



General Services Administration NS2020 Enterprise Infrastructure Solutions (EIS)

Volume 1: Technical

Solicitation Number: QTA0015THA3003
February 22, 2016

Submitted to:

General Services Administration
Mr. Timothy Horan
FAS EIS Contracting Officer
1800 F St NW
Washington DC 20405-0001

Submitted by:

Verizon
22001 Loudoun County Parkway
Ashburn, VA 20147

Verizon Point of Contact:

Kevin K. Anderson
Sr. Contract Manager
703-886-2647 (Office)
571-271-8456 (Mobile)
kevin.k.anderson@verizon.com

Verizon Bidding Entity:

Verizon Business Network Services Inc. on behalf of MCI Communications Services, Inc. d/b/a Verizon Business Services and any additional Verizon entities providing service to the Government for this project (individually and collectively, "Verizon"). Local services are performed by the Verizon ILEC or CLEC in the jurisdiction where services are provided. International services are performed by the appropriate Verizon operating company in the foreign jurisdiction.

Copyright © 2016 Verizon. All Rights Reserved.

This proposal includes data that shall not be disclosed outside the Government and shall not be duplicated, used, or disclosed—in whole or in part—for any purpose other than to evaluate this proposal. If, however, a contract is awarded to this offeror as a result of—or in connection with—the submission of this data, the Government shall have the right to duplicate, use, or disclose the data to the extent provided in the resulting contract. This restriction does not limit the Government's right to use information contained in this data if it is obtained from another source without restriction. The data subject to this restriction are contained in sheets marked with the following disclaimer:

"Use or disclosure of data contained on this sheet is subject to the restriction on the title page of this proposal."

TABLE OF CONTENTS

Executive Summary	1
1 Network Architecture	4
1.1 Understanding [L.29.1, M.2.1]	4
1.1.1 Verizon's Evolving Intelligent Networking Services	7
1.1.2 Verizon OneNetwork	9
1.1.3 Verizon Wireless Service (MWS) and Integration	10
1.2 Compliance with EIS Service Requirements [J.19].....	10
1.3 Quality of Services [L.29.1, M.2.1]	11
1.3.1 Verizon Quality Service Delivery Architecture	11
1.3.1.1 Compliance with Standards.....	11
1.3.1.2 Experienced Personnel	12
1.3.1.3 Service Lifecycle	12
1.3.2 Quality Ordering, Billing and Reporting Services.....	12
1.3.2.1 Enterprise Business Support System (BSS)	13
1.3.2.2 Customer Enablement Portals	13
1.3.2.3 Ordering/Provisioning	13
1.3.2.4 EIS BSS Sensitive Government Data.....	14
1.3.2.5 Enterprise Service Billing	14
1.3.3 Adherence to Service Levels	14
1.3.3.1 Verizon Labs and Test Centers	14
1.4 Service Coverage [L.29.1, M.2.1].....	16
1.5 Security [L.29.1, M.2.1].....	16
1.5.1 Risk Management Framework Plans	17
1.5.2 External Traffic Routing (ETR).....	17
1.6 SOW Items.....	18
2 Technical Response to EIS Services [L.29].....	19
2.1 Data Services [C.2.1].....	19
2.1.1 Virtual Private Network Service (VPNS) [C.2.1.1]	19
2.1.1.1 Understanding [L.29.2.1, M.2.1]	19
2.1.1.2 Quality of Services [L.29.2.1, M.2.1].....	24
2.1.1.3 Service Coverage [L.29.2.1, M.2.1].....	27
2.1.1.4 Security [L.29.2.1, M.2.1]	27
2.1.2 Ethernet Transport Service (ETS) [C.2.1.2].....	30
2.1.2.1 Understanding [L.29.2.1, M.2.1]	30
2.1.2.2 Quality of Services [L.29.2.1, M.2.1].....	38
2.1.2.3 Service Coverage [L.29.2.1, M.2.1].....	39
2.1.2.4 Security [L.29.2.1, M.2.1]	39
2.1.3 Optical Wave Service (OWS) [C.2.1.3]	40
2.1.3.1 Understanding [L.29.2.1, M.2.1]	40
2.1.3.2 Quality of Services [L.29.2.1, M.2.1].....	43
2.1.3.3 Service Coverage [L.29.2.1, M.2.1].....	43
2.1.3.4 Security [L.29.2.1, M.2.1]	43
2.1.4 Private Line Service (PLS) [C.2.1.4]	44
2.1.4.1 Understanding [L.29.2.1, M.2.1]	44
2.1.4.2 Quality of Services [L.29.2.1, M.2.1].....	45
2.1.4.3 Service Coverage [L.29.2.1, M.2.1].....	46
2.1.4.4 Security [L.29.2.1, M.2.1]	46
2.1.5 Synchronous Optical Network Service (SONETS) [C.2.1.5]	47
2.1.5.1 Understanding [L.29.2.1, M.2.1]	47
2.1.5.2 Quality of Services [L.29.2.1, M.2.1].....	51

2.1.5.3	Service Coverage [L.29.2.1, M.2.1]	52
2.1.5.4	Security [L.29.2.1, M.2.1]	52
2.1.6	Dark Fiber Service (DFS) [C.2.1.6]	52
2.1.6.1	Understanding [L.29.2.1, M.2.1]	52
2.1.6.2	Quality of Services [L.29.2.1, M.2.1]	56
2.1.6.3	Service Coverage [L.29.2.1, M.2.1]	56
2.1.6.4	Security [L.29.2.1, M.2.1]	56
2.1.7	Internet Protocol Service (IPS) [C.2.1.7]	57
2.1.7.1	Understanding [L.29.2.1, M.2.1]	57
2.1.7.2	Quality of Services [L.29.2.1, M.2.1]	59
2.1.7.3	Service Coverage [L.29.2.1, M.2.1]	60
2.1.7.4	Security [L.29.2.1, M.2.1]	60
2.2	Voice Services [C.2.2]	61
2.2.1	Internet Protocol Voice Service (IPVS) [C.2.2.1]	61
2.2.1.1	Understanding [L.29.2.1, M.2.1]	61
2.2.1.2	Quality of Services [L.29.2.1, M.2.1]	71
2.2.1.3	Service Coverage [L.29.2.1, M.2.1]	72
2.2.1.4	Security [L.29.2.1, M.2.1]	72
2.2.2	Circuit Switched Voice Service (CSVS) [C.2.2.2]	73
2.2.2.1	Understanding [L.29.2.1, M.2.1]	73
2.2.2.2	Quality of Services [L.29.2.1, M.2.1]	74
2.2.2.3	Service Coverage [L.29.2.1, M.2.1]	74
2.2.2.4	Security [L.29.2.1, M.2.1]	74
2.2.3	Toll Free Service (TFS) [C.2.2.3]	74
2.2.3.1	Understanding [L.29.2.1, M.2.1]	74
2.2.3.2	Quality of Services [L.29.2.1, M.2.1]	76
2.2.3.3	Service Coverage [L.29.2.1, M.2.1]	77
2.2.3.4	Security [L.29.2.1, M.2.1]	77
2.2.4	Circuit Switched Data Service (CSDS) [C.2.2.4]	77
2.2.4.1	Understanding [L.29.2.1, M.2.1]	77
2.2.4.2	Quality of Services [L.29.2.1, M.2.1]	79
2.2.4.3	Service Coverage [L.29.2.1, M.2.1]	79
2.2.4.4	Security [L.29.2.1, M.2.1]	79
2.3	Contact Center Service [C.2.3]	80
2.3.1	Understanding [L.29.2.1, M.2.1]	80
2.3.1.1	Compliance with EIS Service Requirements [J.19]	81
2.3.2	Quality of Services [L.29.2.1, M.2.1]	92
2.3.3	Service Coverage [L.29.2.1, M.2.1]	93
2.3.4	Security [L.29.2.1, M.2.1]	93
2.4	Colocated Hosting Services (CHS) [C.2.4]	93
2.4.1	Understanding [L.29.2.1, M.2.1]	93
2.4.1.1	Compliance with EIS Service Requirements [J.19]	94
2.4.2	Quality of Services [L.29.2.1, M.2.1]	96
2.4.3	Service Coverage [L.29.2.1, M.2.1]	97
2.4.4	Security [L.29.2.1, M.2.1]	97
2.5	Cloud Service (Cloud) [C.2.5]	98
2.5.1	Infrastructure as a Service (IaaS) [C.2.5.1]	99
2.5.1.1	Understanding [L.29.2.1, M.2.1]	99
2.5.1.2	Quality of Services [L.29.2.1, M.2.1]	105
2.5.1.3	Service Coverage [L.29.2.1, M.2.1]	106
2.5.1.4	Security [L.29.2.1, M.2.1]	106
2.5.2	Platform as a Service [C.2.5.2]	107

2.5.2.1	Understanding [L.29.2.1, M.2.1]	107
2.5.2.2	Quality of Services [L.29.2.1, M.2.1]	110
2.5.2.3	Service Coverage [L.29.2.1, M.2.1]	110
2.5.2.4	Security [L.29.2.1, M.2.1]	110
2.5.3	Software as a Service [C.2.5.3]	111
2.5.3.1	Understanding [L.29.2.1, M.2.1]	111
2.5.3.2	Quality of Services [L.29.2.1, M.2.1]	114
2.5.3.3	Service Coverage [L.29.2.1, M.2.1]	114
2.5.3.4	Security [L.29.2.1, M.2.1]	114
2.5.4	Content Delivery Network Service	115
2.5.4.1	Understanding [L.29.2.1, M.2.1]	115
2.5.4.1	Compliance with EIS Service Requirements [J.19]	118
2.5.4.2	Quality of Services [L.29.2.1, M.2.1]	118
2.5.4.3	Service Coverage [L.29.2.1, M.2.1]	120
2.5.4.4	Security [L.29.2.1, M.2.1]	120
2.6	Wireless Service (MWS) [C.2.6]	120
2.6.1	Understanding [L.29.2.1, M.2.1]	120
2.6.1.1	Compliance with EIS Service Requirements [J.19]	121
2.6.2	Quality of Services [L.29.2.1, M.2.1]	123
2.6.3	Service Coverage [L.29.2.1, M.2.1]	125
2.6.4	Security [L.29.2.1, M.2.1]	125
2.7	Commercial Satellite Communications Service [C.2.7]	126
2.7.1	Understanding [L.29.2.1, M.2.1]	126
2.7.1.1	Compliance with EIS Service Requirements [J.19]	126
2.7.2	Quality of Services [L.29.2.1, M.2.1]	128
2.7.3	Service Coverage [L.29.2.1, M.2.1]	130
2.7.4	Security [L.29.2.1, M.2.1]	130
2.8	Managed Service [C.2.8]	131
2.8.1	Managed Network Service (MNS) [C.2.8.1]	132
2.8.1.1	Understanding [L.29.2.1, M.2.1]	132
2.8.1.2	Quality of Services [L.29.2.1, M.2.1]	138
2.8.1.3	Service Coverage [L.29.2.1, M.2.1]	143
2.8.1.4	Security [L.29.2.1, M.2.1]	143
2.8.2	Web Conferencing Service (WCS) [C.2.8.2]	144
2.8.2.1	Understanding [L.29.2.1, M.2.1]	144
2.8.2.1.1	Compliance with EIS Service Requirements [J.19]	145
2.8.2.2	Quality of Services [L.29.2.1, M.2.1]	152
2.8.2.3	Service Coverage [L.29.2.1, M.2.1]	152
2.8.2.4	Security [L.29.2.1, M.2.1]	152
2.8.3	Unified Communication Service (UCS) [C.2.8.3]	153
2.8.3.1	Understanding [L.29.2.1, M.2.1]	153
2.8.3.2	Compliance with EIS Service Requirements [J.19]	154
2.8.3.2	Quality of Services [L.29.2.1, M.2.1]	157
2.8.3.3	Service Coverage [L.29.2.1, M.2.1]	158
2.8.3.4	Security [L.29.2.1, M.2.1]	158
2.8.4	Managed Trusted Internet Protocol Service (MTIPS) [C.2.8.4]	159
2.8.4.1	Understanding [L.29.2.1, M.2.1]	159
2.8.4.1.1	Compliance with EIS Service Requirements [J.19]	163
2.8.4.2	Quality of Services [L.29.2.1, M.2.1]	170
2.8.4.3	Service Coverage [L.29.2.1, M.2.1]	171
2.8.4.4	Security [L.29.2.1, M.2.1]	171
2.8.5	Managed Security Services (MSS) [C.2.8.5]	172

2.8.5.1	Understanding [L.29.2.1, M.2.1]	172
2.8.5.2	Quality of Services [L.29.2.1, M.2.1]	192
2.8.5.3	Service Coverage [L.29.2.1, M.2.1]	193
2.8.5.4	Security [L.29.2.1, M.2.1]	193
2.8.6	Managed Mobility Service [C.2.8.6]	193
2.8.6.1	Understanding [L.29.2.1, M.2.1]	193
2.8.6.2	Quality of Services [L.29.2.1, M.2.1]	199
2.8.6.3	Service Coverage [L.29.2.1, M.2.1]	200
2.8.6.4	Security [L.29.2.1, M.2.1]	200
2.8.7	Audio Conferencing Service (ACS) [C.2.8.7]	201
2.8.7.1	Understanding [L.29.2.1, M.2.1]	201
2.8.7.1.1	Compliance with EIS Service Requirements [J.19]	202
2.8.7.2	Quality of Services [L.29.2.1, M.2.1]	205
2.8.7.3	Service Coverage [L.29.2.1, M.2.1]	206
2.8.7.4	Security [L.29.2.1, M.2.1]	206
2.8.8	Video Teleconferencing Service (VTS) [C.2.8.8]	207
2.8.8.1	Understanding [L.29.2.1, M.2.1]	207
2.8.8.1.1	EIS Service Requirements Compliance	208
2.8.8.2	Quality of Services [L.29.2.1, M.2.1]	211
2.8.8.3	Service Coverage [L.29.2.1, M.2.1]	212
2.8.8.4	Security [L.29.2.1, M.2.1]	212
2.8.9	DHS Intrusion Prevention Security Service [C.2.8.9]	213
2.8.9.1	Understanding [L.29.2.1, M.2.1]	213
2.8.9.2	Quality of Services [L.29.2.1, M.2.1]	219
2.8.9.3	Service Coverage [L.29.2.1, M.2.1]	220
2.8.9.4	Security [L.29.2.1, M.2.1]	220
2.9	Access Service [C.2.9]	221
2.9.1	Understanding [L.29.2.1, M.2.1]	221
2.9.1.1	Compliance with EIS Service Requirements [J.19]	221
2.9.2	Quality of Services [L.29.2.1, M.2.1]	227
2.9.2.1	Ethernet Access	228
2.9.2.2	Wavelength Access	230
2.9.2.3	Wireless Access (Fixed Wireless)	230
2.9.3	Service Coverage [L.29.2.1, M.2.1]	231
2.9.4	Security [L.29.2.1, M.2.1]	231
2.10	Service Related Equipment (SRE) [C.2.10]	232
2.10.1	Understanding [L.29.2.1, M.2.1]	232
2.10.1.1	Compliance with EIS Service Requirements [J.19]	233
2.10.2	Quality of Services [L.29.2.1, M.2.1]	233
2.10.3	Service Coverage [L.29.2.1, M.2.1]	234
2.10.4	Security [L.29.2.1, M.2.1]	234
2.11	Service Related Labor (SRL) [C.2.11]	234
2.11.1	Approach	234
2.11.2	Service Coverage [L.29.2.1, M.2.1]	236
2.11.3	Security Requirements	236
2.12	Cable and Wiring (C&W) [C.2.12]	237
2.12.1	Understanding [L.29.2.1, M.2.1]	237
2.12.1.1	Inside Cable Plant Management Drawings	238
2.12.1.1	Compliance with EIS Service Requirements [J.19]	238
2.12.2	Quality of Services [L.29.2.1, M.2.1]	239
2.12.2.1	Site Survey	240
2.12.3	Service Coverage [L.29.2.1, M.2.1]	240

2.12.4 Security [L.29.2.1, M.2.1].....	240
3 External Traffic Routing [C.1.8.8].....	240
3.1 Verizon Traffic Aggregation Service (VTAS) Methodology.....	241
3.2 Technical Approach	242
3.2.1 Verizon Classified Support.....	246
3.3 Notification of Non-Participating Traffic, Design Mechanisms to Prevent Bypass, and Traffic Failsafe Mechanism	246
3.4 Location.....	246
3.5 Availability of Cleared Personnel and Smart-Hands Support.....	247
Attachments	i
Attachment A EIS Information Technology Risk Management Framework Plan.....	i
Attachment B MTIPS Risk Management Framework Plan.....	i
Attachment C Assumptions and Conditions	i
Attachment D Technical Volume Abbreviation and Acronym Definitions List	i

LIST OF TABLES

Table 1.3.2.1-1. BSS Provisioning – Enhanced Service Quality.	13
Table 1.3.3.1-1. Strategic Services Center Evaluation Scenario Pods.	15
Table 1.6-1. Verizon EIS Products and Services	18
Table 1.6-2. Verizon EIS Task Order Approach	18
Table 2.1.1.2.1-1. Physical & Logical RFC 4364 Network	24
Table 2.1.1.4-1. VPNS Enhanced Configuration Options	28
Table 2.1.2.1-2. Verizon ETS Offerings.....	31
Table 2.1.4.2-1. Verizon’s PLS Capabilities.....	46
Table 2.1.4.4-1. PLS Characteristics	47
Table 2.1.5.1-1. SONETS Key Business Drivers.....	47
Table 2.2.1.1-1. IPVS Capabilities.....	61
Table 2.2.1.1-1. IPVS Ordering Agency Capabilities.....	63
Table 2.2.1.1-2. IPVS Optional Services	63
Table 2.2.1.1-3. IPVS End User Features	64
Table 2.2.1.1-4. IPVS Standard Applications.....	64
Table 2.2.1.1-5. IPVS Desktop & Mobile Client Features	65
Table 2.2.1.1.1-1. IPVS Managed LAN Activities & Responsibilities	70
Table 2.2.2.1-1. CSVS Services	73
Table 2.2.4.1.1-1. CSDS Mandatory Technical Capabilities.....	78
Table 2.3.2-1. TFS Three Phased Implementation Approach	92
Table 2.4.1.1-1. Verizon CHS Facility Responsibilities.....	95
Table 2.4.2-1. CHS Facility Features.....	97
Table 2.4.2-1. CHS Security Features	98
Table 2.5.1.1-1. Verizon Cloud Off-Premise.....	102
Table 2.5.1.4-1. IaaS Secure Cloud.....	106
Table 2.5.1.4-2. IaaS Logical Security.....	107
Table 2.5.4.2-1. CDNS Business Rules.....	120

Table 2.6.2-1. Verizon Network Service Targets	124
Table 2.6.2-2. Verizon Wireless Key Investments	124
Table 2.7.4-1. █████ Security Frameworks.	131
Table 2.8-1. Managed Service Capabilities.	132
Table 2.8.1.2.2-1. Verizon MNS Service Desk Functions.....	140
Table 2.8.3.2-1. UCS Delivery Framework	157
Table 2.8.4.1-1. MTIPS Transport Collection and Distribution Capabilities.....	162
Table 2.8.4.2-1. MTIPS Security Features	170
Table 2.8.4.2-2. MTIPS Capabilities.....	170
Table 2.8.5.1.1-1. MPS Management and Monitoring	175
Table 2.8.5.1.1-2. Security Dashboard Information.....	175
Table 2.8.5.1.3-1. INRS Proactive Methodology	179
Table 2.8.5.1.4-1. Inbound/Outbound Email Forgery Protection and Filtering Techniques	189
Table 2.12.1.1-1. Inside Cable Plant Drawings.....	238
Table 3-1. National Policy Requirement Functions [C.1.8.8]	240

TABLE OF FIGURES

Figure 1.1-1. Verizon's Multi-Layer Network Architecture	5
Figure 1.1.2-1. Verizon's OneNetwork Architecture.....	9
Figure 2.1.1.1.1-2 QoS at PVC and Port Level	23
Figure 2.1.1.2.1-1. VPNS Network Architecture	25
Figure 2.1.2.1-1. Verizon ETS At-a-Glance.	31
Figure 2.1.2.1-3. ETS Multiplex UNI	35
Figure 2.1.5.2-1. Verizon SONETS Architecture	48
Figure 2.2.1.1-1. Verizon Advanced Communications	62
Figure 2.3.1-2. Verizon Hosted CCS Capabilities.	81
Figure 2.5.1.1-2. Verizon Disk Level Replication.	104
Figure 2.6.1-1. Verizon Wireless Services Network	121

Figure 2.8.1.2-1. Verizon MNS NetOps Functional Capabilities.....	139
---	-----



Figure 2.8.5.1.3-1. INRS Proactive In-Depth Analysis of Program Elements	179
--	-----



Figure 2.11.1-2. EIS SRL Services	235
---	-----



Figure 3.5-1. Onsite Nest Engineering Tasks.....	247
--	-----

Executive Summary

On behalf of Verizon, our partners, and the thousands of employees and customers whose leadership and dedication have driven our vision for next generation government technology, we are pleased to present this EIS proposal to GSA. Verizon is committed to supporting the overarching EIS goal “to make the resulting contracts as flexible and agile as possible to meet and satisfy the widely differing requirements of the federal agencies both now and for the next decade and beyond.”

Our broad technology capabilities, operational discipline, and extensive experience, through 8 years providing services on the Networx and WITS 3 contracts, and decades of experience supporting previous contract generations, make Verizon uniquely qualified to support agency missions for decades to come.



Verizon is committed to the success of the EIS program, and prepared to provide the following:

- **Comprehensive Service Offering:** [REDACTED]
[REDACTED]
[REDACTED]
[REDACTED] For CBSA-based services, Verizon is proposing all mandatory and all optional services. In addition, all CBSA's are covered by at least one service, with many offered across the globe. As a premier wireless provider to the federal government, Verizon is uniquely capable of integrating wireless and wireline technologies to offer dynamic and ubiquitous communications capabilities to improve agency mission execution.
- **Service Excellence:** Verizon is committed to supporting agency missions through service excellence, and has partnered with agencies through expected and unexpected challenges, including ensuring service availability during the 2011 Japanese earthquake and tsunami, wild fires within our National Parks, Hurricanes Katrina and Sandy, and the multi-city Pope Francis visit of 2015, to name a few. Our EIS Customer Service Organization (CSO), led by [REDACTED] and [REDACTED], will continue to provide excellent agency care throughout the EIS contract.
- **Innovative Solutions:** Verizon invested [REDACTED] in 2015 alone in product and solution development, and agencies will benefit from this investment. From Software Defined Networking, to 5G Wireless technologies, Smart Cities solutions, Connected Machines, and Cloud computing, Verizon is positioned to offer cutting-edge and transformational solutions throughout the full EIS period of performance.
- **Enhanced Security:** Verizon processes [REDACTED] security events daily across the globe, and conducted 500+ forensic investigations in 2015. Our yearly DBIR report and award-winning DBIR application (Frost & Sullivan, 2015) set the industry standard for network security and awareness. Protecting government and citizen assets and data is at the foundation of every Verizon solution. As a certified IPSS (EINSTEIN3)

provider, Verizon has been entrusted with securing the networks of some of the largest and most critical agencies, [REDACTED], among others. Our government network operations and security capabilities, coupled with our proven security offerings, including MTIPS and Managed Security Services, ensure agency solutions are continuously secured.

- **Improved Ease of Use:** With our Networx and WITS 3 experience, Verizon uniquely understands agency solution requirements and diverse procurement practices, and is best positioned to offer next generation services via our premier Business Support System that meets the needs of the Federal customer while enhancing the user experience with accurate inventory data and flexible ordering, provisioning, billing and reporting.
- **Low Risk Contract Transition:** With our extensive past performance transitioning contracts of similar size and scope, Verizon will utilize best practices and lessons learned to support agencies' unique requirements for transitions to EIS quickly and with minimal risk.
- **Competitive Pricing:** [REDACTED]
[REDACTED]
[REDACTED]
[REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]

Verizon's proposal represents a continued commitment to offering a breadth of innovative, flexible and secure solutions to meet agency-specific needs, today and over the next 15 years. Our global technical capabilities, coupled with an experienced Management team and Business Support System, ensure service excellence and an experienced hand during contract transition. We take seriously that our solutions help agencies serve and protect the public. To those stake holders, better matters and Verizon is committed to delivering the promise of our solutions. We thank the GSA and

our valued customers for their years of continued partnership and support, and eagerly anticipate collaborating in the future to together achieve the EIS vision.

1 Network Architecture

1.1 Understanding [L.29.1, M.2.1]

To conduct business on a national and global scale now and into the future, it is imperative that the federal government have integrated Information Technology (IT) and network services that are reliable, flexible, scalable, and secure. Verizon currently delivers the spectrum of services required in the EIS RFP on the existing Network and WITS 3 contracts to many federal government customers, [REDACTED]

[REDACTED], as well as to many Global Commercial customers. One of the most critical elements in the success of federal missions is for these network services, and the applications that require them, to be securely and readily available anytime, anywhere.

It is therefore extremely important that the underlying service infrastructure include extensive domestic and global coverage, based on solid technology wrapped in a security framework that protects critical government data. This infrastructure must be one that can adapt and transform with the rapid pace of technology. Without the ability to grow in the future, service providers will lose the ability to successfully support the government's expanding and changing mission objectives.

Verizon's existing Network Architecture will continue to help EIS ordering agencies implement technology solutions that will address their mission objectives. Verizon systems and processes - from initial inquiry, to provisioning, to operation and management - are designed to work together harmoniously within a proven, secure and audit-compliant architecture. The

Verizon Technology Firsts

- **2004-2010.** Verizon reaches 9-way Atlantic Ocean and 8-way Pacific Ocean mesh connectivity, offering the highest availability between the U.S., Europe, and Asia.
- **2005.** First to deploy fiber-to-the-premise with FiOS in the U.S.
- **2009.** Launched "Bandwidth on Demand" features in Global Network.
- **2010.** Verizon Wireless launches the nation's first wide-area Fourth Generation Long Term Evolution 4G LTE network.
- **2011.** First to deploy a standards-based 100 Gbps Ethernet link on long-haul networks in Europe and the U.S.
- **2012.** Verizon first TIC 2.0 Compliant Provider.
- **2014.** First to offer private, secure cloud connectivity to multiple cloud services on demand.
- **2015.** First to deploy Quality of Service on 4G LTE services and Managed SD WAN-as-a-service.
- **2015.** Verizon announces 5G field trials for 2016.

Verizon Network Architecture will adapt to meet each agency's changing needs over the course of the EIS contract. Verizon's existing Network Architecture is an integrated multi-layer services platform, as depicted in **Figure 1.1-1** below. Various elements shown in this figure are described, as follows:



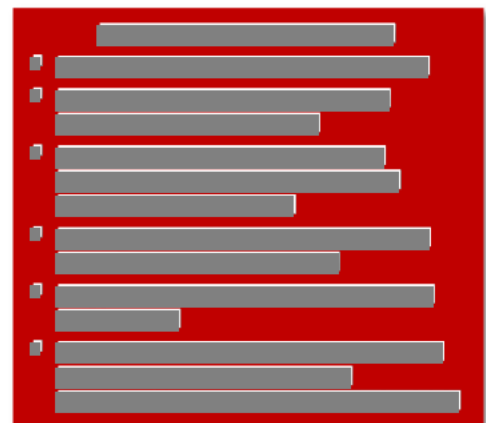
[Redacted text block]

[Redacted text block]

[Redacted text block]

[Redacted text block]

[Redacted text block]



[Redacted text block]

[REDACTED]

[REDACTED]

[REDACTED]

1.1.1 VERIZON'S EVOLVING INTELLIGENT NETWORKING SERVICES

[REDACTED]

[REDACTED]

Dynamic Port (DPort) and Dynamic Committed Access Rate (DCAR). [REDACTED]

[REDACTED]

Software Defined – Wide Area Network (SD-WAN). [REDACTED]

[REDACTED]

Secure Cloud Interconnect (SCI). [REDACTED]

[REDACTED]

Software Defined Perimeter. [REDACTED]

[REDACTED]

1.1.2 VERIZON ONE NETWORK

Verizon's NFV/SDN strategy is to not only deploy services to customers like the government, but to also leverage this paradigm-changing technology for its internal networks and services. This will allow EIS ordering agencies to deploy network solutions faster and simpler, through a more reliable real-time platform. Verizon is deploying these capabilities through its internal "OneNetwork" initiative, as shown in **Figure 1.1.2-1**.



1.1.3 VERIZON WIRELESS SERVICE (MWS) AND INTEGRATION

Verizon MWS and the ability to integrate mobile users, applications, and machine-to-machine (M2M) technologies into secure, reliable solutions are some of Verizon's greatest resources. With the world's largest 4G LTE network, Verizon offers the government access to the best of breed, most advanced networking services and applications. Verizon is the first major carrier to begin testing 5G services. Verizon's Mobile services are directly integrated into the Network Architecture, including services like private wireless network access to VPNS – a service that never touches the public Internet, enhancing security and agency network reliability. Verizon has leveraged its extensive wireless footprint to offer services rapidly and to remote agencies where other providers were unable and/or unwilling to do so. For additional information regarding Verizon MWS or its Managed Mobility Service (MMS), reference **Volume 1, Sections 2.6 and 2.8.6**, respectively.

1.2 Compliance with EIS Service Requirements [J.19]

Standards. Throughout this proposal volume, Verizon states its compliance to various standards.

Interoperability. Verizon complies with **RFP Section C.1.8.6**. Verizon will support interoperability for given service offerings so that a user of a service provided by Verizon is able to communicate with users of services from other EIS contractors with equivalent performance. Interoperability will be made available for any service that is currently commercially offered by Verizon and is interoperable with the services of other EIS contractors. Verizon will also make available any future service interoperability at no additional cost to GSA when Verizon offers the same level of interoperability for its commercially provided service. Since near full interoperability is provided via the Public Switched Telephone Network (PSTN) for circuit switched services, Verizon will support interoperability between voice services, circuit switched data service and wireless services. Verizon will also support connectivity and interoperability for remote and mobile users as specified in the individual service descriptions.

Technical Support. Verizon complies with **RFP Section C.1.8.9**, and will provide customer technical support as a component of each of its EIS services.

508 Compliance. Verizon complies with the Section 508 standards from **RFP Sections C.4.2, C.4.3, and C.4.5**. Refer to **Section 1.1.4.3.1.3, Accessibility in Volume 2 – Management** for additional information. Verizon will post the Voluntary Product Accessibility Template (VPAT) for each service identified in **RFP Section C.4.4** to its web site. Services that execute mission operations and provide the required information, which will be reported via the Internet, email or telephone, will meet the relevant provisions of Section 508, Subparts B, C, and D or will provide equivalent facilitation.

Training will be delivered via meeting and briefings, classrooms, seminars, instructor-led and non-instructor on-line web based self-study, and manuals or desk top guides. The same capabilities provided for Internet reporting will be provided to disabled trainees who are undertaking instructor-led and/or non-instructor on-line web based training. Signers and/or braille products will be provided to disabled trainees when requested in advance by the government.

1.3 Quality of Services [L.29.1, M.2.1]

Verizon will deliver high quality transport, MNS, and security services to ordering agencies. Verizon provides quality through its architecture, people, and service delivery, and its services are designed to be compliant, scalable, reliable, and resilient.

1.3.1 VERIZON QUALITY SERVICE DELIVERY ARCHITECTURE

The following subsections describe the steps Verizon takes to help verify that it delivers quality services via EIS.

1.3.1.1 Compliance with Standards

Verizon adheres to established industry standards to verify that its latest products are interoperable and compatible with many older legacy services. This helps to increase effectiveness and reduce costs. Verizon has been, and is actively, involved in numerous global standards bodies, including the Internet Engineering Task Force (IETF), the

International Telecommunication Union (ITU), and the Metro Ethernet Forum, among others. Verizon is also a founding member of the Open Networking Foundation (ONF), the leading standards body responsible for the development of the emerging SDN standards and protocols. Verizon uses quality management system standards, including ISO 9000 to confirm its offerings support the needs of its customers, while meeting statutory and regulatory requirements related to a particular product or service. Verizon has implemented many industry-first commercial deployments of state-of-the-art technologies, such as 5G wireless services.

1.3.1.2 Experienced Personnel

Verizon has been supporting the government for over 25 years. Verizon employees are specially trained to support the government's needs, and are often called upon to provide out-of-the-box solutions to meet agencies' mission-specific requirements. Verizon delivers dedicated people, knowledgeable in the ways of the federal government, to provide quality services to EIS ordering agencies. Further, as required Verizon provides varying levels and types of cleared personnel.

1.3.1.3 Service Lifecycle

Verizon follows the Information Technology Infrastructure Library (ITIL) v2011 strategic framework for its products and services. Over 8,500 Verizon employees are ITIL and ISO certified. The Verizon Government Network Operations and Security Center (GNOSC) is ISO/IEC 20000-1 certified. Using the ITIL Service Lifecycle methodology (Service Strategy, Service Design, Service Transition, and Service Operation) improves service delivery, communication and information flow between Verizon and the government, thus reducing response times through pre-defined and repeatable processes and procedures.

1.3.2 QUALITY ORDERING, BILLING AND REPORTING SERVICES

Verizon supports quality service delivery with secure ordering, billing, and reporting services. Verizon's service delivery and customer enablement process for EIS includes the elements described in the following sections.

1.3.2.1 Enterprise Business Support System (BSS)

Verizon will leverage commercial best practices, while securing critical government data in its back office BSS. Verizon redesigned the way it conducts business with customers. Using agile development principles, Verizon has enhanced its order processing, provisioning, and billing procedures, putting a strong focus on rapid delivery of services via automation. Improved back office systems will verify that products and services provided under the EIS contract will meet or exceed the government's expectations. **Table 1.3.2.1-1** outlines how Verizon BSS provisioning provides the government with enhanced service quality:

**Award-Winning, Patented
Back Office System**
"Verizon Enterprise Solutions fundamentally transformed the way it does business on a global scale by standardizing processes, optimizing its systems architecture and rationalizing its product suite." – 2015 TM Forum Excellence Award for Agile Business & IT (Service Provider)

Table 1.3.2.1-1. BSS Provisioning – Enhanced Service Quality.

Verizon BSS Provisioning – Enhanced Service Quality
Streamlined ordering and fulfillment process through automation
Straightforward and transparent transactions and secured interfaces
Greater predictability in managing expectations and service delivery
Reduced risk to the organization
Reduced overhead costs for managing projects
Improved ease of doing business
Faster deployment of new services and custom features

1.3.2.2 Customer Enablement Portals

Verizon's EIS portal capabilities allow authorized users to 1) securely order, 2) view network services, 3) see alarms on an account or site-level basis, 4) obtain incident trend analysis, 5) configure services, 6) view inventories, submit change management requests, and 7) consolidate the knowledge that exists in silos across the organization. Leveraging development in Verizon's commercial customer portals, the Verizon EIS portals will include more automation and self-service capabilities and will maximize the delivery of compliant, scalable, reliable, and resilient EIS services through minimal touch back-office systems.

1.3.2.3 Ordering/Provisioning

For the past several years, Verizon has focused significant development on its BSS, which is a series of tools that combine service quoting, ordering, and provisioning, resulting in a seamless and easy-to-use process to efficiently provide customers with the services they need. As the entry point of the Network Architecture, the BSS provides

a highly intelligent flow using automation and auto-population of replicable data elements, resulting in service inquiry milestones being completed in minutes rather than days.

1.3.2.4 EIS BSS Sensitive Government Data

Where government sensitive data is aggregated, Verizon will secure and isolate this data. Verizon's EIS BSS Sensitive government Data Store is within its BSS platform is secured inside the BSS FISMA Moderate boundary. This will verify that critical government data is resilient and resistant to attack.

1.3.2.5 Enterprise Service Billing

The Verizon Network Architecture includes sophisticated billing systems that provide a more flexible and accurate means of invoicing combined products and services to support a solutions-based approach. Both single and multiple invoice options are available based upon site location or service. Verizon has made significant investment in support of electronic exchange of billing data to eliminate unnecessary paper invoices.

1.3.3 ADHERENCE TO SERVICE LEVELS

Once services are placed into operation, Verizon's systems and support organizations will monitor performance and service levels to validate that Verizon services are meeting EIS Service Level Agreements (SLAs). One of Verizon's key strengths in this area is the use of manual



Verizon Innovation Centers, co-located with its Innovation Labs feature state-of-the-art showcases of visionary ideas, IPv6 products, and innovative solutions.

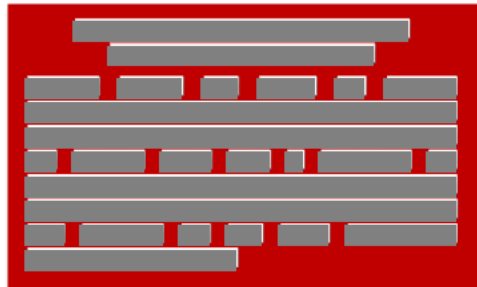
and automated SLA monitoring to quickly identify issues and abnormalities and take corrective action to provide quality services to the government.

1.3.3.1 Verizon Labs and Test Centers

Prior to and during EIS service delivery, Verizon will provide the government with access to Verizon labs and test centers. Verizon has the capability to test IP enabled "devices" that exist in Verizon customer's current and future infrastructures (e.g., mobile

devices, networks, computers, storage, and vehicles) that require integrated networking services to securely produce the envisioned outcomes [REDACTED]

[REDACTED] state-of-the-art showcases of visionary ideas, commercial products, and innovative solutions still in progress. These world-class facilities are an important part of Verizon's innovation process and are available for agencies to visit and work with at any time.



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

[REDACTED] a full proof-of-concept lab that is available to any agency to verify that EIS services are compliant, scalable, reliable, and resilient. The CTC includes nine private rooms where agencies can securely test their solutions with the help of Verizon engineers. [REDACTED]

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



[REDACTED]
[REDACTED]

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

1.4 Service Coverage [L.29.1, M.2.1]

Verizon is a well-established provider of telecommunications services that offers a wide range of services across the country and around the world. As the predominant local exchange carrier (LEC) for the mid-atlantic and northeastern U.S., including the surrounding Washington, DC metropolitan area, Verizon provides advanced services and capabilities to many of the federal agencies headquartered in this area. However, with its extensive metro footprint in nearly all major U.S. cities, and over [REDACTED] on-network Verizon lit buildings throughout the U.S. (including many major government locations), Verizon is more than just the LEC in the DC metro area. The Verizon network includes an IP/MPLS infrastructure covering more than [REDACTED] route miles in over 150 countries. Verizon's OCONUS and non-domestic footprint is also supported by Verizon's host nation agreements, consortiums with partners, MPLS VPN Inter-provider connections (MVIC), and Master Service Agreements (MSAs) with other partners. With this expansive global presence, Verizon provides true end-to-end connectivity and diversity around the world.

Verizon complies with **RFP Section C.1.3** and will support EIS services in a minimum of 25 of the top 100 CBSAs.

1.5 Security [L.29.1, M.2.1]

Verizon's proven security performance on existing and previous GSA contracts, including FTS, Networx, WITS3, and other large telecommunications contracts, demonstrates its ability to effectively and efficiently manage an effort of the size and complexity of EIS. Verizon's Network Architecture is secured across all technologies so Verizon's and its partners' systems and processes will protect key government data and services.

Verizon Security Authority to Operate (ATO) Examples

- Networx/WITS3 BSS
- Federally compliant GNOSC
- MNS ATO
- FedRAMP for IaaS
- FISMA High DHS Services
- IPSS Aggregation
- MTIPS 2.0

At an organizational level, Verizon has developed security management processes to support the personal security/suitability requirements for EIS. This includes internal Verizon system access control processes [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED]

Verizon will enhance its existing compliant security infrastructure to comply with EIS-specific requirements including Risk Management Framework (RMF) Plans, Security Assessment and Authorization (A&A), and System Security Plans (SSP). Verizon will provide higher levels of security for specific services, as required on a TO basis. [REDACTED]

[illegible][illegible]

1.5.2 EXTERNAL TRAFFIC ROUTING (ETR)

All Verizon services offered under EIS including VPNS, ETS, IPS, Cloud, MTIPS, access, and others, which transport Internet, Extranet, and Inter-Agency traffic, will support the ability to identify and route government traffic through a secure [REDACTED] [REDACTED] processing. Verizon is a certified IPSS (E3) provider and

supports the routing of Networx IPS services destined for government agencies to an “aggregation point” where that traffic is scanned [REDACTED] before entering government internet facing networks. Verizon will support a similar model for EIS. Verizon has addressed the ETR requirements in more detail in **Volume 1, Section 3**.

1.6 SOW Items

Verizon proposes the full complement of EIS mandatory and optional services. Verizon’s EIS proposal provides an overview of capabilities and its approach to providing the services identified in **Table 1.6-1** below.

Table 1.6-1. Verizon EIS Products and Services

Service Area	Service
Data Services	<ul style="list-style-type: none"> Virtual Private Network Service (VPNS) (mandatory) Ethernet Transport Service (ETS) (mandatory) Optical Wavelength Service (OWS) (optional) Private Line Service (PLS) (optional) Synchronous Optical Network Services (SONETS) (optional) Dark Fiber Service (DFS) (optional) Internet Protocol Service (IPS) (optional)
Voice Services	<ul style="list-style-type: none"> Internet Protocol Voice Service (IPVS) (optional) Circuit Switched Voice Service (CSVS) (mandatory) Toll Free Service (TFS) (optional) Circuit Switched Data Service (CSDS) (optional)
Contact Center Services	<ul style="list-style-type: none"> Contact Center Service (CCS) (optional)
Data Center Services	<ul style="list-style-type: none"> Colocated Hosting Service (CHS) (optional)
Cloud Services	<ul style="list-style-type: none"> Infrastructure as a Service (IaaS) (optional) Platform as a Service (PaaS) (optional) Software as a Service (SaaS) (optional) Content Delivery Network Services (CDNS) (optional)
Wireless Services	<ul style="list-style-type: none"> Wireless Service (optional)
Commercial Satellite Communications Service	<ul style="list-style-type: none"> Commercial Fixed Satellite Service (CFSS) Commercial Mobile Satellite Service (CMSS)
Managed Services	<ul style="list-style-type: none"> Managed Network Service (MNS) ((mandatory) Web Conferencing Service (WCS) (optional) Unified Communications Service (UCS) (optional) Managed Trusted Internet Protocol Service (MTIPS) (optional) Managed Security Service (MSS) (optional) Managed Mobility Service (MMS) (optional) Audio Conferencing Service (ACS) (optional) Video Teleconferencing Service (VTS) (optional) DHS Intrusion Prevention Security Service (IPSS) (optional)
Access Arrangements	<ul style="list-style-type: none"> Access Arrangements (AA) (mandatory)
Service Related Equipment	<ul style="list-style-type: none"> Service Related Equipment (optional)
Service Related Labor	<ul style="list-style-type: none"> Service Related Labor (optional)
Cable and Wiring	<ul style="list-style-type: none"> Cable and Wiring (optional)

The Verizon EIS proposal serves as a foundation for supporting future TOs. Verizon will carefully evaluate each TO to determine the optimal solution that will best address the given requirements. Verizon’s approach is detailed in **Table 1.6-2** below:

[REDACTED]
[REDACTED]
[REDACTED]

network capacity to latency, and augments the network based on service level standards. VPNS supports Verizon's commitment to the government to continue to implement new technologies and deliver a broad range of value-added e-business solutions. [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

2.1.1.1.1 Compliance with EIS Service Requirements [J.19]

Service Description. Verizon complies with **RFP Section C.2.1.1.1**, and will provide secure, reliable transport of agency applications across its high-speed unified multi-service IP-enabled backbone infrastructure. [REDACTED]

[REDACTED]

Functional Definition. Verizon complies with **RFP Section C.2.1.1.1.1**, and offers three VPNS solutions using its backbone: Remote Site (Intranet), VPNS Extranets (Extranet), and Remote Access (Mobile) (Remote Access).

Intranet. Verizon complies with **RFP Section with C.2.1.1.1.1(1)**, and it extends the reach of an agency's VPN via secure, cost effective, always-on connectivity for small/home office and remote office locations. In this scenario a hardware client is provisioned at each remote location which establishes a secure tunnel between the remote location and the Trusted Internet Connection (TIC) Access Point.

Extranet. Verizon complies with **RFP Section with C.2.1.1.1.1(2)**. Verizon's VPNS Extranet is an arrangement where two or more ordering agencies/partners/vendors or an agency with two or more VPNs, establish virtual connections between their VPNs to make connectivity available to a limited, defined group. Each Extranet customer will have a virtual connection created within the VPNS network to achieve the cross-agency, partner-vendor connection. Using Layer 3 technology, secure connections are established to the other VPNS subscriber without the need to implement and manage IP

Security (IPSec) tunnels. The Extranet feature uses route targets (RTs) selectively applied to a VPN's virtual route forwarding table (VRF), which is mapped to a specific sub-interface at the customer edge (CE) device.

Remote Access. Verizon complies with **RFP Section C.2.1.1.1.1(3)**, and provides secure encrypted remote access to agency VPNs for their mobile workforce and remote employees. This configuration utilizes a VPN software client to establish a secure IPSec tunnel to the TIC Access Point. The VPN client supports popular desktop and mobile platforms including: Windows, Mac OS X, Android and iOS.

Traffic Prioritization and Cost Efficiencies. Verizon complies with **RFP Section C.2.1.1.1.1**, and will accommodate an agency's applications to enable the network to accurately and consistently allow for traffic prioritization and cost-efficiencies. VPNS supports time-critical (voice and video), business-critical (transactions) and non-critical (email) traffic. [REDACTED]. Agencies gain access to these traffic priorities based on the IP precedence settings or DiffServ Code Point (DSCP) settings that they apply to their IP traffic. QoS marking and queuing is supported on TDM, Ethernet, and Satellite access. Verizon supports 802.11p, DSCP, and DiffServ models. [REDACTED]

[REDACTED]



Routing Requirements. Verizon complies with **RFP Section C.2.1.1.1.4(1)** and will meet applicable routing requirements in **RFP Section C.1.8.8**. Encrypted tunnels will be applied and proxied to allow inspection.

Tunneling Standards. Verizon complies with **RFP Section C.2.1.1.1.4(2)** and will provide multiple tunneling standards (i.e., L2TP, GRE, IP-in-IP, MPLS, IPSec, and TLS), as required by agencies.

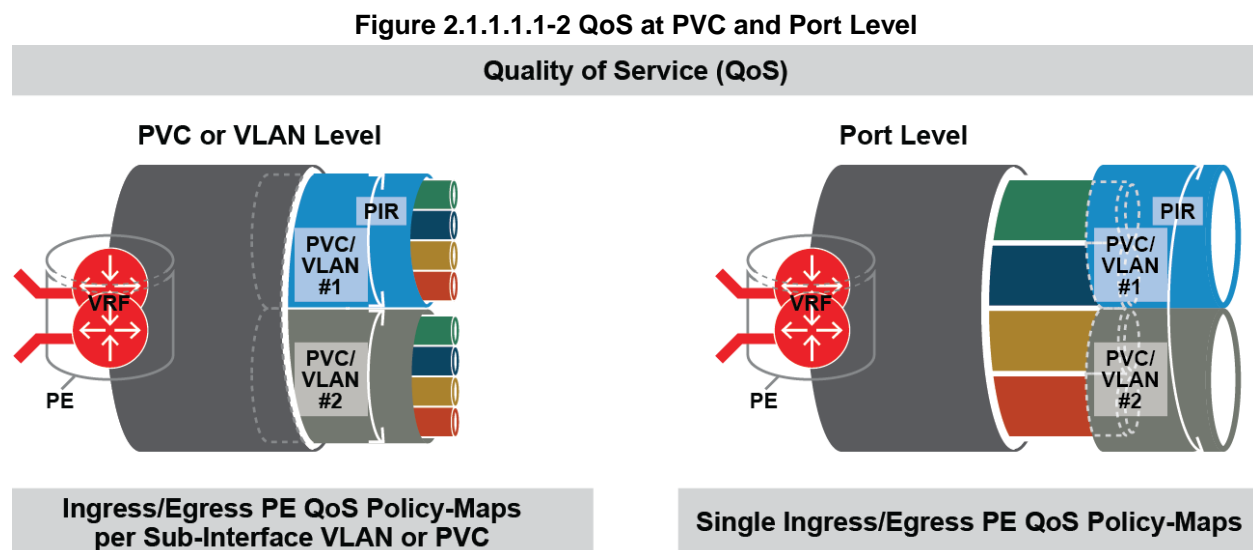
Encryption Levels. Verizon complies with **RFP Section C.2.1.1.1.4(3)**. VPNS will provide various encryption levels (i.e., 3DES, RC4 and AES), as required by agencies.

Authentication Services. Verizon complies with **RFP Section C.2.1.1.1.4(4)**, and will provide authentication services (i.e., RADIUS, Internal LDAP, token integration, PKI, and X.509 certificates), as required by agencies.

IPv4 and IPv6. Verizon complies with **RFP Sections C.2.1.1.1.4(5-6)**. VPNS was designed to meet both current and future needs; therefore, Verizon VPNS supports both IPv4 and IPv6 as both the encapsulating and encapsulated protocol.

QoS Support. Verizon complies with **RFP Section C.2.1.1.1.4(7)** and will support QoS in the following standardized modes: best effort, aggregate customer edge interface level QoS, site-to-site level QoS, IntServ signaled, and DiffServ marked. Verizon's VPNS QoS offerings are in full compliance with the Internet Engineering Task Force (IETF) DiffServ RFCs, and provide the Per Hop Behavior (PHB) envisioned. Verizon's flexible VPNS supports multiple modes of access and transport, and it is the core transport for all Verizon higher level services as it is QoS enabled and secured.

