



## Volume 1 Technical

*This data shall not be disclosed outside of the Government and shall not be duplicated, used, or disclosed in whole or in part for any purpose other than to the extent provided in the EIS Contract. This restriction does not limit the Government's right to use information contained in the data if it is obtained from another source without restriction. The data subject to this restriction is applicable to all pages following in this document. The information contained herein is proprietary, and it contains trade secrets and commercial or financial information that is privileged or confidential and is therefore exempt from disclosure under the provision of 5 USC Section 552. Release of this information is prohibited and subject to the sanctions set forth in 18 USC Section 1905.*

**Table of Contents**

Table of Contents ..... i

List of Figures ..... xv

Volume 1 Technical ..... 1-1

INTRODUCTION ..... 1-1

1.1 Network Architecture [L.29.1, C.1.6] ..... 1-7

1.2 Technical Response [L.29.2; C.2; C.1.8.6; C.1.8.9] ..... 1-16

1.2.1 EIS Services [L.29.2.1; M.4; C.1.2] ..... 1-17

1.2.1.1 Understanding [L.29.2.1.A; M.2.1.1] ..... 1-18

1.2.1.2 Quality of Services [L.29.2.1.B; M.2.1.2] ..... 1-20

1.2.1.3 Service Coverage [L.29.2.1.C; M.2.1.3; C.1.3; C.1.8.5; J.1] ..... 1-21

1.2.1.4 Security [L.29.2; M.2.1.4; C.1.8.7] ..... 1-21

1.3 Mandatory EIS Services [L.29(2)(a), M.2.1, C.1.2] ..... 1-22

1.3.1 Data Service Mandatory ..... 1-22

1.3.1.1 Virtual Private Network Service [L.29.2.1, C.2.1.1, C.4.4] ..... 1-22

1.3.1.1.1 Service and Functional Description [L.29.2.1, M.2.1, C.2.1.1] ..... 1-24

1.3.1.1.1.1 Intranet, Extranet, Remote Access [C.2.1.1.1.1] ..... 1-29

1.3.1.1.1.2 Traffic Prioritization [C.2.1.1.1.1] ..... 1-31

1.3.1.1.2 Standards [L.29.2.1, M.2.1, C.2.1.1.1.2] ..... 1-33

1.3.1.1.3 Connectivity [L.29.2.1, M.2.1, C.2.1.1.1.3] ..... 1-34

1.3.1.1.4 Technical Capabilities [L.29.2.1, M.2.1, C.2.1.1.1.4] ..... 1-34

1.3.1.1.5 Features [L.29.2.1, M.2.1, C.2.1.1.2] ..... 1-38

1.3.1.1.6 Interfaces [L.29.2.1, C.2.1.1.3] ..... 1-39

1.3.1.1.7 Performance Metrics [L.29.2.1, M.2.1, C.2.1.1.4, G.8] ..... 1-39

1.3.1.2 Ethernet Transport Service [L.29.2.1, C.2.1.2, C.4.4] ..... 1-40

1.3.1.2.1 Service and Functional Description [L.29.2.1, M.2.1, C.2.1.2.1, C.2.1.2.1.1] ..... 1-43

---

1.3.1.2.2 Standards [L.29.2.1, C.2.1.2.1.2] .....	1-50
1.3.1.2.3 Connectivity [L.29.2.1, C.2.1.2.1.3] .....	1-50
1.3.1.2.4 Technical Capabilities [L.29.2.1, C.2.1.2.1.4] .....	1-51
1.3.1.2.5 Features [L.29.2.1, C.2.1.2.2] .....	1-53
1.3.1.2.6 Interfaces [L.29.2.1, C.2.1.2.3] .....	1-53
1.3.1.2.7 Performance Metrics [L.29.2.1, M.2.1(c), C.2.1.2.4] .....	1-53
1.3.2 Voice Service (Mandatory) .....	1-54
1.3.2.1 Internet Protocol Voice Service [L.29.2.1, M.2.1, C.2.2.1] .....	1-54
1.3.2.1.1 Service and Functional Description [L.29.2.1, M.2.1, C.2.2.1.1] .....	1-58
1.3.2.1.2 Standards [L.29.2.1, M.2.1, C.2.2.1.1.2] .....	1-60
1.3.2.1.3 Connectivity [L.29.2.1, M.2.1, C.2.2.1.1.3] .....	1-60
1.3.2.1.4 Technical Capabilities [L.29.2.1, M.2.1, C.2.2.1.1.4] .....	1-61
1.3.2.1.5 Features [L.29.2.1, M.2.1, C.2.2.1.2] .....	1-66
1.3.2.1.6 Interfaces [L.29.2.1, M.2.1, C.2.2.1.3] .....	1-69
1.3.2.1.7 Performance Metrics [L.29.2.1, M.2.1(c), C.2.2.1.4] .....	1-70
1.3.2.2 Managed LAN Service [L.29.2.1, M.2.1, C.2.2.1.5] .....	1-70
1.3.2.3 Session Initiating Protocol Trunk Service [L.29.2.1, M.2.1, C.2.2.1.6] .....	1-72
1.3.2.3.1 SIP Trunking Technical Capabilities [L.29.2.1, M.2.1, C.2.2.1.6.1] .....	1-74
1.3.2.3.2 SIP Trunking Features [L.29.2.1, M.2.1, C.2.2.1.6.2] .....	1-74
1.3.3 Managed Service (Mandatory) .....	1-75
1.3.3.1 Managed Network Service [L.29.2.1, M.2.1, C.2.8.1, C.1.8.7] .....	1-75
1.3.3.1.1 Service and Functional Description [L.29.2.1, M.2.1, C.2.8.1] .....	1-78
1.3.3.1.2 Standards [C.2.8.1.1.2] .....	1-80
1.3.3.1.3 Connectivity [C.2.8.1.1.3] .....	1-81
1.3.3.1.4 Technical Capabilities [C.2.8.1.1.4] .....	1-81

