure to generate an email notification is equivalent to a notification that took greater than 15 minutes.</p> <p>Objective(s) Not more than 1 missed or late notification for every 10 notification events during the month. The target time to generate the email notification is 15 minutes or less from the time the event is detected.</p> <p>Immediate Rights and Remedies Credits will be calculated monthly. One (1) Credit will be remedied for missed SLA. One Device Credit equals the monthly recurring fee for the device divided by the number of days in the month of the event. If a series of cases of unmet target levels arise out of the same event, you will only be entitled to a single service credit. Service credits for any series of cases of unmet target levels will, in aggregate during any month, not exceed 50% of the recurring service fee payable for the affected serviced device during that month. Credit remedy is only available from the first full service month the SLA is effective.</p> <p>End-User Escalation Process OTech/STND Escalation Process</p> <p>Monthly Rights and Remedies This SLA is triggered on an immediate basis. Therefore,</p>

Services	Platinum Unavailable Device Notification – Security Services
	Monthly Rights and Remedies do not apply

6.3.14.2.19 e Platinum Health Incident Notification - Monitoring Only, and Management and Monitoring Security Service

Services	Platinum Health Incident Notification – Security Services
<p>Monitoring Only, and Management and Monitoring service - Platinum</p> <p><u>Applies to these services:</u> Firewalls Network Intrusion Detection System (NIDS) Network Intrusion Prevention System (NIPS) Managed SEM - (SEM tool only) Proxy Server</p>	<p>Definition Health Incident Notification is defined as Notification via email in the event a monitored health parameter (e.g. Device CPU Usage, Memory Usage, Disk Usage, Network Usage) exceeds health threshold.</p> <p>Measurement Process Verizon monitors the health of the Serviced Device 24x7 by measuring a number of health parameters once every ten (10) minutes. . In the event a monitored health parameter exceeds health threshold, the event is given an SMC time stamp and a notification is provided to the customer via email. The referenced time is per the Security Management Center (SMC). A time stamp of the Incident creation is recorded at the Verizon SMC taken as reference for measuring the service level. The ending SLA timestamp is when the customer is notified via email and phone. A failure to generate an email notification is equivalent to a notification that took greater than 15 minutes.</p> <p>Objective(s) Not more than 1 missed or late notification for every 10 notification events during the month. The target time to generate the email notification is 15 minutes or less from the time the event is detected.</p> <p>Immediate Rights and Remedies Credits will be calculated monthly. One (1) Credit will be remedied for missed SLA. One Device Credit equals the monthly recurring fee for the device divided by the number of days in the month of the event. If a series of cases of unmet target levels arise out of the same event, you will only be entitled to a single service credit. Service credits for any series of cases of unmet target levels will, in aggregate during any month, not exceed 50% of the recurring service fee payable for the affected serviced device during that month. Credit remedy is only available from the first full service month the SLA is effective.</p> <p>End-User Escalation Process OTech/STND Escalation Process</p> <p>Monthly Rights and Remedies This SLA is triggered on an immediate basis. Therefore, Monthly Rights and Remedies do not apply.</p>

6.3.14.2.19 f Platinum Active Incident Escalation - Monitoring Only, and Management and Monitoring Security Service

Services	Platinum Active Incident Escalation – Security Service
<p>Monitoring Only, and Management and Monitoring service - Platinum</p> <p><u>Applies to these services:</u></p> <p>Firewalls</p> <p>Network Intrusion Detection (NIDS)</p> <p>Network Intrusion Prevention (NIPS)</p> <p>Managed SEM - (SEM tool only)</p> <p>Proxy Server</p>	<p>Definition Active Incident Escalation is when a Harmful Attack Incident or Insufficient Info Incident is escalated to the customer.</p> <p>Measurement Process When an incident is classified as a Harmful Attack Incident or Insufficient Info Incident, the incident is given an SMC time stamp and a notification is provided to the customer via email for an Insufficient Info Incident or by email and phone for a Harmful Attack Incident. The referenced time is per the Security Management Center (SMC). A time stamp of the Incident creation is recorded at the Verizon SMC taken as reference for measuring the service level. The ending SLA timestamp is when the customer is notified via email or email and phone.</p> <p>Objective(s) Provides the minimum level that the Service needs to achieve in any particular month.</p> <p>Objective Levels for Incident Handling are:</p> <ul style="list-style-type: none"> • Not more than 1 in 100 Harmful Attack Incident notifications took more than 15 minutes but not more than 60 minutes to generate an email notification • Not more than 0 Harmful Attack Incident notifications took more than 60 minutes to generate an email notification • Not more than 5 in 100 Insufficient Info Incident notifications took more than 30 minutes but not more than 120 minutes to generate an email notification • Not more than 0 Insufficient Info Incident notifications took more than 120 minutes to generate an email notification <p>Immediate Rights and Remedies Credits will be calculated monthly. One (1) Credit will be remedied for missed SLA or two (2) Credits for Harmful Attack Incident notification beyond 60 minutes. One Device Credit equals the monthly recurring fee for the device divided by the number of days in the month of the event. Credit remedy is only available from the first full service month the SLA is effective. Service credits for any series of cases of unmet target levels will, in aggregate during any month, not exceed 50% of the recurring service fee payable for the affected serviced device during that month.</p> <p>End-User Escalation Process OTech/STND Escalation Process</p> <p>Monthly Rights and Remedies This SLA is triggered on an immediate basis. Therefore, Monthly Rights and Remedies do not apply.</p>