Multi-VRF is a feature for Verizon VPNS customer agencies that want multiple logical MPLS VPNs designed on a common physical local access loop. Agencies can choose whether they want a common QoS policy for all VPNs or specific QoS policy for each VPN on IP traffic leaving Verizon's VPNS network to the agency routers. QoS policies for Multi-VRF are shown in **Figure 2.1.1.1.1-2**.



QoS Access Networks. Verizon complies with **RFP Section C.2.1.1.1.4(8)** and will support QoS across a subset of the access networks, as listed in the RFP.

Application Level QoS. Verizon complies with **RFP Section C.2.1.1.1.4(9)** and will support the DiffServ application level QoS.

Temporary Access User Authentication. Verizon complies with **RFP Section C.2.1.1.1.4(15)** and will allow an agency to choose from alternatives for authentication



Every PE router is diversely trunked into two diverse P-core routers so a node will never become isolated. Dual P-core routers are deployed at each P-core site, and diversely trunked into the Verizon optical mesh high-speed wavelength backbone. Verizon's Global MPLS High-Speed Core routers are optimized for 10GE, 40GE and 100GE transport speeds and [REDACTED]

[REDACTED]. Verizon has an internal Data Traffic Engineering organization responsible for monitoring, capacity planning and traffic engineering the VPNS backbone. This organization will verify that diversity, capacity and network architecture requirements are met so the VPNS network will perform to the VPNS Service Level Agreement (SLA) standards. Increases in capacity can be driven by not only trended and projected peak utilization growth rates but also network diversity requirements. P-core routers employ Route Diversity for trunking associated

with the Verizon VPNS network to include logical trunk, physical trunk, and physical fiber path diversity to deliver multiple layers of service resiliency.

Physical trunk or fiber path diversity is defined as trunks that ride on physically diverse fiber paths. This diversity is provided at the fiber transmission level and physical fiber conduit path level. Verizon Data Traffic Engineering designs the trunks for facilities to meet both Logical and Physical trunking diversity. The Data Traffic Engineering organization utilizes network modeling tools to provide restorability options based on single card failures, node failures and right-of-way or cable (fiber path) system failures. Intelligence within the core trunking systems enable failure algorithms to be aware of whether or not an alternative Label Switch Path is either logically diverse or physically diverse based on the ability to associate multiple logical paths to the same fate or group treatment when choosing an alternative backup MPLS path.

Verizon has designed the VPNS backbone with the ability to reroute around trunk failures based on the number of trunks that exist out of any given location and the utilization associated with them. For example, when a trunk fails, there must be enough capacity on the remaining trunk(s) to support all bandwidth previously supported by the failed trunk.

2.1.1.2.2 Access Types

Verizon will connect government locations and trusted business partners' networks using its VPNS [REDACTED]

Connections use a variety of access technologies selected and sized to meet the specific bandwidth requirements of the agency's location and/or end users.

Figure 2.1.1.2.2-1 illustrates the available access technologies. This highly flexible set of connectivity enables agencies to select the best access to meet their network, bandwidth, application and cost needs.



Office CE 6 IPsec Tunnel Connections Mobile User

2.1.1.3 Service Coverage [L.29.2.1, M.2.1]

Verizon will support EIS services in a minimum of 25 of the top 100 CBSAs and in compliance with **RFP Section C.1.3** will provide VPNS to all government locations within each of its selected CBSAs.

2.1.1.4 Security [L.29.2.1, M.2.1]

Verizon operates with security components built into its framework (see **Table 2.1.1.4-1**) as well as the VPNS network architecture to offer agencies secure reliable network infrastructure in support of their missions. An internal Verizon security organization helps implement proper controls so that the VPNS operates within designed levels of confidentiality, security, and availability.

Verizon has several internal organizations that provide support functions for the VPNS network. All of these internal groups and their personnel have strict policies and controls in place to allow secure communication with and in support of the VPNS architecture.

Verizon's VPNS is certified and accredited to carry DoD sensitive information, as required by the DoD Instruction 5200.40, Defense Information Technology Security Certification and DoD Manual 8510.1-M, DITSCAP Application Manual.

[illegible]

Enhanced Configuration Options	
<ul style="list-style-type: none">	

Layered Security Architecture. Verizon complies with RFP Section C.2.1.1.1.4(10) and will provide isolation of the exchange of traffic and routing information to only those sites that are authenticated and authorized members of a VPN. Verizon will provide layered security architecture to verify that attackers will not find a single point of entry but will be faced with multiple levels of security.

Authenticated VPNS Access & Full Routing Capabilities. Verizon complies with RFP Section C.2.1.1.1.4(11-12) and has engineered its VPNS to remain completely private and separate from the public Internet. However, due to the need for agency locations, personnel and devices to securely connect to the private network using public Internet-based technologies, including broadband (i.e., DSL, FTTP, public wireless gateways, hotspots, cellular network connections), Verizon offers a secure method for authenticated users to connect to its VPNs. This method conforms to the federal government Trusted Internet Connections (TIC) Reference Architecture Document, Version 2.0, and utilizes certified TIC portals existing at Verizon's Managed Trusted Internet Protocol Service (MTIPS) (Section 2.8.4) gateways. Verizon currently operates MTIPS gateways situated at east and west coast locations offering secure redundant geographically diverse high availability entry points. Within each MTIPS gateway, Verizon has implemented TIC remote access only zones, which serve as the termination point for external connections and utilize a standard set of security controls to monitor, authenticate, and filter data flows that enter/exit the TIC access point.

Security Management System. Verizon complies with **RFP Section C.2.1.1.1.4(13)** and will support the inclusion of encryption, decryption, and key management profiles as part of the security management system.

Agency-Owned and Managed Internal Security Mechanisms. Verizon complies with **RFP Section C.2.1.1.1.4(14)** and will support an agency deploying its own internal security mechanisms in addition to those deployed by Verizon, in order to secure specific applications or traffic at a granularity finer than a site-to-site basis.

Security Standards.

[REDACTED]

2.1.2 ETHERNET TRANSPORT SERVICE (ETS) [C.2.1.2]

2.1.2.1 Understanding [L.29.2.1, M.2.1]

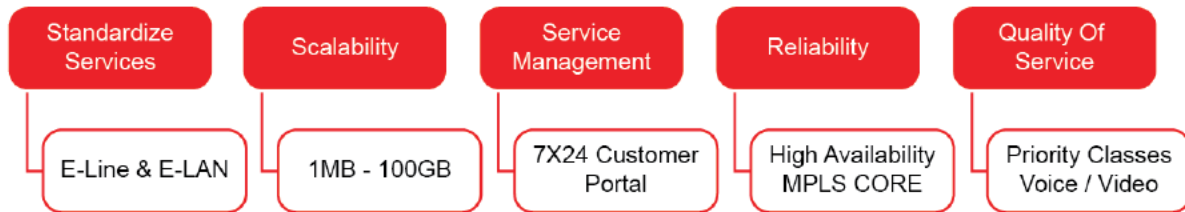
The Verizon Ethernet Transport Services (ETS) portfolio contains products that correspond to the Metro Ethernet Forum (MEF) definitions of E-LINE, and E-LAN, and interoperates with Ethernet Access. For additional information about Ethernet Access, refer to **Section 2.9 Access Arrangements**. Verizon was one of the first carriers to offer ETS, beginning in 2002. Continued development in the Ethernet market has made Verizon a leading provider of ETS. **Figure 2.1.2.1-1** provides an at-a-glance view of Verizon's Ethernet platform. Verizon

Verizon Ethernet Highlights

- Simplicity, scalability, and interoperability provide tangible benefits and cost-savings over legacy TDM solutions.
- Prevalent use of Ethernet within agency LANs makes the extension of Ethernet access across the WAN a natural evolution.
- Allows Agencies to better align access speeds based on the contracted bandwidth for the end-to-end service.
- Affords plug and play provisioning and scaling while TDM solutions require hardware reconfiguration.
- Future Proof Investment Protection: The scalability of Ethernet allows easy upgrades, protecting the bulk of investment in Ethernet, switching infrastructure.

ETS provides the government with flexible, scalable standards based sets of Layer 2 network services provisioned over an MPLS infrastructure. Verizon currently provides ETS on Networx to federal agencies today. Ordering agencies will benefit from reduced time in the switch and reduced overhead because "repacking" into another data byte is not necessary when data moves from Ethernet LANs to an Ethernet WAN.

Figure 2.1.2.1-1. Verizon ETS At-a-Glance.



Verizon's ETS will allow ordering agencies to choose "off-the-shelf" equipment that costs less and provides better scalability in the future than TDM equipment does. A bandwidth upgrade of an existing Ethernet Virtual Connection (EVC) requires no Service Related Equipment (SRE) replacement whereas TDM requires a significant investment in new SRE. ETS enables agencies to increase bandwidth quickly because no additional equipment or network build is required. Verizon ETS will also allow agencies to procure only bandwidth that is needed because Ethernet bandwidth can be purchased in smaller increments than TDM or SONET technology.

ETS conforms to the product groupings that correspond to the MEF definitions of E-Line, E-LAN and Ethernet Access. **Table 2.1.2.1-2** summarizes the Verizon ETS products offerings, which are also described below.

Table 2.1.2.1-2. Verizon ETS Offerings.

Service Type	Service Name	Service Description	Key Applications
E-LINE (Ethernet Line)	Dedicated E-Line	Point-to-point Ethernet connectivity offering dedicated bandwidth in Metro, C., and International spaces	Storage Data mirroring Business continuity management
	Switched E-Line	Point-to-point Ethernet connectivity offering switched bandwidth in Metro, National U.S., and International spaces	Large file transfers Class-of-Service-aware capability
E-LAN (Ethernet LAN)	Switched E-LAN	Multipoint Ethernet connectivity with classes of service supporting WAN needs for Metro, National U.S., and International spaces	LAN-LAN, VoIP Distance learning Content Delivery Convergence

2.1.2.1.1 Compliance with EIS Service Requirements [J.19]

Service Description. Verizon complies with **RFP Section C.2.1.2.1**. ETS is implemented over Verizon's MPLS backbone, where Ethernet links are transported using MPLS label switched paths inside an outer MPLS "tunnel".

Dedicated or Shared Service. Verizon complies with **RFP Section C.2.1.2.1**. ETS will be provided either as a dedicated or shared service, as required, on a TO basis.

Private Line and Private LAN. Verizon complies with **RFP Section C.2.1.2.1.1**. ETS supports private line and private LAN.

Routing Requirements. Verizon complies with **RFP Section C.2.1.2.1.4(1)** and will support applicable routing requirements as defined in the RFP, confirming encrypted tunnels are proxied to allow inspection. Verizon will meet the requirements for routing as presented in **Section 3** of this proposal volume.

Geographical Coverage – Intra-City, Inter-City ETS. Verizon complies with **RFP Section C.2.1.2.1.4(2)(a-b)**. Verizon ETS is a seamless end-to-end service on a global scale (Intra-City, Inter-City, CONUS/Metro, and OCONUS/Non-Domestic). Verizon's ability to offer ETS on this scale is due in part to the expansive access arrangements with third party vendors all over the world. On an individual TO Verizon will notify the agency of any protocol issues that impact the delivery of the ETS.

UNIs. Verizon complies with **RFP Section C.2.1.2.1.4(3)** and will support Ethernet UNIs for Layer 2 and 3 clients. Layer 3 clients are agency devices that support Layer 3 protocol packets such as IPv4, IPv6. UNI types supported include 10 Mbps, 100 Mbps, 1000 Mbps and 10 Gbps.

Virtual Connections. Verizon complies with **RFP Section C.2.1.2.1.4(4)**. Verizon ETS will support Ethernet Virtual Connections (EVC), which are used to define the association of two or more UNIs. Ethernet Access must be of sufficient bandwidth to support the sum of all EVCs on a UNI.

Service Delivery Point. Verizon complies with **RFP Section C.2.1.2.1.4(5)** and will support the delivery of the ETS at the agency's SDP via a UNI.

TDM Services. Verizon complies with **RFP Section C.2.1.2.1.4(6)**. Verizon ETS will support circuit emulation services at the TO level for TDM services.

EVCs. Verizon complies with **RFP Section C.2.1.2.1.4(7)**. Verizon ETS provides point-to-point, multi-point-to-multi-point, and point-to-multi-point EVCs.

EVC Multiplexing. Verizon complies with **RFP Section C.2.1.2.1.4(8)** and its ETS will support EVC Multiplexing.

Rate Limiting. Verizon complies with **RFP Section C.2.1.2.1.4(9-10)** and will support rate-limited throughput access links (i.e., 1 Gbps. port rate limited in 100 Mbps. Increments), as well as rate limiting at the agency's SDP and the individual VLAN ingress and egress. Ethernet access speeds are not rate limited, as this is done on a per EVC level.

Physical Interfaces. Verizon complies with **RFP Section C.2.1.2.1.4(12)(a)**. Verizon ETS will comply with applicable UNIs referenced in RFP Section C.2.1.2.3 of the RFP.

Traffic Profiles. Verizon complies with **RFP Section C.2.1.2.1.4(13)(a-d)** and will support the following traffic profiles: Committed Information Rate (CIR), Committed Burst Size (CBS), Peak Information Rate (PIR), and Maximum Burst Size (MBS). The agency subscribed bandwidth for an EVC is known as the CIR. The CIR defines the amount of bandwidth that will be delivered. CIR applies to all CoS types.

Performance Parameters. Verizon complies with **RFP Section C.2.1.2.1.4(14)**, the performance metrics listed in the RFP – Av, Latency, Jitter (Packet), Grade of Service (GOS), Time to Restore, and Grade of Service (Packet Loss=1-GOS).

Service Frame Delivery. Verizon complies with **RFP Section C.2.1.2.1.4(15)(a-c)**.

[REDACTED]

VLAN Tags. Verizon's complies with **RFP Section C.2.1.2.1.4(16)(a-c)** and its ETS

[REDACTED]

[REDACTED]. The VLAN IDs are locally significant on a per-port basis. Tagged (non-Transparent) Ethernet Virtual Connections (EVCs) or Flows will allow only Ethernet frames with VLAN IDs valid for a given Ethernet Access UNI (port) to pass. Frames with invalid VLAN IDs for a UNI are discarded. Valid VLAN IDs are either supplied by the agency to Verizon or Verizon will assign a VLAN ID for all customer Ethernet frames associated with a Tagged EVC/Flow.

Agencies also have the option of requesting EVC or Flow VLAN transparency. With VLAN transparency, Verizon will pass all customer tagged and untagged frames received from the agency on a given UNI. Verizon stacks a VLAN service tag on all of these frames, and this s-tag is used to differentiate these frames from other frames within the network. This s-tag is removed before the frames are returned to the customer with the customer's VLAN tag remaining intact.

For Tagged EVCs/Flows, the VLAN IDs are ordered by the agency or Verizon will select and provision the VLAN IDs in the Network Interface Device (NID). Any invalid VLAN ID received from the customer (i.e., a VLAN ID that has not been ordered/provisioned) is dropped at this point. This virtually eliminates the ability for an agency to "spoof"

another customer's VLAN ID assignments because only those defined as valid for this UNI are passed.

Ethernet frames are checked at each switching point to ensure that they have a valid VLAN ID. Switching decisions are based on the VLAN ID, and any Ethernet frames that do not have a valid VLAN ID for that port are discarded.

Service Multiplexing. Verizon complies with **RFP Section C.2.1.2.1.4(17)**. Service Multiplex UNI requires the use of 802.1Q tagged service frames that provide separation between unique EVCs provisioned over the Ethernet access link, as illustrated in **Figure**



■ Ethernet Access UNI supporting All-to-One Bundling or Service Multiplexing requires the use of VLAN tags, in addition to standard Ethernet overhead, inter-packet gap, and preamble. Throughput is measured at the Ethernet Link level including all applicable overhead, IPG and preamble bytes. The maximum obtainable throughput will vary based on the length of packets that are being transmitted. If a customer is shaping at Layer 2, they should shape for a value less than the line rate.

Bundling. Verizon complies with **RFP Section C.2.1.2.1.4(18)**. The All-to-One Bundling configuration type allows for an agency to have provisioned a single transparent EVC over the Ethernet access circuit. To achieve this, an All-to-One bundling UNI will include a Service Tag (S-tag) on all entering frames and remove the S-tag on all exiting frames.

Performance Monitoring (optional). Verizon complies with **RFP Section C.2.1.2.1.4(20)(a-i)**. At a TO level, Verizon will provide proactive Performance Monitoring, to include: signal failure, signal degradation, connectivity of loss of connectivity, frame loss, errored frames, looping, denial of service (DoS), mis-inserted frames, and maintenance parameters.

Maintenance Functions. Verizon complies with **RFP Section C.2.1.2.1.4(21)(a-c)** and will support maintenance functions to include: alarm suppression, loopbacks (intrusive and non-intrusive), and protection switching, restoration, etc.

Network Topologies. Verizon complies with **RFP Section C.2.1.2.1.4(22)(a-d)**. Verizon ETS supports network topologies that include point-to-point, point-to-multi-point, multi-point-to-multi-point, and rings.

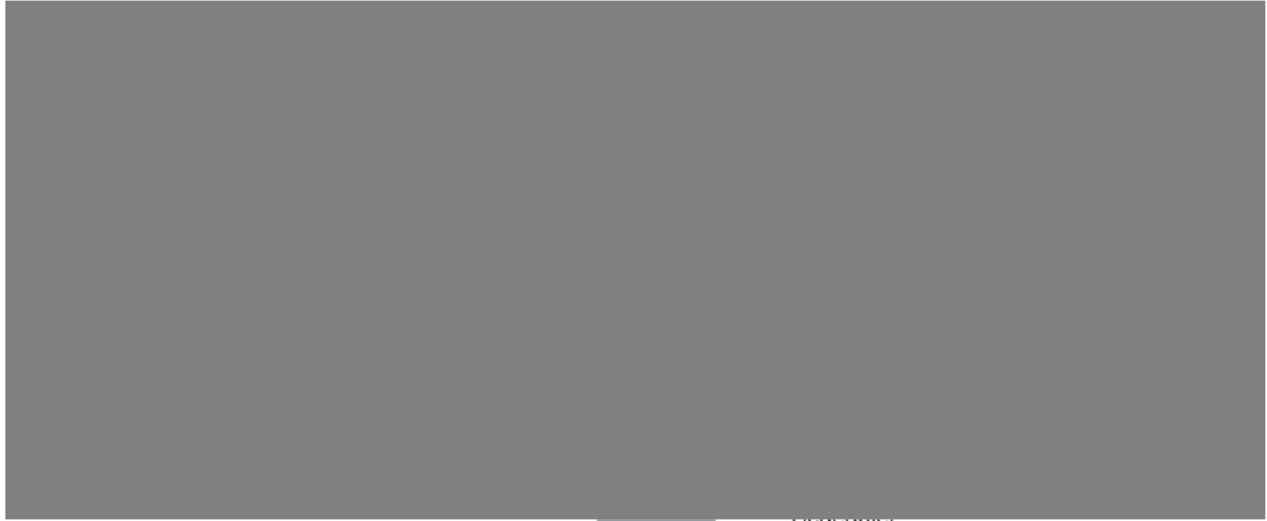
Geographical Diversity. Verizon complies with **RFP Section C.2.1.2.1.4(23)**. ETS supports geographic diversity for added reliability. This allows agencies to plan geographic diversity into their disaster recovery plans, even if their alternate service is provided from the same or a different contractor.

Bridging. Verizon complies with **RFP Section C.2.1.2.1.4(24)**. ETS supports bridging in compliance with IEEE 802.1Q 2014.

Virtual Connections. Verizon complies with **RFP Section C.2.1.2.1.4(25)** and its ETS supports virtual connections for point-to-point Ethernet, and multi-point-to-multi-point connections, up to 100 Gbps.

Quality of Service (QoS). Verizon complies with **RFP Section C.2.1.2.1.4(26)** and will support traffic prioritization that enables higher priority traffic to be transmitted first. Verizon's ETS products (switched E-Line and E-LAN) offer four Classes of Service (CoS). [REDACTED]

[REDACTED]



Schedule



[Redacted text block]

[Redacted text block]

[Redacted text block]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED].

Traffic Reconfiguration and Connection Modifications. Verizon complies with **RFP Section C.2.1.2.1.4(27)**. Verizon ETS supports traffic reconfiguration that provides the ability of an agency to modify a specific service connection subsequent to the establishment of the connection. Changes to an established connection may include upgrade/downgrade of speeds that do not result in physical equipment changes.

Bandwidth on Demand. Verizon complies with **RFP Section C.2.1.2.2(1)** and will support bandwidth increments and decrements on demand, as agreed between itself and the agency. Verizon will indicate what increments are available to modify the contracted bandwidth in near real time. Options for incremental/reduction steps include at least 1, 10, 100 or higher Mbps. Provisioning time for this feature will not exceed 24 hours per instance unless otherwise agreed by the agency and Verizon on a case-by-case basis.

Stipulated Requirements. Verizon complies with the **Functional Definition (C.2.1.2.1.1)**, and all applicable **Standards (C.2.1.2.1.2)**, **Connectivity (C.2.1.2.1.3)**, **Interfaces (C.2.1.2.3)**, and **Performance Metrics (C.2.1.2.4)** RFP requirements.

2.1.2.2 Quality of Services [L.29.2.1, M.2.1]

Verizon ETS utilizes proven Ethernet based technology to provide Switched or Dedicated point-to-point, point-to-multipoint or meshed any-to-any connections. ETS offers highly available, scalable, efficient and cost-effective bandwidth that is ideal for subscribing agency's extended networks as many locations can be connected with speeds up to 100 Gbps.

Verizon works closely with agencies to assess their business applications' sensitivity to packet delivery, latency, availability, and time-to-repair prior to proposing an Ethernet solution. Verizon will evaluate each location to understand which Ethernet Access

solution is right for the subscribing agency's networking needs. Verizon architects its solutions based on key network performance drivers, like device availability, latency, and packet loss, with the built-in flexibility to quickly scale the network as bandwidth needs change. Verizon will provide intra-agency LAN-LAN connectivity including metro, long haul, and global connections. These can be point-to-point or multipoint connections. Verizon will also provide inter-agency LAN-LAN connections, connecting from one agency to another.

Verizon can provide agencies with a seamless network platform with the capabilities, feature sets, and interfaces required, in addition to a global reach and reliability in all of the Core Based Statistical Areas (CBSAs). Verizon's ETS includes 24x7 customer service, advanced reporting capabilities, and competitive service-level agreements. Verizon ETS offerings provide flexible and configurable capabilities to allow agencies to tailor their network to support different traffic needs.

2.1.2.3 Service Coverage [L.29.2.1, M.2.1]

Verizon will support EIS services in a minimum of 25 of the top 100 CBSAs and in compliance with **RFP Section C.1.3** will provide ETS to all government locations within each of its selected CBSAs.

2.1.2.4 Security [L.29.2.1, M.2. .1]

The Verizon ETS is managed for security and risk per Verizon's EIS IT Risk Management Framework (RMF) Plan in **Volume 1, Attachment A**. Appropriate security measures for the selected access solution will be implemented on a TO basis for Internet and related traffic that requires aggregation (reference **Section 3, External Traffic Routing**) to provide security and confirm the integrity of government data. If additional security measures are required they will be addressed at the TO level.

IEEE 802.3. Verizon complies with **RFP Section C.2.1.2.1.4(11)** and privacy and security will be supported per IEEE 802.3 as defined at the TO level.

Security Filters. Verizon complies with **RFP Section C.2.1.2.1.4(19)**. Standard security filters will be supported.

2.1.3 OPTICAL WAVE SERVICE (OWS) [C.2.1.3]

2.1.3.1 Understanding [L.29.2.1, M.2.1]

Verizon's Optical Wave Service (OWS) provides for the transport of high bandwidth optical point-to-point circuits across Verizon's managed shared wavelength network. Verizon's transport network currently uses 100 Gbps waves on a state-of-the-art reconfigurable optical add-drop multiplexer (ROADM) network, which minimizes latency and increases bit error rate (BER) performance. Verizon has been deploying ROADMs since its inception. The OWS includes Verizon fiber, plus fiber integrated from third party vendor relationships, or agency access into its OWS platform. OWS provides a dedicated path for each point-to-point circuit and can be used to connect an agency designated premises to another designated premises, an agency designated premises to a Point-of-Presence (POP) location, to interconnect POP locations, and to connect to other Verizon optical services, such as Dedicated Ring.

2.1.3.1.1 Compliance with EIS Service Requirements [J.19]

OWS Connection Types. Verizon complies with **RFP Section C.2.1.3.1.4(1-3)** and will support non-domestic (optional), Domestic, and metro wavelengths.

Transmission Rates. Verizon complies with **RFP Section C.2.1.3.1.4** and will support wavelengths at 1, 2.5, and 10 Gbps; options for 40 and 100 Gbps; and optional rates beyond 100 Gbps may also be supported, if and when such transmission rates become available.

Clock Transparency. Verizon complies with **RFP Section C.2.1.3.1.4(2)(a-b)** and will support the levels of clock transparency identified in the RFP.

Protocol Transparency – Metro. Verizon complies with **RFP Section C.2.1.3.1.4(3)** and will support Metro wavelengths that are rate and protocol independent.

Protocol Transparency – Domestic and Non-Domestic. Verizon complies with **RFP Section C.2.1.3.1.4(4)** and will support Domestic and Non-Domestic Wavelengths that are rate and protocol independent.

Byte Transparency. Verizon complies with RFP Section C.2.1.3.1.4(5)(a-c), including all byte transparency requirements in the RFP.

Framed Wavelength Concatenation. Verizon complies with RFP Section C.2.1.3.1.4(6). For framed wavelengths, Verizon will support standard/virtual concatenation and channelized UNIs .

Wavelength Channelization (Optional). Verizon complies with RFP Section C.2.1.3.1.4(7). For framed wavelengths, Verizon will support channelized.

SDP Hand-Off. Verizon complies with RFP Section C.2.1.3.1.4(8), including all SDP hand-off requirement identified in the RFP.

Access Methods. Verizon complies with RFP Section C.2.1.3.1.4(9)(a-c), including access methods to the ordered wavelength service for an end-to-end offering; indicating alternatives, if necessary; and specifying the appropriate reach of optical interfaces and the mediation devices or gateways needed.

Government Furnished Property (GFP)/Service Related Equipment (SRE). Verizon complies with RFP Section C.2.1.3.1.4(10)(a-c) and provides multi-vendor interoperability support to the GFP/SRE by completing connectivity using the appropriate UNIs in the three cases identified in the RFP.

Single Wavelength Transport. Verizon complies with RFP Section C.2.1.3.1.4(11) and will confirm that a single wavelength is capable of transporting different types of traffic without the need to use a separate physical wavelength to run IP, Ethernet, etc.

Customer Network Management Level 1 (Optional). Verizon complies with RFP Section C.2.1.3.2(1) and will provide monitoring via Customer Network Management (CNM) Level 1 (optional). Agency personnel will be able to monitor wavelength(s) via alarm messages from the OTN into a software user interface via the Verizon Enterprise Center (VEC) dashboard.

Customer Network Management Level 2 (Optional). Verizon complies with **RFP Section C.2.1.3.2(2)** and will provide management and monitoring of CNM Level 2 (optional) capabilities.

Equipment Protection 1:1 – GFP/SRE. Verizon complies with **RFP Section C.2.1.3.2(3)** and will provide Equipment Protection 1:1 - GFP/SRE to the client interfaces at the SDP as specified in the RFP.

Equipment Protection 1+1 – GFP/SRE. Verizon complies with **RFP Section C.2.1.3.2(4)** and will provide Equipment Protection 1+1 - GFP/SRE to the User to Network Interfaces at the SDP as specified in the RFP.

Network Side Equipment Protection. Verizon complies with **RFP Section C.2.1.3.2(5)** and will provide Equipment Protection - Network side where two channels face the network or full redundancy and equipment protection at the SDP.

Geographically Diverse Wavelengths. Verizon complies with **RFP Section C.2.1.3.2(6)** and will support geographically diverse wavelengths.

Protected Non-Domestic and OCONUS Wavelengths (Optional.) Verizon complies with **RFP Section C.2.1.3.2(7)** and will support protected Non-Domestic and OCONUS Wavelengths (optional).

Protected CONUS Wavelength (Optional). Verizon complies with **RFP Section C.2.1.3.2(8)** and will support protected CONUS Wavelengths using transmission protocols to provide resiliency.

Protected Metro Wavelength. Verizon complies with **RFP Section C.2.1.3.2(9)**, including: protection on a per-wavelength basis; restoration times below 60 ms for single failure; equipment protection, SDPs and UNIs.

Stipulated Requirements. Verizon complies with the **Service Description (C.2.1.3.1)**, **Functional Definition (C.2.1.3.1.1)**, and all applicable **Standards**

(C.2.1.3.1.2), Connectivity (C.2.1.3.1.3), Interfaces (C.2.1.3.3), and Performance Metrics (C.2.1.3.4) RFP requirements.

2.1.3.2 Quality of Services [L.29.2.1, M.2.1]

Verizon's OWS service is driven by Verizon's industry leading OTN network. Verizon is one of a limited number of carriers in the world that offers this high bandwidth, reliable transport. Verizon OWS offers various agency interfaces, transparency and protected/non-protected fiber schemes to meet the unique needs and requirements of the government. Verizon OWS leverages the fiber already in the ground, which prevents the need for future re-engineering due to differences between actual fiber losses and stated design assumptions (a frequent phenomenon in "non-telco" optical designs). Verizon OWS requires no startup cost or capital outlay making it an attractive option for agencies requiring high bandwidth capacity between locations.

Verizon OWS relies on the use of Optical Transport Network (OTN) and Ultra Long Haul transport network technologies to provide best-in-class service. Verizon continually deploys advances in optical transport technology (e.g., Colorless, Directionless, Contentionless (CDC) reconfigurable optical add-drop multiplexers (ROADMS)). This helps drive costs down and increases efficiency, allowing Verizon to offer more features and functions in its services to the government.

2.1.3.3 Service Coverage [L.29.2.1, M.2.1]

Verizon complies with **RFP Section C.1.3** and will support OWS in a minimum of 25 of the top 100 CBSAs.

2.1.3.4 Security [L.29.2.1, M.2.1]

The Verizon OWS is managed for security and risk per Verizon's EIS IT Risk Management Framework (RMF) Plan in **Volume 1, Attachment A**. Appropriate security measures for the selected access solution will be implemented on a TO basis for Internet and related traffic that requires aggregation (reference **Volume 1, Section 3, External Traffic Routing**) to provide security and confirm the integrity of government data. If additional security measures are required they will be addressed at the TO level.

Verizon uses wavelength-division multiplexing (WDM) to comb multiple signals on laser beams at various infrared (IR) wavelengths for transmission along a shared fiber optic media network. Each laser is modulated by an independent set of signals. Wavelength-sensitive filters, the IR analog of visible-light color filters, are used at the receiving end. Verizon is responsible for configuring the wavelength frequency used by each agency, and the filters used at the receiving end prevent the possibility of another agency intercepting a different wavelength.

2.1.4 PRIVATE LINE SERVICE (PLS) [C.2.1.4]

2.1.4.1 Understanding [L.29.2.1, M.2.1]

[REDACTED] t. Verizon delivers this capability from subrate T1s through OC-768, with the Verizon Private Line Service (PLS) portfolio. Under EIS, Verizon will transition existing circuits or provision new circuits and provide agency premises wiring and equipment as dictated by TOs. Verizon

[REDACTED]. Verizon's transition record in implementing and migrating large networks with complex multi-services is [REDACTED]. Verizon PLS is provided over dedicated circuit paths provisioned over SONET rings, which offer automatic restoral capability in the event of a fiber cut, thus resulting in a high level of service availability.

2.1.4.1.1 Compliance with EIS Service Requirements [J.19]

Applicable Routing Requirements. Verizon complies with **RFP Section C.2.1.4.1.4(1-3)**. Verizon PLS will meet applicable routing requirements confirming any encrypted tunnels (see **Section 3.0** for Verizon's response to the External Traffic Routing requirements) are applied and proxied to allow inspection, provide transparency to standards-based protocols used by GFP and data transparency treatment of all bit sequences transmitted by GFP through the SDP.

PLS Categories. Verizon complies with **RFP Section C.2.1.4.1.4(1-16)** and will support the following categories of PLS: DS0, T1, T3, E1, E3, OC-1 (optional), OC-3,

OC-12, OC-48, OC-192, OC-768 (optional), Subrate DS-0 (optional), Analog Line (4KHz) (optional), fractional T1 (optional), and fractional T3.

Multipoint Connection. Verizon complies with **RFP Section C.2.1.4.2(1)** and will allow the interconnection of three or more subscribers' premises, as follows: Branch-Off, Drop-and-Insert.

PLS Circuit Routes. Verizon complies with **RFP Section C.2.1.4.2(2)** and will provide different routes for PLS circuits based on the following arrangements:

Transport Diversity. Verizon complies with **RFP Section C.2.1.4.2**. Between connecting POPs, Verizon will supply two or more physically separated routes for PLS circuits, and these diverse routes will not share common telecommunications facilities or offices. Verizon will maintain a minimum separation of 30 feet throughout all diverse routes. Where uncompromised diversity is not available, Verizon will exert best efforts to propose an acceptable arrangement along with documentation describing the compromise. If diversity is not available or the compromised diversity is not acceptable to the government, it will be negotiated on an individual case basis.

Transport Avoidance. Verizon complies with **RFP Section C.2.1.4.2**. Between connecting POPs, Verizon will provide the ability for an agency to define a geographic location or route on the network to avoid. Where avoidance is not available, Verizon will exert best efforts to propose an acceptable arrangement along with documentation describing the reasons for the unavailability.

Stipulated Requirements. Verizon complies with the **Service Description (C.2.1.4.1)**, **Functional Definition (C.2.1.4.1.1)**, and all applicable **Standards (C.2.1.4.1.2)**, **Connectivity (C.2.1.4.1.3)**, **Interfaces (C.2.1.4.3)**, and **Performance Metrics (C.2.1.4.4)** RFP requirements.

2.1.4.2 Quality of Services [L.29.2.1, M.2.1]

Verizon supports the PLS standards listed in the EIS RFP with the appropriate interface for bandwidth speeds from DS0 through OC-768/STM-256. As a result, Verizon supports termination of PLS services to any Government Furnished Equipment (GFE)

that complies with these standards. Verizon PLS is transparent and will carry government data, as required, for the appropriate service and technology standard.

Verizon's advanced networking technologies, including Optical Transport Network (OTN) deployment, high availability MESH services, and global backbone will accelerate agencies' efforts in realizing efficiencies by identifying areas for consolidation and modernization. Verizon has been a leader in the deployment of Optical Mesh technology, which enables the switching of services residing and connected via wavelengths within the Verizon global backbone in the event of a reduced service quality or outage fault. This allows Verizon to offer high availability services across the globe. Verizon has also spent the last several years deploying OTN technology, which provides for advanced networking capabilities and supports bandwidths up to 100 Gbps and beyond. Refer to **Table 2.1.4.2-1** for a list of Verizon PLS capabilities. Verizon PLS offers reliable guaranteed network availability and protected connectivity for mission critical applications, including voice, data, and video traffic.

Table 2.1.4.2-1. Verizon's PLS Capabilities

Verizon PLS Capabilities	
▪ Global SONET / SDH network	▪ End-to-end Service Level Agreement
▪ High quality reliable digital service	▪ Fully managed by Verizon
▪ Maximum security	▪ High bandwidth speeds
▪ Built-in Protection Capabilities	
▪ Verizon's vast fiber network provides diverse fiber routes, owned, managed and operated by Verizon resulting in the most efficient possible connections.	
▪ Verizon's flexible Metro and Long haul private line options offer a wide range of connectivity.	
▪ One Single Point-Of-Contact for ordering, billing, agency services and fault management.	

2.1.4.3 Service Coverage [L.29.2.1, M.2.1]

Verizon complies with **RFP Section C.1.3** and will support PLS in a minimum of 25 of the top 100 CBSAs.

2.1.4.4 Security [L.29.2.1, M.2.1]

The Verizon PLS is managed for security and risk per Verizon's EIS IT Risk Management Framework (RMF) Plan in **Volume 1, Attachment A**. Appropriate security measures for the selected access solution will be implemented on a TO basis for Internet and related traffic that requires aggregation (reference **Section 3, External Traffic Routing**) to provide security and confirm the integrity of government data. If additional security measures are required they will be addressed at the TO level.

Verizon's PLS provides dedicated private transport services to maximize data security and transmission integrity. Verizon's high-capacity, point-to-point connections can transport voice, video, and data traffic. With Verizon PLS an ordering agency's information travels across the link so it stays safe and secure. **Table 2.1.4.4-1** list additional characteristics of PLS connections:

Table 2.1.4.4-1. PLS Characteristics

PLS Connection Characteristics
Dedicated Connections. Private Line circuits are committed to a single agency.
Protocol Independence. PLS is protocol independent and can transport data, voice, video and IP as Layer 2 or Layer 3 traffic.
Bandwidth Management. Because a Private Line circuit is dedicated to a single agency, the agency has complete control of bandwidth prioritization and Quality of Service (QoS) on the link.

Verizon PLS provides unmatched privacy and security over dedicated transmission circuitry and can support agencies from civilian to DoD and the Intelligence Community.

2.1.5 SYNCHRONOUS OPTICAL NETWORK SERVICE (SONETS) [C.2.1.5]

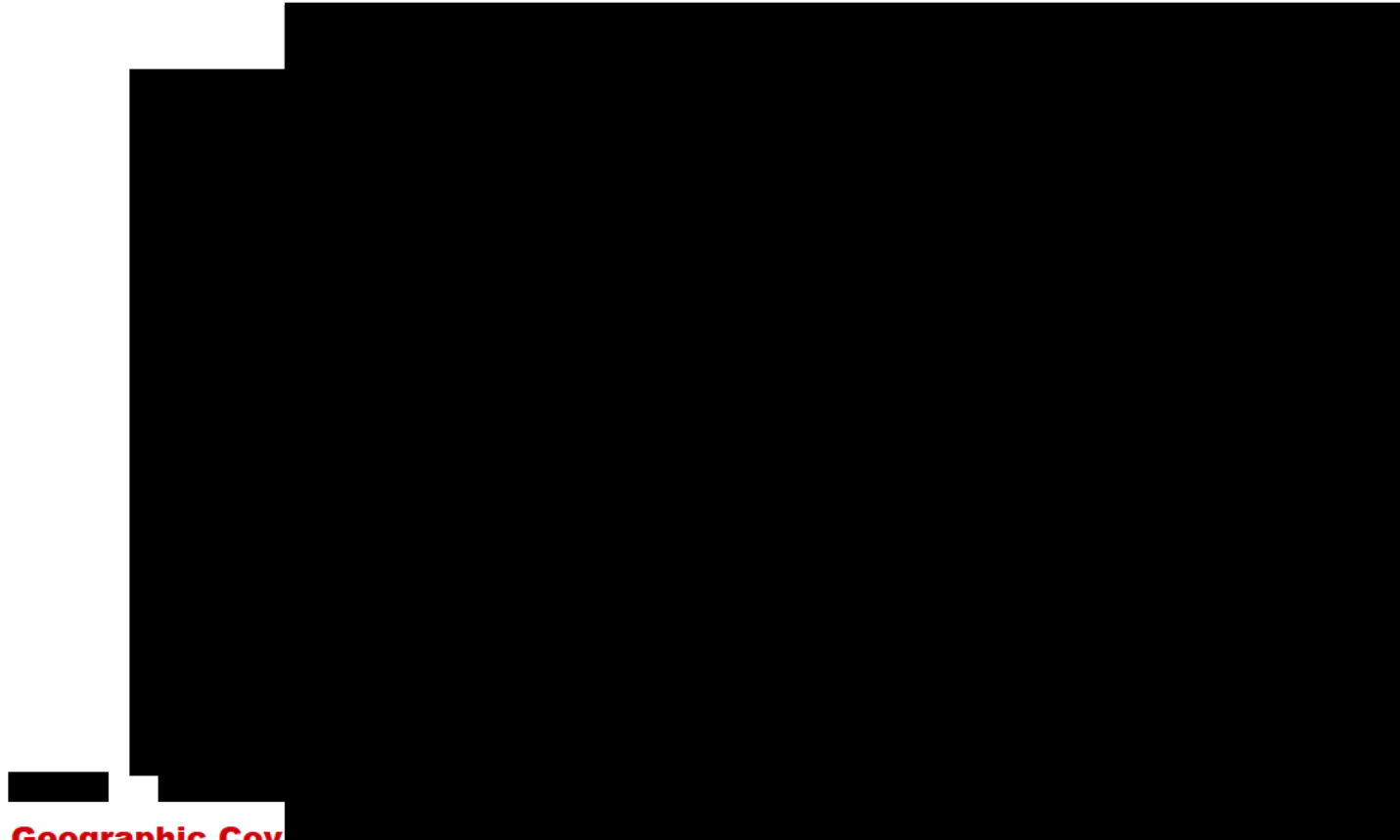
2.1.5.1 Understanding [L.29.2.1, M.2.1]

Verizon's Synchronous Optical Network Service (SONETS) provides high quality, restorable Intra- and Inter-LATA communications with a SONETS handoff over SONETS self-healing ring technology at speeds from OC-3 to OC-192. This service is available with concatenation (full bandwidth) or channelized handoffs. Verizon's OC-3 and OC-12 services can be either linear or restorable. In the increasingly demanding IT environment, many key business drivers can be fulfilled through SONETS, such as those listed in **Table 2.1.5.1-1**:

Table 2.1.5.1-1. SONETS Key Business Drivers

Verizon SONETS Key Business Drivers
▪ Seamless connectivity between geographically diverse sites.
▪ High bandwidth requirements to support mission critical applications.
▪ Data center connectivity.
▪ Disaster recovery and business continuity solutions.
▪ Flexible network services that adapt to new project requirements.
▪ Backhaul for private PBX voice traffic.
▪ Cost-effective solutions that fit within current IT budgets.
▪ Available both within the metropolitan area and between regions.

Dedicated SONETS Ring (DSR) is a resilient, self-healing, high-capacity transport network capable of interconnecting multiple agency locations within the agency network, and enhanced to provide next generation SONETS (see **Figure 2.1.5.2-1**). DSR can be used to construct network backbones over which high-speed, high-volume voice, video, data and Storage Area Networking (SAN) applications can travel. The figure below illustrates a multi-node SONETS ring that can be utilized to link two or more agency locations.



Geographic Cov

offers SONETS in metro areas, nationwide (CONUS) and globally (OCONUS and Non-Domestic).

Gateway Functionality (Optional). Verizon complies with **RFP Section C.2.1.5.1.4(2)**. SONETS provides gateway functionality (SONETS to Synchronous Digital Hierarchy (SDH) and SDH to SONETS conversion) as needed by agency.

Network Topologies. Verizon complies with **RFP Sections C.2.1.5.1.4(3)(a-c)**. SONETS supports point-to-point, ring and mesh topologies.

Protection Methods. Verizon complies with **RFP Section C.2.1.5.1.4(4)(a-b)**. On the Tributary Side, Verizon will support Automatic Protection Switching (APS). On the network side, Verizon will support Unprotected, Mesh Protected, Unidirectional Path Switched Ring (UPSR), Bidirectional Line Switched Ring (BLSR), 1+1, and Bidirectional Path Switched Ring (BPSR) or equivalent as an option on a TO basis.

Transmux Capability. Verizon complies with **RFP Sections C.2.1.5.1.4(5)(a-e)**. SONETS will provide transmux capabilities, as applicable and in compliance with the RFP.

Concatenation Methods (Optional). Verizon is able to offer this optional feature in **RFP Section C.2.1.5.1.4(6)** on an Individual Case Basis (ICB) and will evaluate the requirements at a TO level.

Performance Monitoring. Verizon complies with **RFP Section C.2.1.5.1.4(7)**. Verizon will support the performance monitoring parameters specified in the RFP. Monitoring of parameters will be for each individual minute and recorded in registers of 15 minutes. The last eight 15-minute registers will be archived and made accessible to the agency. Verizon will store all measurements for the past 24 hours in a register.

Error Seconds (ES). Verizon complies with **RFP Section C.2.1.5.1.4(7)(a)**. ES will be counted as 1-second intervals containing at least 1 error. Verizon will measure performance based on percent of error seconds. For all EIS users, percent ES will be less than 0.25 percent during the measurement period.

Severe Error Seconds (SES). Verizon complies with RFP Section C.2.1.5.1.4(7)(b) and will measure performance based on percent of SES. For all EIS users, percent SES will be less than 0.035 percent during the measurement period.

Synchronization and Timing Methods. Verizon complies with RFP Sections C.2.1.5.1.4(8)(a-b) and will support External and Line Timing.

Reserved. C.2.1.5.1.4(9)

Next Generation SONETS (Optional). Verizon complies with RFP Section C.2.1.5.1.4(10) will evaluate the requirements on a TO basis.

SONETS Network. Verizon complies with RFP Sections C.2.1.5.1.4(11)(i-iii). Verizon's network will support Framed Mapped and Transparent Generic Framing Procedure, as well as Virtual Concatenation.

Data Communications Channel (DCC). Verizon complies with RFP Section C.2.1.5.1.4(12) and will provide the agency with the ability to establish communication between its edge devices (optional).

Integrated Control Plane (Optional). Verizon complies with RFP Section C.2.1.5.1.4(13) and will support Integrated Control Plane.

Channelization (Optional). Verizon complies with RFP Sections C.2.1.5.2(1)(1-6) and will support SONETS interfaces to the CPE to seamlessly interface with Verizon's SONETS network for data transport. All applicable channelized arrangements as listed in the RFP will be supported.

DS1 Rate Synchronization (Optional). Verizon complies with RFP Section C.2.1.5.2(2) and will provide the agency with DS1 Rate Synchronization Service. The DS1 will be delivered through External Timing.

SONETS Performance. Verizon complies with **RFP Sections C.2.1.5.2(3)(1-2)**; all SONETS contracted by ordering agencies will comply with the performance indicators and the Performance Metrics (ref. **RFP Section C.2.5.2.4**) referenced in the RFP.

Equipment Protection. Verizon complies with **RFP Section C.2.1.5.2(4)** and will provide protection to the client interfaces at the SDP, where the protection channel is bridged to the failed working channel.

Framing for Electrical Interfaces. Verizon complies with **RFP Section C.2.1.5.2(5)**. The formats for electrical interfaces referenced in the RFP will be supported.

Geographic Diverse Protection. Verizon complies with **RFP Section C.2.1.5.2(6)**. The Geographic Diverse Protection feature will ensure a minimum separation of 25 feet between the diverse circuits end-to-end. Verizon will confirm that the diverse circuits are specifically flagged to prevent disconnection during network grooming activity.

Local and Remote Node Multiplexing. Verizon complies with **RFP Section C.2.1.5.2(7)**. The Local and Remote Node Multiplexing feature will enable the multiplexing of different low-speed circuits onto a high-speed SONETS signal, such as SONETS OC3 and OC12.

Stipulated Requirements. Verizon complies with the **Service Description (C.2.1.5.1)**, **Functional Definition (C.2.1.5.1.1)**, and all applicable **Standards (C.2.1.5.1.2)**, **Connectivity (C.2.1.5.1.3)**, **Interfaces (C.2.1.5.3)**, and **Performance Metrics (C.2.1.5.4)** RFP requirements.

2.1.5.2 Quality of Services [L.29.2.1, M.2.1]

Verizon's Global SONETS network provides high quality reliable digital service with the security of a dedicated connection. Verizon's SONETS is fully managed by Verizon with aggressive Service Level Agreements (SLAs). Verizon offers agencies a single point-of-contact for ordering, billing, customer service and fault management. Centralized

provisioning and maintenance is an inherent SONETS benefit. Verizon manages an agency's network end-to-end within Verizon's footprint, which provides end-to-end-circuit visibility and facilitates prompt repairs.

Dependable, customizable, and safe, SONETS connections will keep agencies' critical operations up and running with a protection path that enables restoration with limited (if any) downtime in the event of line breaks or outages. Verizon's SONETS ring network provides dedicated facilities for greater reliability. In the event of a connection failure or service outage, agency traffic is automatically rerouted via the opposite direction of the ring, thus helping to maintain service connectivity and provide peace of mind. Agencies can rely on Verizon's SONETS services to transport mission-critical voice, data, and video applications over resilient, self-healing ring architecture. Verizon DSR is structurally built with redundancy to eliminate and avoid loss of services. The dedicated ring architecture is designed to route traffic around any failures, providing reliable, secure communications. Verizon DSR services offer 24x7 monitoring and support, and competitive SLAs.

2.1.5.3 Service Coverage [L.29.2.1, M.2.1]

Verizon complies with **RFP Section C.1.3** and will support SONETS in a minimum of 25 of the top 100 CBSAs.

2.1.5.4 Security [L.29.2.1, M.2.1]

The Verizon SONETS is managed for security and risk per Verizon's EIS IT Risk Management Framework (RMF) Plan in **Volume 1, Attachment A**. Appropriate security measures for the selected access solution will be implemented on a TO basis for Internet and related traffic that requires aggregation (reference **Section 3, External Traffic Routing**) to provide security and confirm the integrity of government data. If additional security measures are required they will be addressed at the TO level.

2.1.6 DARK FIBER SERVICE (DFS) [C.2.1.6]

2.1.6.1 Understanding [L.29.2.1, M.2.1]

Verizon operates one of the largest fiber networks in the world with almost [REDACTED]

[REDACTED]

These partnerships will allow Verizon to provide the government a unique set of combined DFS assets. Additionally, with this combined capability Verizon and its partners can offer agencies DFS at the Metro and Long Haul (National and International) level.