---

1.3.3.1.4.1 Design and Engineering Services [C.2.8.1.1.4.1] .....	1-81
1.3.3.1.4.2 Implementation, Management and Maintenance	
[C.2.8.1.1.4.2] .....	1-84
1.3.3.1.5 Features [C.2.8.1.2] .....	1-89
1.3.3.1.6 Interfaces [C.2.8.1.3] .....	1-90
1.3.3.1.7 Performance Metrics [M.2.1.2, C.2.8.1.4, G.8] .....	1-90
1.4 Optional EIS Services [L.29.2.1-3, M.4, C.1.2] .....	1-90
1.4.1 Data Services .....	1-90
1.4.1.1 Optical Wavelength Service [L.29.2.1, C.2.1.3] .....	1-90
1.4.1.1.1 Service and Functional Description [L.29.2.1, M.2.1,	
C.2.1.3.1] .....	1-91
1.4.1.1.2 Standards [C.2.1.3.1.2] .....	1-92
1.4.1.1.3 Connectivity [C.2.1.3.1.3] .....	1-93
1.4.1.1.4 Technical Capabilities [C.2.1.3.1.4] .....	1-93
1.4.1.1.5 Features [C.2.1.3.2] .....	1-95
1.4.1.1.6 Interfaces [C.2.1.3.3] .....	1-96
1.4.1.1.7 Performance Metrics [M.2.1, C.2.1.3.4, G.8] .....	1-96
1.4.1.1.7.1 Framed Wavelength Performance .....	1-96
1.4.1.1.7.2 Transparent Wavelength Performance .....	1-96
1.4.1.1.7.3 In-Service Monitoring .....	1-96
1.4.1.1.7.4 Performance Levels .....	1-96
1.4.1.2 Private Line Service [L.29.2.1, C.2.1.4; C.4.4] .....	1-97
1.4.1.2.1 Service and Functional Description [L.29.2.1, M.2.1,	
C.2.1.4.1.1] .....	1-98
1.4.1.2.2 Standards [C.2.1.4.1.2] .....	1-99
1.4.1.2.3 Connectivity [C.2.1.4.1.3] .....	1-99
1.4.1.2.4 Technical Capabilities [C.2.1.4.1.4] .....	1-100
1.4.1.2.5 Features [C.2.1.4.2] .....	1-101
1.4.1.2.5.1 Multipoint Connection .....	1-101

---

1.4.1.2.5.2 Special Routing .....	1-101
1.4.1.2.6 Interfaces [C.2.1.4.3].....	1-102
1.4.1.2.7 Performance Metrics and Quality of Service [M.2.1, C.2.1.4.4, G.8].....	1-103
1.4.1.3 Synchronous Optical Network Services [L.29.2.1, C.2.1.5; C.4.4]	1-103
1.4.1.3.1 Services and Functional Description [L.29.2.1, M.2.1, C.2.1.5.1.1] .....	1-104
1.4.1.3.2 Standards [C.2.1.5.1.2].....	1-106
1.4.1.3.3 Connectivity [C.2.1.5.1.3].....	1-106
1.4.1.3.4 Technical Capabilities [C.2.1.5.1.4].....	1-107
1.4.1.3.5 Features [C.2.1.5.2] .....	1-108
1.4.1.3.6 Interfaces [M.2.1, C.2.1.5.3, G.8].....	1-109
1.4.1.3.7 Performance Metrics [M.2.1, C.2.1.5.4, G.8].....	1-109
1.4.1.4 Dark Fiber Services [L.29.2.1, C.2.1.6, C.4.4].....	1-110
1.4.1.4.1 Service and Functional Description [L.29.2.1, M.2.1, C.2.1.6.1.1] .....	1-111
1.4.1.4.2 Standards [C.2.1.6.1.2].....	1-114
1.4.1.4.3 Connectivity [C.2.1.6.1.3].....	1-114
1.4.1.4.4 Technical Capabilities [C.2.1.6.1.4].....	1-115
1.4.1.4.5 Features [C.2.1.6.2] .....	1-117
1.4.1.4.6 Interfaces [C.2.1.6.3].....	1-118
1.4.1.4.7 Performance Metrics [M.2.1, C.2.1.6.4] .....	1-118
1.4.1.5 Internet Protocol Service [L.29.2.1, C.2.1.7; C.4.4].....	1-118
1.4.1.5.1 Service and Functional Description [L.29.2.1, M.2.1, C.2.1.7.1.1] .....	1-119
1.4.1.5.2 Standards [C.2.1.7.1.2].....	1-121
1.4.1.5.3 Connectivity [C.2.1.7.1.3].....	1-122
1.4.1.5.4 Technical Capabilities [C.2.1.7.1.4].....	1-122
1.4.1.5.5 Features [C.2.1.7.2] .....	1-123