6.3.14.2.19 g Standard Change Request Acceptance – Management and Monitoring

Services	Standard Change Request Acceptance – Security Services
<p>Management and Monitoring - Standard</p> <p><u>Applies to these services:</u> Firewalls</p> <p>Network Intrusion Detection System (NIDS)</p> <p>Network Intrusion Prevention System (NIPS)</p> <p>Managed SEM (SEM) - (SEM tool only)</p>	<p>Definition</p> <p>Change Request Acceptance is defined as the acceptance of customer’s change request before implementation of the change request.</p> <p><u>Excludes these services:</u> Proxy Server</p> <p>Measurement Process</p> <p>The starting SLA timestamp begins with the submission of the customer change request recorded at the Service Management Center (SMC) submitted via the dashboard or by phone. The order will be given an “Open” status in the system. Once Verizon Business accepts the order for implementation the status will be updated to “Accepted” in the Security Dashboard. The Verizon Security Dashboard “Accepted” timestamp will constitute the ending SLA timestamp.</p> <p>Objective(s)</p> <p>The Service will provide acceptance of the customer change request in a time period not to exceed:</p> <ul style="list-style-type: none"> • 24 hours for a Regular Change Request • 4 hours for a Fast-track Change Request • 2 hours for an Urgent Change Request <p>Immediate Rights and Remedies</p> <p>Credits will be calculated monthly. One Device Credit equals the monthly recurring fee for the device divided by the number of days in the month of the event. Credit remedy is only available from the first full service month the SLA is effective.</p> <p>End-User Escalation Process OTech/STND Escalation Process</p> <p>Monthly Rights and Remedies</p> <p>This SLA is triggered on an immediate basis. Therefore, Monthly Rights and Remedies do not apply</p>

6.3.14.2.19 h Platinum Change Request Acceptance - Management and Monitoring

Services	Platinum Change Request Acceptance – Security Services
<p>Management and Monitoring - Platinum</p> <p><u>Applies to these services:</u> Firewalls</p> <p>Network Intrusion Detection System (NIDS)</p> <p>Network Intrusion Prevention System (NIPS)</p> <p>Managed SEM (SEM) -(SEM tool only)</p> <p>Proxy Server</p>	<p>Definition Change Request Acceptance is defined as the acceptance of customer’s change request before implementation of the change request.</p> <p>Measurement Process The starting SLA timestamp begins with the submission of the customer change request recorded at the Service Management Center (SMC) submitted via the dashboard or by phone. The order will be given an “Open” status in the system. Once Verizon Business accepts the order for implementation the status will be updated to “Accepted” in the Security Dashboard. The Verizon Security Dashboard “Accepted” timestamp will constitute the ending SLA timestamp.</p> <p>Objective(s) The Service will provide acceptance of the customer change request in a time period not to exceed:</p> <ul style="list-style-type: none"> • Within 24 hours of submission for a Regular Change Request • Within 1 hour of submission for a Fast-track Change Request • Within 1 hour of submission for an Urgent Change Request <p>Immediate Rights and Remedies Credits will be calculated monthly. One Device Credit equals the monthly recurring fee for the device divided by the number of days in the month of the event. Credit remedy is only available from the first full service month the SLA is effective.</p> <p>End-User Escalation Process OTech/STND Escalation Process</p> <p>Monthly Rights and Remedies This SLA is triggered on an immediate basis. Therefore, Monthly Rights and Remedies do not apply</p>