Verizon DFS partners extend the Verizon network footprint over [REDACTED] route miles, and will allow fiber-based connectivity between major data centers, carrier PoPs, and government buildings. Verizon DFS enables agencies control of their network and provides immense bandwidth for a lower cost than lit circuits. DFS offers a physically secure, private platform that agencies can craft to specific service configurations, based on factors like security, latency, and other priorities. Verizon's DFS is an optimal solution for agencies that need major bandwidth, physical security, and control in support of a variety of applications, data computing, information storage and high definition video. The Verizon DFS team has unique expertise in creating custom solutions and a track record of successful implementations.

2.1.6.1.1 Compliance with EIS Service Requirements [J.19]

Configuration Alternatives. Verizon complies with **RFP Section C.2.1.6.1.4(2)(a-d)** and will support the following network topologies: point-to-point, route diversity ring/single drops, route diversity ring/dual drops, star configurations, and hybrid configurations.

Fiber Service Delivery Point (FSDP). Verizon complies with **RFP Section C.2.1.6.1.4(1)** and will support the SDP at either the fiber patch panel where fibers terminate at a government location or the collocation facility where the agency has installed its optronics, as required by the agency. Verizon will meet Optical Fiber conditions when delivering DFS to an agency.

Optical Fiber. Verizon complies with **RFP Section C.2.1.6.1.4(1)(a)**. The Optical Fiber will meet the standards specified in **RFP Section C.2.1.6.1.2** and Verizon will

provide the number of fiber strands to be delivered at the FSDP, as specified by the agency.

Ducting. Verizon complies with **RFP Section C.2.1.6.1.4(2)** and will provide the number of ducts between connecting locations and the number of fiber strands running in each duct, as specified by the agency.

Future Growth (Optional). Verizon complies with **RFP Section C.2.1.6.1.4(3)** and will include an additional duct running in parallel to the working duct(s), if possible.

Channel Count. Verizon complies with **RFP Section C.2.1.6.1.4(4)(a-b)**. Deployed fibers will be able to support a minimum of 80 DWDM wavelengths or user data with spacing, and of operating in the "C", "S" and "L" bands.

Gateways. Verizon complies with **RFP Sections C.2.1.6.1.4(5)(a-g)** and will provide the ability to add and drop traffic via gateway locations and will fulfill sub-requirements a-g in this section of the RFP and provide updates on improvements or expansions throughout the life of the contract.

Service Components. Verizon complies with **RFP Section C.2.1.6.1.4(6)(a-c)**; DFS service components will include Trunks, Laterals, and Building Entrances.

Colocation Service. Verizon complies with **RFP Section C.2.1.6.2(1)** and will provide the ability to add/drop traffic (gateways) and to regenerate and amplify traffic where needed.

Duct. Verizon complies with **RFP Section C.2.1.6.2(2)** and will support the number of ducts (conduits) as specified by the agency that will be included in the service (optional).

Dark Fiber Local Loop. Verizon complies with **RFP Section C.2.1.6.2(3)** and will provide Dark Fiber connection between the agency's location and Verizon's wire center or outside plant (hut or regeneration location).

Diverse Route Single Drop. Verizon complies with **RFP Section C.2.1.6.2(4)** and will verify that two diverse paths are available on the network to prevent service interruptions if a fiber on either of two paths is damaged. A single add/drop location/network element will be used in this arrangement with automatic protection switching capabilities.

Diverse Route Dual Drop (Optional). Verizon complies with **RFP Section C.2.1.6.2(5)**. As an option, Verizon will provide two diverse paths end-to-end to prevent service interruptions caused by a failure either in Verizon's network or at the drop's path. A second contractor will provide the diverse route should the agency require full diversity for protection, unless the working link provider is able to do so.

Inter-City Connectivity. Verizon complies with **RFP Section C.2.1.6.2(6)**. As an option, Verizon will support a dark fiber connection between agency's locations in metro areas, CONUS and OCONUS.

Multiple Duct (Optional). Verizon complies with **RFP Section C.2.1.6.2(7)** and can upgrade to multiple ducts.

Splicing. Verizon complies with **RFP Section C.2.1.6.2(8)** and will support joining two or more lengths of optical fiber cables by way of either fusion or mechanical splicing.

Off Net Laterals. Verizon complies with **RFP Section C.2.1.6.2(9)** and will provide fiber cables, funded by the agency, from the agency's premises to the nearest splice point on the cable trunk. The cable length may vary from a few meters to several kilometers.

Stipulated Requirements. Verizon complies with the **Service Description (C.2.1.6.1)**, **Functional Definition (C.2.1.6.1.1)**, and all applicable **Standards (C.2.1.6.1.2)**, **Connectivity (C.2.1.6.1.3)**, **Interfaces (C.2.1.6.3)**, and **Performance Metrics (C.2.1.6.4)** RFP requirements.

2.1.6.2 Quality of Services [L.29.2.1, M.2.1]

Verizon's DFS starts with a team of experienced network designers who evaluate an agency's requirements, as documented within the TO, to propose a solution. Verizon's DFS team will carefully review the proposed solution with the agency to confirm it meets the requirements prior to implementation. DFS offers many advantages to agencies looking to operate their own private networks in order to meet bandwidth, latency and diversity requirements.

With DFS, Verizon can provide agencies with an extensive global network with significant fiber in the [REDACTED]. Verizon's DFS partners are dedicated to continually growing the network through new construction and acquisitions. Verizon offers the ability to custom design solutions for both long haul and metro fiber connections between government facilities and bringing these connections to carrier neutral collocation facilities. Verizon's expansive collocation facility list offers immediate access to the most important domestic and international networks, content providers and Internet Service Providers (ISPs). Combining Verizon's collocation capabilities with its existing dark fiber footprint offers timely delivery of interconnection services.

2.1.6.3 Service Coverage [L.29.2.1, M.2.1]

Verizon complies with **RFP Section C.1.3** and will support DFS in a minimum of 25 of the top 100 CBSAs.

2.1.6.4 Security [L.29.2.1, M.2.1]

The Verizon DFS is managed for security and risk per Verizon's EIS IT Risk Management Framework (RMF) Plan in **Volume 1, Attachment A**. If additional security measures are required they will be addressed at the TO level.

Verizon's DFS provides secure intercity connectivity to take control of agency networks and meet growing bandwidth, latency and special diversity demands. [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

2.1.7 INTERNET PROTOCOL SERVICE (IPS) [C.2.1.7]

2.1.7.1 Understanding [L.29.2.1, M.2.1]

Verizon helps agencies harness the power the Internet offers through a full suite of Internet Protocol Services (IPS) that span broadband, dedicated, fiber-to-the-premises, and VPN options designed to provide global availability, secure accessibility, reliable performance, and swift navigation.

Verizon IPS includes mature offerings with proven technology and capabilities that provide low risk in terms of outages, Denial of Service (DoS) attacks, and performance issues on the WAN link. [REDACTED]

[REDACTED]

2.1.7.1.1 Compliance with EIS Service Requirements [J.19]

Routing Requirements. Verizon complies with RFP Section C.2.1.7.1.4(1) and will meet applicable routing requirements specified in RFP Section C.1.8.8.

IPS Ports. Verizon complies with RFP Section C.2.1.7.1.4(2) and will provide IPS ports at the peak data rates specified by the customer.

Access Services. Verizon complies with RFP Section C.2.1.7.1.4(3) and will support appropriate access services to connect customers' SDPs to Verizon's IPS.

IPS Network. Verizon complies with RFP Sections C.2.1.7.1.4(4)(a-d). Verizon's network will have established public peering arrangements from its network to the Internet, private peering arrangements from the network with redundant links to connect to its private peering partners, support for the government-assigned and InterNIC-registered IP addresses and domain names, and primary and secondary DNS to provide redundant authoritative name servers for the customer.

Verizon's peering arrangements are designed to provide agencies with high levels of performance and efficiency in traffic distribution. [REDACTED]

[REDACTED]

[REDACTED] It uses direct point-to-point links for peering interconnection.

[REDACTED]

[REDACTED]

Peering interconnections take place across a mixture of public Internet exchange points (IXPs) and direct interconnections with nearly all countries using a public IXP for at least a portion of the peering traffic exchanged. [REDACTED]

[REDACTED]

[REDACTED]

Border Gateway Protocol (BGP). Verizon complies with RFP Section C.2.1.7.1.4(5) and will provide support for the Border Gateway Protocol (BGP) for EIS customers with registered Autonomous System (AS) numbers.

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

Class of Service (CoS). Verizon complies with RFP Section C.2.1.7.2(1)(1-3) and will accommodate and itemize an agency's applications using CoS markings so the network will consistently allow for traffic prioritization and cost-efficiencies. The CoS or prioritization levels may be categorized as premium, enhanced, and standard.

Stipulated Requirements. Verizon complies with the relevant Standards (C.2.1.7.1.2), Connectivity (C.2.1.7.1.3), Interfaces (C.2.1.7.3), and Performance Metrics (C.2.1.7.4) RFP requirements.

2.1.7.2 Quality of Services [L.29.2.1, M.2.1]

[REDACTED]. The network carries traffic flow at the highest transmission rates available today (40 Gbps domestically with a resilient backbone sized at 100 Gbps). The backbone features a fast converging core protected against fiber cuts by true optical switches that restore traffic in less than 50 milliseconds. This attention to design allows agencies to confidently utilize Verizon IPS knowing of its high reliability and expandability to support future growth.

2.1.7.2.1 Global Scale and Flexible Options for Delivery and Management

Verizon's scale, delivery, and management options provide agencies the flexibility to invest in innovation, manage costs, and maintain operational controls in the proper balance.

2.1.7.2.2 Network Monitoring

The Verizon Government Network Operations and Security Centers (GNOSCs) [REDACTED] offer agencies individualized support for their Internet solutions, and oversee and direct network monitoring activities at Verizon Global Network Operations Centers (NOCs) [REDACTED]. Both the customer edge device and the devices in the Verizon network are monitored every 30 seconds via Internet Control Message Protocol (ICMP). Syslog data is analyzed for any indication of service outage, degradation, and other network anomalies.

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

configuration to support their mission needs. Please refer to **Section 3** of this proposal volume for additional information regarding Verizon's compliance with **RFP Section C.1.8.8**, National Policy Requirements.

Verizon IPS using Ethernet access is more scalable than traditional TDM circuits. Agencies can upgrade through a wide range of Internet bandwidths without having to install different local access circuits. Bandwidth speeds can be increased and decreased, as needed. Verizon's IPS will support native IPv4, Dual Stack (IPv4 plus IPv6), native IPv6, and tunneled IPv6 in the Americas, EMEA, and Asia-Pacific regions.

2.1.7.3 Service Coverage [L.29.2.1, M.2.1]

Verizon complies with **RFP Section C.1.3** and will support IPS in a minimum of 25 of the top 100 CBSAs.

2.1.7.4 Security [L.29.2.1, M.2.1]

The Verizon IPS is managed for security and risk per Verizon's EIS IT Risk Management Framework (RMF) Plan in **Volume 1, Attachment A**. If additional security measures are required they will be addressed at the TO level.

Verizon IPS is backed by the support of its skilled teams that monitor the network 24x7. Verizon NOCs employ best practices to provide world-class performance and support to their customers. Verizon also maintains a staff of security experts who provide 24x7 dedicated Internet customer support for security incidents. Verizon's dedicated security experts in the GNOSCs monitor the networks for virus and worm activity to help identify and resolve any network-based security issues.

Verizon will comply with RFP Section H.27 Acceptable Use Policy, and the Government's AUP shall prevail over the terms of any other AUP used by Verizon or any of its subcontractors.

2.2 Voice Services [C.2.2]

2.2.1 INTERNET PROTOCOL VOICE SERVICE (IPVS) [C.2.2.1]

2.2.1.1 Understanding [L.29.2.1, M.2.1]

Verizon will provide a compliant Internet Protocol Voice Service (IPVS) solution based on Verizon's hosted Voice over Internet Protocol (VoIP) platform that has been commercially available for over two years. Verizon is in the process of implementing a new, fully redundant platform which will be located in two geo-diverse data centers and will be customized to meet the unique requirements of the federal government. Verizon currently provides IPVS services to many public sector () and commercial customers.

Verizon's hosted IPVS platform is an advanced communications system designed to support a wide variety of agency requirements including single and multi-site deployments for small, medium, and large agencies. The base service will provide on-net and off-net calling termination, as well as interworking with CONUS, OCONUS and Non-Domestic PSTN networks.

As a way to provide added value to the government, Verizon's platform will provide ordering agencies with the ability to upgrade and add Verizon's Unified Communications Service (UCS) (detailed in **Section 2.8.3**) with capabilities like video calling, audio/video conferencing, instant messaging, presence, and collaboration applications.

IPVS Service Description. Verizon IPVS offers enterprises custom-built, end-to-end communications solutions that are delivered securely and reliably via the Verizon network. **Table 2.2.1.1-1** below lists additional IPVS capabilities and **Figure 2.2.1.1-1** shows how "Verizon Advanced Communications" encompasses several hosted VoIP services, as well as Session Initiation Protocol (SIP) Trunking.

Table 2.2.1.1-1. IPVS Capabilities

IPVS Capabilities	
<ul style="list-style-type: none">■ Unlimited domestic local and long distance calling■ Enhanced business voice features■ Carrier-grade, redundant platform architecture■ Administrator and User Web portals	<ul style="list-style-type: none">■ 24x7 support■ Customer training■ Simple Installation■ Local Number Portability

Figure 2.2.1.1-1. Verizon Advanced Communications



IPVS is delivered over a carrier-grade architecture specifically designed to meet or exceed government requirements. The platform is located in the U.S. and is supported by U.S. based employees of Verizon's GNOSCs (Government Network Operations and Security Centers) [REDACTED]. Verizon IPVS and related back office systems will support IPv4, IPv6 and dual stack environments.

Service Model. The Verizon IPVS Service Model is based on Verizon fully managing the platform including capacity, performance, reporting, compliance, and back-office integration. In addition, Verizon provides tools for streamlined site assessment, ordering, provisioning and remote management. Customers are provided with on-line training options, access to a self-service administration portal and a unified helpdesk for full lifecycle support. This service model is designed to allow ordering agencies to leverage their existing assets and support processes to obtain high quality services at a low price point.

Platform Support. Verizon will fully manage the service delivery platform including design, implementation, maintenance, configuration management, security certification, patching, and software upgrades on an ongoing basis in a manner that is transparent to end-user agencies. Verizon also provides ongoing network performance monitoring so adequate resources are available as the number of users increases throughout the lifecycle of the EIS contract. Platform hardware/software, networking/security infrastructure, end-to-end SLA management tools, data center resources and platform intra-connectivity will be the responsibility of Verizon. **Table 2.2.1.1-1** identifies the capabilities ordering agency administrators and end users will have access to.

Table 2.2.1.1-1. IPVS Ordering Agency Capabilities

IPVS Administration	
IPVS Ordering Agency Administrators	<ul style="list-style-type: none"> Assign users, phones, and stations Setup Auto Attendant, Hunt Group, Group Paging Manage features for end-users Maintain Phone Inventory
IPVS Ordering Agency Administrators and End Users	<ul style="list-style-type: none"> Access and manage voicemail and unified messaging settings Visual Voicemail Manage personal calling features in real-time Define custom time of day, day of week, call handling rules 24x7 access to an administrator/end-user portal to manage the service, monitor performance, and submit tickets, as necessary Round the clock technical and software support via a single helpdesk

Verizon reinforces this support with a full range of optional services, as listed in **Table 2.2.1.1-2** below:

Table 2.2.1.1-2. IPVS Optional Services

IPVS Optional Services
Network Design and Engineering.
Site Assessment/Remediation.
Robust customer training options including a welcome kit, quick reference guides, video tutorials and on-site instructor-led web training.
Site implementation services for WAN, LAN, and end-user devices.
Post implementation close support to confirm newly added end users are able to maintain productivity throughout the implementation phase.

Verizon IPVS Service Components. Verizon IPVS utilizes into an ordering agency's existing wide and local area network (WAN/LAN). In the standard offer, both the router and network switch are agency provided although Verizon also offers fully managed WAN/LAN equipment and services as an option. Verizon IPVS is an "over-the-top" service that places voice calling on top of the underlying network fabric (Verizon provided or third party), as depicted in **Figure 2.2.1.1-2**. The handsets, network probe and optional gateways are connected to a network switch that sits behind the agency's edge router. The Receptionist and Mobile Clients are optional applications to address additional agency needs.



Table 2.2.1.1-3. IPVS End User Features

IPVS End User Features		
3-way Conference Calling	Call Waiting	IP Telephony Manager (Subscriber)
Call Forward – All	Caller ID	Last Number Dialed
Call Forward – Busy	Class of Service Restriction	Multi-Line Appearance
Call Forward - Don't Answer	Directory Assistance	Specific Call Rejection
Call Hold	Distinctive Ringing	Speed Dial
Call Number Suppression	Do Not Disturb	Voice Mail
Call Park	Hotline	Auto Attendant
Call Pickup	Hunt Groups	
Call Transfer	IP Telephony Manager (Administrator)	

Table 2.2.1.1-4 lists the applications included with Verizon's IPVS solution.

Table 2.2.1.1-4. IPVS Standard Applications.

IPVS Standard Applications	
Mobile App	The Mobile App allows the use of an Apple or Android smartphone as an endpoint of the IPVS service, allowing single number reach and enabling customers to always appear to be calling from their office regardless of their actual location.
UCS Desktop Client	The UCS desktop client supports the following features: Desktop Softphone: A native Microsoft® Windows® and Apple OS® soft client that provides voice calling for VoIP and desk phones Voice calling (VoIP) Voice calling (desk phone control) IPVS call settings Instant Messaging and Presence Integration with Outlook or Lync

Desktop and Mobile Client. Verizon IPVS clients allow end-users to communicate easily and efficiently with co-workers and customers while at their desks or on the go using the features listed in **Table 2.2.1.1-5**:

Table 2.2.1.1-5. IPVS Desktop & Mobile Client Features

IPVS Desktop & Mobile Client Features
Instant messaging with presence
Desktop sharing (optional upgrade)
Point-to-point video calling (optional upgrade)
Instant meeting audio conferencing (optional upgrade)
Inbound Fax
Single number reach whether in the office or mobile
Presents agency caller ID whether on agency or personal smartphone

Handsets, Phones and Headsets. Verizon will support, on a best effort basis, utilization of customer provided phone sets. For the best end-user experience, use of Verizon-provided high definition handsets is recommended.

Verizon's IPVS also supports a variety of SRE, such as dedicated conference room phones and headsets, incorporating industry standards.

Analog Telephone Adapters/Analog Gateways. Verizon's IPVS certified SRE provides ordering agencies with support for traditional user-to-network interfaces (UNI's), including analog telephones and ISDN BRI endpoints. Additional gateway options provide the possibility to interconnect to local PSTN trunks (analog/ISDN PRI) for site survivability, and 911 calling applications.

Network Probes. To provide the required end-to-end SLA adherence and reporting requirements, IPVS includes provisioning a probe at the ordering agency's site. The probe, which is placed on the agency LAN, is used by Verizon to perform a variety of functions, such as: troubleshooting of voice issues; providing technicians with network diagnostics; and pinpointing problematic devices and network conditions quickly.

Augmented 911/E911 Service. Verizon's IPVS gives ordering agency's end users the ability to move throughout the enterprise while supporting 911 call delivery and correct location reporting. The location reported for the user will be associated with the service address of the DID assigned to that user. As end users move, they are able to modify their geographic location details through the IPVS web portal.

As an optional enhancement to IPVS, for agencies that require additional granularity for location reporting, Verizon offers professional services engagements to map the end user agency enterprise by building, zone or office number.

Verizon also supports the IPVS Public Service Answering Point (PSAP) connection feature option and provides secure remote access to the government via a web browser to allow for maintenance of the government's profile on an ongoing basis (e.g., to account for moves, adds, deletions, or other changes).

Professional Services. A key component of IPVS is a full range of professional services, which can be designed to any ordering agency's unique requirements.

IPVS Professional Services

- Service Design and Engineering
- Site Survey/Remediation
- On-Site Installation
- Train the Trainer or End User On-Site Training

ASIST. The Verizon ASIST team will contact new agency/sites within 24-48 hours after activation to conduct a "Wellness Check". This dedicated support is available for the first 20 business days of service to confirm customer satisfaction.

IPVS ASIST Personalized Assistance

- Onboarding
- Number Porting
- Use of Admin and End-User Dashboards
- Use of phone equipment
- Configuring Auto Attendants, Hunt groups, and other features

Service Requirements and Assumptions. Primary service locations shall be designated by customers for each of its end users (per assigned telephone number) at the time services are activated. The customer is responsible for notifying Verizon of any changes in service locations for its end users. Accurate information regarding the origination point of calls is necessary for emergency services, appropriate rate information, and proper application of taxes and surcharges. Consequently, it is a material condition of voice over IP services that end user customers provide Verizon with accurate information regarding service location.

2.2.1.1.1 Compliance with EIS Service Requirements [J.19]

Non-Domestic Locations. Verizon complies with RFP Section C.1.2 and provides Voice services to non-domestic locations, as defined in J.1.2.

Hosted and Premises-Based IPVS. Verizon complies with **RFP Section C.2.2.1.1** and **C.2.2.1.1.4**. Over Verizon's IP network, Verizon will provide network-based (hosted) and premises-based IPVS over the Verizon-provided IP network. Verizon will also provide a Managed LAN Service and SIP Trunking Service.

IPVS Technical Capabilities. Verizon complies with **RFP Section C.2.2.1.1.4** and will include unlimited on-net to on-net and on-net to CONUS off-net calling and support off-net calling to CONUS, OCONUS, and Non-Domestic locations. Verizon will enable calling between EIS users and PSTN end points. Verizon will also provide a remote access capability that, once enabled, provides users with the ability to use any landline or cell phone to make or receive phone calls as if they were making or receiving calls with VoIP phones.

Additional IPVS Capabilities. Verizon complies with **RFP Section C.2.2.1.1.4(1-9)**. Verizon's IPVS will provide capabilities for 1) real time transport of voice, facsimile, and TTY communications, 2) and delivery of ANI information (when provided from the originating party), 3) interoperation with public network dial plans (e.g., North American Numbering Plan and ITU-E.164), 3) private network dial plans and support direct dialing, and 5) non-commercial, agency-specific 700 numbers, 6) IPVS will provide access to public directory and operator assistance services, 7) unique directory numbers for on-net government locations, including support for existing government numbers, 8) support the capability to initiate automatic callback and 9) 3-way calling.

Gateways for Interoperability. Verizon complies with **RFP Section C.2.2.1.1.4**. Verizon will provide the following gateways for interoperability between Verizon's IP-based network and the PSTN, or with agency UNIs, as required by ordering agency.

Station Mobility. Verizon complies with **RFP Section C.2.2.1.1.4**. Verizon will provide the capability to support station mobility, enabling IP users to dynamically move their IP phones within the agency's enterprise wide network and access IP services. Verizon's methodology is based on user log-in. When they change locations and log-in, calls will then be delivered to the new location.

Interoperability with Agency Firewalls. Verizon complies with **RFP Section C.2.2.1.1.4**. Verizon's IPVS will have the capability to traverse and successfully interoperate with agency firewalls and security layers. Verizon will verify IPVS compatibility with individual agency firewalls during the service delivery process.

Security Practices/Safeguards. Verizon complies with **RFP Section C.2.2.1.1.4**. Verizon will provide and regularly update and audit security practices and safeguards - including SIP-specific gateway security for SIP firewalls - for: 1) Denial of Service; 2) Intrusion; and 3) Invasion of Privacy.

Emergency Service Requirements. Verizon complies with **RFP Section C.2.2.1.2**. Verizon will full comply with emergency service requirements, including location identification and routing requirements.

IPVS Features. Verizon complies with **RFP Sections C.2.2.1.2(1-4)**. Verizon's IPVS will offer the following capabilities/features, meeting all minimum requirements and providing the functionality/features set forth in **RFP Section C.2.2.1.2**: 1) Voice Mail Box, 2) Auto Attendant, 3) Three-way Conference Calling, and 4) augmented 911/E911 Service (Optional).

Additional IPVS Features. Verizon complies with **RFP Section C.2.2.1.2**. Verizon's IPVS will include all features (1-23) listed in this section of the EIS RFP.

Managed LAN Service. Verizon complies with **RFP Section C.2.2.1.5** and will offer a Managed LAN Service (MLS) as an option to IPVS users. The MLS will provide and manage LAN networking hardware components to extend the IPVS from site demarcation point to the terminating user device. The associated Layer 2 equipment provided by Verizon will support Power over Ethernet (PoE). Verizon will provide, manage, maintain, repair, or replace all Verizon-owned equipment necessary to provide components of the MLS.

IPVS Site Demarcation Point Extension. Verizon complies with **RFP Section C.2.2.1.5(1)** and will provide the hardware and licensing necessary to extend the IPVS

site demarcation point to the terminating device, for both hosted and premises-based solutions.

Interoperability with VoIP-ready Cabling Infrastructure. Verizon complies with **RFP Section C.2.2.1.5(2)**. Verizon's hardware/software solution will interoperate with the ordering agency's VoIP-ready cabling infrastructure and Verizon will identify any cabling limitations with regard to either form of VoIP solution on a TO basis.

Ongoing Maintenance and Upgrades. Verizon complies with **RFP Section C.2.2.1.5(3)** and will be responsible for the ongoing maintenance and upgrades of the Verizon-owned equipment used to provide the MLS. If Verizon replaces, makes any changes to its equipment or device software, or reprograms user devices in order to meet the required service performance level, the government will not incur any additional cost.

Installation Time Intervals. Verizon complies with **RFP Section C.2.2.1.5(4)** and will propose installation time intervals for additional user devices at sites already using an MLS.

No Wireless Device/Components, Data Video. Verizon complies with **RFP Section C.2.2.1.5(5-6)**. The MLS will not include any wireless devices or components on the LAN and will not support other services unless requested and approved by the government.

Authorized Devices. Verizon complies with **RFP Section C.2.2.1.5(7)**. Verizon will confirm that only authorized user devices (as determined by the ordering agency) can operate on the MLS.

Monitor, Manage and Restore 24x7. Verizon complies with **RFP Section C.2.2.1.5(8)**. Verizon will monitor, manage and restore the MLS on a 24x7 basis.

LAN Management Activities. Verizon complies with **RFP Section C.2.2.1.5(9)**. Verizon will specify the LAN management activities being provided as part of the MLS, and identify those activities considered customer responsibilities in a) configuration

management, b) moves, adds, changes, disconnects (MACDs), c) service/alarm monitoring and fault management, d) ticket creation, e) proactive notification, and f) trouble isolation and resolution on a TO basis, as shown in **Table 2.2.1.1.1-1**.

Table 2.2.1.1.1-1. IPVS Managed LAN Activities & Responsibilities

Activity	Verizon	Customer
Configuration Management	Verizon will maintain configuration records and provide to customer upon request.	
Moves, Adds, Changes, Disconnects (MACDs)	Verizon will provision any Moves, Adds or Changes based on customer requests/orders.	Ordering agency is expected to provide details of requested changes, in writing to Verizon, as well as connection of GFE cabling to Verizon's Managed LAN devices.
Service/Alarm Monitoring and Fault Management	Verizon will provide full alarm monitoring and notification to designated customer contacts.	Customer is expected to provide up-to-date information on who should be notified in the event of a service impacting alarm or condition.
Ticket Creation	Verizon will work the ticket to resolution.	Customer is responsible for initiating a ticket for any service impacting condition agency users identify.
Proactive Notification	Verizon will provide proactive notification for any scheduled maintenance activity that may impact service continuity.	Customer will acknowledge notification.
Trouble isolation and resolution	Verizon will provide trouble isolation and resolution once a ticket is opened.	Customer is responsible for initiating a ticket for any service-impacting condition agency users identify.

Proactive Notification. Verizon complies with **RFP Section C.2.2.1.5(10)**. Verizon will provide proactive notification of major and minor alarms to the MLS via email to the contacts identified by the ordering agency. Alarm notifications will be sent to all identified POCs within 15 minutes of alarm detection by Verizon.

Escalation Path. Verizon complies with **RFP Section C.2.2.1.5(11)**. Verizon will define the escalation path for trouble tickets for both network and hardware issues. This escalation path will be identified by level of severity and will include personnel for each level of escalation as well as guidelines and timing for the next step in escalation.

SIP Trunking Service. Verizon complies with **RFP Sections C.2.2.1.6 and C.2.2.1.6.1(1-4)**. SIP Trunking will be integrated with IPVS to support calling to on-net and off-net locations and provide the following capabilities to enable SIP users to establish and receive telephone calls between both on-net locations and the PSTN: 1) automatic call routing; 2) bandwidth QOS management; 3) trunk bursting; and 4) telephone number blocks (DID).

Designed for customer locations equipped with an IP PBX, IP Trunking service is delivered via a standards-based SIP trunk directly to the customer's IP PBX. IP Trunking offers single and multi-site configurations and is certified for use with most

major IP PBX platforms. Verizon currently provides SIP Trunking to federal customers via both the Networx and WITS3 contracts. In addition, Verizon offers IP Integrated Access which supports legacy PBXs using TDM-to-IP media gateways which are provided as SRE.

Stipulated Requirements. Verizon understands the IPVS **Functional Definition (C.2.2.1.1.1)** and complies with the **Service Description (C.2.2.1.1)**, **Standards (C.2.2.1.1.2)**, **Connectivity (C.2.2.1.1.3)**, **Interfaces (C.2.2.1.3)**, and **Performance Metrics (C.2.2.1.4)** requirements referenced in the EIS RFP.

2.2.1.2 Quality of Services [L.29.2.1, M.2.1]

IPVS. Verizon performs a thorough Quality of Service assessment of the environment in which IPVS is being delivered. Verizon's pre-qualification tools and network probes are both designed so IPVS agencies have a high-quality voice experience. The pre-qualification test is conducted prior to order submission and verifies the ordering agency's network is equipped to carry voice. The test activity will include DHCP, Firewall and DNS proxy settings, as well as bandwidth validation. The access layer bandwidth will determine how many simultaneous calls can be safely handled at the end user location. If any of the tests fail, the agency is provided with guidance on changes that are needed before placing an order.

Additionally, a network probe is provided at no cost to IPVS customers and is shipped out with the phones. The probe is plugged into the customer's network and, in the event of a service affecting issue, allows Verizon's Help Desk to remotely diagnose issues. If the agency is having an underlying network problem, and if that network is provided by Verizon, the Help Desk will reach out to their network counterparts to jointly resolve the issue. If a problem is encountered with a third party network provider, the agency will be asked to initiate a ticket with that provider and Verizon will work with the third party network provider to restore service as quickly as possible.

Flexibility. As a long time service provider, Verizon is uniquely qualified to design and support an architecture that enables growth of the platform according to government user needs. Geographic coverage and the ultimate number of transactions (based on

growth of the user base) have been taken into consideration for design of the platform. The long term roadmap for IPVS is to provide optional UCS functionality designed to meet ordering agency requirements. Verizon also regularly performs upgrades to the latest release of the platform software, and offers new functionality as it becomes available/supportable for ordering agencies.

SIP Trunking Service. The platform is fully redundant and has been serving Verizon customers for over 10 years. Verizon currently provides SIP Trunking to federal customers via both the Networx and WITS 3 contracts. Verizon monitors the backbone of their networks 24x7. Probes collect statistics from these networks, which are then used to develop metrics to verify quality of service (QoS). Verizon also monitors networks using a proprietary telecommunication network supervisory system designed with distributed alarm processing and redundant backup to ensure real time status, performance, and control capabilities. Verizon's SIP Trunking service uses a standards-based QoS scheme to a high quality of service while mitigating call quality issues. Verizon offers a leading edge performance service level agreement for QoS that includes variations in Mean Opinion Score, jitter, packet delivery, network availability, and/or denial of service.

SIP Trunking Service

Verizon SIP Trunking provides a full line of industry leading features including the ability to share concurrent call capacity across locations as well as the ability to burst above provisioned concurrent call levels.

2.2.1.3 Service Coverage [L.29.2.1, M.2.1]

Verizon complies with **RFP Sections C.1.2** and **C.1.3** and will provide IPVS to non-domestic locations as specified in **RFP Section J.12**. Verizon will support IPVS in a minimum of 25 of the top 100 CBSAs.

2.2.1.4 Security [L.29.2.1, M.2.1]

The Verizon IPVS is managed for security and risk per Verizon's EIS IT Risk Management Framework (RMF) Plan in **Volume 1, Attachment A**. Appropriate security measures for the selected access solution will be implemented on a TO basis for Internet and related traffic that requires aggregation (reference **Section 3, External**

Traffic Routing) to provide security and confirm the integrity of government data. If additional security measures are required they will be addressed at the TO level.

2.2.2 CIRCUIT SWITCHED VOICE SERVICE (CSVS) [C.2.2.2]

2.2.2.1 Understanding [L.29.2.1, M.2.1]

As a long time provider of Circuit Switch Voice Services (CSVS) to federal agencies Verizon understands how ordering agencies use and rely on these services. Verizon will continue to support agencies on the existing network while providing a smooth transition to enhanced and alternative service offerings at the agency's own pace. Verizon can help customers prepare for and implement new technologies, such as Voice over Internet Protocol (VoIP) or Unified Communications Service (UCS) (see **Section 2.8.3**), that can broaden and improve the way they do business. Verizon is a premier provider of the services described in **Table 2.2.2.1-1**:

Table 2.2.2.1-1. CSVS Services

CSVS Services
Business Line Service , which provides extensive nationwide coverage for remote locations; and is a basic communications circuit linking the local end offices to the subscriber telephone, key system, fax machine, or modem.
Centrex is a fully managed, network-hosted phone service that replicates most of the functionalities of an on-site Private Branch Exchange (PBX) system.
ISDN PRI/BRI provides advanced digital access, allowing multiple services to be accessed over a single service arrangement; and offers a central, office-based service arrangement as an alternative for individual access services.
Digital PBX Trunks . Provides communication circuits between the local end office (Class 5) and the ordering agency's PBX.

2.2.2.1.1 Compliance with EIS Service Requirements [J.19]

CSVS Capabilities. Verizon complies with **RFP Sections C.2.2.2.1.4(1-5)** and will provide capabilities, such as numbering plans, network intercepts, and voice quality at least equal to 64 kbps. In addition optional capabilities include user-to-user signaling via ISDN D-channel and voice quality at least equal to 64 kbps PCM. Verizon also complies with emergency service requirements, including location identification and routing requirements.

CSVS Features. Verizon complies with **RFP Sections C.2.2.2.2(1-13)** and will provide all of the mandatory features listed in the EIS RFP.

Stipulated Requirements. Verizon complies with the **Service Description (C.2.2.2.1)**, **Functional Definition (C.2.2.2.1.1)**, and all applicable **Standards**

(C.2.2.2.1.2), Connectivity (C.2.2.2.1.3), Interfaces (C.2.2.2.3), and Performance Metrics (C.2.2.2.4) RFP requirements.

2.2.2.2 Quality of Services [L.29.2.1, M.2.1]

Verizon understands that reliable and robust local service is the foundation for many enterprises and ordering agencies. Verizon operates its local voice networks using a combination of Digital Switching Equipment at the end office as well as a combination of protected Optical Networking and highly resilient MPLS transport in the core. This technology, coupled with well-established support processes provides a fast, efficient, and reliable network for their customers.

Verizon offers one of the industry's broadest product portfolios—including voice, data, and wireless—to meet ordering agencies' communications needs. Verizon has the coverage and experience with simplified, reliable local voice services to help end user agencies focus on their core business while controlling costs.

2.2.2.3 Service Coverage [L.29.2.1, M.2.1]

Verizon complies with **RFP Sections C.1.2** and **C.1.3** and will provide CSVS to non-domestic locations as specified in **RFP Section J.12**. Verizon will support CSVS in a minimum of 25 of the top 100 CBSAs.

2.2.2.4 Security [L.29.2.1, M.2.1]

The Verizon CSVS is managed for security and risk per Verizon's EIS IT Risk Management Framework (RMF) Plan in **Volume 1, Attachment A**. If additional security measures are required they will be addressed at the TO level.

2.2.3 TOLL FREE SERVICE (TFS) [C.2.2.3]

2.2.3.1 Understanding [L.29.2.1, M.2.1]

Verizon Toll Free Service (TFS) combines basic and advanced features designed to help ordering agencies manage their inbound calls more effectively. TFS includes basic inbound toll free calling, supplemented by advanced feature and call routing capabilities, including intelligent call routing and network-based Interactive Voice Response (IVR).

Verizon TFS is an inbound calling service that terminates on an ordering agency's existing switched number or facility (POTS, Centrex or Wireless) or dedicated circuit or IP termination. Toll Free prefix numbers currently available include 800, 888, 877, 866, 844 and 855. **Figure 2.2.3.2-1** illustrates Verizon's TFS architecture:



Verizon TFS connects to and interoperates with the Public Switched Telephone Network (PSTN), including both wireline and wireless originations and terminations. This provides ubiquitous domestic and non-domestic connectivity. TFS supports both dedicated and switched PSTN terminating access arrangements. Switched access supports traffic that terminates on ILEC (not Verizon) owned and operated facilities that are part of the PSTN. Dedicated access supports traffic that terminates on full time dedicated facilities provisioned to an ordering agency's SDP by Verizon or an ILEC on Verizon's behalf.

2.2.3.1.1 Compliance with EIS Service Requirements [J.19]

TFS Technical Capabilities. Verizon complies with all TFS technical capabilities listed in **RFP Sections C.2.2.3.1.4(1-12)**. Verizon will act as the responsible organization for assignment and maintenance of toll free numbers, if requested by the ordering agency, support toll free number portability, accommodate any presently assigned agency toll free numbers and assign agency requested "vanity" toll free numbers, if available. In addition, Verizon offers universal international toll free number

service, as requested; and provides the ability for a single toll free number to terminate at multiple locations (SDPs), and the ability for multiple toll free numbers to terminate at a single location(SDP). TFS will provide a busy signal or recorded announcement for all calls that encounter network congestion and/or terminating egress congestion. A network intercept to recorded announcements will be provided when a call cannot be completed for various conditions defined in the EIS RFP. TFS provides the ability for customized network intercept recorded announcements with options for the custom announcement to be a) recorded by Verizon or; b) recorded remotely by the ordering agency, and the ability to have all announcements recorded in English and Spanish languages (other languages will be optional). TFS provides a referral message to callers of a disconnected toll free number with an option for a referral telephone number to be provided. TFS will provide dialed number identification service (DNIS) and will identify and provide the calling parties Automatic Number Identification (ANI).

TFS Features. Verizon complies with **RFP Sections C.2.2.3.2(1-28)** and will comply with all TFS features identified in the RFP.

TFS Feature Reports. Verizon complies with **RFP Section C.2.2.3.2.1** and will comply with all TFS feature reporting requirements in the RFP.

Stipulated Requirements. Verizon complies with all **Service Description (C.2.2.3.1), Functional Definition (C.2.2.3.1.1), Standards (C.2.2.3.1.2), Connectivity (C.2.2.3.1.3), Interfaces (C.2.2.3.3) and Performance Metrics (C.2.2.3.4)** RFP requirements.

2.2.3.2 Quality of Services [L.29.2.1, M.2.1]

Verizon currently operates two physically diverse management systems that receive and maintain two sets of network information. With Verizon's internal data network systems, not only will this information be maintained in a protected dual environment, but also it will be supported by geographical diversity. Verizon also provides a hot backup for access to information.

The Verizon network provides virtually non-blocking, P.01 grade of service and network availability of 99.9974%, 24x7. Verizon maintains these standards through strict adherence to internal operations standards, frequent testing, and a highly fault-tolerant hierarchical switched network design.

Verizon operates full-featured digital switches at Verizon junction locations that have mature service capabilities. These switches are part of rich, active product lines that will continue to include new service interfaces within Verizon's advanced IP Call Center Service portfolio. Verizon also has an extensive network of POPs that are fully integrated with service scalability and facilitate transition to advanced services. In addition, all service elements are widely deployed in Verizon's commercial network, providing demonstrated scalability and flexibility.

2.2.3.3 Service Coverage [L.29.2.1, M.2.1]

Verizon complies with **RFP Sections C.1.2** and **C.1.3** and will provide TFS to non-domestic locations as specified in **RFP Section J.12**. Verizon will support TFS in a minimum of 25 of the top 100 CBSAs.

2.2.3.4 Security [L.29.2.1, M.2.1]

The Verizon TFS is managed for security and risk per Verizon's EIS IT Risk Management Framework (RMF) Plan in **Volume 1, Attachment A**. If additional security measures are required they will be addressed at the TO level.

2.2.4 CIRCUIT SWITCHED DATA SERVICE (CSDS) [C.2.2.4]

2.2.4.1 Understanding [L.29.2.1, M.2.1]

As data and multimedia application usage expands within the government, requirements for digital connectivity on a dial-up basis increase, particularly regarding on-demand video conferencing. To support these and other applications, Circuit Switched Data Service (CSDS) provides synchronous, full duplex, digital data transmission rates up to DS1, including integral multiples of DS0 data rates (i.e., NxDS0, where N = 1 to 24) to on-net and off-net locations.

The Verizon circuit switched network is provisioned and managed to the same high standards as its data services, and supports the automatic disabling of echo cancellers on data CSDS calls. For international CSDS calls, Verizon's international gateway switches select clear channel trunks to avoid compression or echo cancellation equipment, so high quality CSDS service is based on an all-digital backbone, digital switches, and digital access facilities. Verizon currently and successfully provides these services today on the Networx and WITS3 contracts.

2.2.4.1.1 Compliance with EIS Service Requirements [J.19]

CSDS Mandatory Technical Capabilities. Verizon complies with **RFP Section C.2.2.4.1.4** and will provide mandatory technical capabilities listed in the EIS RFP and summarized below in **Table 2.2.4.1.1-1**.

Table 2.2.4.1.1-1. CSDS Mandatory Technical Capabilities

CSDS Mandatory Capabilities	
1. Uniform Numbering Plan	
a. Unique directory number for all on-net government locations	
b. Same uniform numbering plan as proposed for CSVS integrated with the CSVS Plan	
2. Authorization Codes for CSDS	
3. For calls terminating to off-net locations, the bandwidth requested by the originating on-net location will be limited to the bandwidth limitations in the PSTN between Verizon's network and the called location	
4. Calling capability that does not require scheduling	
5. Provision of network-derived clocking to the DTE or PBX/Multiplexer (MUX) at the SDP	
6. Following call establishment, all bit sequences transmitted by the DTE will be transported as data/bit transparent and will maintain data/bit sequence integrity	
7. Categories of dialable information-payload bandwidth, as follows:	
a. DS0 Category – dialable bandwidth will be DS0 (i.e., 56 kbps and 64 Kbps) data rate	
b. DS1 Category – dialable bandwidth will be DS1 (i.e., 1.536 Mbps) data rate	
c. Multi-rate DS0 Category – dialable bandwidth will be NxDS0, where N=1 to 24	

CSDS Mandatory Capabilities
8. For the Multi-rate DS0 category, Verizon will provide:
a. Appropriate dialing sequence for initiating calls with different bandwidths
b. Transport of all bit sequences transmitted by the DTE as data/bit transparent after establishment of the dialing sequence

CSDS Optional Technical Capabilities. Verizon complies with **RFP Section C.2.2.4.1.4** and will provide the following optional technical capabilities: 1) Multirate DS1 Category; 2) DS3 Category; 3) SONET Level-I (i.e., OC-1) Category; 4) SONET Level-II (i.e., Multirate OC-1) Category; and, 5) SONET Level-III (i.e., Multirate OC-3) Category.

CSDS Optional Features. Verizon complies with **RFP Section C.2.2.4.2** and will support the following optional features: 1) Dial-In; and 2) User-to-user signaling via ISDN D-Channel.

Stipulated Requirements. Verizon complies with the **Service Description (C.2.2.4.1)**, **Functional Definition (C.2.2.4.1.1)**, and all applicable **Standards (C.2.2.4.1.2)**, **Connectivity (C.2.2.4.1.3)**, **Interfaces (C.2.2.4.3)**, and **Performance Metrics (C.2.2.4.4)** RFP requirements.

2.2.4.2 Quality of Services [L.29.2.1, M.2.1]

As a leading provider of CSDS to the federal government, Verizon will continue to support ordering agencies with the same high level of service currently being provided. Currently the user-to-user signaling feature has been grandfathered. Verizon will continue to support CSDS for existing customers but no new customers will be added.

2.2.4.3 Service Coverage [L.29.2.1, M.2.1]

Verizon complies with **RFP Sections C.1.2** and **C.1.3** and will provide CSDS to non-domestic locations as specified in **RFP Section J.12**. Verizon will support CSDS in a minimum of 25 of the top 100 CBSAs.

2.2.4.4 Security [L.29.2.1, M.2.1]

The Verizon CSDS is managed for security and risk per Verizon's EIS IT Risk Management Framework (RMF) Plan in **Volume 1, Attachment A**. If additional security measures are required they will be addressed at the TO level.

2.3 Contact Center Service [C.2.3]

2.3.1 UNDERSTANDING [L.29.2.1, M.2.1]

Verizon's Call Center/Customer Contact Center Service (CCS) provides cost effective multi-media contact center solutions that enable agencies to efficiently and effectively deliver customer service to their clientele across multiple contact channels (voice, fax, email, and Internet website, etc.) by providing a single network call queue or multiple call queues, where applicable. CCS may be used in conjunction with Verizon's Toll Free Service and other network services to facilitate agency communications with the general public, businesses, and other agencies. Verizon will provide Call Queue Management Services and Call Answering Services as a part of the CCS portfolio. Verizon has extensive experience in delivering CCS and currently provides CCS for many federal agencies including the [REDACTED]

[REDACTED] the existing Networx contract.

The CCS Call Management Service provides real-time management of routing and distribution of multi-media calls from multiple channels to the contact center. Call Queue management also provides management of routing and distribution of contacts from multi-media channels (i.e. voice, email, facsimile, agency web site). Intelligent routing and distribution of contacts will be determined according to the real time operating status of the ordering agencies' contact center(s) and their business rules. CCS is available for single site, multiple site, and enterprise wide agency contact centers. Verizon's CCS is a multimedia service and will interoperate with the ordering agencies' CCS communications channels.

The advantage to hosting within Verizon's network is the ability to quickly add capacity to the solution as the agency's call volumes increase. The hosted solutions are often provided as a service within Verizon's network, which can accommodate scale up/down, as needed. These services can also be provided at the agency's premises and the same customizable approach applies. Verizon engineers can work with agencies to appropriately size the best and most cost-efficient solution.

2.3.1.1 Compliance with EIS Service Requirements [J.19]

CCS Delivery Methods. Verizon complies with **RFP Section C.2.3.1.4.1(1)** and will provide the required independent service delivery methods, as detailed within the following sections. Verizon CCS can meet the needs of large and small scale agencies with simple and complex requirements. CCS offerings range from standard services to customized solutions.

Host Based Call Management Service. Verizon complies with **RFP Section C.2.3.1.4.1(1)** and will provide the required components for Hosted CCS Call Management Service at a Verizon-provided location. Necessary components include, but are not limited to hardware, software, inside wiring and power. **Table 2.3.1.1-1** below lists the capabilities of Verizon's Hosted CCS Call Management Service:

Figure 2.3.1-2 below lists the capabilities of Verizon's Hosted Call Center Services:

Figure 2.3.1-2. Verizon Hosted CCS Capabilities.

Hosted Call Management Service	
▪	Management of call queue(s) for routing and distribution of contacts (calls) from multi-media channels and prioritizing queue and contacts (calls) within the queue, as required.
▪	Traversing and successfully interoperating with ordering agency firewalls and security layers.
▪	Interoperating with the ordering agencies' CCS communications channels.
▪	Monitoring of the CCS trunks, agents, and agent groups for call quality by authorized agency personnel.
▪	Management of specific network queue, call-routing algorithms, contact center agent profiles, and reports. At a minimum, capabilities will include: authentication with password protection, performing scheduled and real time changes, and viewing the CCS configuration, audit trail and change log history.
▪	Providing a wide variety of required real time, periodic, historic logs and reports.
▪	Transmitting and delivering music on hold (or recordings) to the originating caller.
▪	Performing a "Discovery Session" with key stakeholders to gather information required to meet the ordering agencies CCS needs.
▪	Supplying terminal devices (e.g. phones, IP phones, softphones, etc.) required for delivery of CCS using the SRE catalog, if requested by the ordering agency.
▪	Accommodating agency contact center closings by providing announcements, messages, or re-routing of contacts.

Premises Based Call Management Service. Verizon complies with **RFP Section C.2.3.1.4.1(2)** and will provide the necessary components required for CCS Call Management Service to be located at an agency-provided location. This includes, but is not limited to, CCS hardware and software. Hardware and operating software for Premises solutions can be agency provided or can be ordered under EIS as Service Related Equipment (SRE). Verizon will provide the hardware and operating system specifications to the ordering agency, and will install, configure and maintain the CCS

applications. The ordering agency will provide the power, inside wiring, and a physical location for the CCS equipment.

Verizon's Premises Based Call Management Service capabilities include complete turnkey call center operation, including the appropriate network services, technology, personnel, business processes and workflows, training, and reporting to respond to caller inquiries and meet pre-determined performance.

Premises Based Call Answering Service. Verizon complies with **RFP Section C.2.3.1.4.1(3)**. Verizon-provided personnel will work at an agency-provided location where the agency will provide the work space, furniture, workstation hardware, software, and all necessary building utilities required for the contact center.