6.3.14.2.19 i Standard Change Request Implementation - Management and Monitoring

Services	Standard Change Request Implementation – Security Services
<p>Management and Monitoring - Standard</p> <p><u>Applies to these services:</u> Firewalls Network Intrusion Detection System (NIDS) Network Intrusion Prevention System (NIPS) Managed SEM (SEM) - (SEM tool only)</p>	<p>Definition Change Request Implementation is defined as the implementation of customer’s change.</p> <p><u>Excludes these services:</u> Proxy Server</p> <p>Measurement Process The start SLA timestamp is when the order is given the status of “Accepted” (for implementation) as recorded at the Verizon Service Management Center (SMC) taken as reference for measuring the service level. When the Change Request has been implemented and given the status of “Requiring your Validation” via the Security Dashboard, this constitutes the ending SLA timestamp.</p> <p>Objective(s) The Service will provide implementation of the customer change request in a time period not to exceed:</p> <ul style="list-style-type: none"> • In a scheduled maintenance window (mutually agreed time) for a Regular Change Request • Within 36 hours for a Fast-track Change Request • Within 8 hours for a Urgent Change Request <p>Immediate Rights and Remedies Credits will be calculated monthly. One Device Credit equals the monthly recurring fee for the device divided by the number of days in the month of the event. Credit remedy is only available from the first full service month the SLA is effective.</p> <p>End-User Escalation Process OTech/STND Escalation Process</p> <p>Monthly Rights and Remedies This SLA is triggered on an immediate basis. Therefore, Monthly Rights and Remedies do not apply.</p>

6.3.14.2.19 j Platinum Change Request Implementation - Management and Monitoring

Services	Platinum Change Request Implementation – Security Services
<p>Management and Monitoring - Platinum</p> <p><u>Applies to these services:</u> Firewalls</p> <p>Network Intrusion Detection System (NIDS)</p> <p>Network Intrusion Prevention System (NIPS)</p> <p>Managed SEM (SEM) - (SEM tool only)</p> <p>Proxy Server</p>	<p>Definition Change Request Implementation is defined as the implementation of customer’s change.</p> <p>Measurement Process The start SLA timestamp is when the order is given the status of “Accepted” (for implementation) as recorded at the Verizon Service Management Center (SMC) taken as reference for measuring the service level. When the Change Request has been implemented and given the status of “Requiring your Validation” via the Security Dashboard, this constitutes the ending SLA timestamp.</p> <p>Objective(s) The Service will provide implementation of the customer change request in a time period not to exceed:</p> <ul style="list-style-type: none"> • In a scheduled maintenance window (mutually agreed time) for a Regular Change Request • Within 36 hours for a Fast-track Change Request • Within 4 hours for a Urgent Change Request <p>Immediate Rights and Remedies Credits will be calculated monthly. One Device Credit equals the monthly recurring fee for the device divided by the number of days in the month of the event. Credit remedy is only available from the first full service month the SLA is effective.</p> <p>End-User Escalation Process OTech/STND Escalation Process</p> <p>Monthly Rights and Remedies This SLA is triggered on an immediate basis. Therefore, Monthly Rights and Remedies do not apply.</p>

6.3.14.3 Administrative Service Level Agreements (M)

SLAs have been established for various aspects of the administrative responsibilities associated with the Contract resulting from the award of the RFP for Module 3. Specific administrative responsibilities as described throughout this RFP Section 6.3. are included in this Section 6.3.14.3.

Bidder understands the Requirement and shall meet or exceed it? Yes X No _____

Reference: document _____

location _____ page _____ paragraph _____

Description:

Verizon understands and will comply with this requirement as specified.

6.3.14.3.1 Administrative Fee Reports/Electronic Fund Transfer Notification Delivery Intervals (M)

Administrative Tools, Reports and Applications	Administration Fee Reports Delivery Intervals
<p>OTech/STND Detail of Services Billed Report by Agency 6.3.15.2.3</p> <p>OTech/STND Detail of Services Billed Report by Service 6.3.15.2.2</p> <p>Receipt of Electronic Fund Transfer Notification</p>	<p>Definition</p> <p>The reports and electronic fund transfer notification include the total monthly administrative fee monies owed OTech/STND.</p> <p>Measurement Process</p> <p>These reports and electronic fund transfer shall be received within 60 calendar days from the end of each calendar month that a bill is rendered.</p> <p>Objectives</p> <p>Deliver reports and electronic fund transfer notification within 60 calendar days from the end of the calendar month that a bill is rendered.</p> <p>OTech/STND Rights and Remedies</p> <p>0.5 percent of month's administrative fees shall be paid to OTech/STND 61 calendar days from the end of each calendar month that a bill is rendered.</p> <p>Customer Rights and Remedies</p> <p>N/A</p>

Bidder understands the Requirement and shall meet or exceed it? Yes No

Reference: document _____

location _____ page _____ paragraph _____

Description:

Verizon understands and will comply with this requirement as specified.