Each CCS Call Answering Service solution is customizable and can include full turnkey technology and agents, or a partial solution containing either just technology or just agents. The solutions are guided by the ordering agencies' requirements – from business processes to security items, and the technology is based on the services required. The agents will be assessed at the skill levels required.

Host Based Call Answering Service. Verizon complies with **RFP Section C.2.3.1.4.1(4)**. Verizon personnel will work at a Verizon location where it will provide the work space, furniture, workstation hardware, software, and all necessary building utilities for the contact center. Verizon Hosted CCS Call Answering Service solutions are customizable and can range from fully managed to include moves, adds and changes (MACs), or partially managed where Verizon maintains the platform functionality only. The sizing of the platforms will be based on the ordering agency's capacity requirements.

Network Call Queue. Verizon complies with **RFP Section C.2.3.1.4.2(1)** and will provide the capability for a network call queue, and the ability to prioritize queues and contacts (calls) within a queue, to manage the routing and distribution of contacts from multi-media channels (i.e. voice, email, facsimile, agency web site).

Intelligent Routing and Distribution. Verizon complies with **RFP Section C.2.3.1.4.2(2)**. Intelligent routing and distribution of contacts will be determined according to the real time operating status of the ordering agencies' contact center(s) and its business rules.

Ordering Agencies' CCS Communications Channels. Verizon complies with **RFP Section C.2.3.1.4.2(3)**. Verizon's CCS is a multi-media service and will interoperate with the ordering agencies' standards based CCS communications channels.

Agency Firewalls and Security Layers. Verizon complies with **RFP Section C.2.3.1.4.2(4)** and will provide the ability to traverse and successfully interoperate with compatible agency firewalls and security layers. Verizon will verify with the agency that its firewall is compatible with its CCS during the delivery process.

Service Observation. Verizon complies with **RFP Section C.2.3.1.4.2(5)** and will support service observation, which provides options for silent monitoring (default) and three way audio conferencing. It will be made available for monitoring both local and remote agents and will support local and remote observers. Service observation is secure and will only be available to authorized agency designated individuals.

Ordering Agency Authorized Designated Individuals. Verizon complies with **RFP Sections C.2.3.1.4.2(6)(a-d)** and will provide the ordering agency with the ability to manage its specific network queue, call routing algorithms, contact center agent profiles and reports. Verizon will allow authorized agency designated individuals to make real time and scheduled changes.

CCS Reporting. Verizon complies with **RFP Section C.2.3.1.4.2(7)** and will provide reports, as required by the OCO.

Real Time Reporting – CCS Queue Status. Verizon complies with **RFP Sections C.2.3.1.4.2(8)(a-i)**. Verizon will provide the ordering agency with access to graphical, real-time reporting of the CCS queue status. Real-time reporting monitors

performance and identifies all interactions by contact channel and agent status. Reports include summaries and totals, where applicable.

Queue Status. Verizon complies with **RFP Section C.2.3.1.4.2(9)** and will provide the ability to inform the call of the queue status (including the callers estimated wait time) when agency-defined thresholds are exceeded and the option for announcing expected wait times to callers prior to them entering the queue. Agencies will have the ability to change recorded announcements.

Transmit and Deliver. Verizon complies with **RFP Section C.2.3.1.4.2(10)** and will provide the ability to transmit and deliver music on hold (or recordings) to originating callers.

CCS Terminal Devices. Verizon complies with **RFP Section C.2.3.1.4.2(11)** and will supply terminal devices such as phones and softphone applications required for delivery of CCS, if requested by the ordering agency. Terminals can support caller ID and an optional name/message display (where applicable). Terminal devices will be ordered through as SRE.

Agency CC Closings and Holidays. Verizon complies with **RFP Section C.2.3.1.4.2(12)** and will accommodate agency contact center closings (e.g., scheduled holidays, unplanned closings, maintenance activities, etc.) by providing announcements, messages, or re-routing of contacts during the period when the CC is closed. Verizon CCS is a 24x7 service and allows Verizon customers to dynamically manage their CCS hours of operations based on their ever changing needs. Verizon will assist agencies with these types of changes, as needed. Verizon can support email, voice, facsimile, and chat (Internet), when applicable. Verizon will provide agency authorized personnel with the capability to monitor the CCS trunks, agents, and agent groups for call quality.

Contact Center Operation. Verizon complies with **RFP Section C.2.3.1.4.3(1)** and will provide agencies with contact center operation that may include network services,

technology, personnel, business processes and workflows, training, and reporting to respond to caller inquiries and meet pre-determined performance or agency satisfaction levels.

Caller Inquiries during Agency Operating Hours. Verizon complies with **RFP Section C.2.3.1.4.3(2)(a)** and will receive and accurately respond to caller inquiries during established agency operating hours within the agreed upon (Key Performance Indicators (KPIs).

Caller Inquiries During Non-Operational Hours. Verizon complies with **RFP Section C.2.3.1.4.3(2)(b)** and will manage and accurately respond to caller inquiries received during non-operational hours and holidays according to the ordering agency's needs.

Back Office Systems or Databases. Verizon complies with **RFP Section C.2.3.1.4.3(2)(c)** and CCS will be interoperable with the ordering agencies' required back office systems or databases (if required and as identified by the ordering agency) to deliver the specified agency service functions at the agreed upon performance levels.

Resources, Processes, and Technology. Verizon complies with **RFP Section C.2.3.1.4.3(2)(d)** and will provide resources, processes, and technology to reasonably accommodate inquiries from different types of callers as identified by the ordering agency, which includes responding to inquiries from callers that may have foreign language requirements or callers with disabilities but not limited to speech disabilities, deaf, hard-of-hearing, deaf-blind, or blind.

Rapid Capacity Increases (Crisis/High Priority). Verizon complies with **RFP Section C.2.3.1.4.3(2)(e)** and will quickly increase capacity in crisis or high priority situations, and will quantify its ability to deliver call answering services in terms of capacity, extended operating hours, increased staffing, additional language support and implementation start-up time. Verizon has experience in rapidly responding to a wide variety of crises, such as 9/11 and Hurricanes Katrina, Irene and Sandy. To gain a

deeper understanding of Verizon's commitment to rapid response, reference **Section 9**, in **Volume 2 – Management** for Verizon's **National Security and Emergency Preparedness Implementation Plan**.

Call Answering Resources. Verizon complies with **RFP Section C.2.3.1.4.3(3)** and will provide call answering resources, as needed, to meet the requirements specified in the agency service order, in compliance with **RFP Table C.2.3.1.4.4**.

Call, Recording & Monitoring. Verizon complies with **RFP Section C.2.3.1.5(1)** and will provide digital recording and monitoring of inbound and outbound multimedia contacts and associated data to capture the caller experience. At a minimum, date, time, duration, caller ID information (if available), dialogue, and agent identity will be captured and recorded.

Collaborative Browsing. Verizon complies with **RFP Section C.2.3.1.5(2)**. Verizon CCS will allow bi-directional sharing of web pages between the CC agent and the caller. It will enable callers to request a co-browse session with a CC agent and the agent will have the ability to highlight text and scroll to a specific section of a web page. The agent will be able to push a web page to the caller and vice-versa, and agents will be able to transfer control of a collaborative browsing session to another agent and log all collaborative interactions between the agent and caller. Verizon CCS allows CC agents to mask fields and inputs of private/sensitive information.

Computer Telephony Integration. Verizon complies with **RFP Section C.2.3.1.5(3)**. CCS provides Computer Telephony Integration (CTI) capabilities, which enable the transfer of caller information and agency specified data between Verizon and agency specified systems simultaneously with the associated inbound contact channel (call).

Customer Contact Information. Verizon complies with **RFP Section C.2.3.1.5(4)** and will provide an application to track, document, and manage the agency's CCS contacts across multiple contact channels. The application will provide the ability to:

record caller contact and account information, caller contact history, status and nature of inquiry, data and time of the contact, call disposition, and the agent handling the inquiry, as well as the ability to assign and escalate inquiries according to business rules, and to assign a unique case or record number to each inquiry. Verizon CCS will allow for the creation and use of scripted responses for CC agents to use, and the system will provide summary and detailed management reports.

E-mail Response Management. Verizon complies with **RFP Section C.2.3.1.5(5)** and will provide E-mail Response Management (ERM) that will assign a tracking ID to each email and route email communication according to agency specified-business rules. The ERM will provide automatic response and acknowledgement, email classification, prioritization and routing based on business rules, filtering capability, content analysis and knowledge base for suggested and personalized responses, management and real-time exception reports, and multiple language support (English and Spanish). The ERM will be compatible with the ordering agency's email application

IVR. Verizon complies with **RFP Section C.2.3.1.5(6)** and will provide an IVR application that allows callers to be provided with information based on input from telephone DTMF key pad inquiries or via speech recognition. The minimum capabilities are listed below:

Pre-Recorded Announcement Messages. Verizon complies with **RFP Section C.2.3.1.5(6)(1)**. The agency may select pre-recorded announcement messages with the ability for announcements to allow for a caller to opt out during an announcement to a predefined termination. Such announcements will be played from the beginning for each caller and provide the ability to be recorded in (a) U.S. English, (b) Spanish (American) and (c) other foreign languages after obtaining ordering agency script approval.

Caller Information. Verizon complies with **RFP Section C.2.3.1.5(6)(2)**, and will leave caller information via telephone DTMF keypad signal or speech.

Caller-Entered DTMF/Speech Messages. Verizon complies with **RFP Section C.2.3.1.5(6)(3)**; a means for the ordering agency to retrieve caller-entered DTMF or speech messages

Caller Information Transcription. Verizon complies with **RFP Section C.2.3.1.5(6)(4)**. For transcription of caller information, Verizon will provide (a) transmission of the recorded voice files and DTMF data for each call to the agency and (b) a report of caller responses that transcribes the caller-provided information for the ordering agency based upon the agency's needs and transmits it to the agency. Verizon will provide transcription reports from English and Spanish speaking callers.

Database Queries. Verizon complies with **RFP Section C.2.3.1.5(6)(5)**; The database will either be housed at the ordering agency, at a location at the ordering agency's discretion, or housed in a Verizon location and updated by the ordering agency.

Agency-Provided Name and Address Database. Verizon complies with **RFP Section C.2.3.1.5(6)(6)** and will allow callers to hear and verify their names and addresses in an agency-provided name and address database after the caller has entered his or her telephone number via DTMF, or based on the caller's ANI (Text to Speech).

Speech Recognition. Verizon complies with **RFP Section C.2.3.1.5(6)(7)** and will support speech recognition as a valid caller input. Verizon will support at a minimum, all spoken numeric digits as well as "yes" and "no". English and Spanish will be supported and Verizon will accept and process 95 percent (minimum) of the above speech responses. The speech responses not accepted will be routed to a default location designated by the ordering agency.

Surveys. Verizon complies with **RFP Section C.2.3.1.5(6)(8)** and agencies will have the ability to perform surveys (via DTMF or speech) to IVR callers. Survey results will be provided electronically to the ordering agency.

Facsimile Fax Back. Verizon complies with **RFP Section C.2.3.1.5(6)(9)** and will provide the facsimile "fax back" ability, which will permit callers to retrieve agency-specific documents or forms. Verizon will fax back the requested documents within one hour of the initial call and retry a minimum of 13 attempts over a six hour interval in order to complete the request. There will be an option for a fax cover sheet (standard or customized).

Caller IVR Selections. Verizon complies with **RFP Section C.2.3.1.5(6)(10)** and per agencies' options, callers' IVR selection(s) information will be transferred to the agency.

IVR Capacity. Verizon complies with **RFP Section C.2.3.1.5(6)(11)**. Verizon's IVR capacity will be configured such that the application answers a call within 3 ring cycles for 99% of the offered call volume (measured on an hourly basis).

Features for Hearing Impaired & Speech Disabilities. Verizon complies with **RFP Section C.2.3.1.5(6)(12)** and CCS features will be available to individuals who are hearing impaired or have speech disabilities via electronic means in Baudot and ASCII/TTY code formats including text chat.

Summary Report. Verizon complies with **RFP Section C.2.3.1.5(6)(13)** and will provide a summary report that provides (at a minimum) information on the caller, average call duration, caller opt out (transfer) and disposition of the calls within the IVR application on a daily, weekly and monthly basis.

IVR Reports. Verizon complies with **RFP Section C.2.3.1.5(6)(14)** and will make any IVR reports that are available with Verizon's equivalent commercial offerings.

IVR Agency Based Database. Verizon complies with **RFP Section C.2.3.1.5(7)** and will provide the ability to route calls and provide information based upon a database query(s) of information provided by a database location at the ordering agency premises. The query(s) could be to single, redundant, or multiple databases depending on agency specifications and the complexity of the application.

Verizon will implement and provide the appropriate interface and connectivity for its IVR application to successfully query and access the ordering agency's database(s). The IVR caller will have the ability to retrieve, review, and modify information located at the agency based database based on the ordering agency needs. The agency database(s) can be a mainframe or server-based relational database. An agency defined default routing plan will be used if the database does not respond to the network query within 250 milliseconds.

IVR Speech Recognition. Verizon complies with **RFP Section C.2.3.1.5(9)** and will provide natural speech recognition for IVR applications with the ability (at a minimum) to recognize spoken vocabulary, digits, zip codes, credit card numbers, credit card expiration date, account numbers, and alpha numeric characters. At a minimum, Verizon will provide natural speech recognition abilities and vocabularies for both English (American) and Spanish (American) dialects. The minimum accuracy threshold for speech recognition will be at least 95 percent.

Language Interpretation Service. Verizon complies with **RFP Section C.2.3.1.5(10)(1-5)** and will provide telephone language interpretation services. The service will be available, on demand, for three way conferencing with the contact center agent and foreign language caller to provide interpretation between the caller's foreign language and English and vice versa. This feature will have the following minimum capabilities: 24x7 Availability, Toll Free Number Accessibility, Caller Foreign Language Identification, Interpreter provided within one minute of request, Management Reports identifying the date, time, duration, interpreter, and identity of the agent requesting the service. Verizon will propose and provide a list of the foreign languages available for interpretation.

Outbound Dialer. Verizon complies with **RFP Section C.2.3.1.5(11)(1-8)** and will provide the ability for automated outbound dialing. The dialer service will have the ability to support either centralized or distributed contact center environments according to the ordering agency's needs. The dialer will have the following minimum capabilities:

automatic initiation of domestic/non-domestic outbound calls, call conferencing and call transfer capabilities, predictive dialing, preview dialing, receipt and management of inbound calls, support agent blending, support service observation, and reporting.

Text Chat. Verizon complies with **RFP Section C.2.3.1.5(12)(1-7)** and will provide the ability to enable the CC agents to engage in real-time text chat with callers from its web site. The text chat will provide the following minimum capabilities: archive text chat sessions (create transcripts, allow agents to manage multiple text chat sessions, allow file transfers, view the active web page the text chat caller is on, provide log of text chat sessions, provide an automatic spell check and grammar check option that is enabled when typing in active session, and supervisor chat monitoring.

Web Call Back. Verizon complies with **RFP Section C.2.3.1.5(13)** and will provide the ability for a customer to request a call back by filling out a form on the agency's web site. The call back algorithm will be based on the availability of a CC agent. The call back request will be automatically distributed to the most appropriate agent based on availability of an agency (within agency operating hours).

Web Call Through. Verizon complies with **RFP Section C.2.3.1.5(14)** and will provide the ability to allow customers browsing the agency's web site the ability to call through and simultaneously have a voice conversation with a CC agent.

Workforce Management. Verizon complies with **RFP Section C.2.3.1.5(15)(1-3)** and will provide a workforce management (WFM) system that automates forecasting and scheduling calculations based on real time and historical contact center data. The WFM will enable agencies to effectively schedule resources, accurately forecast call volumes and analyze/review performance statistics for single or multiple sites and blended applications. The workforce management system provides the following minimum capabilities: it will forecast staffing needs including agent skills, skill levels and shifts, it will forecast contact volumes and workload - overall call volume and by contact channel, it also provides agency scheduling and creation of optimized agent schedules by shift and skill.

Virtual Queue. Verizon complies with **RFP Section C.2.3.1.5(16)** and will provide a feature that allows callers to choose to remain waiting on-line for an attendant or to receive a call back in turn.

Stipulated Requirements. Verizon complies with the **Service Description (C.2.3.1)**, **Functional Definition (C.2.3.1.1)**, and all applicable **Standards (C.2.3.1.2)**, **Connectivity (C.2.3.1.3)**, **Interfaces (C.2.3.1.6)**, and **Performance Metrics (C.2.3.1.7)** RFP requirements.

2.3.2 QUALITY OF SERVICES [L.29.2.1, M.2.1]

Verizon transitions clients via proven methodologies for program implementation, testing, and performance, and integrates the Verizon support team with each client's operations teams. As a trusted partner, Verizon leverages proven tools and strategies to assist in mitigating risks and protecting the customer experience.

Verizon utilizes a focused transition team to provide a seamless implementation from contract signature to go-live. The Verizon transition strategy is comprised of proven implementation and operational steps designed to provide a successful migration from an agency's current operational state to its desired state of greater efficiency and effectiveness. Verizon's approach taps into its proprietary talent acquisition tools and processes to maintain productivity and quality while transferring operations management.

Verizon leverages the learning and key takeaways from other government agency support programs. The Verizon "Three-Phase Implementation Approach," described in **Table 2.3.2-1**, has been used for projects of all shapes and sizes, and is a tried-and-true methodology for minimizing overall project risk.

Table 2.3.2-1. TFS Three Phased Implementation Approach

TFS Three-Phased Implementation Approach	
Definition and Assessment Phase.	Information gathering and solution design take place between the agency and the Verizon Team to confirm our solutions are appropriately tailored to meet the agency's specific requirements.
Implementation Phase.	Both the agency and the Verizon Team actively participate in the deployment of the solutions developed.
Service Delivery Phase.	Ongoing management and improvement for the solutions deployed is performed over the life of the project.

2.3.3 SERVICE COVERAGE [L.29.2.1, M.2.1]

Verizon complies with **RFP Section C.1.3** and will support CCS in a minimum of 25 of the top 100 CBSAs.

2.3.4 SECURITY [L.29.2.1, M.2.1]

The Verizon CCS is managed for security and risk per Verizon's EIS IT Risk Management Framework (RMF) Plan in **Volume 1, Attachment A**. If additional security measures are required they will be addressed at the TO level.

2.4 Colocated Hosting Services (CHS) [C.2.4]

2.4.1 UNDERSTANDING [L.29.2.1, M.2.1]

The Verizon Colocated Hosting Service (CHS) offers a highly secure environment to deploy computing, network, storage and information technology (IT) infrastructures. Verizon's world-class data centers help agencies reduce the capital and operational expenses required to house and protect mission-critical applications and systems. Several Verizon facilities offer extensive carrier-neutral options.

Verizon is a leading global provider of IT infrastructure services, delivered on a robust and advanced operations platform. As depicted in **Figure 2.4.1-1 below**, Verizon leverages purpose-built data centers in the United States with access to massive and diverse network connectivity from more than [REDACTED] global carriers. Verizon delivers government agencies a comprehensive suite of managed solutions including data center/cloud, managed hosting, collocation, network, and security services.

Verizon is in a unique position to provide its Enterprise Cloud Services delivered from Tier III+ secure data center facilities. [REDACTED]

[REDACTED] facility infrastructure, network connectivity, security, and managed services that are unmatched in the telecommunications industry. [REDACTED]

[REDACTED] benefits to ordering agencies requiring a secure and reliable solution for their data and network infrastructures. [REDACTED]

[REDACTED] advantageous for Continuity of Operations Planning (COOP).



2.4.1.1 Compliance with EIS Service Requirements [J.19]

Co-location Facility Security and Access. Verizon complies with **RFP Section C.2.4.1**, and will provide a secure location with cage and racks, site surveillance, external traffic access as required, and 24x7 government access to leased space and Government Furnished Property (GFP) in the co-location facility.

CHS Capabilities. Verizon complies with **RFP Section C.2.4.1(1-5)** and will provide co-location facilities that will support redundant and high-availability power to GFP, redundant Uninterruptible Power Supplies (UPS), Very Early Smoke Detection Apparatuses (VESDA), fire suppression systems; and redundant cooling systems. The Verizon colocation service description base configuration for a full rack is based on one 208W, 20A, single phase power, and that the rack is located in open (non-caged) floor space. Verizon's CHS offering supports all other RFP stated variations of power scenarios, depending on power and configuration availability at the requested data center as non-basic power ICB. Full rack space is available at Verizon's FISMA-

compliant (per C.2.4.2) [REDACTED]

[REDACTED]. Orders will be accepted pending the availability of pre-existing FISMA- compliant (per C.2.4.2) space and power at time of order. Verizon understands that customers may have unique security requirements and/or requirements for physical protection of the colocation equipment. Verizon has experience in implementing physical protections – from key locked cabinet to biometrics in caged environments. Verizon will address individual customer security and other requirements per the EIS requirements on an individual task order basis.

Verizon Facilities. Verizon complies with **RFP Sections C.2.4.4(1)(a-f)**, and will be responsible for the actions listed in **Table 2.4.1.1-1**:

Table 2.4.1.1-1. Verizon CHS Facility Responsibilities

Verizon CHS Facility Responsibilities	
a)	Damage or injury to persons or property occasioned through the use, maintenance, management, and operation of Verizon facilities, GFP, or other equipment by, or by the action of, Verizon or its employees and agents;
b)	Completing reasonably necessary pre-delivery preparations for the delivery site, site security, or storage facilities to temporarily or permanently accommodate the GFP in a safe and secure manner;
c)	Relocating GFP from initial receiving points or temporary storage facilities to the final Verizon facility and installation site;
d)	Preparing the final installation site including the provisioning of necessary physical space, environmental systems, and network connectivity;
e)	Facilitating GFP setup, including assembling, loading, configuring, testing, and (at end of life) crating and packing GFP for return; and
f)	Providing contractor personnel with all required national citizenship, security clearances, training, and technical certifications to receive, use, maintain, manage, operate, package, transport, or ship sensitive and secure GFP.

Government Access. Verizon complies with **RFP Section C.2.4.4(2)**, and will provide authorized government personnel and third-parties with access to GFP at specified times, in specified locations, as mutually agreed upon between the government and Verizon.

Remote Monitoring. Verizon complies with **RFP Section C.2.4.4(3)**, and will provide service management capabilities that allow authorized users to remotely monitor facilities and equipment status in real-time.

Alarms. Verizon complies with **RFP Section C.2.4.4(4)**, and will present alarms to the authorized user in real-time for facility and communication failures.

Continuous Updates. Verizon complies with **RFP Section C.2.4.4(5)**, and will continuously update and present to the user the status of power for each rack, cooling, environment temperature, entry/exit logs, smoke detection, and connectivity.

Stipulated Requirements. Verizon complies with applicable **Standards (C.2.4.2), Connectivity (C.2.4.3), Features (C.2.4.5), and Performance Metrics (C.2.4.5.1)** requirements in the EIS RFP.

2.4.2 QUALITY OF SERVICES [L.29.2.1, M.2.1]

Verizon's scalable CHS solutions will allow ordering agencies to upgrade space, connectivity and services as requirements evolve.

Ordering agencies also have choices and redundancies in the communication infrastructures Verizon CHS facilities provide that are matched by few other enterprise-class collocation providers anywhere in the world. Verizon supports the mission-critical needs of network-based systems, supplying performance monitoring and systems management, and providing mission-critical IP infrastructures.

Verizon also offers technical support, installation, staging, and additional network engineering services. Verizon technical support allows ordering agencies to remotely access their equipment to perform simple troubleshooting or maintenance tasks. Advanced technical support is also available at select locations. Verizon installation services will help ordering agencies avoid the costs of sending technicians to Verizon collocation facilities to service equipment and supervise installation activities. Verizon's staging services can help turn almost any network environment into a simple plug-and-play process, helping to reduce the time required for agencies to install and load final

configurations at Verizon collocation facilities. Other network engineering services, available at select locations, may help with the timely and efficient implementation of ordering agency's collocation projects and may help agencies reduce or eliminate the costs involved with hiring, training, and maintaining its own engineering staff.

Verizon provides industry leading Service Level Agreements (SLAs) for power and environmental systems through a number of redundant subsystems designed to alleviate single points of failure throughout the delivery path. Verizon offers [REDACTED] SLAs for power and environmental systems through several redundant subsystems (power SLAs only apply to clients with dual power feeds). Thanks to these redundant systems, ordering agencies should not experience any power loss during maintenance windows. Verizon's scalable collocation solutions allow ordering agencies to upgrade space, connectivity and services as their requirements evolve. **Table 2.4.2-1** provides information on some of the CHS facility features.

Table 2.4.2-1. CHS Facility Features

CHS Facility Features
Facilities Infrastructure. Raised floors are at least 20 inches above the concrete flooring, raised floor loading can accommodate 150 lbs. per square foot, loading docks each have a load leveler providing up to 20,000 pounds of capacity and commercial-grade freight elevators.
Colocation Installation/Staging Services. Verizon employs professional, highly-trained technicians who can handle equipment and cabling, and can perform work at Verizon data centers.
Remote/Smart Hands. Verizon Remote/Smart Hands help reduce costs and maximize uptime with on-site services and troubleshooting or maintenance tasks with on-site technical personnel.
Additional Services. Skilled Verizon engineers for on-site engineering and migration planning are also available based on agency needs.

2.4.3 SERVICE COVERAGE [L.29.2.1, M.2.1]

Verizon complies with **RFP Section C.1.3** and will support CHS in a minimum of 25 of the top 100 CBSAs.

2.4.4 SECURITY [L.29.2.1, M.2.1]

The Verizon CHS is managed for security and risk per Verizon's EIS IT Risk Management Framework (RMF) Plan in **Volume 1, Attachment A**. If additional security measures are required they will be addressed at the TO level.



Verizon's collocation services offer a highly secure environment to deploy computing, network, storage and IT infrastructures. Security in Verizon CHS facilities is listed in **Table 2.4.4-1:**

2.5 Cloud Service (Cloud) [C.2.5]

Verizon will provide EIS ordering agencies with access to a variety of Cloud services, such as Infrastructure, Platform, Software as a Service (IaaS, PaaS, and SaaS), and Content Delivery Network Services (CDNS). For EIS, Verizon has an ecosystem of partners and its own FedRAMP-certified cloud services. **Table 2.5-1** outlines this ecosystem of cloud partners, their services and essential inherent cloud characteristics as defined in NIST SP 800-145.



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

Compliance with EIS Service Requirements [J.19] – Cloud Service. Verizon complies with **RFP Section C.2.5** and all Verizon cloud services for EIS will be FedRAMP compliant and Verizon will support the five essential characteristics and four deployment models of cloud services defined in NIST SP 800-145 listed in the RFP and outlined above in **Tables 2.5-1** and **2.5-2**.

2.5.1 INFRASTRUCTURE AS A SERVICE (IAAS) [C.2.5.1]

2.5.1.1 Understanding [L.29.2.1, M.2.1]

Verizon is proposing its FedRAMP Infrastructure as a Service (IaaS) Enterprise Cloud Federal Edition. The Verizon IaaS provides agencies with the agility to implement ideas faster, scale quickly, and drive growth.

Enterprise-Class Computing and Storage to Meet Organizational Needs. Verizon Cloud, whether it is Public, Private, or a Hybrid solution, provides reliable access to high-performance computing (virtual machines) and storage capabilities (see **Figure 2.5.1.1-1**) with global scale and high availability. [REDACTED]

[REDACTED] Ordering agencies can tailor their Cloud deployments to suit a vast array of applications, service levels, and security policies. Agencies can test, optimize, deploy, and maintain the applications and information needed to remain informed, productive and competitive.



Workload Deployment Flexibility. From simple, high-value workloads like Dev/Test, to mission critical workloads running ERP, Verizon Cloud offers ordering agencies the flexibility to run workloads spanning the entire application adoption spectrum – each with services tailored to their own needs. Agencies can choose the deployment and compute mix that best suits their business and security needs, including public, virtual private, or private Cloud delivered off premise or wholly managed on premise.

Global Scale, Enterprise Expertise, Driven Approach to Hybrid Cloud. Verizon IaaS offers comprehensive solutions designed to help ordering agencies easily and efficiently manage workloads. Verizon's solutions expertise spanning private cloud, public cloud, collocation, and networking can offer a consolidated and organized approach to meet agencies' specific Cloud and data needs. The government can easily bridge existing private, public and hybrid Clouds as well as traditional IT and collocation environments while maintaining strong security and application performance. With Verizon's expansive footprint, ordering agencies can deploy workloads over

multiple facilities, and leverage storage resources for applications, backups, file sharing, and more.

Network Powered for Speed and Execution. Verizon's cross-portfolio private network capabilities enable quick, secure exchange of information between customer-facing and business critical applications, as well as reliable, proven performance to support Cloud application delivery and business execution during times of peak need. Fast provisioning capabilities allow agencies to source and federate with other Clouds (e.g., Verizon Secure Cloud Interconnect (SCI) Service) providing another means for secure hybrid Cloud solutions. SCI uses the high-performing connections of Verizon's Private IP network to securely link workloads to existing locations, to partners, and even to a select ecosystem of cloud service providers. The reliability, speed and diversity of the network provides an end-to-end environment for Cloud-based applications. SCI, combined with other network services, offers a complete and integrated solution.

Security and Transparency. Verizon Cloud is designed to help ordering agencies meet changing compliance and security requirements (e.g., DOD Level 2 Provisional Authority, PCI, NIST 800-53, SSAE16, ISO 27001, HIPAA, FedRAMP, DIACAP, and FISMA). Verizon deploys world-class security solutions and experts across business environments to enable easy and concise access to information about an agency's Cloud (performance, location, hardware and software versions, logs, etc.). Verizon Cloud offers flexible deployment of compute resources (CPU, memory, and storage) allowing agencies to provision and manage their virtual servers from Verizon's geographically diverse data centers around the world. Agencies can also control load balancers and firewall resources allocated to an environment without requiring specialized knowledge or assistance.

Verizon Cloud Management. Cloud resources are configured and provisioned into the ordering agency Cloud Space by the authorized Cloud administrator based on the needs of the workload or project. The appropriate deployment option is selected for a workload based on foundational criteria including geography, performance, and deployment type to support the IaaS resources that will fulfill the technical requirements

specified by the Cloud administrator. Multiple Cloud Spaces can be provisioned to support a variety of business and technical requirements.

Verizon Private Off / On Premise Cloud. Verizon Cloud Private Off-Premise provides physical segmentation of compute and storage resources within the Verizon Cloud to isolate compute and storage to a single agency with the benefit of shared data center components, Cloud management tools, and Verizon management staff. Private Cloud deployed within a Verizon data center provides ordering agencies with the flexibility of the Cloud with the peace of mind that comes with a fully managed service. Verizon Cloud Private On-Premise is Verizon Cloud deployed on agency premises that is managed remotely by Verizon. **Table 2.5.1.1-1** lists the features of Verizon Cloud Private Off- and On-Premise.

Table 2.5.1.1-1. Verizon Cloud Off-Premise

Verizon Cloud Off-Premises
▪ Hardened and automated virtualization environment provided as a service;
▪ Low initial cost based on a Deployment and Installation (D&I) cost;
▪ Centralized Management from Verizon for Tier 2-3 issues;
▪ Consistent and Standardized Verizon Customer Support;
▪ Option to contract separately, deploy into Verizon Colocation and Managed Hosting and cross connect locally with low latency and data charges;
▪ Verizon supports private Cloud management and hands-on operations;
Verizon Cloud On-Premises
▪ Support management functions including capacity expansion, infrastructure audits, and inventory management.
▪ Day-to-day management agencies will perform any real-time hands-on operations with direction from Verizon.

Verizon Cloud Storage. Verizon Cloud Storage lets ordering agencies securely store, access, and protect non-transactional data in the Cloud, making it readily available and accessible via the Internet in practically any location around the world with high availability and performance. This secure and high performing, object-based storage solution is highly durable, utilizing self-healing and continuous data integrity checks. Verizon Cloud Storage includes:

Providing a Secure Storage Environment. Verizon Cloud Storage is built into the Verizon Cloud portfolio using the same level of security as demanded by agencies and high-security financial institutions.




Local Storage Connectivity. Users and applications are distributed globally and need to access data from anywhere on the network. Verizon Cloud Storage provides access around the globe through the Internet using industry standard, common access protocols.

Verizon Cloud Backup. Verizon Cloud Backup provides ordering agencies with a simple to use disk-based back-up and recovery solution for data protection and business continuity planning. Employing a disk-only topology removes the risk of unreliable tape-based backup systems and media, maintaining that data is both readily available and not subject to the transport or environmental risks with tape infrastructure.

Tight integration with the Verizon Cloud Console enables agencies to click-to-provision backup services for Verizon Cloud workloads and as a true utility service, agencies pay for the capacity of the virtual machines protected and the incremental versions of changed blocks. The stored data amount is significantly reduced by deduplication and compression features, which also drives down bandwidth utilization, helping reduce the overall backup windows.

Verizon Cloud Disaster Recovery. Verizon Cloud Disaster Recovery provides agencies with a simple to use, disk-based, disaster recovery solution for workloads running on Verizon Cloud. Employing a disk-only topology, it reduces the management complexity involved in an application-based replication solution, and increases the efficiency of data transfer between the production and disaster recovery cloud locations.

Verizon employs disk level replication technology to track block changes of the disks running in Verizon Cloud. This disk mirroring process, illustrated in **Figure 2.5.1.1-2**, is asynchronous, meaning that changes are collected and updated based upon the recovery point objective (RPO).



The service is built upon a disk replication technology that links the data volumes at ordering agencies' primary Verizon Cloud data center directly to the disaster recovery volume at the alternative Verizon Cloud location. Changes in the data volumes are transmitted between data center on a regular basis, with the goal of keeping data on disk synchronized in the event of a disaster.

2.5.1.1.1 Compliance with EIS Service Requirements [J.19]

Provisioning Computing and Networking Resources; Supporting FedRAMP and Overlay Requirements; IaaS Subservices. Verizon complies with **RFP Section C.2.5.1.1**. Verizon IaaS will provide a solution for provisioning required computing and networking resources and supporting the FedRAMP and TIC overlay requirement. IaaS will be composed of the Private Cloud IaaS, Data Center Augmentation with Common ITSM, Cloud-based Data Center Support Service, and Cloud Professional Services. The Private Cloud IaaS subservice will offer a private cloud IaaS solution that includes virtual machines, storage, and server hosting. The Data Center Augmentation with Common ITSM subservice will enable augmentation of already-virtualized agency premises Data Center resources with dynamically expandable and contractible virtualized cloud-based resources and provide the following mandatory capabilities: 1) Ability to manage both cloud virtual resources and the agency data center's virtual resources with interoperable monitoring and control capabilities; 2) Verizon's management platform will include a visual indicator of which

resources are in the cloud and which are premises resources; 3) (Optional) Ability to integrate with agency's data center management platform. [RFP Section C.2.5.1.1.4.2]

Features. Verizon complies with **RFP Section C.2.5.1.2**. Verizon's IaaS will include the following features: 1) optional "bare metal" physical servers; and 2) data management and analytics.

Stipulated Requirements. Verizon complies with the **Service Description (C.2.5.1.1)**, **Functional Definition (C.2.5.1.1.1)**, and all applicable **Standards (C.2.5.1.1.2)**, **Connectivity (C.2.5.1.1.3)**, **Interfaces (C.2.5.1.3)**, and **Performance Metrics (C.2.5.1.4)** RFP requirements.

2.5.1.2 Quality of Services [L.29.2.1, M.2.1]

As a platform, Verizon's facilities and computing infrastructure are built to high availability standards. To protect against wholesale outage risks, Verizon facilities incorporate triple-redundant power supplies, multiple carriers (not just Verizon), intra-facility compute failure recovery processes, and geographical diversity. At the application layer, Verizon will work with the agency on a TO basis to identify availability requirements of systems to be hosted and design a solution to meet them. Verizon Cloud infrastructure has an [REDACTED] with the provisioning services running at 99.5 percent.

Verizon Cloud Storage lets agencies securely store, access, and protect its non-transactional data in the Cloud. This secure and high performing, object-based storage solution is highly durable and makes use of self-healing and continuous data integrity checks to provide, local and geographic redundancy [REDACTED]

[REDACTED] so agencies can confidently store their critical data long term. Through a single management console, the agency configures where and how data is stored and maintained.

2.5.1.3 Service Coverage [L.29.2.1, M.2.1]

Verizon complies with **RFP Section C.1.3** and will support IaaS in a minimum of 25 of the top 100 CBSAs.

2.5.1.4 Security [L.29.2.1, M.2.1]

The Verizon IaaS is managed for security and risk per Verizon's EIS IT Risk Management Framework (RMF) Plan in **Volume 1, Attachment A**. Appropriate security measures for the selected access solution will be implemented on a TO basis for Internet and related traffic that requires aggregation (reference **Section 3, External Traffic Routing**) to provide security and confirm the integrity of government data. If additional security measures are required they will be addressed at the TO level.

Verizon Cloud is FedRAMP compliant and will continue to achieve federal security certifications for new services Verizon adds to its existing authorized service suite FedRAMP package ID: AGENCYVERIZONECFE. Security documentation can be obtained from the Government Joint Authorization Board. Verizon's perspective on "**what is a secure cloud?**" is grounded in three fundamental themes, as shown in **Table 2.5.1.4-1**:

Table 2.5.1.4-1. IaaS Secure Cloud.

IaaS Logical Security
Strong logical and physical controls that provide a secure base upon which to build;
Governance and controls that create standardized and repeatable processes that streamline operations help make the cloud more stable and reliable and maintain strong security for data and applications;
Value-added security services that allow organizations to expand their security posture.



Base Security. Deployments are located in purpose-built, cloud-enabled data centers built to support SSAE 16 / SAS 70 Type II specifications with redundant power and cooling systems that help preserve operations. Advanced Cloud computing security control systems include interior and exterior video monitoring, access control systems and 24x7 monitoring by an on-site guard and Verizon's Network Operations Center.

Logical Security. Verizon operates a second logical layer of defense through virtualization tools and a complete suite of security services that are delivered, managed and maintained by Verizon's 24x7 Government Network Operations Security Center (GNOSC) In Verizon's ongoing efforts to ensure the confidentiality, integrity and availability of networks, resources and data for both Verizon's infrastructure and customers' cloud environments, Verizon Cloud uses a number of processes for the protection of the IaaS management backplane for Compute, Network, Storage and Management, as described in **Table 2.5.1.4-2**:

Table 2.5.1.4-2. IaaS Logical Security.

IaaS Logical Security
Implement security controls at the compute layer in several ways including strong security at the hypervisor and operating system (OS) layers;
Use strong administrator and back-end authentication to protect access to the Verizon Cloud Management servers and server infrastructure;
Secure the network layer in a variety of areas, including core virtualization network controls, network data segmentation, firewall capabilities, intrusion detection, and DDoS detection and mitigation;
Leverage industry-standard storage area network (SAN) segmentation techniques so that SAN resources are logically separated and do not have visibility to other client instances;

Verizon leverages hypervisor level segmentation techniques so that data isolation is performed at the OS layer and no two client operating systems are shared.

Secure Connectivity. Multiple options exist for secure connectivity to customer VMs. Verizon Cloud provides SSL VPN or LAN-to-LAN (L2L) connectivity into the Cloud through integrated VPN capabilities. As required in a TO, depending on the selected access solution, Verizon will ensure that appropriate security measures are implemented for Internet and related traffic that requires aggregation (see **Section 3** of this proposal volume) to confirm security and the integrity of government data.

Governance, Risk and Compliance. To facilitate the ongoing and continuous management of Verizon Cloud products, Verizon dedicates an entire team of Governance, Risk, and Compliance (GRC) experts to support agency requirements.

2.5.2 PLATFORM AS A SERVICE [C.2.5.2]

2.5.2.1 Understanding [L.29.2.1, M.2.1]

Verizon has an extensive strategy to deliver Platform as a Service (PaaS) to EIS agencies. The strategy involves a combination of partner ecosystem and internally developed Verizon PaaS capabilities.

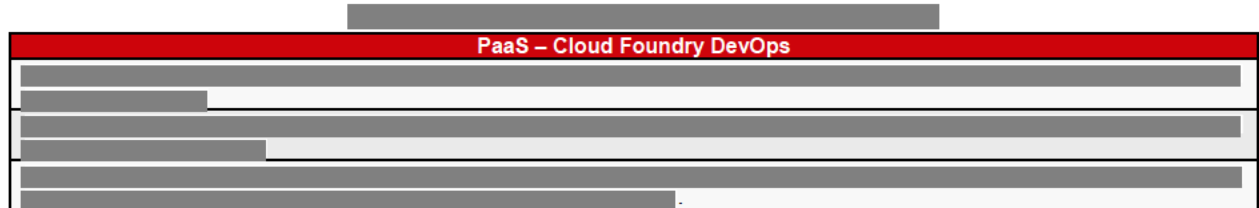
[REDACTED] support federal agencies and along with developing its own PaaS Verizon is developing a partner ecosystem that will deliver similar development services to ordering agencies. [REDACTED]

[REDACTED] These services provide the government with a complete set of PaaS tools to build employee-facing apps that are mobile, create agency-facing apps that deepen the user experience, and can integrate and connect more easily and faster with ordering agency enterprises. This will also allow the developer to build more engaging agency apps and connect those apps [REDACTED], allowing the government to forge better agency relationships, deliver superior service, and anticipate needs. [REDACTED]

t. [REDACTED]

Verizon will utilize the Cloud Foundry Platform to deliver a highly scalable, open source, automated means for DevOps. Cloud Foundry is an open standard for cloud applications. It is designed to make DevOps the normal state of computing and is built for fast-cycle innovation of cloud applications, as described in **Table 2.5.2.1-1**. For the Government, this means faster speed to deliver services to their agencies. For

development, it means scalable and continuous deployment. For operations, it means faster cycle time and higher reliability. For everyone, open source means no vendor lock-in.



Verizon PaaS will enable developers to provision and bind web and mobile apps with leading platform and data services such as Jenkins, MongoDB, Hadoop, MySQL, RabbitMQ, Redis, etc. on a unified platform. It will empower government users to deliver applications and update them with new features at a velocity and scale, allowing enterprises to innovate with disruptive speed. Verizon is looking to provide the ideal self-service platform for development teams of any size to start small and rapidly evolve new ideas into complex applications, increasing business agility. Additionally when this service is ready for government use it will be a FedRAMP compliant solution. Ordering agencies will be able to access Verizon PaaS either securely through IPS services or via a dedicated VPNS solution. **Figure 2.5.2.1-1** depicts the overall PaaS approach for ordering agency delivery.



2.5.2.1.1 Compliance with EIS Service Requirements [J.19]

Verizon PaaS Capabilities and Tools. Verizon complies with **RFP Section C.2.5.2.1.4**. Verizon's PaaS solution will provide the following types of capabilities from commercially available software platforms: 1) compliance with national policy; 2) developer tools; 3) database systems; 4) big data solution platform; 5) directory; 6) testing tools. Verizon will provide tools to allow the client agency to fully access PaaS related data from the cloud in a usable format as needed.

Stipulated Requirements. Verizon complies with the **Service Description (C.2.5.2.1)**, **Functional Definition (C.2.5.2.1.1)**, and all applicable **Standards (C.2.5.2.1.2)**, **Connectivity (C.2.5.2.1.3)**, **Interfaces (C.2.5.2.3)**, and **Performance Metrics (C.2.5.2.4)** RFP requirements.

2.5.2.2 Quality of Services [L.29.2.1, M.2.1]

Verizon PaaS is delivered via Verizon's partners' FedRAMP-certified platforms. As Verizon continues to enhance Verizon's PaaS offerings, Verizon will require any partner to have an existing FedRAMP ATO, as well as delivering Verizon's PaaS services as they are commercially developed and achieve a FedRAMP ATO. Verizon partners' PaaS solutions offer resiliency and are built to high availability standards. To protect against wholesale outage risks, the facilities incorporate redundant power supplies, multiple carriers, intra-facility compute failure recovery processes, and geographical diversity. At the application layer, Verizon will work with the ordering agency on a TO basis to identify availability requirements of systems to be hosted and design a solution to meet them. The architecture can be built with agency prescribed high availability and disaster recovery configurations.

2.5.2.3 Service Coverage [L.29.2.1, M.2.1]

Verizon complies with **RFP Section C.1.3** and will support PaaS in a minimum of 25 of the top 100 CBSAs.

2.5.2.4 Security [L.29.2.1, M.2.1]

The Verizon PaaS is managed for security and risk per Verizon's EIS IT Risk Management Framework (RMF) Plan in **Volume 1, Attachment A**. Appropriate security

measures for the selected access solution will be implemented on a TO basis for Internet and related traffic that requires aggregation (reference **Section 3, External Traffic Routing**) to provide security and confirm the integrity of government data. If additional security measures are required they will be addressed at the TO level. **Table 2.5.3.4-1** lists the FedRAMP PaaS ATO identifiers for Verizon PaaS services:

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

2.5.3 SOFTWARE AS A SERVICE [C.2.5.3]

2.5.3.1 Understanding [L.29.2.1, M.2.1]

Verizon's Software as a Service (SaaS) offering is designed to provide a variety of Enterprise class services based on Verizon discussions and experience in the public sector market. Verizon's solutions are based on both its internal Cloud capabilities as well as its [REDACTED] additional Cloud based services to GSA and ordering agencies. Verizon is proposing [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED] is comprised of the [REDACTED]

[REDACTED]

and the backend infrastructure that supports the operations of these products. [REDACTED] performs security assessments of application code and web site/web services testing without any software to install or manage. Static Code Scanning of code such as Java, .NET, and other major programming languages for security defects are performed in the [REDACTED] at the code layer followed by an audit review by an [REDACTED]. Dynamic Web Site and Web Services testing use [REDACTED] software as the scan engine, followed by a review from an [REDACTED].

Future SaaS intends to deliver pre-certified, market-leading applications in big data, security, and software development, by developing a SaaS ecosystem. This approach reduces speed innovation cycles with easy, predictable deployments of new applications. With Verizon Cloud SaaS ecosystem, ordering agencies can quickly

deploy software products and templates. The Verizon Cloud SaaS ecosystem enables agencies to quickly procure Verizon Cloud Services and save time on configuration, deployment and fine tuning, deploying with the applications you need, when an agency needs them to support their mission with pre-certified, world-class applications; consolidated billing and first-level support; and speedy, predictable and efficient deployments. Verizon SaaS will deliver specific services on a TO basis, based on ordering agency requirements.

Connecting SaaS in a Hybrid Environment. These services can be delivered and connected to new or existing Cloud services via Verizon's proposed networks service delivered and in tandem with its Secure Cloud Interconnect (SCI) Service. Verizon provides high-performance private connectivity to agency workloads through SCI, allowing agencies to take advantage of application flexibility, business agility and cost control of the cloud while maintaining high security and privacy standards. SCI uses the high-performing connections of Verizon's Private IP network to securely link agency workloads to their existing locations, to authorized partners, and even to a select ecosystem of cloud service providers. The reliability, speed and diversity of the network provide an end-to-end environment for cloud-based applications. SCI, combined with other network services, offers a complete and integrated solution.

SaaS and MNS Integration. Verizon SaaS will be integrated for monitoring, ticketing, change management and other ITIL based processes that are managed via the Verizon MNS platform. Also, both internal to Verizon and external to its partners, SaaS will be monitored by the Verizon Government Network Operations and Security Centers (GNOSCs) as described in **Section 2.8. Figure 2.5.3.1-1** depicts Verizon's operating concept for delivering SaaS to ordering agencies.

The MNS platform is optimized for scalability, performance, availability, and security and provides a process to preclude unauthorized changes to IT systems while controlling and coordinating approved changes to global infrastructure, systems, applications, and services.

2.5.3.1.1 Compliance with EIS Service Requirements [J.19]

Verizon SaaS Capabilities. Verizon complies with **RFP Section C.2.5.3.1.4** and current National Policy regarding access to agency data in data centers as defined in **C.1.8.8**. Verizon will provide the following SaaS capabilities including, but not limited to: Customer Relationship Management (CRM) tools; Enterprise Resource Planning (ERP) tools; Human Capital Management (HCM) tools; Desktop applications; Office automation tools; Security tools; Others as defined in the TO. The agency retains exclusive ownership over all of its data in the cloud. Verizon will provide tools to allow the client agency to fully access SaaS-related data from the cloud

Stipulated Requirements. Verizon complies with the **Service Description (C.2.5.3.1)**, **Functional Definition (C.2.5.3.1.1)**, and applicable **Standards (C.2.5.3.1.2)**, **Connectivity (C.2.5.3.1.3)**, **Interfaces (C.2.5.3.3)**, and **Performance Metrics (C.2.5.3.4)** RFP requirements.

2.5.3.2 Quality of Services [L.29.2.1, M.2.1]

The Verizon Cloud SaaS ecosystem offering will provide GSA and ordering agencies with a wide variety of SaaS solutions that will deliver a wide variety of service. SaaS is based on Verizon's partner ecosystem will deliver SLAs/KPIs that at a minimum will meet the GSA overarching requirements and will address and support any additional KPIs that are released on a TO basis. The Verizon Cloud SaaS ecosystem will continue to evolve over time as new vendor services are added.

2.5.3.3 Service Coverage [L.29.2.1, M.2.1]

Verizon complies with **RFP Section C.1.3** and will support SaaS in a minimum of 25 of the top 100 CBSAs.