6.3.14.3.2 Invoicing Accuracy (M)

Administrative Tools, Reports and Applications	Invoicing Accuracy
<p>Invoices for all proprietary products, services and features provided through CALNET II</p>	<p>Definition Contractor to provide detailed and accurate invoices as stated in RFP Section 6.3.11</p> <p>Measurement Process Contractor caused material errors occurring on an invoice shall be either corrected or a correction process established by Contractor within 60 days of the invoice.</p> <p>Objectives 100 percent invoice accuracy</p> <p>OTech/STND Rights and Remedies OTech/STND Escalation Process</p> <p>Customer Rights and Remedies Escalation to Contractor's Account Manager Escalation to OTech</p>

Bidder understands the Requirement and shall meet or exceed it? Yes No

Reference: document _____

location _____ page _____ paragraph _____

Description:

Verizon understands and will comply with this requirement as specified.

6.3.14.3.3 Report Delivery Intervals (M)

Administrative Tools, Reports, and Applications	Report Delivery Intervals
<p>Customer Inventory Report Section 6.3.16.5</p> <p>Service Level Agreement Reports Section 6.3.16.6</p> <p>OTech/STND Fiscal Inventory Report of All Services Section 6.3.15.2.1</p> <p>Trouble Ticket/SLA Credits Fiscal Report Section 6.3.15.2.4</p> <p>OTech/STND Service Order/Provisioning Fiscal Report Section 6.3.15.2.5</p> <p>DVBE Tracking Fiscal Report Section 6.3.15.2.6</p> <p>Service Location Report Section 6.3.15.2.7</p> <p>General Customer Profile Information Section 6.3.15.2.8</p> <p>Quarterly Completed Contracted Service Project Work Reports (Coordinated and Managed Projects) Section 6.3.17.1</p>	<p>Definition</p> <p>All reports shall meet the Requirements and be fully functional and provided in accordance with the timelines required in Section 6.3.16</p> <p>Measurement Process</p> <p>See the objectives below</p> <p>Objectives</p> <p>Deliver all reports within 3 Business Days of the mutually agreed or OTech/STND designated Delivery Dates from Section 6.3.16</p> <p>OTech/STND Rights and Remedies</p> <p>\$400 and \$100 per week thereafter for each report</p> <p>Customer Rights and Remedies</p> <p>Escalation to OTech/STND</p>

Administrative Tools, Reports, and Applications	Report Delivery Intervals
and Section 6.3.17.2	

Bidder understands the Requirement and shall meet or exceed it? Yes No

Reference: document _____

location _____ page _____ paragraph _____

Description:

Verizon understands and will comply with this requirement as specified.

6.3.14.3.4 Tools and Report Implementation (M)

Administrative Tools, Reports, and Applications	Tools and Report Implementation
Public Web Site Section 6.3.16.1 Private Web Site Section 6.3.16.2 Customer Trouble Ticket Reporting and Tracking System Section 6.3.16.3 Network Monitoring Application/Tool Section 6.3.16.4 Customer Inventory Report Section 6.3.16.5 Service Level Agreement Reports Section 6.3.16.6 Fiscal Management Databases Section	<p>Definition All Contactors provided tools and reports shall be functioning and accepted by the State based on the implementation timeline.</p> <p>Measurement Process Within 45 Business Days after Contract award, the Contractor and OTech/STND shall agree to the implementation timeline dates for the reports and tools listed in this table. Unless mutually agreed upon, the implementation timeline shall not exceed 9 months following the Contract award date.</p> <p>Objectives All tools and reports shall meet the Requirements and be fully functional and accepted by the State and provided in accordance with the timeline required in Section 6.3.18.1 and agreed upon by OTech/STND.</p>

Administrative Tools, Reports, and Applications	Tools and Report Implementation
<p>6.3.15.2 OTech/STND Fiscal Inventory Report of All Services Section 6.3.15.2.1 OTech/STND Detail of Services Billed Report by Service Section 6.3.15.2.2 OTech/STND Detail of Services Billed Report by Agency Section 6.3.15.2.3 Trouble Ticket/SLS Credits Fiscal Report Section 6.3.15.2.4 OTech/STND Service Order/Provisioning Fiscal Report Section 6.3.15.2.5 DVBE Tracking Fiscal Report Section 6.3.15.2.6 Service Location Report Section 6.3.15.2.7 General Customer Profile Information Section 6.3.15.2.8</p>	<p>Additional or replacement tools and reports shall be fully functional and accepted by the State by dates agreed upon by OTech/STND and the Contractor.</p> <p>OTech/STND Rights and Remedies \$1000 per tool/report on the first Business Day after due date and \$250 per week thereafter</p> <p>Customer Rights and Remedies N/A</p>

Bidder understands the Requirement and shall meet or exceed it? Yes No

Reference: document _____

location _____ page _____ paragraph _____

Description:

Verizon understands and will comply with this requirement as specified.