2.5.3.4 Security [L.29.2.1, M.2.1]

The Verizon SaaS is managed for security and risk per Verizon's EIS IT Risk Management Framework (RMF) Plan in **Volume 1, Attachment A**. Appropriate security measures for the selected access solution will be implemented on a TO basis for Internet and related traffic that requires aggregation (reference **Section 3, External Traffic Routing**) to provide security and confirm the integrity of government data. If additional security measures are required they will be addressed at the TO level. [REDACTED]

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

2.5.4 CONTENT DELIVERY NETWORK SERVICE

2.5.4.1 Understanding [L.29.2.1, M.2.1]

Verizon has teamed with the proven Content Delivery Network Service (CDNS) provider, [REDACTED] to simplify content delivery and deliver secure application performance solutions. Together, the team provides enhanced network visibility and control to help improve the performance and reliability of web- and IP-based applications. [REDACTED] have a successful history in delivering CDNS to federal government agencies, such as the [REDACTED] [REDACTED] CDNS delivers a superior online experience to complement Verizon's various managed services solutions.

The proposed CDNS solution for ordering agencies will be delivered via a Distributed Computing Platform service. The CDNS will improve the robustness and resilience of an agency's web services as well improve as both live and on demand streaming events, and handle instantaneous and large variations in web content demand that may otherwise exceed the capacity of the agency's data center and web infrastructure. The proposed [REDACTED] CDNS solution will be provided as a managed service and will operate independently of the agency's infrastructure. The CDNS platform will be able to handle instantaneous and large peaks in web traffic and deliver improved content and streaming delivery performance to the end users of an agency's web sites. [REDACTED] maintains a robust Distributed Computing Platform.

External Web Site Requirements

- **Real Time Streaming (Webcasting).** In support of live, "real time" web streaming, the encoder will either "push" the content into [REDACTED] or the entry point of the [REDACTED] will "pull" the encoded stream into the network. From the entry point, the stream will be fed into the [REDACTED] confirming that the stream is available from the edge servers and to retain the reliability and quality of the web stream content. The [REDACTED] uses sophisticated techniques to provide high quality stream delivery to the edge regions. In turn, the edge regions are subsequently able to disseminate the streams to designated end-users. [REDACTED]

employs a proprietary procedure that further reduces the time required for buffering and initiating each stream, creating a consistently high quality user experience.

- **On-Demand Streaming.** Verizon's CDNS solution complies with the following: one terabyte of online storage for caching; government retaining full control over cache usage, configuration, and file retention; and allowing ordering agencies to change the stream bit rate from 384 Kb/s per stream to 1Mb/s per stream.

In addition to supporting the delivery of web site content, [REDACTED]

[REDACTED]

industry media formats [REDACTED]

Public Website Interface Requirements and Protections

- **IP Protocols – IPv4 and IPv6 (including IPsec).** [REDACTED] [REDACTED] high performance delivery of content and applications from any IPv4 origin site to all end-users across the hybrid IPv4/IPv6 Internet without requiring agencies to incorporate significant changes to their existing networking infrastructure.

[REDACTED] – making an IPv6 compliant infrastructure, even in circumstances when an agency's back end infrastructure is currently using IPv4. This means that if an agency's backend infrastructure is a legacy IPv4 configuration, and a requesting client uses IPv6, [REDACTED] accept the request in IPv6 and communicate with the backend infrastructure in IPv4, which in effect represents a re-translation to IPv6 after retrieving content from the origin and transmitting back to the end-user.

Traditional caching services and dynamic acceleration services work effectively with such IPv6 support features.

If the IPv6 or IPv4 client makes a request to an agency's site, [REDACTED] can easily determine if the user will be best served over IPv6. The requesting user will receive IPv6 and IPv4 addresses of optimal servers. The end-user client will then be able to retrieve content quickly from a nearby Edge server using the protocol of choice. If the platform determines that the end-user is best served by IPv4 then only IPv4 addresses of Edge Servers will be returned. This will allow Agencies to receive their content over direct, high performance routes from optimal servers, regardless of the protocol being employed.

This service will enable Agencies to remain with an IPv4 backend based on its specific requirements for any period of time while still maintaining full compliance with IPv6 clientele. Agencies may migrate to an IPv6 infrastructure using their pre-established timeframes without adversely affecting their ability to communicate with the public at large. With today's slow growth and adoption of IPv6 by end-users, the need for content providers to use IPv6 in a commercial production setting will vary based on the particular business needs and demands. [REDACTED]

■ **Domain Name Service.** [REDACTED]

2.5.4.1 Compliance with EIS Service Requirements [J.19]

Content Distribution. Verizon complies with **RFP Section C.2.5.4.1.4(1)**, and will provide the content distribution capabilities (Static Content Download Service, Real-time Streaming (Webcasting) and On-Demand Streaming) as listed in the EIS RFP.

Site Monitoring/Origin Server Performance Measurements. Verizon complies with **RFP Section C.2.5.4.1.4(2)(a-b)**, and will deliver the site monitoring capabilities listed in the EIS RFP.

CDNS Features. Verizon complies with **RFP Section C.2.5.4.2**. Verizon CDNS will provide the following features: 1) Failover Service; 2) Redirection and Distribution Service (Global Load Balancing) (optional).

Stipulated Requirements. Verizon complies with the **Service Description (C.2.5.4.1)**, **Functional Definition (C.2.5.4.1.1)**, and all applicable **Standards (C.2.5.4.1.2)**, **Connectivity (C.2.5.4.1.3)**, **Interfaces (C.2.5.4.3)**, and **Performance Metrics (C.2.5.4.4)** RFP requirements.

2.5.4.2 Quality of Services [L.29.2.1, M.2.1]

The Verizon solution can be scaled appropriately on-demand to handle any traffic surges agency sites may experience.

Live Webcast Testing.

[REDACTED]

Failover Service.

[REDACTED]

[REDACTED]

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

Redirection and Distribution Service (Global Load Balancing). [REDACTED]

[REDACTED]

Web Page Caching. [REDACTED]

[REDACTED]

[REDACTED]

Table 2.5.4.2-1. CDNS Business Rules.

CDNS Business Rules
Flexible cache key to allow caching of pages with session identifiers in their URLs
Cache post responses to allow caching of requests involving posts
Ability to generate and accommodate redirects
Ability to set, read, and modify cookies
Session ID support to allow the automatic creation of sessions and the creation of session cookies or tokens
Downstream caching
Forward Path modification
Ability to re-write selective parts of pages dynamically on provider's platform
A user friendly, quick methodology provided to purge cache for immediate refresh from the origin server

2.5.4.3 Service Coverage [L.29.2.1, M.2.1]

Verizon complies with **RFP Section C.1.3** and will support CDNS in a minimum of 25 of the top 100 CBSAs.

2.5.4.4 Security [L.29.2.1, M.2.1]

The Verizon CDNS is managed for security and risk per Verizon's EIS IT Risk Management Framework (RMF) Plan in **Volume 1, Attachment A**. If additional security measures are required they will be addressed at the TO level. T [REDACTED]

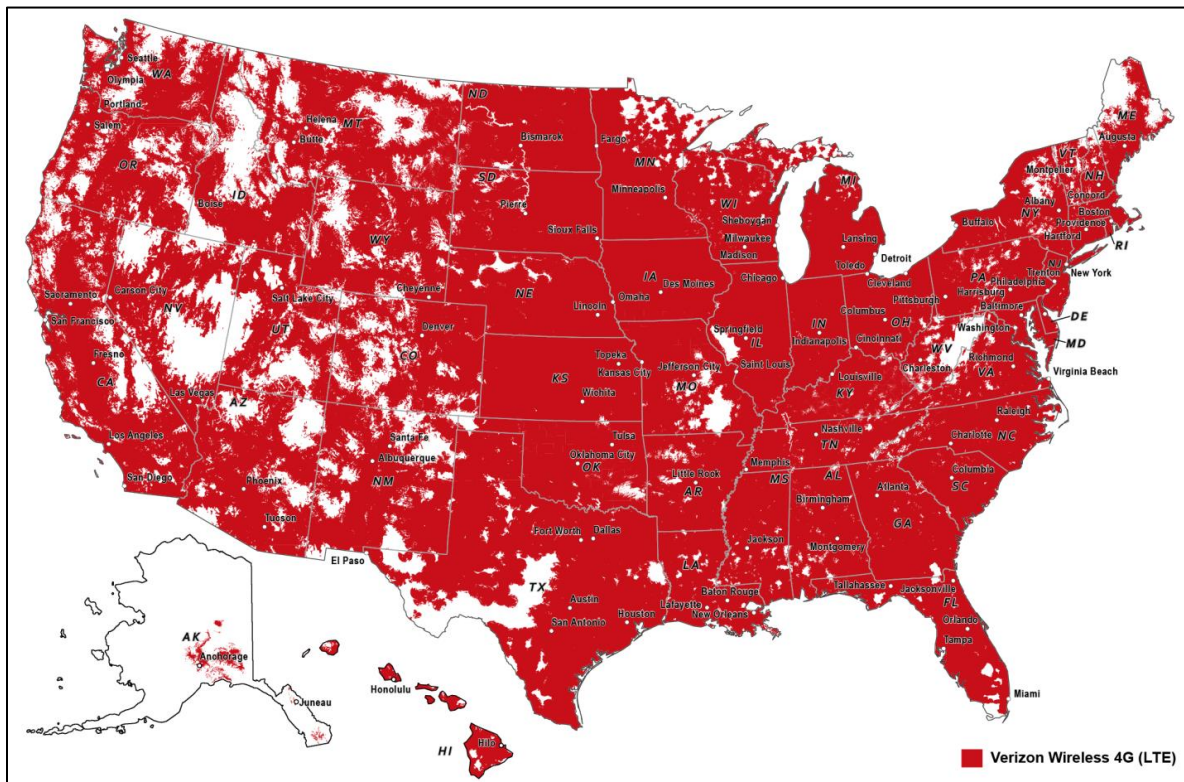
2.6 Wireless Service (MWS) [C.2.6]

2.6.1 UNDERSTANDING [L.29.2.1, M.2.1]

Verizon Wireless operates the nation's most reliable and largest wireless 4G LTE network, depicted in **Figure 2.6.1-1** below. Verizon provides wireless service to organizations of all sizes including small businesses, Fortune 500 corporations, and the federal and state governments. [REDACTED]

[REDACTED], which consistently earns top rankings from independent consumer reporting and testing institutions for network quality and performance. Investment in next generation 5G technology is ongoing with initial trials expected to start by the end of 2016.

Figure 2.6.1-1. Verizon Wireless Services Network



2.6.1.1 Compliance with EIS Service Requirements [J.19]

Originate and Receive Calls. Verizon complies with RFP Section C.2.6.1.4(1).

Verizon MWS will meet the requirement to make calls to and receive calls from mobile phones, fixed wireless networks and satellite-based networks.

Mobile Devices. Verizon complies with RFP Section C.2.6.1.4(2)(a-b) and will provide mobile devices (smartphones and cellular phones) for procurement. Verizon offers a variety of devices equipped with FIPS 140-2 encryption. Audio, video and recording functionality can be disabled by the user of the device or non-camera device models are available. Simultaneous voice and data will be available whenever users are in a Verizon 4G LTE coverage area.

Wireless Service Plans. Verizon complies with RFP Section C.2.6.1.4(3)(a-d) and (f-g). Reference Section 2.8.6 for information about Verizon's compliance with RFP Section C.2.6.1.4(3)(e) and Verizon's mobility applications for mobile device management. Pooling of domestic data (gigabytes) within the same billing account at a

level specified by the ordering agency (e.g., an entire agency or multiple sub-bureaus within an agency) can be done provided the ordering agency specifies “account share” vs. “profile share” when the account is being setup.

Section B.2.6 provides that contractors “may prohibit unlimited data add on or data only plans from being purchased for machine to machine (M2M) or similar types of applications (e.g., automated video feeds), or as a substitute for a private line or a dedicated data connection.” Legal and privacy reasons dictate that contractors cannot monitor how, but only how much, a customer uses its connection. Verizon, based on its extensive experience serving consumer, commercial and government markets, has identified usage by a government user in excess of 5GB within a single billing period as the threshold above which it can be reasonably certain the user is using the service in a manner prohibited by B.2.6. Therefore, anyone using more than 5GB per line in a given month is presumed to be using the service in a manner prohibited by B.2.6, and we reserve the right to immediately limit throughput or amount of data transferred exceeding 5GB in a given month. For purposes of this contract, we are raising this limit to 25GB. We will discuss with the customer whether the user should be reverted to an appropriate alternate plan in accordance with Section B.2.6 (“In these cases, the customer may purchase a limited data add on or data only plan or obtain an M2M plan”). Verizon Wireless does not engage in “network optimization,” the intentional slowing of data speeds for high volume users in congested areas without warning to the user. The foregoing limitations are consistent with the Verizon Wireless unlimited data offering under GSA Schedule 70 and GSA Federal Strategic Sourcing Initiative (FSSI) Wireless.

Wireless Enhanced 911 Rules. Verizon complies with **RFP Section C.2.6.1.4(4)** and will meet the enhanced 911 rules requirements referenced in the RFP.

Directory Assistance with Call Completion. Verizon complies with **RFP Section C.2.6.2(2)** and will meet the directory assistance requirements referenced in the RFP.

Domestic to Non-Domestic Calling. Verizon complies with **RFP Section C.2.6.2(3)** and will meet the domestic to non-domestic calling requirements referenced in the RFP.

International Mobile Roaming. Verizon complies with **RFP Section C.2.6.2(4)** and will meet the international mobile roaming requirements referenced in the RFP.

Personal Hotspot. Verizon complies with **RFP Section C.2.6.2(5)** and will meet the personal hotspot requirements in the United States only. A Domestic Personal Hotspot, for an additional monthly recurring charge, can be added to a Voice & Unlimited Data Plan or an Unlimited Data Only Plan. Data is unlimited; therefore, an overage CLIN is not applicable. Verizon Wireless will limit throughput of data speeds should 25GB of data be used within a given bill cycle, by user/MTN, for the remainder of the bill cycle.

Indoor Cellular System. Verizon complies with **RFP Section C.2.6.2(6)**. Verizon offers 3G and 4G LTE network extenders for customers today. If it is determined that a customized solution is necessary to increase indoor coverage, Verizon Wireless will provide a detailed implementation and pricing schedule, which is outside the scope of this proposal. A separate contract for this effort would be required.

Push to Talk with Group Talk. Verizon complies with **RFP Section C.2.6.2(7)** and will meet all push to talk with group talk requirements referenced in the RFP.

Stipulated Requirements. Verizon understands and agrees with the MWS **Functional Definition (C.2.6.1.1)**, and complies with applicable **Standards (C.2.6.1.2)**, **Connectivity (C.2.6.1.3)**, **Interface (C.2.6.3)**, and Performance Metrics requirements in the EIS RFP.

2.6.2 QUALITY OF SERVICES [L.29.2.1, M.2.1]

Recognizing that reliable wireless service is critical to government business, Verizon Wireless has established extensive preventive maintenance measures, network monitoring and system backup capabilities. These measures, coupled with Verizon's internal performance processes, enable Verizon to provide its customers with levels of

wireless service reliability that distinguish it from other national wireless carriers. Verizon is committed to customer satisfaction in all facets of its performance and are pleased to offer the network service level targets detailed in **Table 2.6.2-2**:

Verizon Network Service Level Targets*	
[REDACTED]	[REDACTED]
	[REDACTED]
	[REDACTED]
	[REDACTED]
	[REDACTED]
	[REDACTED]
	[REDACTED]
[REDACTED]	[REDACTED]
	[REDACTED]
[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]

[REDACTED]. In no event shall the failure to meet the above network service goals subject Verizon to any penalties or damages of any kind. In addition to building the nation's most reliable and largest wireless network, Verizon has been regularly investing in technologies to enhance the value and usability of its network for business and government applications. Examples of such investment are detailed in **Table 2.6.2-2** below:

Verizon Wireless Investment Examples	
[REDACTED]	[REDACTED]
	[REDACTED]
	[REDACTED]
[REDACTED]	[REDACTED]
	[REDACTED]
	[REDACTED]
	[REDACTED]
	[REDACTED]
[REDACTED]	[REDACTED]
	[REDACTED]
	[REDACTED]
[REDACTED]	[REDACTED]
	[REDACTED]
	[REDACTED]
	[REDACTED]
	[REDACTED]
[REDACTED]	[REDACTED]
	[REDACTED]
	[REDACTED]
[REDACTED]	[REDACTED]
	[REDACTED]
	[REDACTED]

[illegible]

Verizon complies with **RFP Section C.1.3** and will support MWS in a minimum of 25 of the top 100 CBSAs.

Verizon includes Alaska as part of our domestic cellular coverage; however, the feature functionality of the service is dependent upon the manufacturer of the customer device. Regardless, the domestic voice and data plan pricing still apply.

The Verizon MWS is managed for security and risk per Verizon's EIS IT Risk Management Framework (RMF) Plan in **Volume 1, Attachment A**. If additional security measures are required they will be addressed at the TO level.

E911. Verizon complies with **RFP Section C.2.6.1.4(4)**, the Wireless Enhanced 911 (E911) Rules including Phases I and II as stipulated by the Federal Communications Commission. Verizon's mobile network routes 911 calls to designated emergency call

takers known as Public Safety Answering Points (PSAPs). E911 automatically provides call takers with the mobile phone number, cell site and sector, and the estimated latitude and longitude location of the 911 caller if the PSAP is capable of receiving it.

WPS. Verizon complies with **RFP Section C.2.6.2(1)** and will meet the WPS requirements referenced in the RFP.

2.7 Commercial Satellite Communications Service [C.2.7]

2.7.1 UNDERSTANDING [L.29.2.1, M.2.1]

Verizon will provide Commercial Satellite Communications Service (CSCS) that will deliver voice, data and Internet services to land-based, maritime, or aeronautical users using one- or two-way communications via satellite.

Verizon will also provide Commercial Fixed Satellite Service (CFSS) that will deliver satellite capacity that can be used to support communications and applications at an agency-specified throughput between two or more specified end points. This service can be used for applications like distance learning, continuity of operations, broadcast video and associated audio, including encrypted communications.

Verizon CSCS provides satellite bandwidth and uplink/downlink teleports. Verizon will use to provide space segments to meet the requirements specified in individual TOs and, at a minimum, the performance requirements listed in the EIS RFP. Verizon's CSCS includes IRIsatellite transponder space or bandwidth and teleport uplink and downlink services along with earth terminals and support systems required to access the end-user's network.

2.7.1.1 Compliance with EIS Service Requirements [J.19]

Mobile or Fixed Satellite Communications (COMSATCOM). Verizon complies with **RFP Section C.2.7.1.1** and will provide mobile or fixed commercial satellite communications (COMSATCOM) services to include, but not be limited to: satellite bandwidth, satellite service plans, contractor provided earth terminals, radio frequency equipment, satellite phones, interfaces and support services.

Satellite Frequency Bands. Verizon complies with **RFP Section C.2.7.1.1**; COMSATCOM will be provided in any commercially available communications satellite frequency band to include, but not limited to, S-, C-, L-, X-, Ku-, Ka- and UHF bands.

Performance Requirements. Verizon complies with **RFP Section C.2.7.1.3** and will provide space segments to meet the requirements specified in individual TOs and, at a minimum, the performance requirements specified in the RFP.

Dedicated Capacity Requirements. Verizon complies with **RFP Section C.2.7.1.3**. For dedicated capacity requirements, unless otherwise specified in individual TOs, Verizon will provide satellite bandwidth on a non-pre-emptible basis unless otherwise specified in the TO. That is, the bandwidth shall not be preempted for any reason and will be replaced in the event of failure.

Leased Earth Terminal Services. Verizon complies with **RFP Section C.2.7.1.3** and will provide Verizon- (or partner-) operated and -maintained leased earth terminal (ET) services as specified in individual TOs.

Certified Earth Terminals. Verizon complies with **RFP Section C.2.7.1.3**; ETs provided by Verizon and its partners are certified as acceptable for service by the satellite system operator of the specific system on which the ET is to be used.

CFSS Satellite Internet. Verizon complies with **RFP Section C.2.7.1.3** and will provide CFSS Satellite Internet Service (SIS), which will provide Internet access and domestic and international voice service.

Commercial Mobile Satellite Service (CMSS) Support. Verizon complies with **RFP Section C.2.7.1.3** and will support internet access, voice calling, SMS texting, Fax, streaming services, and machine-to-machine.

CFSS Features. Verizon and its partners comply with **RFP Section C.2.7.2(1-6)**. CFSS features provided by Verizon include: Capacity, Coverage, Network Monitoring (Net OPS), EMI/RFI Identification, Characterization, Geolocation, Interoperability (Net Ready), and Information Assurance.

Satellite Phones & Terminals. Verizon complies with **RFP Section C.2.7.2.**

Verizon will provide satellite handheld phones and Broadband Global Access Network (BGAN) terminals. Satellite phones will be tri-mode, if requested, which provides satellite, CDMA and GSM connectivity for the ultimate flexibility. Data terminals or BGAN units will also be provided that can support simultaneous voice and data connections from a small lightweight satellite terminal. [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

Stipulated Requirements. Verizon complies with the **Functional Definition (C.2.7.1.1)**, and all applicable **Standards (C.2.7.1.2)** and **Performance Metrics (C.2.7.3)** RFP requirements.

2.7.2 QUALITY OF SERVICES [L.29.2.1, M.2.1]

Verizon will provide compliant, scalable, reliable and resilient services using the combination of third party vendors, where needed, along with Verizon expertise in the areas of terrestrial backhaul and network connectivity, network management and existing Verizon satellite infrastructure.

Verizon will [REDACTED] implement satellite bandwidth and end-to-end solutions across the globe, where the requirement resides. [REDACTED] corporate network, video and Internet solutions to governments, organizations and companies [REDACTED]

[REDACTED]

[REDACTED]



Verizon works with partner teleports for in-region uplink and downlink services where those needs reside. [REDACTED]

[REDACTED]
[REDACTED]
[REDACTED]

Backhaul connectivity options include Verizon network backbone access from Verizon-owned teleports, [REDACTED]

[REDACTED]

[REDACTED] Combining these options with the global satellite fleet reaches of [REDACTED] flexible options for connecting back to the trusted terrestrial network no matter where the end-user is in the world.

Management and support of the requested satellite services will be provided 24x7 [REDACTED]

[REDACTED]

[REDACTED] Support includes fault detection, carrier measurement and monitoring, problem resolution and payload reconfigurations.

One of the ways Verizon plans to accommodate growth and advances in technology [REDACTED]
[REDACTED] next generation satellite technology [REDACTED]

2.7.3 SERVICE COVERAGE [L.29.2.1, M.2.1]

Verizon complies with **RFP Section C.1.3** and will support CSCS in a minimum of 25 of the top 100 CBSAs.

2.7.4 SECURITY [L.29.2.1, M.2.1]

The Verizon CSCS is managed for security and risk per Verizon's EIS IT Risk Management Framework (RMF) Plan in **Volume 1, Attachment A**. If additional security measures are required they will be addressed at the TO level.

Verizon will utilize security-compliant infrastructure in providing the satellite network and terrestrial backhaul. [REDACTED] satellites and associated operation systems from unauthorized access, use, disclosure, disruption, modification, or destruction to maintain integrity, confidentiality and availability.

FISMA and FIPS 200. Verizon complies with **RFP Section C.2.7.2**. In accordance with FISMA guidelines, [REDACTED] implemented policies and procedures to reduce information technology security risks to an acceptable level. [REDACTED]

[REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED] Verizon CSCS meets the requirements assigned against a low-impact information system (per FIPS 200), as described in the current revision of NIST SP 800-53, "Security Controls for Federal Information Systems and Organizations."

Verizon CSCS employs command encryption at the TO level, when requested, and [REDACTED] benefit from command encryption. [REDACTED]

complies with NIST SP 800-53 and DoD standards for IA (i.e., DoDI 8500.2 and DoDI 8581.01), based on the specified MAC and confidentiality level requirements of an individual TO. At a minimum, [REDACTED] low impact or MAC III system for its end-to-end solutions provided to the government.

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

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

2.8 Managed Service [C.2.8]

Verizon's enhanced Managed Services platform securely and centrally manages GSA and subscribing agency IT infrastructures, their systems and applications, and the services that electronically interconnect and provide information services to agency and civilian employees, while providing enterprise and site-specific visibility into the status of IT services. It was built with the requirements and needs of the federal government in mind and built to be technology-agnostic, providing service management capabilities for best-in-class vendors, providers, manufacturers and a wide variety of IT systems, services, and functions. Verizon currently provides Managed Network Services (MNS) solutions to both [REDACTED]

[REDACTED]

[REDACTED]

Verizon's enhanced Managed Services platform is a common, standardized architecture that supports other specific managed services (e.g., LAN/WAN, Physical/Virtual Server, Cloud, Mobility, Desktop Operating System (OS)) and enables advanced infrastructure services, like software-defined networking, software-defined perimeters, and future SaaS-based solutions.

Verizon's Government Network Operations and Security Center (GNOSC) will use the

platform to provide agencies with a “single pane of glass” view of their infrastructure with advanced cyber analytics to detect and prevent security issues. The platform is a unified, flexible, secure, scalable, and resilient IT Service Management framework that will enable agencies to provide higher quality services, aligned with their mission imperatives, as listed in **Table 2.8-1**:

Table 2.8-1. Managed Service Capabilities.

Managed Service Capabilities
Better manage network resource utilization with the goal of achieving lower costs.
Rapidly provision devices on-demand.
Establish and maintain consistent service levels.
Provide continuous monitoring aligned with the NIST Risk Management Framework (NIST Special Publication 800- 37).
Accurately and efficiently manage hardware and license distribution.
Maintain and control network and IT infrastructure configurations.
Assist with technology compliance (designed to meet Federal and industry best practices, including the NIST SP 800 series guidelines, FISMA, and Information Technology Infrastructure Library (ITIL) 2011.
Leverage Verizon's expansive MNS experience (over 25 years, 3,000 customers, and 370,000 devices).

2.8.1 MANAGED NETWORK SERVICE (MNS) [C.2.8.1]

2.8.1.1 Understanding [L.29.2.1, M.2.1]

Verizon's Managed Network Service (MNS) is comprised of best-of-breed commercial-off-the-shelf (COTS) products integrated with backbone monitoring/alarms that are designed to modernize and deliver global network infrastructure, technologies, and operational management services to the GSA and its agencies. MNS provides enhanced strategic information sharing, enterprise Information Technology (IT) services management, and command and control in a unified, centralized, highly-automated and sustainable system, designed to meet FISMA High security standards. Verizon's MNS is optimized for scalability, performance, availability, and security and provides a process to prevent unauthorized changes to IT systems, while controlling and coordinating approved changes to global infrastructure, systems, applications, and services. MNS solutions can coordinate and synchronize IT service(s) provisioning with global support, and can be integrated with other GSA and contractor enterprise management systems to provide holistic situational awareness of the entire enterprise.

MNS solutions provide agencies with the ability to request, configure, and provision new network infrastructures as well as efficiently make changes to existing services to meet service requirements. MNS solutions provide extensive reporting, including Standard Management Functional Area (SMFA) data metrics derived from Fault, Configuration,

Accounting, Performance, and Security Management (FCAPS) functions applied to IT infrastructure, systems, and services. MNS will support the virtual and physical circuits for all underlying EIS access and transport services implemented using MNS, as required.

MNS solutions allow agencies to have a robust and resilient global enterprise management system that enables and delivers faster, better informed decisions provided by secure, seamless access to information, regardless of computing device or location. These technical features and functions combined with the efficiencies and benefits that stem from automation, shared resources, secure data centers, and a high availability infrastructure make Verizon MNS a transformational solution that will provide GSA and its agencies the ability to rapidly deploy and obtain information from a flexible, standardized infrastructure, while effectively managing associated IT systems and infrastructure resources across multiple security enclaves.

2.8.1.1.1 Compliance with EIS Service Requirements [J.19]

Design and Engineering Services. Verizon complies with **RFP Section C.2.8.1.1.4.1(1-3)** and will provide design and engineering services that satisfy agency requirements, as specified in the RFP and TOs.

Develop, Implement, and Manage Comprehensive Solutions. Verizon complies with **RFP Section C.2.8.1.1.4.2(1)(a-d)** and will develop, implement, and manage comprehensive solutions, such as Access, Transport, Customer premises, and security solutions using the EIS services and their enhancements, in order to meet agency-specific requirements.

Hardware, Firmware and Related Software. Verizon complies with **RFP Section C.2.8.1.1.4.2(2)** and will supply and manage the hardware, firmware and related software (i.e., routers, switches, encryption devices, CSUs/DSUs, hubs, adapters and modems) required by the agency to deliver managed services.

Performance Monitoring and Real-Time Visibility. Verizon complies with **RFP Section C.2.8.1.1.4.2(3)(a-b)** and will provide tools to monitor performance of

agency-specific networks (i.e. transport services, access circuits, government edge routers), and provide real-time visibility of transport and access services performance.

24x7 Network Management. Verizon complies with **RFP Section C.2.8.1.1.4.2(4)(a-f)** and will manage the network in real-time, 24x7; support remote management capabilities from the NOC defined in the TO; proactively monitor utilization and packet loss and errors, probing in 15-minute intervals, at most, to confirm proper equipment/network operations and performance; assess and report access-and-transport services performance and SLAs, and on agency-specific network capacity and performance, and address agency-specific network capacity and performance issues. Today, [REDACTED]

SNMP Data Feeds. Verizon complies with **RFP Section C.2.8.1.1.4.2(5)** and will support SNMP data feeds that may enable the agency to utilize applications to analyze and interpret the raw data to provide reports on managed equipment information, as applicable.

Network Configuration Management. Verizon complies with **RFP Section C.2.8.1.1.4.2(6)(a-i)** and will manage network configuration activities, including, but not limited to: adding a protocol; adding, moving or removing CPE; changing addressing, filtering, and traffic prioritization schemes; optimizing network routes; updating equipment software and/or configuration (i.e. firewall and virtual private network (VPN) security devices); upgrading or downgrading bandwidth; implementing and maintaining configuration changes and databases for all agency-specific devices; auditing government router configurations. All changes will be made in accordance based on the Verizon ITIL change management process, as agreed to with end user agencies on a particular TO.

IP Address Management. Verizon complies with **RFP Section C.2.8.1.1.4.2(7)** and will provide customer IP address management, as applicable, and will submit agency-

completed American Registry for Internet Numbers (ARIN) justification requests for specified IP allocations, assuming IP addresses are available.

Equipment Monitoring and Access Control. Verizon complies with **RFP Section C.2.8.1.1.4.2(8)** and will monitor and control access to equipment under its control, including limiting access to authorized personnel, implementing passwords and user permissions as directed and approved by the agency. Verizon implements a role based access controls (RBAC) throughout the MNS platform. Agencies will identify particular users who have access to specific reports, devices, and applications, and Verizon will include them in the MNS RBAC.

Off-Site Equipment Configuration Backups. Verizon complies with **RFP Section C.2.8.1.1.4.2(9)** and will regularly perform off-site equipment configuration backups, in order to confirm the availability of recent configuration data or restoration purposes. Verizon will provide the agency secure access to backup logs, as needed.

Hardware/Software Upgrades, Updates, Patch Deployments and Bug Fixes. Verizon complies with **RFP Section C.2.8.1.1.4.2(10)** and will perform necessary hardware and software upgrades, updates, patch deployments and bug fixes as soon as they become available, and will implement updates in coordination and mutual agreement with the agency; test new releases to resolve any security concerns, verify compatibility with the agency environment, minimize service disruptions, and maintain equipment functionality. All changes will be made in accordance based on the Verizon ITIL change management process, as agreed to with end user agencies on a particular TO.

Preventative and Corrective Maintenance. Verizon complies with **RFP Section C.2.8.1.1.4.2(11)** and will provide preventative and corrective maintenance for agency-specific devices under Verizon management. All changes will be made in accordance based on the Verizon ITIL change management process, as agreed to with end user agencies on a particular TO.

Proactive Problem Identification and Notification. Verizon complies with **RFP Section C.2.8.1.1.4.2(12)(a-q)**. The key to MNS solutions is the ability to streamline IT operations management across all agencies by providing proactive management tools that automatically respond to and mitigate potential incidents before they impact customers. Proactive management and control requires the deployment of tools that automate the management of network services and includes the inter-relationships among the numerous transport, circuit, network, IT, and security devices that make up a given service. There are three levels of Situational Awareness of managed IT elements, as described below:

- **Level 1 – Perception.** Perceiving the ongoing operations is the first step in achieving situational awareness
- **Level 2 – Comprehension.** MNS analyzes, correlates, and determines the root cause of events to understand the impact the event would have on IT services management on both a focused and global perspective
- **Level 3 – Projection.** MNS extrapolates the information and data from Situational Awareness Levels 1 and 2 to develop a more complete picture of the status of the IT enterprise elements and the potential impact of events on the managed elements

Verizon will proactively detect problems, open/close tickets, respond to alerts and promptly report situations that adversely affect throughput to the impacted agency; provide notification of alarms, network troubles and service interruptions via email, telephone, or as specified in the TO. Further, based on the requirements defined in a particular TO, Verizon will act as Tier 1/2/3 as required, and via an ebond with the agency management system send automated notifications, open/close tickets, and respond to call from agency NOC personnel for transport services.

Real / Near-Time Access to Installation Scheduling. Verizon complies with **RFP Section C.2.8.1.1.4.2(13)(a-d)** and will provide real or near real-time access to installation schedules detailing the progress of activities such as the implementation of equipment, access and transport circuits, and ports, as applicable to track the provisioning process through completion at any time. Verizon will also provide the

agency with real or near real-time access to network statistics and performance information including equipment data availability, throughput delay statistics, CoS settings, application level performance information, trouble reporting and ticket tracking tools, and security logs.

Inventory Tracking Tools. Verizon complies with **RFP Section C.2.8.1.1.4.2(14)** and will provide inventory tracking tools to maintain and track agency circuit, transport service and equipment inventory information.

Secure Access to Current and Historical Information. Verizon complies with **RFP Section C.2.8.1.1.4.2(15)(a-k)** and will provide the agency with secure access to current and historical information, including but not limited to: bandwidth and service quality information; burst analysis identifying under/over utilization instances; data errors; delay, reliability and data delivery summaries; end-to-end network views' exception analysis; link, port and device utilization; network statistics; protocol usage; CPU utilization; and traffic, port and protocol views, as applicable.

GFP and SRE Maintenance & Repair. Verizon complies with **RFP Section C.2.8.1.2(1)** and will maintain and repair GFP and SRE via Verizon's ITIL based change management process which requires a ticket to be opened and closed for each change.

Agency-Specific Help Desk Services. Verizon complies with **RFP Section C.2.8.1.2(2)** and will provide agency-specific help desk services and shared or dedicated NOCs and SOC's to meet agency requirements. Verizon will also offer direct unbonding services between ordering agency NOC/SOC and Verizon GNOSC based on individual TO requirements.

Agency-Specific Development Services. Verizon complies with **RFP Section C.2.8.1.2(3)** and will support agency-specific development services, which address the agency's potential need to test equipment, software and applications (i.e. IP VPN, voice and data services) on Verizon's network prior to purchase and deployment. Testing will

be performed at the agency's discretion and structured in collaboration with the contractor.

DHS EINSTEIN Enclaves. [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED] see **Section 3**
for additional information). [REDACTED]

[REDACTED]

[REDACTED]

Support UNIs for EIS Access. As defined and required on a TO, Verizon complies with **RFP Section C.2.8.1.2** and support underlying UNIs for EIS access and transport services implemented using Verizon MNS.

Stipulated Requirements. Verizon complies with the **Service Description (C.2.8.1.1)**, **Functional Definition (C.2.8.1.1.1)**, and all applicable **Standards (C.2.8.1.1.2)**, **Connectivity (C.2.8.1.1.3)**, **Interfaces (C.2.8.1.3)**, and **Performance Metrics (C.2.8.1.4)** RFP requirements.

2.8.1.2 Quality of Services [L.29.2.1, M.2.1]

Verizon designed its MNS architecture with high availability as a minimum baseline requirement and builds upon that. The architecture has no single point-of-failure. MNS is comprised of Primary and Recovery/Continuity of Operations (DR/COOP) systems located in secure data processing. Automatic failover between each system maintains high-availability enterprise management and situational awareness of GSA/agency systems. The automated switching between MNS systems and locations is controlled through the use of redundantly configured load balancing systems. Verizon's MNS currently uses industry-leading databases for the Primary, and DR/COOP systems. Data from each database is automatically replicated to the other database instance, keeping databases up-to-date. Personnel who provide service management functions possess security clearances at the highest level of the security enclave being

monitored. The MNS service desk and technical personnel will actively and collaboratively monitor and respond to MNS events, incidents, and problems. MNS has a hierarchy of functions and capabilities (see **Figure 2.8.1.2-1**) that can be implemented, as required, to meet agency-specific service management requirements.

Figure 2.8.1.2-1. Verizon MNS NetOps Functional Capabilities.

IP Management	System Management	Security Management	Enterprise Services
IP Network Management System	Hardware Systems Management	Network Access Control	Enterprise Services Management System
Firewall Element Management	Storage Systems Management	IP Network Vulnerability Scanner	Domain Name Service (DNS) Management
Router Element Manager	Backup and Recovery Management	Security Information Management System	IP Capacity, Availability, and Performance Monitoring
Switching System Element Manager	Virtualization Management	Identify and Access Management System	Database Monitoring and Management
Virtual Private Network (VPN) Management	Performance Management	Insider Threat Mitigation System	Directory Services Integration and Management
Parent-Child Dependency Mapping	Configuration Management	Continuous Monitoring	Application Management

The MNS management platform has several distinguishing components, one of which is the method in which it interfaces with managed devices. A connection is made directly to the console which allows the system to monitor messages sent to standard output and alert on them. Additionally, the system performs keystroke capture of any activities taken on a managed device (both GUI and CLI) and also blocks any human access that is attempted outside previously approved change or incident windows.

2.8.1.2.1 MNS Description

Verizon's MNS will be staffed on a continuous 24x7 basis by appropriate Verizon and third-party personnel (with applicable certifications and/or clearances, as necessary) who provide operations management of the systems, infrastructure, and applications supporting GSA and agency IT operations. Verizon designed its MNS using COTS applications with the ability to deliver enterprise IT network, technologies, and capabilities, such as centralized and automated configuration management and Information Security Continuous Monitoring (ISCM) on a global basis.

2.8.1.2.2 MNS Service Desk

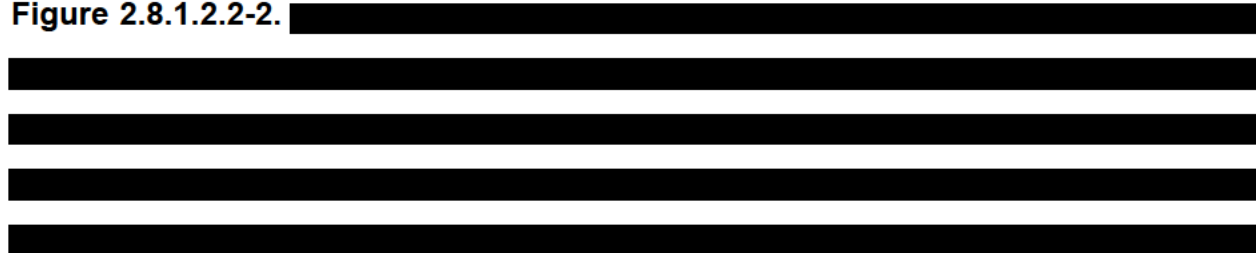
The MNS service desk is the focal point for operations management functions. Ordering agencies access the MNS service desk system using standard web browser technology (e.g., Microsoft Internet Explorer, Firefox, etc.) by accessing centralized portals certified to comply with the requirements of Section 508 of the Americans with Disabilities Act (ADA), or by using e-mail messages, chat session(s), or telephone. The MNS service desk provides various functions, as listed in **Table 2.8.1.2.2-1** below:

Table 2.8.1.2.2-1. Verizon MNS Service Desk Functions.

MNS Service Desk Functions
Distinct, yet fully integrated, IT Infrastructure Library (ITIL)-based incident and problem management processes
Single, purpose-built Configuration Management Database (CMDB)
Seamless integration with other service management solutions (change, asset, service level, service request, identity, and knowledge management)
Simplified interfaces for rapid incident and problem creation and closure
Built-in process flow taskbar and interactive process model based on ITIL 2011 processes

The MNS ticketing function is accessed using a standard web browser. The ticket view is defined by the function being requested (e.g., open incident, request change, etc.). MNS service desk screens can be modified to meet individual customer requirements (e.g., graphics, specific data fields, etc.). The service desk dashboard provides graphic-based data displays depicting Key Performance Indicators (KPI) on managed services, systems, applications, and infrastructure. The data associated with each graphic is available through a “point-and-click” function and provides analysis, advanced reporting, and situational awareness of GSA or agency applications and services.

MNS Manager of Managers (MOM). The MNS solution architecture adheres to the Manager-of-Managers (MOM) conceptual framework depicted on the next page in **Figure 2.8.1.2.2-2.**



[REDACTED]

[REDACTED]

The MNS MOM provides real-time, centralized monitoring of information technology. The MOM assimilates data from disparate applications and operations environments providing management, operations personnel, and customers with real-time, customizable views of faults, services, and KPI. Dashboards provide users with customizable views, offering an array of images, graphical maps, charts, tables, and event lists that can be tailored to individual technician and agency requirements.

[REDACTED]



The MNS portal provides access to a unified dashboard that provides users with application monitoring, individual user transactions, and technical metrics associated with the monitored system(s). Metrics are provided in real-time with the ability to analyze and trend monitored system performance levels and service level management

metrics. The portal can also provide alerting functions from the managed elements. The MOM correlates data sent by element manager applications that monitor managed elements and services (e.g., network infrastructure, virtual and physical servers and their associated/installed applications). The correlation function is enhanced by a Root Cause Analysis (RCA) that is accomplished automatically on events, incidents, and problems reported to the MOM. This meets the fundamental requirement for effective enterprise service management in that it provides a current and consistent baseline of information about the status of the global IT enterprise.

2.8.1.2.3 MNS Program Management Office (PMO)

Verizon's MNS PMO functions as a seamless, integrated unit with centralized control and is staffed by experienced technical, management, and business personnel who are skilled in the information technology services required for MNS. The PMO coordinates within Verizon to make resources available as part of a TO and provides agencies with information on milestones and status periodically and on an ad hoc basis. Clearly defined lines of authority within the Verizon corporate structure, between core team members, and to the end customer, support internal executive oversight and present a cohesive team that is ready to deliver quality work, on time, and on budget. The Program Manager leads the Verizon PMO and is supported and supplemented by solution-specific Verizon delivery organizations and back office support resources.

2.8.1.2.4 Migration and Transition Strategy

Verizon has directional transition plans that outline the overall conceptual steps Verizon will use to transition an existing enterprise management system from GSA or other contractors to the Verizon MNS. For individual TOs, Verizon will tailor its transition plan to accommodate the size and scope of the agency, network, or service to be transitioned. Verizon requires coordination and cooperation between Verizon, the customer agency, and any applicable third-party contractors. Knowledge transfer is essential, and Verizon will need access to any applicable systems data, architecture diagrams, and configuration data. In return, Verizon will provide the transition schedule and plan to GSA or customer agency within an agreed-upon timeframe prior to the

implementation of the plan, for review and approval.

2.8.1.3 Service Coverage [L.29.2.1, M.2.1]

Verizon complies with **RFP Section C.1.3** and will support MNS in a minimum of 25 of the top 100 CBSAs.

2.8.1.4 Security [L.29.2.1, M.2.1]

The Verizon MNS is managed for security and risk per Verizon's EIS IT Risk Management Framework (RMF) Plan in **Volume 1, Attachment A**. Appropriate security measures for the selected access solution will be implemented on a TO basis for Internet and related traffic that requires aggregation (reference **Section 3, External Traffic Routing**) to provide security and confirm the integrity of government data. If additional security measures are required they will be addressed at the TO level.

The MNS architecture was built to FISMA High standards. The management platform was configured at two geographically separate locations (see **Figure 2.8.1.4.1-1**) and can keep data associated with a given location and/or security enclave on separate storage devices in Federal Information Processing Standards (FIPS)-compliant encrypted format. Separate MNS portal systems providing access to the MNS catalog and other MNS functions are installed on each security enclave within the area of operations associated with a given location. The portals require the use of 2-factor Identity and Access Management (IdAM) credentials to provide bi-directional access to services and reports.

2.8.2 WEB CONFERENCING SERVICE (WCS) [C.2.8.2]

2.8.2.1 Understanding [L.29.2.1, M.2.1]

Verizon proposes its proven Web Conferencing Service (WCS) currently delivered on Networx, which supports collaboration on a global scale. Verizon's WCS enables users to share presentations with meeting participants while they listen on an accompanying conference call. Planned or ad hoc, simple presentations, embedded videos, or complex design drawings, ordering agencies can collaborate on a robust and secure platform without the need for anyone to travel.

[REDACTED] The Verizon Conferencing interface for Net Conference provides a consistent experience for leaders and participants as they join their net conference. Ordering agencies can also select a more customized experience [REDACTED] and can benefit from Verizon invoice integration.

[REDACTED]
[REDACTED]
[REDACTED]. All of this

collaboration data flows through Verizon's secure, high performance network with the lowest delay possible.



Once the connection is made, the [REDACTED] Network manages the synchronous real-time interaction that makes up an online meeting. Verizon WCS is designed to be compatible and integrate with its other conferencing services and Unified Communications platforms.

2.8.2.1.1 Compliance with EIS Service Requirements [J.19]

Capability to Collaborate. Verizon complies with **RFP Section C.2.8.2.1.4(1)**. With Verizon WCS tools, WebEx leaders can conduct real time document sharing, transfer files, and use a collaborative whiteboard in a private and secure.

Authentication and Password. Verizon complies with **RFP Section C.2.8.2.1.4 (2) (a)**. Login names and passwords are created by the individual presenters that utilize Verizon WCS to deliver a presentation to an audience. Passwords must meet the complexity requirements. Login Names must be eight characters or longer, but no more than 40 characters. Passwords must contain an uppercase letter and/or a number and cannot be the same as the previous password. Once valid Login Names and Passwords

are created presenters will authenticate via Manage My Meetings, where Instant Net and Customized Net accounts are created and managed.

Customized Greeting or Message Screen. Verizon complies with **RFP Section C.2.8.2.1.4 (2) (b)**. In Customized Net Conference powered by WebEx, an ordering agency has the option to customize welcome text.

Online Help. Verizon complies with **RFP Section C.2.8.2.1.4 (2) (c)**. Online material and documents compliment a live help desk, available 24x7x365. Online help materials are available for WebEx, and other Verizon Web Conferencing tools. These documents were developed by Verizon and its WCS partners and are available to assist participants and attendees on how to use available features within the WCS application. Online help is available in many varieties such as HTML format, PDF format, recorded sessions, live training sessions, technical support, etc.

Point-to-Point and Multi-Point Web Conference. Verizon complies with **RFP Section C.2.8.2.1.4 (2) (d)**. Verizon WCS supports meetings between two people, and can be used to communicate with thousands of participants. Ordering agencies have global access to Verizon WCS. Verizon WCS support personnel can support users sitting on the same network and users on multiple networks coming from different locations around the world. Customized Net, through WebEx, also provides multi-point Web conferences.

Interoperate with Internet and IP Networks. Verizon complies with **RFP Section C.2.8.2.1.4 (3)**. Verizon Net Conferencing is easily accessible via any Internet connection and can access ordering agency IP networks.

Browser Software Compatibility. Verizon complies with **RFP Section C.2.8.2.1.4 (4)**. Verizon supports all major browsers and will work with ordering agencies to ensure compatibility.

Test Compatibility. Verizon complies with **RFP Section C.2.8.2.1.4 (5)**. Verizon WCS is fully compliant with this requirement. Verizon will provide web-based tools for

users to test and verify that their desktop software is compatible with WCS service prior to the scheduled conference. In order to test their browsers and desktop software, users will go to the Net Conferencing web site, select “Download Net Conferencing Plug-ins,” then select “Check your Browser.” All necessary plug-ins will be automatically downloaded. If required, Verizon will provide the user with plug-ins to deliver WCS service. The browser “plug in” software will be limited to utilities required for the user to playback, participate in, or lead a web conference session. Verizon understands that this can include “plug ins” that enable ordering agency users to playback recorded conferences from their web browser, develop WCS presentation slides within existing ordering agency owned software applications (i.e., Microsoft PowerPoint) or view WCS from mobile devices such as a Personal Digital Assistant (PDA) where applicable.

Dynamic Content. Verizon complies with **RFP Section C.2.8.2.1.4 (6)**. The WebEx web conferencing service supports dynamic content, with the ability to use AVI, flash, .gif, and HTML files.

Available on Demand. Verizon complies with **RFP Section C.2.8.2.1.4 (7)**. Verizon Instant Net Conference provides leaders with a consistent and persistent meeting ID and password to use at any time. Instant and Customized Net conferences are available to presenters on demand once they have been created. Instant Net services are persistent meetings that are created by presenters with conference details that never change, unless changed by the leader. Leaders access and manage their Instant Net conferences via Manage My Meetings. Customized Net conferences are scheduled or started instantly by presenters through the personalized ordering agency web site. The newest CMR – Collaboration Meeting Room allows for this also.