6.3.14.3.5 Tool Availability (M)

Administrative Tools, Reports, and Applications	Tool Availability
<p>Public Web Site Section 6.3.16.1</p> <p>Private Web Site Section 6.3.16.2</p> <p>Customer Trouble Ticket and Tracking System Section 6.3.16.3</p> <p>Network Monitoring Application/Tool Section 6.3.16.4</p> <p>Fiscal Management Database(s) Section 6.3.15.1</p>	<p>Definition</p> <p>The monthly availability percentage for each tool equals the Scheduled Uptime per month less Unavailable Time divided by Scheduled Uptime per month multiplied by 100 per tool. Scheduled uptime is based on 7x24 x number of days in the month.</p> <p>Measurement Process</p> <p>OTech/STND shall report any failure or problem to the Customer Service center and a trouble ticket shall be opened.</p> <p>The tool is unusable during the time the ticket is recorded as open until restoration of the tool. Stop clocks in Section 6.3.14.2.2 shall apply.</p> <p>The Availability percent shall be calculated by adding the duration times for all trouble tickets opened on a single tool within the calendar month.</p> <p>Objectives</p> <p>100 percent Functional 90percent of the time for each tool, measured on a monthly basis.</p> <p>OTech/STND Rights and Remedies</p> <p>\$400 per month, per tool</p> <p>Customer Rights and Remedies</p> <p>Escalation to OTech/STND</p>

Bidder understands the Requirement and shall meet or exceed it? Yes No

Reference: document _____

location _____ page _____ paragraph _____

Description:

Verizon understands and will comply with this requirement as specified.

6.3.14.4 Glossary of SLA Related Terms (M)

The following SLA definitions apply to this Contract:

SLA	Definition
Availability percent	The Scheduled Uptime less Unavailable Time divided by Scheduled Uptime multiplied by 100.
Average Monthly Usage Cost (AMUC)	A means of calculating rights and remedies for usage-based outages. AMUC shall be derived by dividing the total business day usage minutes in a month by the number of business days in the month in which the failure occurs. This will produce a daily average of usage minutes which can be multiplied by the cost for the associated service to produce an average daily cost of the service for the current month. AMUC rights and remedies will be a number of those average daily costs rebated back to the customers impacted by the service outages that trigger the associated service level agreements.
Catastrophic Outage 1 CAT 1	The total loss of service to 50 or greater End-Users at the same address.
Catastrophic Outage 2 CAT 2	A total failure of the Contractor's (or subcontractor's or Affiliate's) network Equipment nearest the End-User locations regardless of where the failure occurs in the network.
Catastrophic Outage 3 CAT 3	The total loss of any service type on a network wide basis.
CAT Outage	Catastrophic outage as further defined above for CAT 1, CAT 2, and CAT 3 outages.
Excessive Outage	An Excessive outage shall be defined as a trouble ticket opened with the Contractor on a service, for more than twelve hours
IP Contact Center Service Outage	The total loss of an IP Contact Center Service at a single End-User location.
Jitter	Variations in transfer delay measured from Contractor to Customer hand-off to remote Contractor to Customer hand-off (CCH to CCH).
Mean Time to Respond	The time it takes the Contractor to call back the Customer acknowledging receipt of the trouble ticket or incident report by the Contractor helpdesk personnel.
Packet Loss	Packet loss measured from Contractor's hand off to Customer at each end of data channel.
Response Duration from Receipt of Order	The interval for Contractor response to initial request from Customer when initiating a project request.
Provisioning	New service, adds, moves and changes.
Scheduled Uptime	The total time less time required for scheduled maintenance or scheduled upgrades

SLA	Definition
Total Monthly Recurring Charges (TMRC)	The monthly recurring charges for the transport and service. All charges that comprise the total monthly reoccurring cost per service.
Transmission Delay	Round trip: the average round trip transfer delay measured from Contractor to Customer Hand-Off One way: the average one way transfer delay measured from Customer Hand-Off
Unavailable Time	Includes Catastrophic Outages. The total hours from when a trouble ticket is opened until the problem is restored minus stop clock condition durations.

Bidder understands the Requirement and shall meet or exceed it? Yes X No _____

Reference: document _____

location _____ page _____ paragraph _____

Description:

Verizon understands and will comply with this requirement as specified.

Section 6.3 Internet Protocol Services – MODULE 3

TABLE OF CONTENTS

6.3	INTERNET PROTOCOL SERVICES.....	6
6.3.1	MODULE 3 RFP REQUIREMENTS.....	15
6.3.1.1	Designation Of Requirements.....	15
6.3.1.2	Compliance With Section 4 (M)	17
6.3.2	HOSTED STANDALONE IP TELEPHONY SERVICES (M-O)	17
6.3.2.1	Hosted Standalone IP Telephony Business Line Services (M-O)	29
6.3.2.2	Hosted Standalone IP Telephony Business Line Service Customer Provided Equipment (CPE) (M-O)	37
6.3.2.3	Hosted Standalone IP Telephony features (M).....	40
6.3.2.3.1	Echo Cancellation Support (M).....	40
6.3.2.3.2	Voice Compression (M)	42
6.3.2.3.3	Packet Play-Out Algorithms (M)	43
6.3.2.3.4	Tone Processing (M)	44
6.3.2.3.5	Fax Support (M)	45
6.3.2.3.6	Packet Encapsulation (M)	45
6.3.2.3.7	Signaling Support (M).....	46
6.3.2.3.8	Network Management (M).....	47
6.3.2.3.9	Hosted Standalone IP Telephony Security (M).....	48
6.3.2.4	Hosted Standalone IP Telephony Voice Mail Services (M-O).....	51
6.3.2.5	Hosted Standalone IP Telephony Audio Conferencing (M-O).....	54
6.3.2.6	Statewide Hosted Standalone IP Telephony Services in Additional Specific Geographic Locations/Availability (D).....	66
6.3.3	IP TRANSPORT FOR CONVERGED SERVICES (M).....	75
6.3.3.1	Security (M).....	79
6.3.3.2	Traffic Engineering and Quality of Service (QoS) (M).....	83
6.3.3.3	Multi-Protocol Support (M).....	86
6.3.3.4	Quality of Service Interoperability (M)	88
6.3.3.5	Unified Network Management (M)	89
6.3.3.6	Network Considerations (M)	92
6.3.3.7	Multiple Classes of Service (COS) (M).....	95
6.3.3.8	IP and Network IP Transport Services (M-O)	97
6.3.4	CONVERGED SERVICES, IP TELEPHONY SERVICES (M-O)	125
6.3.4.1	Converged Services, IP Phone Hardware features (M-O):.....	134
6.3.4.2	Converged Services, IP Telephony features: (M-O).....	138
6.3.4.2.1	Echo Cancellation (M-O)	138
6.3.4.2.2	Voice Compression (M-O).....	140
6.3.4.2.3	Packet Play-Out Algorithms (M-O)	140

6.3.4.2.4	Tone Processing (M-O)	141
6.3.4.2.5	Fax Support (M-O)	142
6.3.4.2.6	Packet Encapsulation (M-O)	143
6.3.4.2.7	Signaling Support (M-O)	144
6.3.4.2.8	Network Management (M-O)	144
6.3.4.3	Converged Services, IP Telephony Business Line Services (M-O)	146
6.3.4.4	Converged Services, IP Telephony Security (M)	155
6.3.4.5	Converged Services, IP Telephony Voice Mail Services (M-O)	158
6.3.4.6	Converged Services, Managed IP Audio Conferencing (M-O)	161
6.3.5	CONVERGED SERVICES, IP CONTACT CENTER APPLICATIONS (M-O)	172
6.3.5.1	IP Network Based Automatic Call Distributor (ACD) (M-O)	172
6.3.5.1.1	IP Network Based Basic Agent Package (M-O)	177
6.3.5.1.2	IP Network Based Basic Supervisor's Package (M-O)	181
6.3.5.1.3	IP Network Based System Administrator Software Package(M-O)	186
6.3.5.1.4	Management Information System Tracking For Contact Centers (M-O)	188
6.3.5.1.5	IP Network Contact Center Maintenance (M)	194
6.3.5.1.6	Additional Maintenance Options (M-O)	197
6.3.5.2	IP Network Based Interactive Voice Response (IVR) System (M-O)	198
6.3.5.3	IP Network Based Specialized Call Routing (M-O)	214
6.3.5.4	Computer Telephone Integration (CTI) for IP Network Based ACD (M-O)	218
6.3.6	CONVERGED SERVICES, IP COMMUNICATION APPLICATIONS – OTHER SERVICES (M-O)	221
6.3.6.1	Managed IP Video Conferencing Services (M-O)	221
6.3.6.2	Unified Messaging (D)	227
6.3.7	GENERAL TRAINING REQUIREMENTS (M)	233
6.3.7.1	Orientation and Training (M)	239
6.3.7.2	Contract Services Training (M)	242
6.3.7.3	Contract Management Training (M)	245
6.3.7.4	Training Plan (M)	247
6.3.7.5	Training Oversight & Coordination (M)	249
6.3.8	OTHER SERVICES (M-O)	250
6.3.8.1	Cable And Wire Services (M-O)	250
6.3.8.1.1	Simple Wiring Services, Extended Termination Wiring Services (M-O)	250
6.3.8.1.2	Station Wiring Services (D)	252
6.3.8.1.3	Inside Wiring Services (D)	255