Reservation System. Verizon complies with **RFP Section C.2.8.2.1.4 (8)**. Verizon's WCS provides leaders the ability to schedule meetings as a single event or as a recurring meeting up to a year in advance through Verizon Reserved Net Conference service. Leaders may schedule Reserved Net Conferences by calling reservationists or using Verizon's easy-to-use online scheduling tool. There is no need to schedule

meetings with Instant Net Conference. Once the subscription is created, leaders may conduct a meeting at any time. Reserved Net Conference allows leaders to select to have a meeting recur on a daily, weekly or monthly basis. Instant Net Conferences do not require reservations, but the meeting information may be given out to future participants at any time. For example, a leader may tell a group to meet every week at this time using this Meeting ID and password.

Email Notification. Verizon complies with **RFP Section C.2.8.2.1.4 (9)**. Verizon WCS offers various methods of providing email notification, meeting invitations and RSVP capabilities to leaders depending on their needs and their chosen platform. Customized Net Conference integrates with both Outlook and Lotus Notes. Instant Net provides a simple interface to send out invitations.

Extend Scheduled Conference Time. Verizon complies with **RFP Section C.2.8.2.1.4 (10)**. Leaders can extend the start time and duration of reserved meetings. Additional participants may be added as well. Instant Net Conference is available for as long as the leader needs it and can hold up to 100 participants without warning.

Authentication and Encryption. Verizon complies with **RFP Section C.2.8.2.1.4 (11)**. Participants and leaders must provide passwords before joining. Leaders may lock the Net Conference so additional participants can't join. Leaders may view any participant and request identification and eject them from the meeting. SSL encryption is available on all web conferences.

URL with Login and Password. Verizon complies with **RFP Section C.2.8.2.1.4 (12)**. URLs are provided in confirmation and invitation emails, sent by conference leaders who use Verizon's reservation system to notify participants.

Passwords. Verizon complies with **RFP Section C.2.8.2.1.4 (13)**. Participants and leaders must provide passwords before joining.

Simultaneous Participants. Verizon complies with **RFP Section C.2.8.2.1.4 (14)**. Reserved conferences can support up to 1,500 simultaneous participants with

application sharing, 2,500 without application sharing. Instant conferences can support up to 100 simultaneous participants. Customized Net Conferencing can accommodate 1,000 with sharing, 3,000 without sharing, and 200 simultaneous. Verizon does not have a limit on the number of simultaneous web conferences that can be conducted at one time.

Firewalls and Security Layers. Verizon complies with **RFP Section C.2.8.2.1.4 (15)**. Verizon WCS is firewall friendly and interoperable, and Verizon technical support will work with companies to ensure that there are no issues. Verizon WCS will work with Networx agencies to test and verify that there are no issues with compatibility or firewalls.

Operator Assistance. Verizon complies with **RFP Section C.2.8.2.1.4 (16)** and will provide the option for operators to stand by during the meeting, able to answer questions for leaders and participants on Reserved Net conferences.

Annotation. Verizon complies with **RFP Section C.2.8.2.1.4 (17)**. All of the Verizon Web conference solutions allow for a variety of pointers and annotation. By simply checking a box, the leader may select to allow participants to annotate on the presentation. The WebEx platform distinguishes which participant or leader adds the annotation to add clarity in workgroup situations.

Participant List. Verizon complies with **RFP Section C.2.8.2.1.4 (18)**. During a meeting, leaders see the status of the participants. Leaders may also view and download participant lists immediately after their meeting.

Group Web Surfing. Verizon complies with **RFP Section C.2.8.2.1.4 (19)**. Leaders can easily show Web sites to participants during the meeting. Participants can watch the leader use web based applications to learn how to use them. With WebEx, leaders and participants may annotate on the page to discuss web design projects.

File Transfer. Verizon complies with **RFP Section C.2.8.2.1.4 (20)**. Verizon WCS solutions powered by WebEx can provide file transfer. Leaders can specify which

participants receive the file, and participants have the option to save the file or reject the transfer. Specialists are available to assist participants in troubleshooting, joining, conducting formal Q&A sessions and collaborating on documents in real time.

Multiple Presenters. Verizon complies with **RFP Section C.2.8.2.1.4 (21)**. Verizon WCS is designed for multiple presenters. Specialists are available to assist leaders and participants in troubleshooting, joining, or conducting formal Q&A with multiple presenters.

Video Webcasts. Verizon complies with **RFP Section C.2.8.2.1.4 (22)**. Verizon WCS will support video webcasts to over 3,500 participants, as needed.

Polling and Voting. Verizon complies with **RFP Section C.2.8.2.1.4 (23)**. Verizon WCS provides polling and various feedback methods. Verizon supports the WebEx Center packages that allow leaders flexibility to create multiple choice, open ended and yes/no questions. All WCS platforms provide a means for participants to signal leaders when they have a question.

Feedback. Verizon complies with **RFP Section C.2.8.2.1.4 (24)**. Verizon WCS, powered by WebEx allows for leaders to create polls during the meeting. Leaders may immediately see the results and decide if they would like to share the results with the participants.

Meeting Lobby. Verizon complies with **RFP Section C.2.8.2.1.4 (25)**. Verizon Net Conferencing allows leaders to lock and unlock the meeting. Leaders control who can join the active conference.

Printing. Verizon complies with **RFP Section C.2.8.2.1.4 (26)**. With WebEx, both leaders and participants can transfer files and print if the leader enables the feature.

Text Chat. Verizon complies with **RFP Section C.2.8.2.1.4 (27)**. Verizon Net Conferencing supports text chat in all solutions. Leaders easily enable this feature in either platform. A participant selects another participant or a leader and types in the

chat window. When a leader enables chat, When enabled, WebEx chat allows participants to send private or public chats to other participants or to the leader. Participants may use this tool to send a question to all the presenters.

Survey. Verizon complies with **RFP Section C.2.8.2.1.4 (28)**. With WebEx, leaders can post a survey on a Web site and then guide the class to the survey through the Web Slide tool, which is powered by WebEx Training Center and allows leaders to direct participants to tests or surveys posted on the WCS site.

Streaming Audio. Verizon complies with **RFP Section C.2.8.2.2 (1)**. Verizon's streaming audio service allows for broadcast feature, the audio may be streamed along with slides or alone. Verizon WCS also offers Net Replay, where the session is recorded and participants may view the presentation and hear the audio over the Internet.

Streaming Video. Verizon complies with **RFP Section C.2.8.2.2 (2)**. WebEx enables a live streamed view, via Web cam, of the leader synchronized with data sharing during the presentation (slideshow, application sharing, etc.). WebEx also allows for multi-point video within a session.

Web Based Presentation Replay. Verizon complies with **RFP Section C.2.8.2.2 (3)**. Verizon provides a full service hosted replay with the capability to replay (or playback) Web based presentations for participants that were unable to attend the live conference. The replay shall be available for a minimum of 30 days after the initial conference. Verizon will provide the ordering agency an option for extending the conference replay, in 30 day increments, for a period of 1 year. Net Replay is available, where participants may view the presentation and hear the audio over the Internet. Leaders can define how long files are available to a defined group. FTP enables leaders to download the recording and post to their own site. Customized Net via WebEx provides a way for leaders to record the Web conference and save to the desktop or another site or via their customized URL.

Interfaces. Not applicable. WCS is a browser-based service.

Stipulated Requirements. Verizon complies with the **Service Description (C.2.8.2.1)**, **Functional Definition (C.2.8.2.1.1)**, and applicable **Standards (C.2.8.2.1.2)**, **Connectivity (C.2.8.2.1.3)**, and **Performance Metrics (C.2.8.2.4)** RFP requirements.

2.8.2.2 Quality of Services [L.29.2.1, M.2.1]

As depicted in **Figure 2.8.2.1-1**, the Verizon WCS will provide EIS customers with a web conferencing service that enables global collaboration. Verizon WCS offers an extensive list of features presented in the previous section. Ordering agencies can select a combination of features based on the platform selected and the requirements of the individual net conference.

2.8.2.3 Service Coverage [L.29.2.1, M.2.1]

Verizon complies with **RFP Section C.1.3** and will support WCS in a minimum of 25 of the top 100 CBSAs.

2.8.2.4 Security [L.29.2.1, M.2.1]

Verizon has developed effective Web based solutions that can support the ordering agency's business needs along with the level of security necessary to work in confidence. Verizon E-Meetings and MyMeetings websites have the following controls in place:

- HTTPS with 128-bit encryption is used for all ordering agency account management via the E-Meetings and MyMeetings portals.
- Verizon Conferencing representatives have the ability to grant and disable access to online tools

The Verizon WCS is managed for security and risk per Verizon's EIS IT Risk Management Framework (RMF) Plan in **Volume 1, Attachment A**. If additional security measures are required they will be addressed at the TO level.

2.8.3 UNIFIED COMMUNICATION SERVICE (UCS) [C.2.8.3]

2.8.3.1 Understanding [L.29.2.1, M.2.1]

Verizon's Unified Communications Service (UCS) is a hosted and managed service based on industry standard collaboration tools. In response to GSA's requirements, Verizon is implementing a fault-tolerant, Geo-Diverse instance of the UCS platform, dedicated to federal agencies. As designed, the platform will meet all required functional, operational and security requirements. Verizon's Hosted UCS delivers business-grade communications and collaboration services, offering the flexibility of a premises-based solution with the simplicity of a hosted solution. UCS provides support for a wide variety of end user devices, such as: call control (audio/video); integrated/unified voicemail; presence and Instant Messaging; secure, VPN-less end user access to enterprise mobility, providing improved ease of use; and audio, web and video conferencing.

UCS integrates with existing Verizon services, such as Verizon's VPNS (MPLS Network), SIP Trunking, ACS, WCS, and VTS. The flexibility built into the UCS platform permits extensibility into future services. UCS integrates communications services into Enterprise Resource Planning (ERP) and Customer Relationship Management (CRM) resources, such as SAP, Oracle, Salesforce, and Jive as an option. Ordering agencies using these applications then have the ability to click-to-call, view presence statuses and instant messages, or launch web conferences directly from the applications. This creates seamless communications directly within the application, which increases business agility. Verizon's approach to deploying, managing, and upgrading collaboration applications and services is based on the ability of an ordering agency to have predictable business outcomes.

2.8.3.1.1 UCS Architecture



2.8.3.2 Compliance with EIS Service Requirements [J.19]

UCS Capabilities. Verizon complies with **RFP Section C.2.8.3.1.4(1)** and will provide support to enable UC capabilities via many devices.

Unified Messaging. Verizon complies with **RFP Section C.2.8.3.1.4(2)(a-d)**. UCS Unified Messaging (UM) will provide user access to and management of voice mail, e-mail and fax messages through the same inbox or interface, modular messaging with access to messages from phones and PCs via various interfaces, including browsers, the UC Messaging Directory, which will logically represent a telephony hardware device and a telephony dial plan for the enterprise to support a specific UM feature, and the integration of UM with existing telephony infrastructure.

Mobile Integration. Verizon complies with **RFP Section C.2.8.3.1.4(3)(a-f)**. Mobile Integration will provide users with a single identity, which (i) allows them to handle business calls from their desks and mobile phones; (ii) provides the ability to have calls forwarded to any phone and to use a single number for making and receiving calls; and

(iii) hands off calls from cellular to Wi-Fi connections and vice versa on smart phones. Mobile Integration also enables users to initiate phone calls, retrieve voice mail and corporate directories, access instant messaging and participate in video conferencing. In addition, Mobile Integration provides features that are accessible from mobile phones, laptops and tablets, provides access to corporate directories and visual voice mail, features seamless handoff between cellular and Wi-Fi calls, and allows calls to or from mobile devices to take place anywhere and anytime as if they are going to / coming from the desk phone numbers.

Unified User Interface. Verizon complies with **RFP Section C.2.8.3.1.4(4)(a-r)**. UCS includes a Unified User Interface that provides the following:

- a) The ability for users to access UC capabilities from a variety of devices in a variety of ways
- b) Features like presence, instant messaging, integrated soft phones, voice conferencing, video calling and conferencing
- c) Voice activation that integrates seamlessly with other business communication systems
- d) Real-time communications, like instant messaging, presence that identifies which participant is speaking within a conference call, voice-to-video and –email
- e) Non-real-time communications (e.g., email, text, messaging, fax, and voice mail)
- f) Collaboration and data sharing (e.g., electronic bulletin boards, e-Calendar, Audio/Video/Web conferencing)
- g) The ability for users to access messages from: IP and mobile smart phones, web browsers, e-mail and desktop clients, PCs, and supported tablets.
- h) Instant Messaging (IM) between two or multiparty users
 - i) The ability to display presence status
 - j) Presence integration with ordering agency collaboration applications (e.g., automatic presence updates due to calendar collaboration)
- k) Web cameras, speakers and microphones
- l) File transfer capabilities

- m) Scheduled and ad-hoc web conferencing capabilities with audio, video, screen sharing, virtual white boarding, PC-to-PC and multiparty data sharing including desktop, application, presentation, virtual whiteboard, annotation sharing and the ability to poll participants.
- n) Contact groups
- o) Enhanced secure access to instant messaging from within the ordering agency's enterprise network, Internet or through a variety of devices and software (optional)
- p) Agency-managed IM administration
- q) Single sign-in capabilities
- r) Automated and/or staffed UCS-dedicated 24x7 service desk

Quality of Service. Verizon complies with **RFP Section C.2.8.3.1.4(5)(a-c)** and will provide the following capabilities to support the QoS, if UCS is provided over Verizon's IP network: configuration options for QoS, traffic prioritization, QoS queuing methods and scheduling.

Premises-Based WAN Optimizer. Verizon complies with **RFP Section C.2.8.3.1.4(6)**. The UCS will provide a premises-based WAN optimizer to collect only the changes from each site, if the compilation of the current status of all users being logged on is transmitted over the ordering agency WAN.

IPv4 and IPv6 Compliance. Verizon complies with **RFP Section C.2.8.3.1.4(7)**. The UCS will support both IPv4 and IPv6 and will be able to communicate over IPv4-only, IPv6-only and/or dual stack networks.

Voice Quality Level. Verizon complies with **RFP Section C.2.8.3.1.4(8)** and recognizes that Mean Opinion Score (MOS) scores are affected by many characteristics of a VoIP deployment, most notably Jitter, Packet Loss and Delay. In order to maximize voice quality, Verizon has a prescribed set of processes that are followed with every deployment of new customer endpoints. These include site assessment services designed so the customer network will be able to support the various applications that will be deployed, and the use of a fault tolerant design for the platform and its own

network fabric. For ordering agencies using Verizon's access network between the customer site and the Hosted UCS platform, Verizon offers a variety of options designed to verify real time traffic is properly configured and prioritized to help provide the highest possible level of performance. For Verizon's various hosted VoIP offerings 4.0 MOS score is supported as the standard SLA benchmark.

Stipulated Requirements. Verizon complies with the **Service Description (C.2.8.3.1)**, **Functional Definition (C.2.8.3.1.1)**, and all applicable **Standards (C.2.8.3.1.2)**, **Connectivity (C.2.8.3.1.3)**, **Interfaces (C.2.8.3.3)**, and **Performance Metrics (C.2.8.3.4)** RFP requirements.

2.8.3.2 Quality of Services [L.29.2.1, M.2.1]

Verizon uses a structured approach for the delivery of UCS called the Unified Communications & Collaboration Delivery Framework. The UCS Delivery Framework includes the activities needed to Prepare, Plan, Design, and Implement UCS services. The UCS Delivery Framework, refined over years of deployment, is described in **Table 2.8.3.2.-1** below.

Table 2.8.3.2-1. UCS Delivery Framework

Prepare	The Prepare phase is focused in large part on creation of the business case, This output requires an understanding of the customer's larger vision, any mission requirements, the financial investment, and the technologies involved. From these inputs, the business case is built and a technology strategy is developed along with the high-level architecture to meet those needs with the scope of work.
Plan	In the Plan phase, the Verizon UC Delivery Framework approach helps to assess the existing environment to determine whether it can support the proposed solution. This is done via a series of interviews that includes Account team, Implementation team, and Customer.
Design	In the Design phase, the Verizon UC Delivery Framework approach helps to develop a comprehensive detailed design via a series of workshops with customer and implementation team.
Implement	In the Implement phase, the Verizon UC Delivery Framework approach uses repeatable, yet customizable processes for implementation that were developed and agreed upon in the planning and design phases.

2.8.3.2.1 Complementary Service Offerings

The UCS service is dependent on other required and optional EIS services, as described below:

VPNS. The underlying fabric is provided as a separate service. UCS is supported over Verizon's VPNS and can also be supported with customer provided third party network connectivity. For mission critical sites demanding the highest level of reliability possible,

Verizon recommends dual access connections and routed connectivity to both instances of Verizon's UCS platform.

SIP Trunking. SIP trunking can be used to provide PSTN access and is available as a separate service under the contract.

Local PSTN Access. As an alternative, ordering agencies may utilize premise-based gateways with direct analog/ISDN connectivity to the local voice service provider of their choosing. This option is usually employed to improve survivability in the event the site is isolated from the host UCS platform.

Other EIS Products and Services. Verizon also offers the following services which complement the UCS service: IP phones, VPNS, Managed LAN/WAN, Managed IP PBX, Site Services, implementation services, and professional services. Further, Verizon UCS is designed to integrate with its conferencing services, including WCS (**Section 2.8.2**), ACS (**Section 2.8.7**), and VTS (**Section 2.8.8**).

2.8.3.3 Service Coverage [L.29.2.1, M.2.1]

Verizon complies with **RFP Section C.1.3** and will support UCS in a minimum of 25 of the top 100 CBSAs.

2.8.3.4 Security [L.29.2.1, M.2.1]

The Verizon UCS is managed for security and risk per Verizon's EIS IT Risk Management Framework (RMF) Plan in **Volume 1, Attachment A**. If additional security measures are required they will be addressed at the TO level.

Security Practices and Safeguards. Verizon complies with **RFP Section C.2.8.3.1.4(9)** and will implement security practices and safeguards that minimize susceptibility to security issues and prevent unauthorized access. Verizon will also comply with agency specific security policies, regulations and procedures.

In order to support the unique security requirements of the federal government, Verizon's UCS is based on a geographically diverse instance dedicated to government users. This instance (platform/application) is certified at the FISMA moderate level based on FIPS Publication 199 and Special Publication 800-60 Rev. 1

The main difference, with respect to federal requirements, is that the hardware used is based on the particular manufacturer's 'G' sku list. The 'G' sku list is a list of federally tested and compliant technologies made in the USA. Further, these solutions are hosted in facilities that meet the government's need for physical security and reliability and are physically isolated from other commercial offerings. Verizon's federal hosting solutions begin with the most basic things, such as a physically secure site and federal-only infrastructure.

Security is implemented at each layer of the architecture including Virtual Route Forwarding VPN's, customer specific VLAN's and Firewall Access Control Lists. Customer specific security requirements are normally addressed during the planning and design phase when developing a customer's UCS implementation.

2.8.4 MANAGED TRUSTED INTERNET PROTOCOL SERVICE (MTIPS) [C.2.8.4]

2.8.4.1 Understanding [L.29.2.1, M.2.1]

Verizon designed and implemented its MTIPS solution to safeguard federal information systems. This solution leverages strengths that are a result of Verizon's status as the largest global provider of Internet services, the largest provider of telecommunications services to the U.S. Government, and the provider of industry-defining managed service offerings for the past 15 years. As an existing MTIPS provider under Networx, Verizon is positioned to help GSA offer a comprehensive and ever-growing suite of MTIPS services to agencies.

The MTIPS program's overarching objective is to physically and logically connect federal agencies to the public Internet and/or other external networks, as required by the ordering agency, in full compliance with the Office of Management and Budget's (OMB) Trusted Internet Connections (TIC) initiative (M-08-05) announced in December 2007. Verizon MTIPS is compliant with the OMB TIC 2.0 mandate and with GSA MTIPS requirements.

Verizon complies with the annual DHS Cybersecurity Compliance Validation (CCV) process and will continue to participate in this program for its EIS MTIPS offering. MTIPS systems and TIC portal components support IPv4 and IPv6 protocols in

accordance with OMB Memorandum M-05-22 and the “IPv6 Transition Guidance” issued by the Federal CIO Council, Architecture and Infrastructure Committee.

Verizon has built two physically independent and diverse TIC domestic portals that provide complete redundancy to the Verizon Internet Exchange Points. The Verizon TICs are diversified from each other by east and west coast location builds.

The Verizon facilities that host the shared MTIPS components and the associated Security Operations Center (SOC) systems are certified to the FISMA High level by an independent third party. Verizon uses its purpose-built U.S. Government client-only Government Network Operations Security Center (GNOSC) with service-specific dedicated resources to provide the required security functions in support of the MTIPS offering. [REDACTED]

[REDACTED]

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

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

The TIC Portal monitoring and management systems at the Verizon GNOSC are dedicated to the management and monitoring of U.S. government agencies and are isolated from commercial agencies. The GNOSC serves as the primary system to monitor and support ordering agency infrastructures.

Verizon MTIPS will continue to provide ordering agencies with a secure, managed solution that is fully redundant, scalable, policy-compliant, and reliable. Verizon MTIPS currently meets Networx MTIPS core requirements for Firewall, Intrusion Detection and Prevention System (IDPS), Anti-Virus (AV), and E-Mail Scanning, along with the TIC 2.0 critical requirements as stipulated in the TIC 2.0 Reference Architecture document. The solution also supports the GSA data loss/leak prevention requirement.

Verizon’s MTIPS transport or backhaul is separate from the Public Internet and dedicated exclusively to the Multiprotocol Label Switching (MPLS) platform. Within the

MPLS platform, each MTIPS client is provided with its own private and dedicated VRF instance to ensure the privacy and security of its enterprise traffic within the Verizon MPLS platform to create the agency-trusted DMZ. Verizon uses IPSec tunnels to further encrypt the traffic. Verizon will provide a scalable design and support multiple VRFs per ordering agency, if required.

The aggregated client traffic from the MPLS transport terminates in a large client-shared, service-dedicated router at the edge of the MTIPS portal(s). This shared device provides the connectivity path to the MTIPS facility switch, which in turn passes each individual agency's encrypted VPN traffic to an agency-dedicated Security Sensor Stack hosted and operated by Verizon within the MTIPS Portal. The Security Sensor Stack device provides the virtualization necessary to support the multiple agency specific security policies of each ordering agency.





[Redacted text line]

[Redacted text line]

[Redacted text line]

[Redacted Table Header]	
[Redacted]	[Redacted]
[Redacted]	[Redacted]
[Redacted]	[Redacted]
[Redacted]	[Redacted]
[Redacted]	[Redacted]
[Redacted]	[Redacted]
[Redacted]	[Redacted]
[Redacted]	[Redacted]
[Redacted]	[Redacted]

To accommodate growth and advances in technology, Verizon has invested billions of dollars in its network and cybersecurity infrastructure and continues to invest for the future. The integrity and availability of our infrastructure resources is Verizon's primary concern. To this end, Verizon is continually improving and enhancing its security service offerings to meet the ever-evolving global threat landscape and to maintain compliance

with government initiatives such as EINSTEIN 3, continuous monitoring, and critical infrastructure protection.

In addition to these critical initiatives, Verizon is implementing a new and improved Managed Security Service (MSS) Analytics platform, a state-of-the-art Cyber Security Operations Center (CSOC), and continuous monitoring.

MSS Analytics builds on Verizon's existing Security Event Management (SEM) solution to provide a state-of-the-art security platform that will meet/exceed the needs of ordering agencies now and in the future. The solution provides expanded visibility across network and systems.

2.8.4.1.1 Compliance with EIS Service Requirements [J.19]

Annual CCV Assessment. Verizon complies with **RFP Section C.2.8.4.1**. Verizon is presently in compliance with the annual Cybersecurity Compliance Validation (CCV) process and will continue to participate in this annual DHS program for its EIS MTIPS offering.

Collection Network. Verizon complies with **RFP Section C.2.8.4.1**. The Verizon MTIPS provided transport will serve as a collection network for TIC physical or virtual portal connectivity to insulate the ordering agency's internal network from the Internet and other external networks.

TIC Portals. Verizon complies with **RFP Section C.2.8.4.1**. Verizon has built two (2) TIC Domestic Portals that are physically independent and diverse, providing complete redundancy to the Verizon Internet Exchange Points. The Verizon TICs are diversified from each other by east and west coast location builds. Management staff is provided at each TIC portal facility.

Virtual TIC Capabilities. Verizon complies with **RFP Section C.2.8.4.1** and will provide virtual TIC capabilities upon request for agencies with resources hosted outside their physical boundaries.

Dedicated Monitoring and Management Systems. Verizon complies with **RFP Section C.2.8.4.1.1**. Verizon TIC Portal SOC monitoring and management systems will be dedicated to the management and monitoring of federal government agencies and isolated from commercial agencies.

Access to External Networks. Verizon complies with **RFP Section C.2.8.4.1.4.1(1)(a-e)**. Verizon MTIPS will support all external network access requirements referenced in the RFP. As a Tier 1 ISP, Verizon ensures that its MTIPS portals are connected to the Internet via a Tier 1 Internet infrastructure and peer directly with other Tier 1 ISPs via multiple peering points. This translates to unparalleled policy, management, and technical level controls over service-impacting factors such as latency, capacity, security, and flexibility.

EINSTEIN Protection. Verizon complies with **RFP Section C.2.8.4.1.4.1(2)**. The Verizon MTIPS portals currently support routing traffic to meet the conditions of “external traffic” as defined in TIC 2.0 through an EINSTEIN enclave.

TIC Portal SOC. Verizon complies with **RFP Section C.2.8.4.1.4.1(3)**. The Verizon TIC portal SOC currently supports TIC portal authorities and analysts by identifying security events of interest that may be negatively affecting the TIC portal environment and by providing reports customized to ordering agency requirements. The Verizon GNOSC is an active participant in the Rapid Response Loop and supports TIC 2.0 and Continuous Diagnostics and Mitigation (CDM) dashboard requirements specifications.

ICD 705 SCIF. Verizon complies with **RFP Section C.2.8.4.1.4.1(4)**. Verizon currently provides Sensitive Compartmented Information Facilities (SCIFs) for the exchange of highly secure and sensitive information that may be required to perform threat identification and mitigation activities within the MTIPS platform.

Content Filtering/Inspection. Verizon complies with **RFP Section C.2.8.4.1.4.1 (5)**. The MTIPS platform is capable of supporting content filtering/inspection of

encrypted traffic with documented procedures. The Encrypted Traffic Analysis feature is an Individual Case Basis (ICB) item.

Asymmetric Routing. Verizon complies with **RFP Section C.2.8.4.1.4.1(6)**. The Verizon MTIPS platform is capable of supporting asymmetric routing, correctly processing traffic returning through asymmetric routes to a different MTIPS stateful inspection device; or documenting how return traffic is always forced to return to the originating MTIPS portal stateful inspection device.

FedVRS Support. Verizon complies with **RFP Section C.2.8.4.1.4.1(7)**. The Verizon MTIPS platform is capable of supporting Federal Video Relay Service (FedVRS) at the MTIPS security stack, which incorporates the Transmission Control Protocol (TCP) and User Datagram Protocol (UDP) ports required for FedVRS.

E-Mail Forgery Protection. Verizon complies with **RFP Section C.2.8.4.1.4.1(8)**. The Verizon MTIPS platform is capable of supporting e-mail forgery protection.

E-Signing Procedures for Outgoing E-Mail. Verizon complies with **RFP Section C.2.8.4.1.4.1(9)**. The Verizon MTIPS platform is capable of supporting anti-spoofing standards, such as Domain Keys Identified Mail.

DNS and DNSSEC. Verizon complies with **RFP Section C.2.8.4.1.4.1(10)**. Verizon MTIPS supports DNS and DNSSEC. Verizon maintains physically and logically separate Domain Name Servers (DNSs) with regard to authoritative servers, resolvers only, and DNS Security Extension (DNSSEC).

Uninterrupted Operations. Verizon complies with **RFP Section C.2.8.4.1.4.1(11)**. The Verizon facilities that support the MTIPS program have in-place backup batteries, Uninterruptable Power Supplies (UPS), and generator capabilities for at least 24 hours of uninterrupted operations without the need for refueling. Verizon's electrical systems meet or exceed the building, operating, and maintenance standards as specified by the GSA Public Buildings Service Standards, PBS-100.

IPv6. Verizon complies with **RFP Section C.2.8.4.1.4.1(12)**. MTIPS systems and components of the TIC portals support both IPv4 and IPv6 protocols in accordance with OMB Memorandum M-05-22, and the “IPv6 Transition Guidance” issued by the Federal CIO Council, Architecture and Infrastructure Committee.”

Data Loss/Leak Prevention. Verizon complies with **RFP Section C.2.8.4.1.4.1(13)**. The MTIPS platform supports data loss/leak prevention. Verizon’s MTIPS solution will provide prefabricated rules and content to enable the ordering agency to detect and block potential data leaks quickly and accurately while achieving industry and regulatory compliance.

Internet Bound Traffic. Verizon complies with **RFP Section C.2.8.4.1.4.2(1)**. Verizon is a leading Tier 1 ISP and has one of the most-connected Internet backbone networks in the world. Verizon plays a critical role in the movement of Internet traffic, and expansive IP footprint, advanced security capabilities, and GNOSC facilities provide a high assurance of the ability to successfully implement the MTIPS solution for an ordering agency. Internet bound traffic is routed and secured through one of the two MTIPS portals as mandated by the TIC requirements.

Agency Trusted DMZ. Verizon complies with **RFP Section C.2.8.4.1.4.2(2)**. The Verizon MTIPS platform supports agency level DMZ to ensure agency traffic is protected and physically isolated when transported to the portal and the public Internet. Verizon DMZ components include access loops to the MTIPS transport network, associated Service Related Equipment (SRE), and Verizon Network-Based IP VPN (NB-IPVPN) transport.

Inter-Agency Routing and Inspection. Verizon complies with **RFP Section C.2.8.4.1.4.2(3)**. Inter-agency traffic is routed through and inspected by the Verizon MTIPS Portal if the connection is classified as an external connection.

Encrypted Traffic. Verizon complies with **RFP Section C.2.8.4.2(1)**. The Verizon MTIPS portals are capable of supporting the monitoring, scanning, and filtering of both

inbound and outbound encrypted traffic traversing through the portals. This feature is an Individual Case Basis (ICB) item.

Agency Security Policy Enforcement. Verizon complies with **RFP Section C.2.8.4.2(2)**. Verizon supports the development and management of custom/complex security policies, security regulatory compliance, operational models, and security strategy reviews. The agency specific security policy enforcement is an ICB item.

Forensic Analysis. Verizon complies with **RFP Section C.2.8.4.2(3)**. The MTIPS portals support full, real-time, header and payload, raw packet capture of selected agency's traffic flows and offer subsequent forensic traffic analysis of cyber incidents as a service, as may be required by the agency (administrative, legal, audit, or other operational purposes).

Custom Reports. Verizon complies with **RFP Section C.2.8.4.2(4)**. Verizon offers custom reporting services, including ad hoc reporting by ordering agency, as an ICB service item.

Agency NOC/SOC Console. Verizon complies with **RFP Section C.2.8.4.2(5)**. Verizon provides a customized NOC/SOC console beyond the basic features and functions. This service offers highly customizable features, such as custom/complex security policies, security regulatory compliance, operational models, and security strategy reviews. Customization is an ICB item.

Custom A&A Support. Verizon complies with **RFP Section C.2.8.4.2(6)**. Verizon's custom A&A service supports to agencies with unique requirements or agencies opting for more stringent A&A requirements beyond the NIST High Impact baseline.

External Network Connection. Verizon complies with **RFP Section C.2.8.4.2(7)(a-e)**. Verizon offers a wide selection of connectivity options that allow an ordering agency to connect to external IP networks at their physical locations and that are compliant with TIC portal interconnecting requirements. Verizon supports dedicated external connections to external partners (e.g., non-TIC Federal agencies, externally

connected networks at business partners, state/local governments) with a documented mission requirement and approval. This includes, but is not limited to, permanent VPN over external connections, including the Internet, and dedicated private line connections to other external networks

Encrypted DMZ. Verizon complies with **RFP Section C.2.8.4.2(8)**. Verizon supports FIPS 140-2 compliant encryption from the ordering agency Service Delivery Point (SDP) at the edge of the agency WAN to the MTIPS portal. The service options include applicable FIPS 140-2 compliant SRE as well as management of the SRE.

Remote Access. Verizon complies with **RFP Section C.2.8.4.2(9)(a)(i-iv)**. The Verizon Remote Access support option offers a comprehensive suite of VPN access features, along with powerful security features, allowing administrators to provision remote access through appropriate security policies for a variety of endpoints, including Mac and Windows environments, and the latest iOS and Android devices.

Extranet Connections. Verizon complies with **RFP Section C.2.8.4.2(10)(a-e)**. The Verizon MTIPS portals support extranet connections, allowing VPNs to terminate behind the National Cyber Protection System (NCPS) EINSTEIN device and in front of the agency-specific security controls to allow the firewall and Intrusion Detection and Prevention System (IDPS) to inspect inbound (agency internal) traffic. For outbound traffic, VPNs will terminate behind the NCPS EINSTEIN device and the suite of TIC sensors to inspect outbound (Internet) traffic.

Customized Remote Access. Verizon complies with **RFP Section C.2.8.4.2(10)**. Verizon will support customized remote access for specific agency extranet connection requirements.

Inventory Map. Verizon complies with **RFP Section C.2.8.4.2(11)**. Verizon will provide an inventory mapping service upon request. The portals are fully capable of maintaining and managing a complete map or inventory of all ordering agency networks connected to the TIC access portal.

MTIPS Security. Verizon complies with **RFP Section C.2.8.4.5**. Verizon will assist ordering agencies in verifying that the deployed MTIPS solution remains in compliance with all applicable MTIPS Security standards.

Valid Security A&A. Verizon complies with **RFP Section C.2.8.4.5.3**. Security A&A of the entire Verizon MTIPS shared system is performed in conjunction with GSA. Verizon resources are available to assist with ordering agency WAN/LAN Security Assessment and Authorization needs. The third-party certification of compliance with FISMA high requirements for the shared packet inspection and analysis environment, and of all the other appropriate and shared components of the Verizon MTIPS solution, are provided to MTIPS clients upon request in order to facilitate their A&A activities.

System Security Plan (SSP). Verizon complies with **RFP Section C.2.8.4.5.4(1-27)**. This includes support for a System Security Plan (SSP), Security Assessment Boundary and Scope Document (BSD), and other Security A&A documentation. Reference Attachment B, Section B.7 in Verizon's EIS MTIPS RMF, for a complete list of Verizon MTIPS security deliverables. In addition, Verizon has included an **EIS Supply Chain Resource Management (SCRM) Plan Section 3 of Volume 2 – Management** in compliance with the EIS RFP.

Additional Security. Verizon complies with **RFP Section C.2.4.5.5(1-3)** and the additional security requirements referenced in the EIS RFP.

Personnel Background Investigation. Verizon complies with **RFP Section C.2.8.4.5.5.1** and will perform personnel security/suitability checking in accordance with FAR Part 52.204-9. All Verizon personnel with access to the contracted system that is within the security A&A scope will complete a background investigation in accordance with Homeland Security Presidential Directive-12 (HSPD-12), OMB guidance M-05-24, M-11-11, and as specified in GSA CIO Order 2100.1J and GSA Directive 9732.1D Suitability and Personnel Security to provide services under the EIS contract. The required background investigations for administrative personnel will be a minimum of a National Agency Check with Written Inquiries (NACI) and for technical staff will be a

Minimum Background Investigation (MBI) or higher depending upon their access and control over the systems. GSA will pay for any required background investigations for MTIPS.

Stipulated Requirements. Verizon complies with the **Service Description (C.2.8.4.1)**, **Functional Definition (C.2.8.4.1.1)**, and all applicable **Standards (C.2.8.4.1.2)**, **Connectivity (C.2.8.4.1.3)**, **Interfaces (C.2.8.4.3)**, **Performance Metrics (C.2.8.4.4)** and **General Security Compliance (C.2.8.4.5.1)** RFP requirements.

2.8.4.2 Quality of Services [L.29.2.1, M.2.1]

Verizon has been the provider of industry-defining managed service offerings for the past 15 years. [REDACTED]

[REDACTED], Verizon is the first managed services company to provide both a carrier Internet backbone network and a global managed security services infrastructure for end-to-end security protection and management. Verizon MTIPS solutions are designed to support the special security needs of the federal government. The security features built into Verizon's design are listed in **Table 2.8.4.2-1** below.

Table 2.8.4.2-1. MTIPS Security Features

MTIPS Security Features
System Accredited at the "high impact" security level
A suite of security devices that provide firewall, intrusion detection and prevention, anti-virus and e-mail scanning
Fully-redundant security sensor stacks (automatic failover) for high availability
Systems designed with a High Availability Architecture (dual data centers, dual operation center, redundant equipment within the data centers)
Multi-tiered, scalable SEM with advanced analytics

Verizon architected the MTIPS environment to minimize exposure to the public internet, while maximizing private network access to IP services. MTIPS capabilities are listed in **Table 2.8.4.2-2** below.

Table 2.8.4.2-2. MTIPS Capabilities

MTIPS Capabilities
IPv6 ready
Forward log copies directly from the security stack
Supports Native IP throughput
Works in conjunction with existing Network Security Services
Supports integration with government-approved cloud provider
Supports integration with mobile private network

2.8.4.3 Service Coverage [L.29.2.1, M.2.1]

Verizon complies with **RFP Section C.1.3** and will support MTIPS in a minimum of 25 of the top 100 CBSAs.

2.8.4.4 Security [L.29.2.1, M.2.1]

The Verizon MTIPS is managed for security and risk per Verizon's EIS IT Risk Management Framework (RMF) Plan in **Volume 1, Attachment A**. Appropriate security measures for the selected access solution will be implemented on a TO basis for Internet and related traffic that requires aggregation (reference **Section 3, External Traffic Routing**) to provide security and confirm the integrity of government data. If additional security measures are required they will be addressed at the TO level.

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

2.8.5 MANAGED SECURITY SERVICES (MSS) [C.2.8.5]

2.8.5.1 Understanding [L.29.2.1, M.2.1]

Verizon is proposing its Managed Security Services (MSS) which currently support over 20 different federal agencies. Verizon MSS is a suite of security devices and services that Verizon offers to our federal customers to combat advanced cyber security threats. Events generated from devices that Verizon deploys and turns-up at customer locations are sent back to our Cyber Security Operations Center (CSOC) to be inspected by our Security Event and Incident Management (SEIM) technology for evidence of security breaches or incidents. As incidents are identified the CSOC alerts the customer of the problem and as required works with the customer to resolve the incident. Verizon MSS fully monitors and manages the health and status of deployed devices.

Verizon's security portfolio is recognized by the Gartner group, Frost and Sullivan, and SC Magazine as one of the best security product within the industry. In 2014, Verizon was once again recognized as a Leader in the Gartner Magic Quadrant for Global Managed Security Services providers. Verizon methodically evaluated its MSS portfolio and selected high performing tools and services to offer ordering agencies advanced security functionality. This portfolio provides ordering agencies with the highest quality security in a cost-effective, low-risk environment.

[REDACTED]

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

[REDACTED] Verizon is the first managed services company to

[REDACTED]. Verizon MSS solutions are designed to support the special security needs of the federal government.

Verizon will monitor and manage the ordering agency's MSS portfolio components from its CSOC. The CSOC is an evolution of the SOC that was purpose-built for the Network contract and now supports many U.S. government MSS agencies. The CSOC enhancements include integration with the Verizon Cyber Information Center (VCIC) and Verizon's next generation MSS Analytics Platform. The CSOC is dedicated to supporting U.S. government agencies, is staffed with cleared U.S. citizens, is built to the secret level of support, uses a high availability architecture, provides FISMA support and compliance, and was built to the High level of physical security controls as detailed in NIST Special Publication 800-53 Rev. 4.

Additionally, Verizon's CSOC integrates with Verizon's Response, Intelligence, Solutions, and Knowledge (RISK) Team, adding threat intelligence data from more than 70 unique cyber information sources that help the CSOC analyze threats and broaden risk intelligence on behalf of ordering agencies. This access to intelligence, combined with a Gartner-recognized Security Event Management (SEM) platform; and world-class MSS tools powers Verizon's ability to provide MSS that truly combats security threats, enhances risk decision making, drives fast remediation for day-to-day security operations to give a better understanding of risk, and control costs.

2.8.5.1.1 Managed Prevention Service (MPS) [C.2.8.5.1.1(1)]

Verizon's Managed Prevention Service (MPS) meets or exceeds the requirements in the EIS RFP. Verizon's complete MPS offering will provide ordering agencies with a full suite of managed services integrated within Verizon's managed service infrastructure to provide host and network traffic, analyzing network protocol and application activity to identify and mitigate suspicious activity. Verizon MSS provides innovative cost-effective solutions to improve risk insight, enhance decision making, and drive support for day-to-day security operations. MSS will enable ordering agencies to allocate resources

against both existing and emerging threats. These services provide consistency in handling threats and provide direct access to security experts and industry best practices.

As an industry leader in MSS, Verizon's solution will bring together its research, engineering, design, and implementation know-how to provide the right tools and services to meet ordering agencies' security requirements. Subject Matter Experts (SME) on the MPS toolsets will be available to ordering agencies to provide robust and integrated solutions and Verizon implementation teams will provide seamless and low risk deployments.

Verizon's CSOC will operate 24x7 to protect ordering agencies' networks and traffic from cyber-attacks. Each day, the Verizon CSOC monitors millions of security events. The CSOC solution processes these millions of events and reduces them to a smaller number of actionable events that Verizon provides to ordering agencies or to its INRS function for action.

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED] in

Table 2.8.5.1.1-1.

Table 2.8.5.1.1-1. MPS Management and Monitoring

MPS Components Management and Monitoring
■ MPS Component Availability, Health Monitoring and Service Management
■ MPS Component Maintenance
■ MPS Component Security Management
■ MPS Component Availability Monitoring
■ MPS Component Health Monitoring
■ MPS Component Device Troubleshooting and Restoration
■ MPS Component Asset, Configuration, Patch, and Change Management
■ MPS Component Tuning and Rule Set Management
■ Security Event and Log Collection
■ Threat Analysis
■ Event Analysis and Correlation
■ Incident Reporting, Handling, and Escalation

The Managed Security Services Dashboard is the ordering agencies' tool for reviewing information about their MPS services and for reporting. Available 24x7, the information on the Security Dashboard is updated regularly with varying refresh rates based on the type of data. The Security Dashboard reports security information on devices, individually and aggregated. Ordering agencies can consult the items listed below in **Table 2.8.5.1.1-2**, if applicable.

Table 2.8.5.1.1-2. Security Dashboard Information

Security Dashboard Information
■ Reporting on the availability of MPS Components.
■ A list of incidents classified per location, device, status, and level.
■ 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.
■ To schedule vulnerability scans and view associated reports.
■ A list of planned security updates.
■ The status of change requests.
■ Security intelligence updates.

Additionally, the facilities that host Verizon's MPS monitoring and management (e.g., the threat correlation engines, device element managers, log storage services, etc.) and the associated CSOC systems are purpose-built U.S. government client-only Government Network Operations Security Centers (GNOSCs). The GNOSCs are

staffed exclusively with cleared U.S. citizens and service-specific dedicated resources to provide the required CSOC functions in support of the MPS offering. [REDACTED]

[REDACTED]. The GNOSC architecture includes numerous management tools to minimize the risk of service interruption during transition. [REDACTED]

[REDACTED] recognized by Gartner, Forrester, SC Magazine, and others. [REDACTED] technology carries out [REDACTED] vulnerability scans per month worldwide. Verizon presently supports vulnerability scanning and management for over [REDACTED] internal and external IP addresses via the [REDACTED]. Verizon's customers range from three IP addresses to customers with hundreds of thousands of internal and [REDACTED]

2.8.5.1.3 Incident Response Services (INRS) [C.2.8.5.1.1(3)]

Verizon's INRS proactive services are designed to prevent incidents. INRS consists of onsite consulting, strategic planning, security audits, policy reviews, vulnerability assessments, security advisories, and training. Verizon proposes Verizon's professional security services that meet and exceed the EIS requirements. Verizon's professional security services help agencies plan and defend against possible threats and take fast action to identify and contain incidents when they take place. This dual approach helps agencies proactively secure their sensitive data. Verizon's security specialists have relevant experience forged by over 1,000 customer engagements. The security specialists are accomplished and will work collaboratively with an ordering agency to review security infrastructure and to develop strategic plans.

The teams will work with agencies to identify vulnerabilities and threats to the system and to evaluate the established security posture for verification that adequate security controls have been correctly implemented and are operating as intended in the system infrastructure. Verizon will conduct assessments using a best practice methodology as the key ingredient in the approach to assessing risk.

An effective security program entails implementing a risk-based approach for security components and procedures. Threats are typically categorized into three sets of controls: **Process** (policy and enforcement), **People** (user access to the system), and **Technology** (configuration, logical access control mechanisms, and monitoring of the system). The three control sets are necessary to protect the confidentiality, integrity,

and availability of a system. System owners should never rely solely on technical controls to protect information adequately. A successful security program necessitates embedding security requirements, testing, and evaluation within the development of the system's architecture and the implementation of security policies and procedures.

Over the years working with government agencies, Verizon has gained a deep understanding of the unique challenges of information security in the government environment, which enables Verizon to design service solutions tailored precisely to the needs of ordering agencies.

INRS Reactive. Verizon's INRS reactive services and Rapid Response Retainer consist of telephone and on-site support for responding to malicious events such as 1) Denial of Services (DoS) attacks; 2) virus, worm, and Trojan horse infections; and 3) illegal inside activities, espionage, and compromise of sensitive internal agency databases. INRS reactive services provide an effective method of addressing these security intrusions, thereby providing operational continuity in case of attacks. In addition, INRS reactive offers forensics services that can assist with investigating, apprehending, and prosecuting offenders.

Verizon will leverage and expand on its incident response services already successfully in use at numerous government agencies and global corporations. Verizon's INRS reactive solution draws on a combination of Verizon professional security services and Verizon managed security services resources. Verizon professional security services personnel are industry experts, with extensive government security experience, security clearances, and a host of advanced degrees and industry certifications, including SANS global assurance, Certified Information Systems Security Profession (CISSP), Certified Ethical Hacker (CEH), Certified Information Security Manager (CISM), System Security Certified Practitioner (SSCP), and Project Management Professional (PMP). INRS allows agencies to complement in-house security expertise, or obtain outside assistance with a greater depth and breadth of experience.

Verizon will deliver a proactive and reactive incident response solution that meets the EIS RFP requirements. Using investigative experts, Verizon takes an innovative

approach to incident response and forensic investigation. As opposed to many other organizations, Verizon pursues a holistic approach to network and incident investigation. Rather than just examining one or two direct points of unauthorized activities, Verizon gathers the relevant technical intelligence available from the entire network to build a larger, more cohesive understanding of the incident. Verizon's state-of-the-art, 24x7 incident response and evidentiary forensic services provide lifecycle incident and forensic management.

INRS Proactive. The INRS proactive approach starts with an in-depth evaluation of the systems and/or programs Verizon is contracted to assess. This assessment includes people, process, and technical areas shown in **Figure 2.8.5.1.3-1**.

Figure 2.8.5.1.3-1. INRS Proactive In-Depth Analysis of Program Elements



Following the completion of the assessment, Verizon will follow the INRS proactive methodology, which consists of four phases, as described in **Table 2.8.5.1.3-1**.

Table 2.8.5.1.3-1. INRS Proactive Methodology

Security Dashboard Information	
Phase 1	Verizon identifies and defines the security requirements by reviewing the organization, policy, network and application. This helps Verizon understand business drivers and compliance to determine security requirements.
Phase 2	Verizon carries out review of program, policy and procedures, network architecture, application architecture, organizational structure and interviews with key staff.
Phase 3	Activities identify vulnerabilities through comprehensive scanning, penetration tests, and application and host assessments.
Phase 4	Verizon develops a strategic response plan based on recommendations and findings from the identified security gaps and shortfalls with respect to policy, process, standards, and compliance.

An additional proactive approach provided by Verizon is the training given to all stakeholders preparing staff members for security contingencies. The training covers

procedures and tools, as well as the incident response life cycle. In addition, Verizon will conduct demonstrations, mock drills and vulnerability workshops.

2.8.5.1.4 Compliance with EIS Service Requirements [J.19]

Connectivity. Verizon complies with **RFP Section C.2.8.5.1.3**. Verizon MSS will connect to and interoperate with agency networking environments, including Demilitarized Zones (DMZs) and Secure Local Area Networks (LANs) as required by the subscribing agency.

Design & Implementation Services. Verizon complies with **C.2.8.5.1.4.1(1)** and will provide design and implementation services for its MSS MPS offering. This will include provisioning, installation, configuration, testing, and maintenance of all hardware and software components comprising the solution (e.g., log servers). Verizon and agencies may discuss matters, such as system recommendations, baseline assessments, rules, signature sets, configurations, and escalation procedures.

Software & Hardware Components. Verizon complies with **C.2.8.5.1.4.1(2)** and will provide software and hardware components, including log servers, as applicable.

Load Balancing Capabilities and Redundancy. Verizon complies with **C.2.8.5.1.4.1(3)**. Verizon will implement hardware or software load balancing capabilities and redundancy necessary to meet KPI and agency requirements.

Installation Support. Verizon complies with **C.2.8.5.1.4.1(4)** and will provide installation support to include testing of equipment, testing of software, and loading of any agency-relevant data, as required by the agency.

Maintenance of Configuration Information. Verizon complies with **C.2.8.5.1.4.1(5)**. Verizon will maintain the latest customer-approved configuration information to support restoration, reporting and forensics activities.

Maintenance of Managed Service Capability. Verizon complies with **C.2.8.5.1.4.1(6)**. Verizon will perform maintenance activities based on an ITIL change management process.