6.3.8.2	Services Related Hourly Support (M-O)	258
6.3.9	REQUIRED CUSTOMER PREMISE EQUIPMENT (CPE)	259
6.3.10	END-USER SUPPORT (M)	264
6.3.10.1	General Requirements (M)	264
6.3.10.1.2	Contractor's General Responsibilities (M)	266
6.3.10.2	Planning (M)	270
6.3.10.3	Design (M)	272
6.3.10.4	Provisioning and Implementation Requirements (M)	274
6.3.10.5	Marketing Requirements (M)	277
6.3.11	INVOICING SERVICES (M)	280
6.3.11.1	Invoicing System for Voice & Data Services (M)	281
6.3.11.1.1	Invoicing System Requirements (M)	287
6.3.11.1.2	Flexible Billing Cycles (D)	288
6.3.11.1.3	Addition of New Fields (D)	289
6.3.11.1.4	Automated Refunds (D)	289
6.3.11.1.5	Customer Management Software (D)	290
6.3.11.1.6	DTS/STND Report Management (D)	293
6.3.11.1.7	Invoice Content Requirements (M)	293
6.3.11.1.8	General Invoice System Requirements (M)	295
6.3.11.2	Fraud Detection and Monitoring Services (M)	298
6.3.11.3	Back Billing (M)	303
6.3.11.4	Invoice Audits (M)	304
6.3.11.4.1	Audits (M)	304
6.3.11.4.2	Contractor Invoice Audit Responsibility (M)	306
6.3.11.5	Administrative Fee Collection (M)	306
6.3.11.6	California State Accounting and Reporting System (CALSTARS) (D)	309
6.3.12	CONTRACTED SERVICE PROJECT WORK (M)	314
6.3.12.1	Coordinated Project Work (M)	314
6.3.12.2	Managed Project Work (M)	317
6.3.13	CUSTOMER ADVOCACY (M)	320
6.3.13.1	Customer Service Center (M)	321
6.3.13.2	Escalation Process (M)	323
6.3.13.2.1	Escalation Plan (M)	324
6.3.13.2.2	Technical Resources (M)	325
6.3.13.2.3	Network Outage Response (M)	326
6.3.14	SERVICE LEVEL AGREEMENTS (SLA) (M)	328
6.3.14.1	Service Level Agreement Overview (M)	328
6.3.14.1.1	Technical Requirements versus SLA (M)	330
6.3.14.1.2	Two Methods Of Outage Reporting:	

Customer Or Contractor (M).....	331
6.3.14.2 Network Service Level Agreements (M).....	338
6.3.14.2.1 General Requirements (M).....	338
6.3.14.2.2 Trouble Ticket Stop Clock Conditions (M)	339
6.3.14.2.3 Service Availability Percentage (M)	342
6.3.14.2.3.1 Service Availability Percentage (M) – Converged Services, IP and Network IP Transport Services	343-a
6.3.14.2.3.2 Service Availability Percentage (M) – Dan	344
6.3.14.2.3.3 Service Availability Percentage (M) - Managed Router and Managed LAN Service	345
6.3.14.2.4 Catastrophic Outage 1 (M)	347
6.3.14.2.5 Catastrophic Outage 2 (M)	348
6.3.14.2.6 Catastrophic Outage 3 (M)	349
6.3.14.2.7 Round Trip Transmission Delay (M)	350
6.3.14.2.8 One-Way Transmission Delay (M)	351
6.3.14.2.9 Jitter (M).....	353
6.3.14.2.9.1 Jitter – IDA.....	354
6.3.14.2.9.2 Latency – IDA	355
6.3.14.2.10 Packet Loss (M)	356
6.3.14.2.10.1 Packet Loss – IDA.....	357
6.3.14.2.11 IP Contact Center Service Outage (M)	359
6.3.14.2.12 Excessive Outage (M).....	360
6.3.14.2.13 Notification (M).....	362
6.3.14.2.13.1 Proactive Notification SLA – Managed Router and Managed LAN Service/WLAN Service	363
6.3.14.2.14 Provisioning (M).....	364
6.3.14.2.15 Response Duration from Receipt of Order (M)	368
6.3.14.2.16 Time to Repair (TTR) – Major.....	368-a
6.3.14.2.17 Time to Repair (TTR) – Minor.....	368-b
6.3.14.2.18 Time to Repair (TTR) – Managed Wireless LAN (WLAN) Service.....	368-c
6.3.14.2.19 a Standard Unavailable Device Notification – Monitoring Only and Management and Monitoring Security Service	368-e
6.3.14.2.19 b Standard Health Incident Notification – Monitoring Only, and Management and Monitoring Security Service	368-f
6.3.14.2.19 c Standard Active Incident Escalation – Monitoring Only, and Management and Monitoring Security Service	368-g