Compliance. Verizon complies with **RFP Section C.2.8.5.1.4.1 (7)**. Verizon complies with NIST SP 800-53 Rev. 4 Identification and Authentication controls for high impact systems. Administrative access to Verizon MPS will require multi-factor authentication, as stipulated in the RFP.

Updates and Notifications. Verizon complies with **RFP Section C.2.8.5.1.4.1 (8)-(9)**. Verizon will deploy periodic bug fixes, patches, and updates for its MPS offering as needed. Verizon will notify the subscribing agency as updates become available. Verizon will test all patches and bug fixes and will deploy them once they have been approved by both Verizon and the agency.

Document Configuration and Management. Verizon complies with **RFP Section C.2.8.5.1.4.1 (10)**. Verizon will perform and document configuration and management for its MPS offering to verify that security, access, and information-flow policies are enforced.

Monitoring and Functionality. Verizon complies with **RFP Section C.2.8.5.1.4.1 (11)-(13)**. Verizon will support proactive monitoring for its MPS offering as referenced in the RFP. This will include 24x7 proactive monitoring of the health and status of MPS hardware/software components, and monitoring of the overall performance and load capacity. Verizon will also monitor the service to verify that it provides only necessary functionality, protocols, ports, and services as approved by the customer.

Periodic Validation Activities. Verizon complies with **RFP Section C.2.8.5.1.4.1 (14)**. Verizon will perform and document periodic validation activities (e.g., via scans) to verify that its MPS service configurations are not vulnerable, and that they are enforcing agency policies.

Notification of Failure Events. Verizon complies with **RFP Section C.2.8.5.1.4.1 (15)**. Verizon will notify the agency of MPS-failure events via email, fax, or telephone, as directed by the agency.

SBU Indicators. Verizon complies with **RFP Section C.2.8.5.1.4.1 (16)**. Verizon will be able to receive, handle, and use sensitive but unclassified cybersecurity indicators provided by the agency or the Department of Homeland Security (DHS).

Event Messages. Verizon complies with **RFP Section C.2.8.5.1.4.1 (17)-(19)**. Verizon will support event message requirements as identified in the RFP. This will include verifying that its MPS service statistics, events messages, logs, and suspected attack information are sent via secure means to the agency-specified operation center, and that event messages associated with DHS-provided indicators are sent via secure means to DHS. Verizon will verify that event messages have necessary and consistent timestamps and content as specified in the EIS RFP.

Data Retrieval. Verizon complies with **RFP Section C.2.8.5.1.4.1 (20)**. Verizon will be able to identify and retrieve each agency's data without divulging any other agency's data.

Access to Logs and Service Information. Verizon complies with **RFP Section C.2.8.5.1.4.1(21)(a-k)**. . Verizon will provide the subscribing agency with secure web access to logs and service information as specified in the EIS RFP.

Vulnerability Scanning Service. Verizon complies with **RFP Section C.2.8.5.1.4.2(1-2)**. . Verizon will provide API access to assist customer personnel with tasks such as scanning IP addresses, assessing host vulnerabilities, creating user accounts, and exporting vulnerability data.

Network Vulnerabilities and Countermeasures. Verizon complies with **RFP Section C.2.8.5.1.4.2(1)**. Verizon VSS will periodically scan networks, including operating systems and application software, for potential openings, security holes, and improper configuration.

Notification. Verizon complies with **RFP Section C.2.8.5.1.4.2 (2)**. Verizon VSS will provide the subscribing agency with notifications of vulnerabilities discovered in the customer network. Notifications will be communicated via email, fax, or telephone, as directed by the customer.

Access to Information. Verizon complies with **RFP Section C.2.8.5.1.4.2 (3)**. Verizon will provide the agency with secure Web access to vulnerability information, scan summaries, device/host reports, and trend analyses.

Review Vulnerabilities with Customer. Verizon complies with **RFP Section C.2.8.5.1.4.2 (4)**. Verizon will meet with the subscribing agency on a periodic basis and in ad hoc meetings to review all vulnerabilities discovered in the customer network.

Scan Scheduling Flexibility. Verizon complies with **RFP Section C.2.8.5.1.4.2 (5)**. Verizon will provide scan scheduling flexibility to the agency in order to minimize any interruptions in normal business activities.

Non-Destructive, Non-Intrusive Scans. Verizon complies with **RFP Section C.2.8.5.1.4.2 (6)**. Verizon will provide the agency with non-destructive and non-intrusive vulnerability scans that will not crash systems, disrupt agency operations, or provoke a debilitating DoS condition on the agency system being probed.

Other Analytic Means. Verizon complies with **RFP Section C.2.8.5.1.4.2 (7)**. Verizon VSS will also use other analytical means to ascertain the vulnerability of agency systems if a particular scan is potentially destructive or intrusive.

Regular Updates. Verizon complies with **RFP Section C.2.8.5.1.4.2 (8)**. Verizon will regularly update its VSS scanning engine with new vulnerabilities information to maintain the effectiveness of the service.

Support for Networks. Verizon complies with **RFP Section C.2.8.5.1.4.2 (9)**. Verizon VSS will support networks of any size and/or complexity.

Strategic Plans. Verizon complies with **RFP Section C.2.8.5.1.4.3 (1)**. Verizon will review the EIS subscribing agency's security infrastructure and develop appropriate strategic plans in collaboration with the agency. These plans will detail the incident response process, identify internal resources, assign duties to team members, describe policies, define severity levels, list escalation chains, and specify emergency/recovery procedures.

Support 24x7. Verizon complies with **RFP Section C.2.8.5.1.4.3 (2)**. Verizon INRS will provide the agency with effective incident response support on a 24x7 basis.

Problem Detection System. Verizon complies with **RFP Section C.2.8.5.1.4.3 (3)**. Verizon INRS will include a problem detection system for the diagnosis of alerts and violations.

Suspicious Alerts. Verizon complies with **RFP Section C.2.8.5.1.4.3(4)**. Verizon provides MPS to monitor and manage alerts generated by deployed security devices and tools. For Incident Response, Verizon can analyze complex data to identify evidence of security breach, data compromise, and at-risk data and then share findings with customers. Verizon will perform malcode analysis that will typically focus on the interactions of malcode with the customer's system. Verizon will attempt to determine the functionalities of suspected malicious files. Depending on the nature of the suspected malware functionality, the analysis may include identification of communication channels, a listing of indicators of compromise, and malware response guidelines. Malcode analysis may include the following:

- Code anatomy, which provides an overview of the malware binary content;
- Behavioral analysis, which is a high level overview of the malcode's functioning with the objective of assisting in identifying system changes caused by the malcode and/or communication channels (e.g., IP addresses and domain names) utilized by the malcode; and

- Malware intelligence analysis, which leverages Verizon's intelligence datasets to determine if the malware is already known and/or affiliated with known incidents or actors.

Verizon will issue a report at the end of the analysis of the submitted sample, which will contain any identified findings, indicators of compromise and recommendations for additional analysis.

Immediate Access to Information. Verizon complies with **RFP Section C.2.8.5.1.4.3(5)**. As the Verizon CSOC identifies new vulnerability and severe alert information it will share this data with our MSS customers. Data may include but is not limited to description, target, origin, potential incident impacts, remedies, and prevention measures.

Coordination. Verizon complies with **RFP Section C.2.8.5.1.4.3(6)**. Verizon will coordinate with the agency to handle potential security incidents according to the appropriate response procedures.

Countermeasures. Verizon complies with **RFP Section C.2.8.5.1.4.3(7)**. Verizon INRS personnel will provide best practice countermeasures to contain the security incident, limit its spread, and protect internal systems.

Recommendations. Verizon complies with **RFP Section C.2.8.5.1.4.3(8)**. Verizon will recommend the fixes necessary to mitigate identified vulnerabilities, and the appropriate procedures to guard against future attacks.

Recommendations and Support. Verizon complies with **RFP Section C.2.8.5.1.4.3(9-12)**. Verizon will provide the agency with secure web access to incident analysis findings and recommendations, and will assist the agency in containing the damage and restoring affected systems to their normal operational state. Verizon will also assist the agency in testing restored systems to verify that identified vulnerabilities have been corrected, and will provide dedicated support until resolution of the problem.

Post-Incident Services. Verizon complies with **RFP Section C.2.8.5.1.4.3(13).**

Verizon will provide post-incident investigative and forensics services. This assumes full cooperation and collaboration with the host agency supporting Verizon's efforts to isolate the impacted area, capture and collect data, categorize malicious or illegal events, and perform reconstruction analyses. Verizon will gather, handle and preserve digital evidence in a manner that will assist agencies and law enforcement with administrative actions and legal proceedings. Verizon will analyze digital evidence and provide all information that leads to the origination of a security incident.

Telephone Support and Personnel Deployment. Verizon complies with **RFP Section C.2.8.5.1.4.3 (14)-(15).** Verizon will provide telephone support to the agency, and will deploy cybersecurity personnel to agency sites to handle security incidents, as necessary.

Security Awareness Training. Verizon complies with **RFP Section C.2.8.5.1.4.3(16).** During the Rapid Response Initiation, Verizon will provide security awareness training for agency security personnel. This training is typically geared towards the agency incident response team members. Further training is available through the MSS INRS Rapid Response Retainer CLINS and through task orders.

MSS Features. Verizon complies with **RFP Section C.2.8.5.2** and will provide the MSS features specified in the EIS RFP. Features requirements specified in the RFP, including: firewall, personal firewalls, network intrusion prevention system, endpoint protection, secure web proxy, inbound web filtering, application-level gateway, network behavior analysis, network traffic content analysis and sandboxing, email forgery protection and filtering, email content analysis and sandboxing, user authentication integration, DNSSEC, DNS sinkholing, data loss prevention, DMZs support, extranet support, firewall-to-firewall VPNs, remote client VPNs, EINSTEIN 2, short-term storage, long-term storage, agency-specified policy enforcement, VSS API, advanced analytics.

MPS Features. Verizon complies with **RFP Section C.2.8.5.2(1)(a-w)** and will provide the MPS features as described below:

Firewall and Personal Firewall [C.2.8.5.2(1)(a-b)]. Verizon's Firewall and Personal Firewall solution safeguards internal networks and systems from hostile activity, protecting critical data from compromise and tampering. Verizon implements firewall solutions to ordering agencies' sites to secure networks from the growing number of advanced threats, prevent unauthorized access to or from private networks, and reduce service disruptions caused by malicious attacks. The firewall solution provides advanced firewall technologies based on industry leading, best-of-breed vendors. These vendors consistently lead the market in delivering superior manageability, rich feature sets, and excellent price performance. The firewall and personal firewall solution is scalable to meet requirements of all sizes and complexity—ranging from a combination of premises-based, network-based, personal, and application proxy-based firewall solutions.

Network Intrusion Prevention System [C.2.8.5.2(1)(c)]. Verizon's IPS solution provides intrusion sensors that analyze packet activity for indications of network attack, misuse, and anomalies. The service generates alerts and records suspicious events. In addition, the IPS solutions provide immediate corrective responses, such as dropping or rerouting malicious packets, to stop or alleviate malicious attacks. Verizon's IPS solution will provide advanced management and monitoring services.

Endpoint Protection [C.2.8.5.2(1)(d)]. Verizon Endpoint Security Solutions provide several combined protection mechanisms directly to the desktop/laptop using centrally managed 'endpoint' agents. The protection mechanisms can provide services such as anti-virus, anti-spam, personal firewall, encryption or mechanisms that control whether or not peripheral devices can be connected to the endpoint (e.g., printers or flash drives). An "Endpoint Policy Manager" collects security logs from the various 'endpoint' agents and manages centrally common enforced policies. Host Intrusion Prevention is a host-based intrusion detection and prevention system that protects system resources and applications from external and internal attacks. It provides a manageable and scalable intrusion prevention solution for workstations, notebooks, and critical servers, including web and database servers.

The Endpoint Solution technology blocks zero-day and known attacks. Host Intrusion Prevention is fully integrated with the management console and uses its framework to deliver and enforce IPS, Firewall, and general security policies. The IPS feature details exceptions, signatures, application protection rules, events, and client-generated exceptions. These features consist of IPS options, IPS protection and IPS policies. The Firewall feature contains three policies that protect Windows computers: Firewall Option, Firewall Rules, and DNS Blocking. The General feature contains three policies that can apply to both the IPS and Firewall features. This features Client UI, Trusted Networks, and Trusted Applications. The combination of these policies meet the endpoint protection requirement for host based intrusion.

Secure Web Proxy [C.2.8.5.2(1)(e)]. The Verizon Secure Web Proxy can be configured to explicit, transparent, or Web Cache Communications Protocol (WCCP) mode. The proxy works in-between end-points allowing URL blocking, URL, and domain-based filtering and obfuscation of internal IP addresses.

Inbound Web Filtering [C.2.8.5.2(1)(f)]. The Verizon Inbound Web Filtering offering includes signatures to protect against server side attacks, such as SQL injections, XSS, SOAP, and other vulnerabilities. It includes a full featured Web Application Firewall designed to protect web application servers.

Application-Level Gateway [C.2.8.5.2(1)(g)]. Verizon's Application-Level Gateway helps protect web applications from attacks that aim to exploit vulnerabilities in business critical web applications. Threats against the web infrastructure are monitored and escalated in near real time for immediate action.

Some protocols require a deeper level of inspection to determine the appropriate security action. The Verizon solution uses session helpers to analyze the data in the packet bodies of some protocols and adjust the firewall to allow the protocols to send packets through the firewall. Some of these protocols include: SIP, FTP, TFTP, MMS and more.

Other protocols such as HTTP, SMTP, POP3, IMAP, MAPI, FTP, and IM can be inspected for more in depth security analysis through anti-virus scanning and web filtering.

Network Behavior Analysis [C.2.8.5.2(1)(h)]. Verizon's solution provides real time threat analytics. Verizon's Distributed Denial of Service (DDoS) and Network Behavior Analysis analyze and learn "normal" network traffic, then block potential attacks based on the unusual activity. The DDoS solution will automatically build normal traffic and resource behavior profiles to detect and block behavioral anomalies and DDoS attacks. The Web Application Firewall solution, similarly, will learn "normal" behaviors of web traffic (URL parameters, HTTP methods, session IDs, cookies, schemes, etc.) and block anomalies.

Network Traffic Content Analysis and Sandboxing [C.2.8.5.2(1)(i)]. The solution analyzes network traffic and blocks malicious traffic. The solution inspects unknown objects by executing the file in a sandbox environment. The network analysis and sandboxing will block "known bad" files while forwarding the unknown or suspicious files to the sandbox for a more thorough inspection. The sandbox will work in standalone mode with third party devices to scan files on a network share or in sniffer mode.

Email Forgery Protection and Filtering [C.2.8.5.2(1)(j)]. The email appliance is a complete Email Gateway solution protecting against inbound and outbound threats.

Table 2.8.5.1.4-1 lists inbound and outbound protection techniques:

Table 2.8.5.1.4-1. Inbound/Outbound Email Forgery Protection and Filtering Techniques

Inbound Email Protection Techniques	Outbound Email Protection Techniques
Sender Policy Framework (SPF) checking	Use of SPF records for each domain that explicitly identify the email appliance at Verizon as an approved outbound sender for customer domain
Domain Keys Identified Mail (DKIM) checking	Use of DKIM signing for each protected domain
Access control rules	Ensuring that Pointer (PTR) records exist for all IPs used in outbound mail from the email appliance. This includes any "virtual IPs" being used
Anti-spam header analysis	
Delivery Status Notification (DSN) blowback protection	

Email Content Analysis and Sandboxing [C.2.8.5.2(1)(k)]. The email sandboxing technology is available as an integrated component of existing infrastructure like email. Integration between the Managed Email Gateway and Managed Sandbox makes email less vulnerable to common early stage vectors of attack, such as zero day malware and

advanced threats. The Email Gateway can forward suspicious files to the Sandbox for full sandbox inspection and reporting to prevent unknown zero day viruses from reaching the end user in line. Its “store-and-forward” nature allows the time needed for additional sandbox inspection “in-line” so together they can prevent Advanced Persistent Threats (APTs) from reaching an end user.

User Authentication Integration [C.2.8.5.2(1)(l)]. Verizon will support the integration of the email-based threat mitigation service with the agency's own authentication service, as specified by the ordering agency. In addition to using the agency's authentication, Verizon can integrate with third-party RADIUS and LDAP authentication systems, allowing ordering agencies to re-use existing information sources. The REST API can also be used to integrate with external provisioning systems.

Domain Name System Security (DNSSEC) [C.2.8.5.2(1)(m)]. Verizon will support DNSSEC that is compliant with NIST Special Publication 800-81 Rev 2 and will inspect DNS response packets to detect known and zero-day advanced botnets. For the known botnets, the Verizon solution will inspect the DNS response packets for blacklisted domains according to the callback detectors. For the detection of zero-day advanced botnets, Sensors perform complex heuristic analyses of DNS response traffic.

DNS Sinkholing [C.2.8.5.2(1)(n)]. The IPS Sensor blocks DNS traffic if the DNS response packet contains a blacklisted domain according to callback detectors. If a host attempts to reach a blacklisted domain, it is most likely infected and is now a bot. Then the sensor sends a crafted DNS response back to sinkhole this bot traffic. Verizon's IPS solution checks the DNS packets for blacklisted domains. If the sensor detects a blacklisted domain, it sends a crafted DNS response packet to the corresponding bot.

Data Loss Prevention (DLP) [C.2.8.5.2(1)(o)]. Verizon's DLP solution allows for managing data loss policies, workflow, remediation, reporting, and administration. The DLP solution will scan agency data to discover where sensitive data is stored. It will prioritize the highest risks to expedite remediation and will encrypt, move, or delete sensitive files and folders. With the DLP solution, information is protected against loss and theft. DLP will allow an ordering agency the ability to discover, monitor, protect and

manage sensitive data across servers, endpoints, mobile devices, and even network and storage systems. Outbound communications that include data tagged as sensitive can also be prevented. Verizon's DLP solution allows for managing data loss policies, workflow and remediation, and reporting and administration.

DMZs Support [C.2.8.5.2(1)(p)]. Verizon will support connections to DMZs, which serve as buffers between the agency's private networks and outside public networks. DMZs can apply to Web (HTTP), FTP, email (SMTP), and DNS servers.

Extranet Support [C.2.8.5.2(1)(q)]. Verizon will support connections to extranets, which can facilitate inter-agency interactions or enable the agency to interface with trusted stakeholders. Verizon has multiple ways to provide support including internal interfaces that could have separate Virtual Local Area Networks (VLANs): one for each extranet, DMZ, or specific agency so that traffic from the users on one VLAN does not intrude upon the hosts of the other VLANs.

Firewall-to-Firewall Virtual Local Area Networks (VPNs) [C.2.8.5.2(1)(r)]. Verizon will support firewall-to-firewall VPNs, which establishes secure tunnels between agency firewalls, and also between firewalls and Verizon's operations centers.

Remote Client VPNs [C.2.8.5.2(1)(s)]. Verizon Remote Client VPN provides a comprehensive network security solution for endpoints while improving visibility and control, employing encrypted VPN technology.

EINSTEIN 2 [C.2.8.5.2(1)(t)]. Verizon will interact with DHS to obtain indicators, establish USCERT event feeds, and provide EINSTEIN network flow and detection capabilities for agency-specified traffic.

Short-Term Storage [C.2.8.5.2(1)(u)]. Verizon will provide storage capacity to retain at least 24 hours of agency-specific data generated by the MPS. Traffic will be selectively filtered and stored, and retained data will be made securely available to the agency. As part of the standard work flow, Verizon collects and stores events. These events are viewable by the customer through the Verizon MSS portal.

Long-Term Storage [C.2.8.5.2(1)(v)]. Verizon will provide storage capacity to retain a year of agency-specific data generated by the MPS. Traffic will be selectively filtered and stored, and retained data will be made securely available to the agency.

Agency-Specified Policy Enforcement [C.2.8.5.2(1)(w)]. The Verizon CSOC provides agency-specified policy enforcement.

VSS API Features. Verizon complies with **RFP Section C.2.8.5.2(2)(a)**. Verizon will provide API access to assist customer personnel with tasks, such as scanning IP addresses, assessing host vulnerabilities, creating user accounts, and exporting vulnerability data.

INRS Advanced Analytics Features. Verizon complies with **RFP Section C.2.8.5.2(3)(a)**. Verizon will provide and apply various statistical techniques from the modeling, machine learning, and data mining disciplines to analyze relevant observations for threat discovery, assessment, situational awareness, and prediction. Where applicable, the techniques provided must yield confidence intervals establishing the statistical significance of findings. When statistical significance cannot be established using rigorous, state-of-the-art techniques, the finding must include this caveat.

Stipulated Requirements. Verizon complies with the **Service Description (C.2.8.5.1)**, **Functional Definition (C.2.8.5.1.1)**, and all applicable **Standards (C.2.8.5.1.2)**, **Connectivity (C.2.8.5.1.3)**, **Interfaces (C.2.8.5.3)**, and **Performance Metrics (C.2.8.5.4)** RFP requirements.

2.8.5.2 Quality of Services [L.29.2.1, M.2.1]

Verizon currently provides MSS solutions for government agencies on Networx and other government contracts. This experience makes Verizon highly qualified to continue to support these requirements on the EIS contract. Verizon MSS meets all performance and AQL measures required in the EIS RFP.

Verizon provides managed security services for many government agencies. The Verizon GNOSC protects customer data and provides both secure network and security

operations management capabilities for government agencies and features program management offices for managing Verizon's security services.

2.8.5.3 Service Coverage [L.29.2.1, M.2.1]

Verizon complies with **RFP Section C.1.3** and will support MSS in a minimum of 25 of the top 100 CBSAs.

2.8.5.4 Security [L.29.2.1, M.2.1]

The Verizon MSS is managed for security and risk per Verizon's EIS IT Risk Management Framework (RMF) Plan in **Volume 1, Attachment A**. If additional security measures are required they will be addressed at the TO level.

2.8.6 MANAGED MOBILITY SERVICE [C.2.8.6]

2.8.6.1 Understanding [L.29.2.1, M.2.1]

Verizon's Managed Mobility Service (MMS) solution is designed to verify that enterprise security policies are applied and that mobile devices are managed and controlled even when off the enterprise network. Verizon's MMS solution provides ordering agency mobile users a simple method to access networks and applications regardless of their location or the device being used.

Verizon has also developed methods to help increase user adoption while reducing the need for IT training and technical support. With professional services available to provide proper planning and speedy deployment, agencies will be able to reap the benefits and reduce the difficulty often associated with the transition to a mobile solution. Some of the highlights of the Verizon MMS include: a management platform for myriad devices; simplified access to mission-critical systems; enterprise security policies enforced on mobile devices; and reduced maintenance costs and streamlined operations.

2.8.6.1.1 Compliance with EIS Service Requirements [J.19]

Mobile Device Management (MDM) Capabilities. Verizon complies with **RFP Sections C.2.8.6.1.4.1(a-j)** and fully supports all mandatory MDM capabilities. [REDACTED]

[REDACTED]

[REDACTED] Verizon's MMS supports device management

and other mobile management functions, including policy, security, configuration, application support, and data management.

Device Enrollment. Verizon complies with **RFP Sections C.2.8.6.1.4.1(2)(a-s)** and fully supports all device enrollment requirements.

Device Profiles. Verizon complies with **RFP Sections C.2.8.6.1.4.1(3)(a-m)** and fully supports all device profile requirements.

Device Feature Management. Verizon supports all the features described in **RFP Section C.2.8.6.1.4.1(4)(a-e)**. Different policies can be created and applied with certain actions defined by the agencies.

Data Management. Verizon's MMS solution will provide File Management and Personal Information Management as described in **RFP Sections C.2.8.6.1.4.1(5)(a-b)**. These features are supported by integrating documents, applications, and containerization with application wrapping technologies. This approach allows for data classification and interoperability with back end platforms.

Reports. Verizon complies with **RFP Section C.2.8.6.1.4.1(7-9)**. Verizon will provide Device Inventory Management and Reports, System Performance Reports, and MDM Security/Compliance Reports. Verizon's MMS solution features a set of pre-built reports with the Administrative Console and Software as a Service (SaaS) portal. Administrators can also generate custom reports using the "Custom View" tool to build a variety of different data views. The platform also provides agencies the ability to collect extensive device inventory data, such as installed software applications, hardware, scan processing time; configuration data related to Infrared (IR) connections, Wi-Fi and Bluetooth connectivity, and enhanced phone data. Enhanced phone data includes carrier network, mobile operator and operator network, phone number, device status, and network access point information. For agency-owned devices, the platform can capture network utilization data including inbound/outbound calls, text messages and data utilization. This data can be accessed via the integrated Crystal Reporting Engine,

or via APIs that allow the ordering agency or their Telecom Expense Management (TEM) provider to collect and import the data into their TEM engine/solution.

Additional Capabilities. Verizon complies with **RFP Sections C.2.8.6.1.4.1(10)(a-e)** and understands that additional capabilities may be defined at the TO level.

Application Deployment. Verizon complies with **RFP Sections C.2.8.6.1.4.2(1)(a-e)**. The Verizon MMS's Mobile Application Store (MAS) supports application deployment. There are three different types of applications: free applications on the MAS, for-purchase applications on the MAS, and custom-developed applications. The MMS solution can deploy applications to mobile devices. Depending on agency policies, the MAS can be enabled or blocked from displaying on users devices.

The software inventory is collected during the initial enrollment, and collected thereafter at periodic intervals defined by the ordering agency. This polling reports all applications on a particular device. Applications can be whitelisted or blacklisted based on policies on supported platforms. Application deployment can be controlled by selecting certain groups on the platform and staggered across the board to avoid bandwidth congestion.

Mobile Application Store. Verizon complies with **RFP Section C.2.8.6.1.4.2(2)(a)**. Private applications can be deployed via the MMS and will be available to ordering agencies under the private MAS for agency end users to download. Updates to the application can be uploaded to the MMS solution and the version will pushed to devices. Any private application deployed to the devices will appear in the software device inventory. Application terms can be defined for setting up effective and expiration dates. Applications can also be grouped into categories.

Additional Capabilities. Verizon complies with **RFP Section C.2.8.6.1.4.2(4)** and understands that additional capabilities may be defined at the TO level.

Mobile Content Management. Verizon's MMS includes a Mobile Content Management (MCM) platform that complies with **RFP Section C.2.8.6.1.4.3**. The MCM platform enables secure mobile access to content anytime, anywhere, and on any

device. It protects sensitive content and provides users with a central application to securely access, store, update and distribute documents.

Enroll Device. Verizon complies with **RFP Section C.2.8.6.1.4.4(1)**. Devices can be enrolled under a null policy, or they can be required to undergo approval by the MDM administrator once they have been deemed compliant.

Whitelists/Blacklists. Verizon complies with **RFP Section C.2.8.6.1.4.4(2)**. The Verizon MDM platform supports whitelists/blacklists for mobile devices.

MDM User Attribute Repository. Verizon complies with **RFP Section C.2.8.6.1.4.4(4)**. MDM platform policies are stored in a database.

Action Based on Compliance Rules. Verizon complies with **RFP Section C.2.8.6.1.4.4(5)**. The MDM platform can deploy scanning tools to ensure that application parameters defined by the ordering agency are within guidelines. Custom applications can be wrapped with specific criteria to detect additional security measures. Such measures can be integrated into custom mobile applications and deployments.

Block Device or Erase. Verizon complies with **RFP Section C.2.8.6.1.4.4(6)**. The MDM platform supports blocking and erasure of only managed data. Exception policies can be defined if the device has not been checked in by a certain time, as defined by the ordering agency.

Password Policy Enforcement. Verizon complies with **RFP Section C.2.8.6.1.4.4(7)**. The MDM platform supports all password policy enforcement requirements.

Mask Passwords. Verizon complies with **RFP Section C.2.8.6.1.4.4(8)**. Password entry can be enabled to mask passwords when entered.

Determine Users Making Configuration Change. Verizon complies with **RFP Sections C.2.8.6.1.4.4(9-10)**. The MDM platform's audit functions track all access and logs all changes to the system in the database.

Installation and Configuration. Verizon complies with **RFP Section C.2.8.6.1.4.4(11)**. The MDM platform supports all installation and configuration requirements. With additional integration, the ordering agency can define application-level VPN capabilities to make the user experience even more streamlined. The VPN functionality built into the device can be pushed and managed by the policy.

Send/Receive Encrypted Messages. Verizon complies with **RFP Section C.2.8.6.1.4.4(12)**. The MDM platform supports sending and receiving encrypted messages. This is a simple function that can be enabled or disabled.

Restrict Download/Copy. Verizon complies with **RFP Section C.2.8.6.1.4.4(13)**. The MDM platform supports all download/copy restriction and separate space requirements. An ordering agency can configure attachments within the emails to be blocked completely or to be opened within the container.

GPS Location. Verizon complies with **RFP Section C.2.8.6.1.4.4(14)**. The GPS location of the device is tracked in time intervals set by the ordering agency. The last known location is displayed on the GPS maps built into the MDM platform.

Encrypt Data in Transit. Verizon complies with **RFP Section C.2.8.6.1.4.4(15)**. The MDM platform supports all requirements for encrypting data in transit. The ordering agency will need to define the data and its application classifications. Third-party integrations that allow application wrapping are available; these can be bundled with the MDM platform.

Data at Rest. Verizon complies with **RFP Section C.2.8.6.1.4.4(16)**. The MDM platform supports application containerization. Application wrapping is used to protect ordering agency data using a FIPS 140-2 certificate. The ordering agency will be responsible for ensuring that data in transit is protected.

User Authentication. Verizon complies with **RFP Section C.2.8.6.1.4.4(17)**. The MDM platform supports user authentication from PINs, alphanumeric-based passwords,

and soft/hard tokens. Actual device functionality will depend on the operating system vendor or manufacturer API release.

User Compliance. Verizon complies with **RFP Section C.2.8.6.1.4.4(18)**. Compliance rules on the SaaS model are defined in accordance with ordering agency requirements. Specific actions can be defined when the user's device is out of compliance. A custom message can be sent to the user's device as a pop up message stating that the user's next step is to call the IT helpdesk. Another custom message can be delivered when the device compliance exception is resolved. Any violation of the device compliance is logged under the platform for reporting purposes. Multiple compliance rules and actions can be created and applied to groups. The dashboard view provides a high level view of the overall enterprise compliance status.

Alerting. The MDM platform supports all alerting requirements. Verizon complies with **RFP Section C.2.8.6.1.4.4(19)**. Alerts can be created for specific actions or violations of policies. Messages can be sent to either a group, a specific device, or as a broadcast to all user roles. Custom alerts can be created with different severity levels and can be automated or sent manually. For example, the dashboard view will report on the devices that have not checked in to the platform. Acknowledgement of these messages can be recaptured on the platform.

Audit Reports. Verizon complies with **RFP Section C.2.8.6.1.4.4(20)**. Audit reports can be created for viewing and export per specific requirements. The reporting function can be set up in a multi-tenant platform with a parent-child relationship with role based access. MDM administrator logins are tracked and all actions taken are logged. Reports can be customized to view specific policy violations.

Deployment Support. Verizon complies with **RFP Section C.2.8.6.1.4.5(1)(a)**. The MMS platform supports all deployment support requirements. Verizon maintains processes to ensure the successful deployment of its MMS solutions. Deployments are supported by a service delivery team and supervised by a dedicated program manager as needed. Verizon oversees every step of the deployment process, with project kickoff

and initial requirements gathering all the way to project steady state. The ordering agency's official signoff on the implementation moves the project to a steady state environment.

Enterprise Systems Integration. Verizon complies with **RFP Section C.2.8.6.1.4.5(2)(a)**. Where applicable, Verizon will support enterprise integration for both standard platform deployments or as part of a custom implementation addressed with an SOW. For example, active directory integration is supported within the platform along with access control mechanisms for email. Access control mechanisms prevent users from accessing the email platform unless they have an MDM platform on their devices. This requires support from the ordering agency's email platform and integration team.

Training. Verizon complies with **RFP Section C.2.8.6.1.4.5(3)(a)**. Verizon provides training with MMS platform implementation, including demonstrations of product capabilities and functionalities as well as provisioning of administrative guides and other documentation.

Help Desk. Verizon complies with **RFP Section C.2.8.6.1.4.5(4)(a)**. The Verizon MMS platform features a helpdesk-to-helpdesk approach, available from a project's pilot phase and throughout the remainder of the service lifecycle.

Stipulated Requirements. Verizon complies with the **Service Description (C.2.8.6.1)**, **Functional Definition (C.2.8.6.1.1)**, and applicable **Standards (C.2.8.6.1.2)**, **Connectivity (C.2.8.6.1.3)**, **Interfaces (C.2.8.6.3)**, and **Performance Metrics (C.2.8.6.4)** RFP requirements.

2.8.6.2 Quality of Services [L.29.2.1, M.2.1]

The Verizon MMS solution can be delivered via a variety of models based on the ordering agency TO requirements. Verizon offers a private delivery model: in a Verizon data center or an ordering agency data center; or in a FedRAMP Infrastructure as a Service (IaaS) (**Section 2.5.1**) provided by Verizon. As a result, the solution's resiliency will rely on the supporting infrastructure platform. As a platform, Verizon's facilities and

computing infrastructure are built to the high availability standards. To protect against wholesale outage risks, Verizon facilities incorporate triple-redundant power supplies, multiple carriers, intra-facility compute failure recovery processes, and geographical diversity. At the application layer, Verizon will work with the ordering agency at the TO stage to identify availability requirements of systems to be hosted and design compliant solutions. The architecture can be built to high availability and disaster recovery configurations per ordering agency configurations.

2.8.6.3 Service Coverage [L.29.2.1, M.2.1]

Verizon complies with **RFP Section C.1.3** and will support MMS in a minimum of 25 of the top 100 CBSAs.

2.8.6.4 Security [L.29.2.1, M.2.1]

The Verizon MMS is managed for security and risk per Verizon's EIS IT Risk Management Framework (RMF) Plan in **Volume 1, Attachment A**. If additional security measures are required they will be addressed at the TO level. Verizon partners to be utilized for this service meet the federal regulations and compliance requirements, including FIPS 140-2, NIAP-PP, GRI, FISMA, HIPAA and SOC2.

NIST SP 800-126. Verizon complies with **RFP Section C.2.8.6.1.4.1(6)**. The MMS solution is compliant with NIST SP 800-126 Security Content Automation Protocol (SCAP).

Application Security. Verizon complies with **RFP Section C.2.8.6.1.4.2(3)(a-e)**. The MMS solution's MAS platform supports application security in a number of ways, including the deployment of self-signed certificates. Initial application deployment and subsequent deployment of updates are tracked and audited. Applications and corresponding data usage can be tracked via time and expense management. Mobile applications that have been injected with checks to ensure fraud detection, including device jail-breaking, will be prevented from deployment. The platform supports deployment of applications that have been signed by an ordering agency's certificate.

Mobile Security. Verizon complies with **RFP Section C.2.8.6.1.4.4.** The Verizon MMS solution complies with all mobile security requirements.

Untrusted Devices and Anonymous/Unknown Users. Verizon complies with **RFP Section C.2.8.6.1.4.4(3).** Devices can be enrolled as an option subject to approval by MMS administrators if allowed by agency security policy.

Safeguard PII. Verizon complies with **RFP Section C.2.8.6.1.4.4(21).** The MMS solution is designed with PII safeguard measures as specified by NIST SP 800-122. Data classification is critical for identifying items to be protected and the appropriate security levels. Application wrapping technologies are leveraged to meet NIST and FIPS compliance guidelines.

2.8.7 AUDIO CONFERENCING SERVICE (ACS) [C.2.8.7]

2.8.7.1 Understanding [L.29.2.1, M.2.1]

Verizon proposes its existing Audio Conferencing Service (ACS) currently being delivered on Networx for EIS. Verizon ACS enables multiple participants to talk by phone simultaneously from any location. It is flexible, easy to use, and requires only a telephone (or softphone) to access a conference call. ACS will enable customers to host meetings for a wide range of business applications. ACS is available 24x7. The Verizon ACS offerings include several service levels, each providing various features that can be combined to support any size meeting, on a call-by-call basis.

ACS will give EIS subscribing agencies the flexibility to hold meetings anytime, virtually anywhere. Verizon makes it simple to arrange and conduct an audio conference with participants around the world and can support conferences of a few to several thousand participants. A high level illustration of Verizon's ACS architecture is shown in **Figure 2.8.7.1-1.**

2.8.7.1.1 Compliance with EIS Service Requirements [J.19]

Multi-Point Bridging. Verizon complies with **RFP Section C.2.8.7.1.4(1)** and supports all of the multi-point bridging capabilities specified in the EIS RFP. Verizon ACS provides a sub-conferencing feature and a self-service option with Instant Meeting capabilities. The conference leader may determine whether or not a tone or verbal announcement is heard.

Conference Set-Up Capabilities: Verizon complies with **RFP Section C.2.8.7.1.4(2)(a)-(b)** and will provide User-Controlled and Attendant-Assisted conferences. Authorized users and users with a calling card will be able to establish conference calls by dialing a designated number to access the service. Both Meet-Me and Preset automated modes are supported. Verizon provides the ability for the customer to set up their meet-me conferences using the EIS designated access methods, entering an authorization code or providing the operator with the authorization code. With a standing reservation, participants can reuse the same dial access number

and authorization code for conferences scheduled as a series of regular calls. Operators will also be able to establish a conference.

Reservation System. Verizon complies with **RFP Section C.2.8.7.1.4(3)** and supports all requirements for the ACS reservation system through eMeetings. Audio conferencing calls can be reserved by dialing one of Verizon's global reservation numbers or through its Internet reservation system. An implementation coordinator is assigned with a dedicated reservation center.

Automatic Port Expansion. Verizon complies with **RFP Section C.2.8.7.1.4(4)** and will support automatic port expansion for attended audio conferences. Verizon will provide automatic port expansion on instant (unattended or in other words without operator assistance) to support additional users to the conference in progress beyond the dial-in ports reserved as long as facilities are available.

Conference Tones. Verizon complies with **RFP Section C.2.8.7.1.4(5)**. Verizon ACS allows a customer to select entry and exit methods for participants.

Participant Count. Verizon complies with **RFP Section C.2.8.7.1.4(6)**. The conference coordinator can provide a participant list/count to the customer.

Roll Call. Verizon complies with **RFP Section C.2.8.7.1.4(7)**. Ordering agencies can request a roll call when the conference reservation is scheduled. After participants are connected, the conference coordinator can conduct a roll call.

Attendant Assistance. Verizon complies with **RFP Section C.2.8.7.1.4(8)**. A conference coordinator is available to fulfill special requests on hosted ACS calls.

Audio Recording. Verizon complies with **RFP Section C.2.8.7.2(1)**. Conference calls may be recorded via downloadable file in .mp3 or .wav format and sent to customers for later review.

Translation Services (optional). Verizon complies with **RFP Sections C.2.8.7.2(2)-(3)** and Verizon ACS supports many languages/dialects (including Spanish) through a worldwide language interpretation service, provided by a third-party vendor.

Moderator Led Q&A. Verizon complies with **RFP Section C.2.8.7.2(4)** and Verizon ACS allows ordering agencies to conduct a question and answer session facilitated by a Moderator/Conference Coordinator.

Participant List Report. Verizon complies with **RFP Section C.2.8.7.2(5)**. At the ordering agency's request, Verizon will compile a participant list for Attended Services and Instant Meeting as a self-service option via the Web Moderator.

Password Screening. Verizon complies with **RFP Section C.2.8.7.2(6)**. A conference leader may specify a customer-specific passcode that conference participants must provide before they are entered into the conference.

Download and Replay. Verizon complies with **RFP Section C.2.8.7.2(7)**. Instant Replay Plus allows callers to dial in and listen to replays of a previously held conference or other recorded audio announcement at their convenience.

Transcription. Verizon complies with **RFP Section C.2.8.7.2(8)** and upon request, will provide transcriptions of pre-recorded audio calls.

Temporary Blocking of Ports. Verizon complies with **RFP Section C.2.8.7.2(9)**. Verizon's sub-conferencing features allows for temporary blocking of audio conference participants in order to remove a subset of participants from a conference.

Secured Audio Conference (optional). Verizon complies with **RFP Section C.2.8.7.2(10)** and will support sensitive voice conferences with end-user encryption for discussions of a CUI nature between multiple locations with protection from unauthorized interception (i.e. eavesdropping).

Operator Dial-Out. Verizon complies with **RFP Section C.2.8.7.2(11)**. The service includes the capability to add a participant to a conference via an outbound call from the conference bridge initiated by the conference attendant.

Host Dial-Out. Verizon complies with **RFP Section C.2.8.7.2(12)**. Conference hosts and coordinators can initiate a call from the conference bridge to add a participant to the conference.

Executive Conference. Verizon complies with **RFP Section C.2.8.7.2(13)**. ACS supports executive conferences requiring professional moderator assistance with control of conference attendant functions.

International Global Meet. Verizon complies with **RFP Section C.2.8.7.2(14)** and Verizon ACS will provide in-country local access which is a non-North American toll number assigned to a specific country and bridge. Verizon ACS provide a single source of global collaborative services (audio, Web and video).

Host Controls. Verizon complies with **RFP Section C.2.8.7.2(15)**. ACS allows the conference host to assume control of conference attendant functions.

Stipulated Requirements. Verizon complies with the **Service Description (C.2.8.7.1)**, **Functional Definition (C.2.8.7.1.1)**, and all applicable **Standards (C.2.8.7.1.2)**, **Connectivity (C.2.8.7.1.3)**, **Interfaces (C.2.8.7.3)**, and **Performance Metrics (C.2.8.7.4)** RFP requirements.

2.8.7.2 Quality of Services [L.29.2.1, M.2.1]

Verizon ACS uses audio conferencing media servers designed to provide high capacity, scalability, fault tolerance, maintainability and redundancy. The bridging hardware is designed and manufactured specifically for the collaborative communication industry and delivers a flexible, scalable solution for audio conferencing applications and a rich development platform for Verizon's Unified Communications Service (UCS) (**Section 2.8.3**). The hardware features continuous real-time diagnostics, hot swappable and self-healing system designs and combines high port capacity and expandability with

advanced audio processing technology. [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

2.8.7.3 Service Coverage [L.29.2.1, M.2.1]

Verizon complies with **RFP Section C.1.3** and will support ACS in a minimum of 25 of the top 100 CBSAs.

2.8.7.4 Security [L.29.2.1, M.2.1]

The Verizon ACS is managed for security and risk per Verizon's EIS IT Risk Management Framework (RMF) Plan in **Volume 1, Attachment A**. If additional security measures are required they will be addressed at the TO level.

Verizon has a comprehensive security policy with clearly defined security implementation standards [REDACTED]

[REDACTED]

[REDACTED] in concert with other industry recognized baseline references, to

create a comprehensive baseline security policy tailored to the specific security needs of ordering agencies.

Verizon mandates that all employees sign a strict confidentiality and non-disclosure agreement. Verizon conferencing personnel take several precautions to help protect ordering agency's privacy. Verizon monitors conferences, and all personnel wear headsets so that only the assigned Conference Coordinator can hear what is being said. Only authorized trained personnel are involved with conference calls. When leaders establish their Instant Meeting subscriptions, they will be asked to establish the parameters of the subscription. The leader may change these options at any time prior to activating a conference. The leader can also make decisions on how they want to manage their Instant Meeting calls.

2.8.8 VIDEO TELECONFERENCING SERVICE (VTS) [C.2.8.8]

2.8.8.1 Understanding [L.29.2.1, M.2.1]

Verizon is proposing the same proven Video Teleconferencing Service (VTS) that is offered on Networx. Verizon VTS enables participants in two or more geographically dispersed locations to simulate in-person meetings efficiently and cost-effectively. VTS is not a single service but rather an umbrella of standards-based services and features designed to meet a wide array of requirements for video conferencing. Verizon refers to this suite of products as Open Video Communications (OVC). OVC enables carrier grade visual collaboration between disparate endpoints (equipment) over both private and public networks.

Video is an integral part of Verizon's UCS (**Section 2.8.3**) strategy. Verizon believes visual communications is a foundational component for organizations to resolve the challenge of managing across a distributed workforce. VTS enables ordering agencies to boost employee productivity, improve efficiency, and reduce travel costs and associated carbon emissions.

Verizon works with leading video conferencing equipment manufacturers to provide a complete video offering. VTS includes the equipment and maintenance, planning, design and implementation. EIS ordering agencies may wish to select concierge

services including end-to-end monitoring and management, concierge and reservations services, and bridging services for intra- and inter-agency meetings. [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

2.8.8.1.1 EIS Service Requirements Compliance

Simulate In-Person Meetings. Verizon complies with **RFP Section C.2.8.8.1.4(1)**. VTS enables participants in two or more geographically dispersed locations to simulate in-person meetings efficiently and cost-effectively.

Video and Sharing. Verizon complies with **RFP Section C.2.8.8.1.4(2)**. VTS supports a number of viewing options (e.g. one-way, two-way, and lecture mode meetings), as well as document sharing between participants.

Document Sharing. Verizon complies with **RFP Section C.2.8.8.1.4(3)**; VTS offers WebEx data conferencing services that can be used in conjunction with a video conference. T.120 is required for participants to interactively edit, transfer or share data files and documents within the same IPVTS data stream. The VTS production platform currently supports T.120 with H.320.

Audio Conference Add-On. Verizon complies with **RFP Section C.2.8.8.1.4(4)** and provides audio add-on capability for video conferences. Conference attendees who do not have video access can connect to the conference via an audio-only connection. For Reserved conferences, the reservationist will provide a number that audio participants can dial into, or Verizon can arrange for dial out.

Teleconferencing Bridge. Verizon complies with **RFP Section C.2.8.8.1.4(5)**. The Verizon VTS bridge platform supports connectivity to IP video endpoints, and also provides gateway functionality for interconnection of both IP- and ISDN-enabled video endpoints.

Modes of Operation. Verizon complies with **RFP Sections C.2.8.8.1.4(6)(a)-(c)**. To initiate a conference, a coordinator originates the video conference for each site 15-minutes prior to the conference. Both domestic and international calls may be dialed out. Verizon provides the ability for users in a conference to join by either a preassigned meet-me phone number or by asking a conference coordinator to dial-out to the participant. Both options are available during a teleconference.

Operator Assistance. Verizon complies with **RFP Section C.2.8.8.1.4(7)**. Verizon VTS provides operator assistance in two ways for any issues related to a videoconference. The premier service level provides real-time operator monitoring or participants request assistance.

Audio-Video Synchronization. Verizon complies with **RFP Section C.2.8.8.1.4(8)**. Verizon VTS maintains audio/video synchronization within ± 2 video frames according to the frame rate employed in videoconferences.

Point-to-Point VTS on Demand. Verizon complies with **RFP Section C.2.8.8.1.4(9)**. Users can establish point-to-point on-demand video conferences by dialing directly from one video endpoint to a second endpoint (off-MCU dialing), or by utilizing Verizon's Instant Video service, which provides MCU-based on demand video capability.

Multi-Point Arrangements. Verizon complies with **RFP Section C.2.8.8.1.4(10).**

Verizon's reservation system is used to schedule all "reserved" video conferences. The service supports interconnectivity between different networks. Parties either joining or leaving a conference can be identified either visually or with an entry/exit tone.

Video Format Conversion. Verizon complies with **RFP Sections C.2.8.8.1.4(12)(a-b).** VTS provides video format conversion capabilities that permit operation between: a) National Television System Committee (NTSC) and Phase Alternation by Line (PAL) intera, and b) NTSC and Système Electronique Couleur Avec Memoire (SECAM). VTS also supports CODECs compliant with FTR-1080.

Interoperate with Firewalls and Security Layers. Verizon complies with **RFP Section C.2.8.8.1.4(13)** and Verizon VTS will traverse and successfully interoperate with agency firewalls and security layers. Upon request, Verizon will verify with the agency that the agency firewall is compatible with this service during the service delivery process.

VTS Reports. Verizon complies with **RFP Section C.2.8.8.1.4(14)** and will provide VTS reports in accordance with individual TOs.

Attended Service. Verizon complies with **RFP Section C.2.8.8.2(1)** and will provide call monitoring, roll call, and coordination for a VTS conference.

Verification. Verizon complies with **RFP Section C.2.8.8.2(2)** and will support registration and verification of all video sites. Registration includes gathering site/video equipment information and entering it into the Verizon Reservation System. This provides support teams with critical information to better assist users. Site verification confirms that each site is functioning properly. During site verification, a site's capabilities are tested and confirmed. The results of each site verification are communicated back to the ordering agency, where the verification is either confirmed, or a mechanism to remedy any open issues is provided.

Transcoding. Verizon complies with **RFP Sections C.2.8.8.2(3)(a)-(c)** and supports CODECs compliant with FTR-1080. Support of the optional transcoding requirements will be evaluated on a task-order basis.

Rate Adaptation (optional). Verizon complies with **RFP Section C.2.8.8.2(4)** and will provide data rate adaptation capability to ensure that video endpoints operating at different data rates successfully interconnect on a video teleconference. The rate adaptation feature is supported through the reservation process, and is provided on the VTS bridge platform.

Stipulated Requirements. Verizon complies with the **Service Description (C.2.8.8.1)**, **Functional Definition (C.2.8.8.1.1)**, and all applicable **Standards (C.2.8.8.1.2)**, **Connectivity (C.2.8.8.1.3)**, **Interfaces (C.2.8.8.3)**, and **Performance Metrics (C.2.8.8.4)** RFP requirements.

2.8.8.2 Quality of Services [L.29.2.1, M.2.1]

Verizon will provide EIS ordering agencies with an effective implementation and management strategy for video conferencing services. Verizon's strategy encompasses the various aspects of the project, from initial identification of users, locations, and service requirements to billing and reporting services. Verizon has significant experience creating and delivering new or enhanced services and solutions to the marketplace.

The VTS platform was built for scalability, with 10 Gbps core nodes, and for redundancy, with redundant software, hardware, network connectivity, and geographically between sites. The VTS platform is multi-vendor and offers a wide variety of network topology and access options. VTS is designed to work with the Verizon UCS (**Section 2.8.3**).

VTS is available through VPNS and the public Internet. Use of VPNS provides additional security and the ability to use Quality of Service (QoS) for additional performance enhancement. VTS uses both switched digital and IP Service. Verizon

Conferencing Specialists are available to assist ordering agencies with network choices and will consider both economy and reliability. ISDN (PRI and BRI), IP (Internet and VPNS), and both private and public video networks are supported.

2.8.8.3 Service Coverage [L.29.2.1, M.2.1]

Verizon complies with **RFP Section C.1.3** and will support VTS in a minimum of 25 of the top 100 CBSAs.

2.8.8.4 Security [L.29.2.1, M.2.1]

The Verizon VTS is managed for security and risk per Verizon's EIS IT Risk Management Framework (RMF) Plan in **Volume 1, Attachment A**. If additional security measures are required they will be addressed at the TO level.

[REDACTED]

Secure Central Reservation System. Verizon complies with **RFP Section C.2.8.8.1.4(11)**. Verizon VTS features access to a secure central reservation system used to schedule all "reserved" video conferences. At the heart of the Verizon OVC offering is Verizon's robust VPNS, which enables ordering agencies to effectively communicate over a secure network around the globe. It also provides the foundation for automating business processes between agencies, including e-commerce, shared intranets and extranets. VPNS separates traffic through a VPN, resulting in the security and Quality of Service (QoS) of Layer 2 switching with scalability and any-to-any connectivity of IP.

Security-CUI (optional). Verizon complies with **RFP Section C.2.8.8.2(5)** and will provide transparent and secure VTS communications paths to support sensitive CUI video communications.

Security-Classified (optional). Support of optional requirements for security-classified VTS (**RFP Section C.2.8.8.2[6]**) will be reviewed on a TO basis.

2.8.9 DHS INTRUSION PREVENTION SECURITY SERVICE [C.2.8.9]

2.8.9.1 Understanding [L.29.2.1, M.2.1]

[REDACTED]

2.8.9.1.1 Compliance with EIS Service Requirements [J.19]

Process to Provide Cyber Threat Indicators. Verizon complies with RFP Section **C.2.8.9.1.4(1)**. Verizon is currently supporting the IPSS Program with [REDACTED]

[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED] S.

Demonstrate IPSS Operates as Intended. Verizon complies with RFP Section **C.2.8.9.1.4(2)** [REDACTED]
the IPSS services operate as intended when traffic is present that matches malicious

indicators. [REDACTED]
[REDACTED]

Process that Allows DHS to Direct Actions on Network Traffic. Verizon
complies with RFP Section C.2.8.9.1.4(3) and [REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]

Receive, Accept, Utilize, and Secure GFI. Verizon complies with RFP Section
C.2.8.9.1.4(4) and [REDACTED]
[REDACTED]
[REDACTED].

Automated Means for DHS to Share and Utilize GFI. Verizon complies with
RFP Section C.2.8.9.1.4(5) [REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]

**Leverage Cyber Threat Information and/or DHS IPSS Functional
Capabilities.** Verizon complies with RFP Section C.2.8.9.1.4(6). [REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]

Ensure Application of DHS-Approved Indicators. Verizon complies with RFP
Section C.2.8.9.1.4(7) and [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

Application of Mitigation Capabilities. Verizon complies with RFP Section C.2.8.9.1.4(8) and [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

Non-Disclosure of GFI. Verizon complies with RFP Section C.2.8.9.1.4(9). GFI is not disclosed or shared with any third party or used for purposes not authorized by

[REDACTED]

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

[REDACTED].

Access Approved Federal System Network Traffic. Verizon complies with RFP Section C.2.8.9.1.4(10). [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

Ability to Detect Malicious Network Traffic. Verizon complies with RFP Section C.2.8.9.1.4(11). [REDACTED]

[REDACTED]

[REDACTED]

Support Emerging Detection Methods. Verizon complies with RFP Section C.2.8.9.1.4(12). [REDACTED]

[REDACTED]

[REDACTED]

Detection Malicious Activity within Encrypted Traffic. Verizon complies with RFP Section **C.2.8.9.1.4(13)**. [REDACTED]

Support Unclassified and/or Classified Protection Measures. Verizon complies with RFP Section **C.2.8.9.1.4(14)**. [REDACTED]

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

Ability to Redirect to a Safe Server. Verizon complies with RFP Section **C.2.8.9.1.4(15)**. The current Verizon solution has the ability to redirect DNS traffic to a safe server. Any other application will be addressed as requested in future EIS TOs.

Capturing/Storing Analytically Relevant Data. Verizon complies with RFP Section **C.2.8.9.1.4(16)** [REDACTED]

Retain Only Traffic Associated with Suspected Malicious Activity.

Verizon complies with RFP Section **C.2.8.9.1.4(17)**. The Verizon solution has multiple inspection and enforcement points to verify that only authorized traffic is inspected and only suspected malicious activity is retained. Traffic that is sent for inspection must pass through multiple routers and firewalls, which have access controls programed for authorized traffic only.

Apply DHS-directed Prevention Services. Verizon complies with RFP Section **C.2.8.9.1.4(18)**. The Verizon IPSS team includes Program Management, Operations and IT development teams that support the IPSS service. [REDACTED]

Approved Traffic Aggregation Solution. Verizon complies with RFP Section **C.2.8.9.1.4(19)**. [REDACTED]

Operate as an In-Line Service. Verizon complies with RFP Section **C.2.8.9.1.4(20)** [REDACTED]

Define and Apply DHS IPSS Functional Capabilities at Cyber-Relevant Speed. Verizon complies with RFP Section **C.2.8.9.1.4(21)** and will continue to support the evolution of the IPSS service and define and support a full range of existing and future DHS Intrusion Prevention Services and capabilities. [REDACTED]

Provide Quarantined Malware via the US-CERT Malware Lab. Verizon complies with RFP Section **C.2.8.9.1.4(22)** [REDACTED]

Demonstrate Indicators/Signatures/Countermeasures Operate as Intended. Verizon complies with RFP Section C.2.8.9.1.4(23) [REDACTED]

[REDACTED]

Provide Detection Alerts and Information on Suspicious Traffic. Verizon complies with RFP Section C.2.8.9.1.4(24) [REDACTED]

[REDACTED]

Data to Support Network Traffic Pattern Assessments. Verizon complies with RFP Section C.2.8.9.1.4(25) [REDACTED]

[REDACTED]

Information Related to Indicators/Signatures/Actions/Alerts. Verizon complies with RFP Section C.2.8.9.1.4(26) [REDACTED]

[REDACTED]

Ensure Non-Disclosure of Agency Network Traffic. Verizon complies with RFP Section C.2.8.9.1.4(27). [REDACTED]

[REDACTED]

Testing. Verizon complies with RFP Section C.2.8.9.1.4(28). [REDACTED]

[REDACTED]

15-Minute Discovery Notification. Verizon complies with RFP Section C.2.8.9.1.4(29). [REDACTED]

Detection and Countermeasures. Verizon complies with RFP Section C.2.8.9.2(1-3). [REDACTED]

Stipulated Requirements. Verizon complies with the **Service Description (C.2.8.9.1)**, **Functional Definition (C.2.8.9.1.1)**, and applicable **Standards (C.2.8.9.1.2)**, **Connectivity (C.2.8.9.1.3)**, **Interfaces (C.2.8.9.3)** and **Performance Metrics (C.2.8.9.4)** RFP requirements.

2.8.9.2 Quality of Services [L.29.2.1, M.2.1]

Verizon understands and will comply with all GSA IPSS requirements. Verizon is currently a certified IPSS provider [REDACTED]



2.8.9.3 Service Coverage [L.29.2.1, M.2.1]

Verizon complies with **RFP Section C.1.3** and will support IPSS in a minimum of 25 of the top 100 CBSAs.

2.8.9.4 Security [L.29.2.1, M.2.1]

The Verizon IPSS is managed for security and risk per Verizon's EIS IT Risk Management Framework (RMF) Plan in **Volume 1, Attachment A**. If additional security measures are required they will be addressed at the TO level.

The Verizon IPSS has the following security architectural components and benefits built into the design:

1. Verizon Internet Service, supported by Verizon internal security policies and guidance.
2. Design components that support the sensor and the sensor data center and associated architectural components. These comply with appropriate Intelligence Community Directives (ICD) and DHS Security requirements.
3. DHS-approved solution that has undergone DHS compliance testing. The system has been fully tested and is supported by DHS-vetted and approved program management and operations teams.

2.9 Access Service [C.2.9]

2.9.1 UNDERSTANDING [L.29.2.1, M.2.1]

Access Arrangements (AAs) connect the SDP at an ordering agency location to a Point of Presence (POP) on Verizon's network. The range of line speeds and reliability options Verizon offers provides ordering agency with choices and options they can rely on to satisfy their diverse access needs. Verizon AAs include U.S. domestic and international access.

Access using TDM, Ethernet, Wave, etc. Verizon is the only provider that offers and has provided every type of access: including Time Division Multiplexing (TDM), Ethernet, Cable, Optical Wave Service, Digital Subscriber Line (DSL), Satellite, Dark Fiber Service (DFS), cellular based wireless and other custom arrangements requested by the Government on both the Networx and WITS contracts. Verizon's extensive experience providing all types of access arrangements on both Networx and WITS makes Verizon a low-risk choice for agencies during and after their transition to EIS.

2.9.1.1 Compliance with EIS Service Requirements [J.19]

Options for Customized AA. Verizon complies with **RFP Section C.2.9.1.1(1)-(3)** and will support all of the options for customized access arrangements referenced in the RFP. This will include physically diverse paths from SDP to the POPs of two different contractors, diverse paths from the SDP to the Verizon POP, and redundant paths from the SDP to the Verizon POP.

Special Construction. Verizon complies with **RFP Section C.2.9.1.1(1)-(2)**. Verizon will provide special construction services for the situations specified in the RFP. This will include construction of new access arrangements and enhancement of existing arrangements to increase capacity as requested by the ordering agency. Verizon will also perform special construction to implement alternate routes when deemed necessary as agreed upon by Verizon and the customer.

Site Surveys. Verizon complies with **RFP Section C.2.9.1.1**. On the Network contract today, Verizon's standard practice is to perform a site survey as needed in support of every special construction project, and will continue to do so on EIS. Verizon will continue to deliver a site survey report after the completion of each physical site visit.

AA Capabilities. Verizon complies with **RFP Sections C.2.9.1.4(1)-(2)**. Verizon AA will support integrated access to numerous services, including: voice services, private lines, Private IP and Public IP, along with services that use these technologies as the transport layer. Verizon has demonstrated its ability to support access for these services in both urban and rural areas on the existing telecommunication contracts, and we will continue to support all required forms of access for EIS. AA will support transparency to any protocol.

T1. Verizon complies with **RFP Sections C.2.9.1.4(1)(a)-(b)**. Verizon will provide a T-1 circuit to the customer location. In support of channelized circuit requirements, Verizon will offer a channel bank as an equipment option to perform the channelization.

ISDN PRI. Verizon complies with **RFP Section C.2.9.1.4(2)**. PRI service is delivered on one or more T1 carriers (often referred to as 23B+D) of 1544 Kbps (24 channels). A PRI has 23 "B" channels and 1 "D" channel for signaling. Verizon currently provides these on PRIs on the Network contract, and will continue to support this requirement for EIS.

ISDN BRI. Verizon complies with **RFP Section C.2.8.1.4(3)**. ISDN consists of two “B” channels and one “D” channel. This form of access is often used for voice services and basic data services.

T3. Verizon complies with **RFP Sections C.2.9.1.4(4)(a)-(b)**. Verizon will provide a circuit to the customer location. In support of channelized requirements, Verizon will offer an M1-3 mux as an equipment option to perform the channelization.

E1. Verizon complies with **RFP Sections C.2.9.1.4(5)(a)-(b)**. Verizon will provide an E1 circuit to the customer location. In the case of the channelized requirements, Verizon will offer a channel bank as an equipment option to perform the channelization. In general, E1s are ordered only in foreign countries; for the U.S., a request will be accomplished by binding two T1s, with equipment is added to bond the two circuits.

E3. Verizon complies with **RFP Sections C.2.9.1.4(6)(a)-(b)**. Verizon will provide an E3 circuit to the customer location. In the case of the channelized requirements, Verizon will offer a mux as an equipment option to perform the channelization. For E3s in the U.S., Verizon will provide a DS3 circuit with equipment placed to limit the bandwidth from a DS3 to an E3 connectivity.

SONET OC-3. Verizon complies with **RFP Sections C.2.9.1.4(7)(a)-(b)**. OC3 is a network line with a transmission data rate of up to 155.52 Mbps (payload: 148.608 Mbps; overhead: 6.912 Mbps, including path overhead) using fiber optics. Depending on the system, OC3 is also known as STS3 (electrical level) and STM1 (SDH). While the great majority of requests are for un-channelized connectivity, in order to channelize the circuits, Verizon will offer equipment and cards to provide DS3 circuits as requested.

SONET OC-12. Verizon complies with **RFP Sections C.2.9.1.4(8)(a)-(b)**. OC12/STM4 is a network line with transmission speeds of up to 622.08 Mbps (payload: 601.344 Mbps; overhead: 20.736 Mbps). Verizon will order these services directly from the local providers to provision required network connections. For channelized service,

Verizon will add equipment to channelize the circuits, whether DS-3 or OC-3c, as requested by the customer.

SONET OC-48. Verizon complies with **RFP Sections C.2.9.1.4(9)(a)-(b)**. OC-48 is a network line with transmission speeds of up to 2488.32 Mbps (payload: 2405.376 Mbps [2.405376 Gbps]; overhead: 82.944 Mbps). Verizon will order these services directly from the local providers to provision required network connections. For channelized service, Verizon will offer equipment to channelize the circuits, whether DS-3, OC-3c, or OC-12c, as requested by the customer.

SONET OC-192. Verizon complies with **RFP Sections C.2.9.1.4(10)(a)-(b)**. OC-192 is a network line with transmission speeds of up to 9953.28 Mbps (payload: 9510.912 Mbps [9.510912 Gbps]; overhead: 442.368 Mbps). Verizon will order these services directly from the local providers to provision required network connections. For channelized service, Verizon will offer equipment to channelize the circuits, whether DS-3, OC-3c, OC-12c, or OC-48c, as requested by the customer. An alternative is to provide 10G wave access with TDM cards to offer comparable bandwidth at lower cost.

SONET 768. Verizon complies with **RFP Sections C.2.9.1.4(11)(a)-(b)**. OC-768 is a network line with transmission speeds of up to 39,813.12 Mbps (payload: 38,486.016 Mbps [38.486016 Gbps]; overhead: 1,327.104 Mbps [1.327104 Gbps]). Verizon will order these services directly from the local providers to provision required network connections. For channelized service, Verizon will offer equipment to channelize the circuits, whether DS-3, OC-3c, OC-12c, OC-48c, or OC-192c, as requested by the customer. An alternative is to provide 40G wave access with TDM cards to offer comparable bandwidth at lower cost.

Analog Line (4 KHz). Verizon complies with **RFP Section C.2.9.1.4(12)**. Where telephone access is widely available, dial-up remains useful, and in fact is often the only choice available for rural or remote areas. As needed, Verizon will acquire a POTS line on behalf of the customer to provision this form of access; usage charges and other related charges will be part of the service fee, and will be charged as IPS service. At

present, most federal customers have already transitioned from this form of access to another form of access. This legacy technology is being replaced by cable access and cellular in most rural areas.

DS0. Verizon complies with **RFP Section C.2.9.1.4(13)**. Digital Signal 0 (DS0) is a basic digital signaling rate of 64 kbps, corresponding to the capacity of one voice-frequency-equivalent channel.[1] The DS0 rate, and its equivalents E0 and J0, form the basis for the digital multiplex transmission hierarchy in telecommunications systems used in North America, Europe, Japan, and the rest of the world, for both the early plesiosynchronous systems such as T-carrier and for modern synchronous systems such as SDH/SONET. In most cases, Verizon provisions a DS-0 in multiples through a muxed DS-1.

Subrate DS0. Verizon complies with **RFP Section C.2.9.1.4(14)**. Subrate DS-0s have been grandfathered by most carriers today. As needed, Verizon will provide Subrate DS-0 by ordering a DS-0 access and reducing speeds as required. Verizon believes that Subrate DS-0 speeds will eventually be phased out as services are transitioned to more modern options, such as cellular-based access or broadband cable offerings.

Optical Wavelength. Verizon complies with **RFP Sections C.2.9.1.4(15)(a)-(d)**. Verizon AA will support all of the speeds requested. Verizon uses state-of-the-art DWDM technology that enables several streams of digital information to be put on different wavelengths of light, eliminating interference with one another. This will allow transport of up to 96 channels in a single strand of fiber, which translates into higher capacity and lower cost. Verizon fully supports bi-directional wavelengths (WDM), and has extensive partnerships around the world to supplement coverage in areas outside its footprint.

Dark Fiber. Verizon complies with **RFP Sections C.2.9.1.4(16)(a)-(c)**. Verizon will support all bands required. Dark fiber capacity is typically used by network operators to build SONET and dense wavelength division multiplexing (DWDM) networks, usually involving meshes of self-healing rings. Now, it is also used by end-user enterprises to

expand Ethernet local area networks, especially since the adoption of IEEE standards for Gigabit Ethernet and 10 Gigabit Ethernet over single-mode fiber. Running Ethernet networks between geographically separated buildings is a practice known as "WAN elimination." Verizon will acquire and configure dark fiber as required to meet customer requirements. As needed, Verizon will support either multi-mode or single mode fiber; note that these options will only be available with dark fiber service.

DSL. Verizon complies with **RFP Sections C.2.9.1.4(17)(a)(1)-(3)**. Digital Subscriber Line (DSL) is a family of technologies that are used to transmit digital data over telephone lines. The term DSL is widely understood to mean asymmetric digital subscriber line (ADSL), the most commonly installed DSL technology, for Internet access. DSL service can be delivered simultaneously with wired telephone service on the same telephone line. This is possible because DSL uses higher frequency bands for data. On the customer premises, a DSL filter on each non-DSL outlet blocks any high-frequency interference to enable simultaneous use of the voice and DSL service. SDSL is a type of DSL, which is used for transferring data over copper telephone lines. "Symmetric" means that an SDSL connection has the same maximum upload and download speeds. Verizon embraces both technologies, and has an extensive network that will be used as required by the customer. Verizon supports all the requested speeds in Section C for ADSL, SDSL, and the optional ISDN.

Ethernet. Verizon complies with **RFP Sections C.2.9.1.4(18)(a)(1)-(5)**. Verizon AA will support requirements for Ethernet Access for speeds from 1 Mbps to 100 Gbps. The required increments will be supported through traditional Network to network interfaces. Verizon will support speeds of 10 Gbps and above using dedicated loop technology.

Cable High-Speed. Verizon complies with **RFP Sections C.2.9.1.4(19)(a)(1)-(3)**. Verizon AA will support all cable high speed rates required. Cable Internet is a high speed connection that utilizes existing cable television coaxial cable to transfer and receive data from a computer via the Internet. Fortunately, users of this option do not have to be a current cable television subscriber to take advantage of high speed cable

Internet service, as the service is offered on a standalone basis. Verizon currently provides cable high speed access on the Networx contract; we have extensive provider relationships to offer these services wherever available. It should be noted that Verizon was the only contractor to bid this form of access on Networx, and we will be prepared to support this option on EIS from day one.

[REDACTED]

[REDACTED]

Wireless. Verizon complies with **RFP Sections C.2.9.1.4(21)(a)(1)-(b)(8)**. Verizon AA will support wireless access via both fixed wireless and cellular access methods. Verizon currently supports point-to-point microwave on both unlicensed and licensed frequencies on the Networx Universal contract and will continue to support these options on EIS.

Stipulated Requirements. Verizon complies with the **Access Arrangements Description (C.2.9.1)**, **Functional Definition (C.2.9.1.1)**, and all applicable **Standards (C.2.9.1.2)**, **Connectivity (C.2.9.1.3)**, **Access Diversity and Avoidance (C.2.9.2)**, and **Interfaces (C.2.9.3)** RFP requirements.

2.9.2 QUALITY OF SERVICES [L.29.2.1, M.2.1]

To assure ongoing quality of its access arrangements, Verizon Carrier Access Group holds meetings with its providers periodically to assure that they continue to provide mandated service qualities, including mean-time-to-repair and throughput. Our contracts with the vendors meet or exceed the requirements mandated under the EIS RFP. Verizon's network architecture and interconnects allow reliable TDM service, and to further assure quality of service redundancy and dual entrances are built into Verizon POPs. [REDACTED]

[REDACTED]

[REDACTED] Verizon customer premise equipment can also easily accommodate larger bandwidth requirements with logical provisioning.

2.9.2.1 Ethernet Access

Verizon now offers Ethernet Access in nearly 90 percent of the United States population and maintains relationships with over 350 global partners to offer Ethernet service in 90 countries. Verizon has been adding over 300 access network-to-network arrangements per year, which is in addition to the more than 7,000 on-net Verizon lit buildings where service is available today. Since Verizon already provides all forms of access as mandated under the EIS RFP, GSA can be assured that Verizon is ready to meet ordering agency's needs as soon as required.

Verizon Ethernet access can be delivered through a variety of methods, including Ethernet Hybrid Fiber Coax, Ethernet-over-Gigabit Passive Optical Network (GPON), Ethernet-over-Copper, or Ethernet-over-Fiber. In some cases, access may be provisioned through Verizon-owned hardware placed at the customer premises. This hardware delivers traffic from many customers to an aggregation point, or POP, in Verizon's network. The aggregation point has connections to the edge devices on Verizon's Private IP Network Service (EIS Virtual Private Network Service (VPNS)), Public IP (Internet), and Ethernet networks. As stated above, Verizon has over 350 global partners for these direct connections. Verizon has reached out to small and regional carriers to [REDACTED]

[REDACTED]

[REDACTED]

Verizon's Ethernet services are based on Converged Packet Architecture (CPA) technology and architecture as an approach to building metropolitan and local access networks. The CPA architecture focuses on Ethernet and IP-based services, such as Metropolitan Private Line Ethernet (MPLE), Internet Dedicated Ethernet (IDE - public Internet access using Ethernet connections) and Ethernet access to Verizon's VPNS. In Verizon's CPA network, Ethernet is being used as an encapsulation protocol only, not for its bridging functions. As such, no forwarding decisions will be made based on source or destination addressing of users' Ethernet packets. This allows for

uncompromised individual Ethernet switching devices to scale to greater capacity than previously possible.

The use of Ethernet in Verizon's CPA network architecture offers many advantages to GSA and related agencies. Agencies will be able to connect to Verizon's global network via secure Ethernet interfaces at speeds from 1 Mbps. up to 10 Gbps. Further, As demands for greater bandwidths increase, Verizon will above 10 Gbps. Since Ethernet can accommodate such wide ranges of speeds, Agencies can easily grow their bandwidth without traditional provisioning delays and without being tied to the common TDM bandwidth granularities. This allows Verizon to offer very dynamic and flexible services.

The available Ethernet handoffs at the customer premises include commonly used standard electrical and optical interfaces such as 10BaseT, 100BaseT (FastE), 100BaseFX (Optical FastE), and Gigabit Ethernet (GigE) (Single or Multi-Mode Fiber). Ethernet access data speeds are available (no oversubscription): 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 15, 20, 25, 30, 35, 40, 45, 50, 60, 70, 80, 90, 100, 150, 200, 250, 300, 350, 400, 450, 500, 600, 700, 800, 900 Mbps, and 1 and 10 Gbps. For speeds above 1 Gbps, Verizon will generally use wave technology using Ethernet handoffs at the customer edge to provide the lowest cost solution available for the government.

2.9.2.1.1 Ethernet Access Network Architecture

Verizon Access Arrangement solutions often involve highly customized designs that are developed in support of specific customer requirements, rather than a single type of access. **Figure 2.9.2.1.1-1** depicts examples of several different Ethernet AA configurations. The figure illustrates Verizon's support for all forms of Ethernet Access, whether under the contract definition of dedicated or shared. Typical Shared arrangements from the customer premises, the circuit will either use the Verizon network or another network to connect to the closest network-to-network interconnection. The circuit then travels to the individual service node, whether public Internet, private Internet, or end-to-end Ethernet service. Dedicated Access is when the circuit connects directly from the agency premises to the Verizon Long Distance POP.

2.9.2.2 Wavelength Access

Custom Optical Solutions delivers Dedicated Wavelength Services with Ethernet GigE and 10GigE Local Area Network Physical Layer (LAN PHY) customer handoffs at circuit speeds up to 10 Gbps. These optical services can be used to access a variety of Verizon services. Verizon uses both its own networks and those of competitive carriers to provide wavelength services. These services can currently be provisioned through 40 Gbps and as commercial equipment becomes more readily available will support 100 Gbps.

2.9.2.3 Wireless Access (Fixed Wireless)

Verizon has been a leader in providing unique access solutions for the government through both the Networx and WITS contracts. Recently Verizon designed a hybrid access arrangement solution [REDACTED]

[REDACTED]. The solution, shown in **Figure 2.9.2.3-1**, combined both microwave (Fixed Wireless) and Ethernet access and it allowed Verizon to provide Ethernet access to various remote locations where traditional access arrangements were either not available or would have come at a much higher price due to special construction costs. Verizon has used fixed wireless for many solutions to extend networks to temporary locations, create last mile diversity,

and, as described above, to provide access in rural areas. All use of cellular is included in the wireless service section of the contract and is not included as a mandatory form of access. As a means to back-up access Verizon is fully prepared to provide cellular as a means of access and will propose this as part of individual agency TUC requirements, similar to the United States Army Reserve Command (USARC) today on Network.

2.9.3 SERVICE COVERAGE [L.29.2.1, M.2.1]

Verizon will support EIS services in a minimum of 25 of the top 100 CBSAs and in compliance with **RFP Section C.1.3** will provide AA to all government locations within each of its selected CBSAs.

2.9.4 SECURITY [L.29.2.1, M.2.1]

Verizon's designs are fully compliant with the Federal security policy and required presented in the EIS SOW. Further, Verizon has a stringent set of internal security policies that address physical, personnel, operations, technology, and protection of customer data. In addition, Verizon is a carrier and subject to FCC regulations in regards to additional security controls and practices.

The Verizon AA is managed for security and risk per Verizon's EIS IT Risk Management Framework (RMF) Plan in **Volume 1, Attachment A**. If additional security measures are required they will be addressed at the TO level.

In provisioning, Verizon uses e-bonding to work with carriers directly so that information exposure is kept to a minimum. Verizon's network facilities require all workers to display a badge at all times and access is restricted by card entry only. All POPs are designed

using dual entrances and dual connections and Verizon's interconnections with carriers in these facilities do not directly interconnect to the network, which eliminates exposure to problems that the local provider may be experiencing.

2.10 Service Related Equipment (SRE) [C.2.10]

2.10.1 UNDERSTANDING [L.29.2.1, M.2.1]

Verizon is a leading reseller of telecommunications and information technology products to commercial and government agencies worldwide. Verizon has established relationships with over 3,000 vendors and original equipment manufacturers (OEMs). Verizon provides a robust portfolio of voice, data, video, and security products and customer premises equipment to over 200 federal departments and agencies. Verizon offers these services today via multiple federal contract vehicles, including Washington Interagency Telecommunications System 3 (WITS3) and GSA CONNECTIONS.

Verizon's SRE offerings include equipment required for all EIS mandatory and proposed optional services including switches, routers, PBXs, telephones, servers, firewalls, conferencing-related equipment, microwave systems, free-space optic systems, surveillance systems, sensors, radio-related equipment, satellite earth stations and wireless phones. PBXs, voice-over-IP (VoIP) hardware and software, handsets, video- and audio-conferencing hardware and software, data communications devices, storage, free space optics, and satellite networks devices. Verizon will continually refresh SRE offerings throughout the life of the contract.

Verizon provides an objective, vendor-independent approach to delivering SRE. Verizon provides multiple choices of equipment for each SRE classification.

Verizon has a large group of support personnel across the EIS CBSAs to provide SRE maintenance 24x7. This group maintains a staff of personnel with security clearances for installation and/or configuration as required. Verizon's maintenance plans can be tailored to meet ordering agencies' specific needs and further protect their SRE investments.

2.10.1.1 Compliance with EIS Service Requirements [J.19]

Service Related Equipment. Verizon complies with **RFP Section C.2.10**. When identified in a TO, Verizon will provide networking and security service related equipment, as well as hardware and materials that are incidental to the installation, operation and maintenance of EIS services. All equipment procured via the SRE catalog provided to the government will be new and not previously used or refurbished.

Warranty Service. Verizon complies with **RFP Section C.2.10.1**. Verizon will provide, at no additional cost, a minimum one-year system warranty (or the warranty provided by the OEM, whichever is longer) for all repairs and software ordered under this contract, including all equipment supplied, installed, and integrated by Verizon. The equipment warranty will provide for hardware repairs and the distribution of updated software. Verizon will provide warranty information associated with each product and service delivered to the GSA Contracting Officer (CO) or Ordering Contracting Officer (OCO), if requested. Verizon will repair or replace malfunctioning equipment covered by warranty within five business days or as specified in the TO. Verizon will provide to the government a point of contact for the warranty from 7:00 a.m. – 7:00 p.m. Local Time or for a longer period if so specified in the TO. The warranty shall begin at the time the SRE is delivered.

Verizon will maintain Verizon-provided SRE beyond the warranty period if the customer orders post-warranty maintenance. Verizon will also provide support for discontinued products as long as parts are available from non-OEM suppliers that meet EIS requirements.

2.10.2 QUALITY OF SERVICES [L.29.2.1, M.2.1]

Based on EIS TOs, the Verizon provided SRE will be commercially available and require no additional development. Verizon will verify that all Verizon-provided SRE is compatible with EIS services.

2.10.3 SERVICE COVERAGE [L.29.2.1, M.2.1]

Verizon complies with **RFP Section C.1.3** and will support SRE in a minimum of 25 of the top 100 CBSAs.

2.10.4 SECURITY [L.29.2.1, M.2.1]

Verizon will recommend or offer the requested SRE that meets the security requirements as defined in a particular TO. The Verizon SRE is managed for security and risk per Verizon's EIS IT Risk Management Framework (RMF) Plan in **Volume 1, Attachment A**. If additional security measures are required they will be addressed at the TO level.

2.11 Service Related Labor (SRL) [C.2.11]

2.11.1 APPROACH

Verizon offers GSA and ordering agencies professional services labor under the EIS contract through Verizon's professional services, its proven partners, and third party vendors (TPVs). Verizon will identify and source subject matter experts from its professional services staff directly, or through a combination of Verizon, partner, and TPV staff as required on a particular TO. [REDACTED]

[REDACTED]

Verizon successfully delivers integrated labor resources on both the WITS 3 and Networx contracts today.

As part of its IT, security, and communication solutions for federal agencies, Verizon has built strategic partnerships with some of the nation's leading professional service organizations. Through these partnerships, Verizon is able to deliver high-level services for complex technology solutions, scale nationwide with a broader professional services capability, support customers earlier in the technology decision lifecycle; solve complex integration and deployment issues economically, and provide resources with appropriate security clearances, as required.

In response to an EIS TO, Verizon's Program Management Organization will leverage Verizon's Vendor Management team, the Verizon Professional Services group, and

Verizon TPV to support the TO-specific requirements. Verizon will identify, evaluate, and select the appropriate internal, external, and management team to deliver the required service.



Figure 2.11-2 identifies many of the infrastructure labor-based service areas where Verizon offers support through its own Professional Services or supporting partner and TPV.

Figure 2.11.1-2. EIS SRL Services

Service Area	Description
Architecture Design	[Redacted]
	[Redacted]
	[Redacted]
	[Redacted]
	[Redacted]
	[Redacted]
	[Redacted]
	[Redacted]
	[Redacted]
	[Redacted]
[Redacted]	[Redacted]
[Redacted]	[Redacted]

Service Area	Description
	<ul style="list-style-type: none"> [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED]
	<ul style="list-style-type: none"> [REDACTED] [REDACTED] [REDACTED]
	<ul style="list-style-type: none"> [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED]
	<ul style="list-style-type: none"> [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED]
	<ul style="list-style-type: none"> [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED]

2.11.2 SERVICE COVERAGE [L.29.2.1, M.2.1]

Verizon complies with **RFP Section C.1.3** and will support SRL in a minimum of 25 of the top 100 CBSAs.

2.11.3 SECURITY REQUIREMENTS

As required on a TO, Verizon will provide cleared SRL staff. Further, Verizon will confirm that any partner staff meet the stated personnel security requirements in a TO.

[REDACTED]

[REDACTED]

[REDACTED]

The Verizon SRL is managed for security and risk per Verizon's EIS IT Risk Management Framework (RMF) Plan in **Volume 1, Attachment A**. If additional security measures are required they will be addressed at the TO level.

2.12 Cable and Wiring (C&W) [C.2.12]

2.12.1 UNDERSTANDING [L.29.2.1, M.2.1]

Verizon employs a proven systematic approach to Information Systems Engineering, Installation, and Testing for Cable and Wiring (C&W) to translate EIS TO requirements and performance objectives into design criteria and specifications for the implementation of individual elements and subsystems that will make up that system.



Network Implementation C&W Management Tasks	
<ul style="list-style-type: none">▪ MDF/IDF/Wiring Closet Assessment, Clean-Up, Re-Engineering and Modernization▪ Cable Plant, Cable Trays, Station Wiring, Termination and Patch Panels Survey and Redesign▪ Riser, Backbone, Conduit & Horizontal Distribution Systems Assessment and Design▪ Cable Plant Routing and Re-Engineering & Install (including Cable Trays, Underfloor Cabling, etc.)▪ Cable Plant Management System Integration with BMC or equivalent service management systems▪ Cable Plant Management System Database Population and Data Validation▪ SLA Management (MACD, Fault, Performance & Troubleshoot)▪ End-point Drops and Patch Panel Reengineering and Install	<ul style="list-style-type: none">▪ Cable Plant Validation and Acceptance Testing▪ Cable Plant Drawing and Documentation▪ Cable Plant Management System Installation and Configuration▪ Cable Plant Management System Operational Readiness Testing▪ Structured Cabling, Terminations & Patching Service Management▪ IDF/MDF Environmental and Power Management▪ Cable Plant, Terminations and Patch Panel Security▪ Wiring Closets/IDF/MDF Security Management▪ Cable Plant Testing Record Retention▪ Cable Plant Component Sparing▪ Cable Plant Testing Tools▪ Quality Control and Quality Assurance

In accordance with industry guidelines for Inside Plant racking and cable management appearance, all new cabinets, equipment racks, cable trays, fiber optic patch panels (FOPPs), splice cases, and horizontal and vertical cable infrastructure installed by Verizon will use commercially proven products and best practices. Verizon tracks cable outages with network management software (NMS) and follows MACD procedures for prompt resolution.

Additional ladder racking provisioned by Verizon will match existing ladder racking in the telecommunications room and will be labeled according to BICSI and ANSI/TIA/EIA

standards for horizontal cabling. Verizon will run and label fiber and copper cables at each end for easy identification per ANSI/TIA/EIA-606. Verizon will integrate capacity planning into its cable and wiring service per industry and government standards. As an example, Verizon would size a new HVAC system to support heat loads and BTU requirements of the proposed network element, and would also including an additional 25 percent capacity for future requirements based on the industry standard of 25 percent growth capacity for port counts, cable tray usage, and cable infrastructure.

Rather than using a boilerplate test plan, Verizon's approach to network-centric testing addresses the end-to-end throughput, latency, jitter, and capacity objectives across the network infrastructure. If needed, Verizon will develop and submit a site-specific Transport Network Test Plan to address end-to-end throughput and capacity objectives.

Verizon will inventory equipment and enter pertinent information into its materials and asset-tracking database, continually updating it as the material is moved to the project location. If required, Verizon will supply additional racking required for mounting new UPS systems and battery packs needed to provide sufficient hold-over power for network equipment (switches, routers, and servers).

2.12.1.1 Inside Cable Plant Management Drawings

Verizon will perform sufficient commercial testing to confirm that the installed Inside Plant meets the specifications of the TO. Results will be recorded and provided to the appointed Point of Contact (POC) and/or Lead Engineer with complete and comprehensive documentation of the test.

Table 2.12.1.1-1. Inside Cable Plant Drawings

Cable Plant Drawings
The Customer Edge (CE) Router is the IP router at the agency site that connects to the PE router. The CE is a routing peer of the Inside Plant Drawings . Verizon will provide as-built Inside Plant drawings to reflect actual installation, including but not limited to: new equipment, new cable paths, new power components/circuits, and new grounding system components, etc.
Rack Face Elevation Drawings. Verizon will provide Rack Face Elevations for equipment to reflect actual installation. At a minimum, the level of detail will include manufacturer and model of equipment installed, how it is equipped, patch panels, cable management specifics, and other equipment installed.
Floor Plan Drawings. If the selected equipment does not fit the footprint provided in the Engineering Design Plan, Verizon will red-line the Inside Plant drawing to reflect the required footprint.

2.12.1.1 Compliance with EIS Service Requirements [J.19]

Installation Services. Verizon will comply with **RFP Section C.2.12**. Verizon will provide installation services for equipment necessary to provide telecommunications

services and related supporting IT services. Verizon will also provide the required connectivity using appropriate cabling and wiring, and related trenching, ducting, grounding, and lightning protection systems in accordance with the TO and appropriate standards. Site preparation work done by Verizon under this contract will conform to applicable federal, regional and local codes as well as to accepted industry installation and construction practices.

Building Services. Verizon will comply with **RFP Section C.2.12** and agrees that all planned work and code compliance will be subject to OCO review and approval prior to the start of work. Verizon will provide the tools and test equipment to perform the site preparation as specified in the TO, provide temporary utilities that are not available in the work area, and coordinate any disconnection of utilities. Verizon will provide building additions and/or changes as required to support the telecommunications and IT installation according to individual TO requirements.

Power Systems and Warranty. Verizon will comply with **RFP Section C.2.12** and will expand or modify power systems to provide appropriate environmental controls to support the installation. Verizon will provide a warranty period of at least one (1) year for the premises wiring/cabling after service acceptance.

2.12.2 QUALITY OF SERVICES [L.29.2.1, M.2.1]

Verizon's infrastructure network integration process incorporates system-of-systems planning and design. Verizon will determine the interoperability at interfaces within and external to the system (hardware and software), including the necessary supporting equipment and facilities, and other systems and equipment that will be present or required in the operational environment. Verizon will also conduct or support investigations of systems performance, systems integration, systems interoperability, and problems with fielded systems and recommending alternative solutions. This provides the required flexibility and service coverage needed to accommodate growth, evolution in service requirements, advances in technology, and changes in the regulatory environment.

2.12.2.1 Site Survey

During a standard site survey, Verizon will collect, collate, analyze, and document the technical and supporting information required to complete the detailed engineering of the supporting structures and cable plant upgrade defined in the TO. This detailed information will enable the development of an engineering design to satisfy the infrastructure requirements and the supporting structures and cable spreadsheets.

2.12.3 SERVICE COVERAGE [L.29.2.1, M.2.1]

Verizon complies with **RFP Section C.1.3** and will support C&W in a minimum of 25 of the top 100 CBSAs.

2.12.4 SECURITY [L.29.2.1, M.2.1]

The Verizon C&W is managed for security and risk per Verizon's EIS IT Risk Management Framework (RMF) Plan in **Volume 1, Attachment A**. If additional security measures are required they will be addressed at the TO level.

Verizon's C&W practice utilizes the latest ANSI/BICSI 005 standard, (Electronic Safety and Security (ESS) System Design and Implementation) for C&W security compliance.

3 External Traffic Routing [C.1.8.8]

MTIPS and Internet Protocol Security Service (IPSS) (also known as EINSTEIN 3 or EINSTEIN 3 Accelerated (E3A), since the inception of these programs. Verizon will continue to support these programs on the EIS contract and evolve and secure telecommunications support for the government. Verizon currently supports the National Policy Requirements under **RFP Section C.1.8.8** and will continue to support the following functions identified in **Table 3-1** below:

Table 3-1. National Policy Requirement Functions [C.1.8.8]

National Policy Functions	
National Security/Emergency Preparedness	Verizon services delivered will be in compliance with applicable national policy directives that apply to the national telecommunications infrastructure. Executive Orders (EO) 12472 and 13618 and its successors will be considered in the design and operations of services provided under this contract. See Volume 2, Section 9 for Verizon's National Security and Emergency Preparedness Implementation Plan .

IPv6 support per OMB Memorandum M-05-22	Verizon supports the government's goal to transition from IPv4 to IPv6 infrastructures. Verizon currently supports IPv6 under the Networkx contract. Verizon's IPS has supported IPv6 since the early 2000s. The Verizon MTIPS platform was IPv6 enabled in 2012 so that components, including routing, security functionality, management and portal, support IPv6 services.
Support for OMB Memorandum M-09-32 (EINSTEIN Program)	<p>Verizon supports EINSTEIN 2 enclaves within its MTIPS service and is an approved provider of EINSTEIN 3 services. These programs are available today to support the data security protection needs of ordering agencies. Verizon is meeting requirements of both programs and is expanding these programs to meet agency cyber needs and integrate with Cloud and wireless services. Within the MTIPS environment, Verizon supports the government requirements to allow DHS to collocate equipment. DHS is responsible for the ongoing maintenance and support of the EINSTEIN equipment.</p> <p>Verizon service offerings under EIS (VPNS, ETS, PLS, IPS, Cloud, which includes IaaS, Private Cloud, PaaS, and SaaS, MNS Traffic Aggregation Service, MTIPS, and IPSS, and in future implementations could include other externally routed data services (e.g. OWS, SONETS).transporting Internet, extranet, and Inter-Agency traffic can be routed through a secure DHS EINSTEIN enclave for processing by the latest generation of EINSTEIN capabilities when ordered by the government.</p> <p>Verizon designs, implements, and operates its current service to achieve the required routing of traffic through (including delivery to and receipt of traffic from) DHS EINSTEIN enclaves.</p>

3.1 Verizon Traffic Aggregation Service (VTAS) Methodology

Verizon's VTAS methodology redirects traffic between an ordering agency location and the selected/affected network service through an aggregation facility for analysis. The aggregation facility is a combination of Verizon network based data centers (supporting the Verizon backbone), the associated aggregation equipment and the secure government enclave. VTAS is currently available on IPS and is supporting the IPSS program. The service concept will be expanded to meet the EIS data service offerings identified in **Section C.1.8.8** of the EIS RFP.


Verizon proposes to expand the current VTAS capabilities and use geographically diverse locations in the network data center to provide the networking and service aggregation required. [REDACTED]

[REDACTED]



Verizon has chosen these sites based upon geographic diversity to support all regions of the US with optimal performance. These locations will be within Verizon Network Data Centers, where Verizon houses its networking equipment for its network service offerings (i.e., IPS, VPNS, PL, ETS, etc.). These locations are also located on fiber junction points to optimize network access and minimize latency. Within these locations, Verizon will provide “aggregation enclaves” that consist of the security aggregation and associated networking equipment to support the relocation of traffic for VPNS, ETS, PLS, and IPS Networks. Cloud services, MNS and MTIPS are services transported by an associated network layer.

3.2 Technical Approach

Verizon is proposing the creation of Security Aggregation Enclaves (SAE) that will reside in selected Network Data Centers across the U.S. The SAE will be comprised of a services layer, transport layer, provider equipment layer, aggregation layer and classified co-location, 

[illegible]

The proposed solution has selected major networking hubs/locations that support multiple networking technologies, [REDACTED]

© 2006 The Authors
Journal compilation © 2006 Blackwell Publishing Ltd

As a result of the above, the Commission has concluded that the proposed transaction is not a "restructuring" under the Bankruptcy Code. The Commission's conclusion is based on the fact that the proposed transaction is not a "restructuring" under the Bankruptcy Code. The Commission's conclusion is based on the fact that the proposed transaction is not a "restructuring" under the Bankruptcy Code.

The standard Verizon network interface between carrier equipment is 10/100 Gbps. At each hub there are multiple equipment nodes that are built with carrier class redundancy. This includes support via self-healing fiber rings, diverse access, equipment redundancy, node configuration redundancy, dual power supplies and facility redundancy including battery and generator backup. The proposed solution places the service aggregation router one hop away from the network equipment. This equipment is envisioned to be co-located together with virtually no latency added with the configuration. [REDACTED]

[REDACTED] Verizon performed a SLA review on the IPSS as a deliverable to DHS during service initiation. Verizon identified that SLA metrics are based upon backbone measurements and there would be little impact upon backbone SLA traffic. The actual latency impact depends on traffic flows with source and destination traffic and their geographic location.

While Verizon instrumented the VTAS to provide data and reports on its impact on the performance of traffic through the service, any impact that it may [REDACTED]

[REDACTED] not considered end points for SLA measurement. Verizon will implement tools to measure latency across the VTAS. Verizon will initially leverage its WAN analysis tool, which provides network measurements and reports via a customer portal. The WAN analysis tool will provide information to measure SLA's that include latency, jitter, packet delivery, circuit utilization, and the overall health of the circuit. The WAN analysis tool provides reporting and graphs that will be used to document SLA information for the service.

3.2.1 VERIZON CLASSIFIED SUPPORT

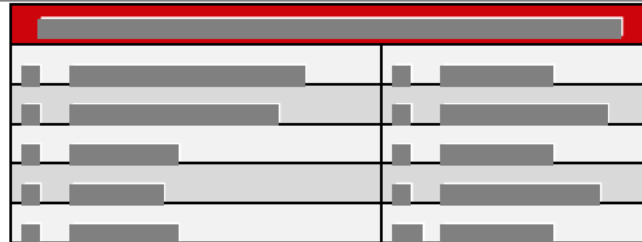
In support of the IPSS program, Verizon has secure resources to support the classified portion of VTAS. Verizon also has government-approved Sensitive Compartmented Information Facility (SCIF) enclaves provided and managed by Verizon, as well as a team of Top Secret/Sensitive Compartmented Information (TS/SCI) cleared personnel.

3.3 Notification of Non-Participating Traffic, Design Mechanisms to Prevent Bypass, and Traffic Failsafe Mechanism

The service uses both administrative and technical control mechanisms to allow only authorized traffic through routing infrastructure. Administratively, the agency must agree to participate in the service. Once it does the list of appropriate IP addresses are provided to Verizon and validated by the customer. These IP addresses are loaded into the External Traffic Routing (ETR) architecture and Access Control Lists (ACL) and firewall filters are placed into the Service Aggregator router, so that only authorized traffic can pass through the infrastructure.

Verizon will notify DHS of unauthorized access, use, disclosure, or retention of Participating Agency data; of a breach of security or information handling requirements or additional instructions provided by DHS regarding the handling of Participating Agency network traffic; and will provide relevant information to DHS that will allow them to assess the scope of any such breach. Verizon supports this today on the IPSS Program with an automated ticketing system currently in place. The ticketing platform automatically sends an email when any service anomaly is identified, and the system will be expanded to support the enhanced traffic aggregation services and networks identified by the Government. This solution provides design mechanisms to prevent bypass and also traffic failsafe mechanisms to pass through the service.

3.4 Location



3.5 Availability of Cleared Personnel and Smart-Hands Support

Smart-Hands support allows the National Cyber Protection System (NCPS) Service Desk to request a TS/SCI-cleared and trained Nest engineer (rather than dispatch their own engineer) to the Nest location. DHS can rely on the onsite Nest engineers to perform the tasks listed in **Table 3.5-1**:

Figure 3.5-1. Onsite Nest Engineering Tasks.

Tasks for Onsite Nest Engineers
Assist in troubleshooting GFE systems and personnel escorts, to include:
▪ Escorting DHS personnel or DHS designee during site visits
▪ Checking indicator lights or system status indicators
▪ Power cycling devices
Inserting CDs or disks
▪ Removing and reinserting small form-factor pluggable (SFP) modules
Swap out of major end item systems, to include:
▪ Servers
▪ Networking equipment
▪ Cryptographic devices
▪ Power units
Swap out of hot swappable components. These are components that can be pulled without interrupting the service provided by that device, to include:
▪ Hard drives
▪ Replace, trace or move of copper and fiber cables
Assist in performing cryptographic re-keys, to include:
▪ Routine
▪ Emergency
▪ Unscheduled or mid-cycle

The NCPS SD may request Smart-Hands support by opening a service request or trouble ticket with the Nest Tier I Helpdesk. The Nest Tier I Helpdesk is available 24x7, 365 days a year to receive NCPS SD calls.

Attachments

Attachment A EIS Information Technology Risk Management Framework Plan

Reference the document entitled “Verizon_Vol 1 Technical_2016-02-22_2_Attachment A EIS IT RMF.docx”.

Attachment B MTIPS Risk Management Framework Plan

Reference the document entitled “Verizon_Vol 1 Technical_2016-02-22_3_ Attachment B MTIPS RMF.docx”.

Attachment C Assumptions and Conditions

Reference the document entitled “Verizon_Vol 1 Technical_2016-02-22_4_ Attachment C Assumptions.docx”.

Attachment D Technical Volume Abbreviation and Acronym Definitions List

Reference the document entitled “Verizon_Vol 1 Technical_2016-02-22_5_ Attachment D Acronyms.docx”.