6.3.14.2.19 d	Platinum Unavailable Device Notification – Monitoring Only, and Management and Monitoring Security Service	368-i
6.3.14.2.19 e	Platinum Health Incident Notification - Monitoring Only, and Management and Monitoring Security Service	368-k
6.3.14.2.19 f	Platinum Active Incident Escalation - Monitoring Only, and Management and Monitoring Security Service	368-l
6.3.14.2.19 g	Standard Change Request Acceptance – Management and Monitoring	368-m
6.3.14.2.19 h	Platinum Change Request Acceptance - Management and Monitoring	368-n
6.3.14.2.19 i	Standard Change Request Implementation - Management and Monitoring	368-o
6.3.14.2.19 j	Platinum Change Request Implementation - Management and Monitoring	368-p
6.3.14.3	Administrative Service Level Agreements (M).....	369
6.3.14.3.1	Administrative Fee Reports/Electronic Fund Transfer Notification Delivery Intervals (M).....	369
6.3.14.3.2	Invoicing Accuracy (M)	370
6.3.14.3.3	Report Delivery Intervals (M).....	371
6.3.14.3.4	Tools and Report Implementation (M).....	372
6.3.14.3.5	Tool Availability (M)	374
6.3.14.4	Glossary of SLA Related Terms (M).....	375
6.3.15	FISCAL MANAGEMENT (M)	377
6.3.15.1	Fiscal Management Database(s) (M)	380
6.3.15.2	Fiscal Management Reports (M)	382
6.3.15.2.1	DTS/ONS Fiscal Inventory Report of All Services (M)	385
6.3.15.2.2	DTS/ONS Detail of Services Billed Report by Service (M).....	387
6.3.15.2.3	DTS/ONS Detail of Services Billed Report by Agency (M)	389
6.3.15.2.4	Trouble Ticket/SLA Credits Fiscal Report (M)	391
6.3.15.2.5	DTS/ONS Service Order/Provisioning Fiscal Report (M).....	393
6.3.15.2.6	DVBE Tracking Fiscal Report (M)	394
6.3.15.2.7	Service Location Report (M).....	396
6.3.15.2.8	General Customer Profile Information (M).....	397
6.3.15.3	DTS/ONS Fiscal Audits (M)	398
6.3.16	MANAGEMENT TOOLS AND REPORTS (M)	399
6.3.16.1	Public Web Site (M)	403
6.3.16.2	Private Web Site (M)	405

6.3.16.3	Customer Trouble Ticket Reporting and Tracking System (M).....	408
6.3.16.4	Network Monitoring Application/Tool.....	416
6.3.16.5	Customer Inventory Report (M).....	417
6.3.16.6	Service Level Agreement (SLA) Reports (M)	418
6.3.16.6.2	SLA Provisioning Report Requirements (M).....	420
6.3.16.6.3	CAT 1, 2 and 3 SLA Report Requirements (M)	421
6.3.17	CONTRACTED SERVICE PROJECT WORK REPORTS (M).....	422
6.3.17.1	Coordinated Project Work Report (M)	422
6.3.17.2	Managed Project Work Report (M)	424
6.3.18	REQUIRED MIGRATION AND TRANSITION STRATEGY (M)	426
6.3.18.1	Migration Plan Requirements of Startup (M)	427
6.3.18.2	Transition-Out Requirements of Termination (M).....	454

Verizon Figures and Tables

Figure 6.3-1.	Standalone IP Telephony Solution.....	11
Figure 6.3-2.	Converged Services IP Transport.....	12
Figure 6.3-3.	Converged IP Telephony Solution.....	13
Figure 6.3-4.	Converged Services - IP Contact Center Applications	14
Figure 6.3-1 (Repeated).	Standalone IP Telephony Solution	27
Figure 6.3.2.3.9-1.	Layered Security Model.....	50
Figure 6.3.2.5-1.	IP Telephony Audio Conferencing	56
Figure 6.3-2 (Repeated).	Converged Services IP Transport	79
Table 6.3.3.5-1.	Managed WAN Services	90
Table 6.3.3.5-2.	Managed Services.....	91
Table 6.3.3.5-3.	Fault Resolution Responsibilities by Service Level.....	91
Figure 6.3.3.6-1.	PIP Network	92
Figure 6.3.3.6-2.	Layer 2	93
Figure 6.3.3.6-3.	Verizon PIP VPN	93
Figure 6.3.3.6-4.	Connectionless IP Traffic.....	94
Table 6.3.3.7-1.	Five Classes of Service.....	96
Figure 6.3-3 (Repeated).	Converged IP Telephony Solution	131
Figure 6.3.4-1.	Vivinet Assessor.....	133
Figure 6.3.4.4-1.	Layered Security Model.....	157
Table 6.3.5.1.4-1.	Additional MIS Tracking System Reports	191
Figure 6.3.14.1.2-1.	IMPACT Architecture.....	336