---

1.4.1.5.6 Interfaces [C.2.1.7.3].....	1-123
1.4.1.5.7 Performance Metrics [M.2.1, C.2.1.7.4, G.8].....	1-123
1.4.2 Voice Service (Optional).....	1-124
1.4.2.1 Circuit Switched Voice Service [L.29.2.1, C.2.2.2] .....	1-124
1.4.2.1.1 Service and Functional Description [L.29.2.1, M.2.1, C.2.2.2] .....	1-125
1.4.2.1.2 Standards [C.2.2.2.1.2].....	1-126
1.4.2.1.3 Connectivity [C.2.2.2.1.3].....	1-126
1.4.2.1.4 Technical Capabilities [C.2.2.2.1.4].....	1-126
1.4.2.1.5 Features [C.2.2.2.2] .....	1-127
1.4.2.1.6 Interfaces [C.2.2.2.3].....	1-128
1.4.2.1.7 Performance Metrics [M.2.1, C.2.2.2.4, G.8].....	1-128
1.4.2.2 Toll Free Service [L.29.2.1, C.2.2.3; C.4.4] .....	1-128
1.4.2.2.1 Service and Functional Description [L.29.2.1, M.2.1, C.2.2.3] .....	1-129
1.4.2.2.2 Standards [C.2.2.3.1.2].....	1-130
1.4.2.2.3 Connectivity [C.2.2.3.1.3].....	1-130
1.4.2.2.4 Technical Capabilities [C.2.2.3.1.4].....	1-130
1.4.2.2.5 Features [C.2.2.3.2] .....	1-132
1.4.2.2.5.1 Feature Reports [C.2.2.3.2.1].....	1-135
1.4.2.2.6 Interfaces [C.2.2.3.3].....	1-136
1.4.2.2.7 Performance Metrics and Quality of Services [M.2.1, C.2.2.3.4, G.8] .....	1-136
1.4.2.3 Circuit Switched Data Service [L.29.2.1, C.2.2.4].....	1-136
1.4.2.3.1 Service and Functional Description [L.29.2.1, M.2.1, C.2.2.4] .....	1-137
1.4.2.3.2 Standards [C.2.2.4.1.2].....	1-138
1.4.2.3.3 Connectivity [C.2.2.4.1.3].....	1-139
1.4.2.3.4 Technical Capabilities [C.2.2.4.1.4].....	1-139

---

1.4.2.3.5 Features [C.2.2.4.2] .....	1-140
1.4.2.3.6 Interfaces [C.2.2.4.3].....	1-140
1.4.2.3.7 Performance Metrics [M.2.1, C.2.2.4.4] .....	1-140
1.4.3 Contact Center Service [L.29.2.1, C.2.3] .....	1-141
1.4.3.1 Service and Functional Description [L.29.2.1, M.2.1, C.2.3].....	1-142
1.4.3.2 Standards [C.2.3.1.2] .....	1-144
1.4.3.3 Connectivity [C.2.3.1.3] .....	1-145
1.4.3.4 Technical Capabilities [C.2.3.1.4].....	1-145
1.4.3.5 Features [C.2.3.1.5].....	1-147
1.4.3.6 Interfaces [C.2.3.1.6].....	1-149
1.4.3.7 Performance Metrics and Quality of Services [M.2.1, C.2.3.1.4, G.8].....	1-149
1.4.4 Colocated Hosting Service [L.29.2.1, C.2.4, C.4.4] .....	1-149
1.4.4.1 Services and Functional Description [L.29.2.1, M.2.1, C.2.4.1, G.8].....	1-150
1.4.4.2 Standards [L.29.2.1, M.2.1, C.2.4.2, G.8].....	1-153
1.4.4.3 Connectivity [L.29.2.1, M.2.1, C.2.4.3, G.8].....	1-153
1.4.4.4 Technical Capabilities [L.29.2.1, M.2.1, C.2.4.4, G.8] .....	1-153
1.4.4.5 Features [L.29.2.1, M.2.1, C.2.4.5, G.8].....	1-154
1.4.4.6 Interfaces .....	1-154
1.4.4.7 Performance Metrics [L.29.2.1, M.2.1, C.2.4.5.1, G.8] .....	1-154
1.4.5 Cloud Services [L.29.2.1, C.2.5; C.4.4] .....	1-155
1.4.5.1 Infrastructure as a Service (IaaS) [L.29.2.1, C.2.5.1; C.4.4].....	1-158
1.4.5.1.1 Service and Functional Description [L.29.2.1, M.2.1, C.2.5.1.1.1] .....	1-160
1.4.5.1.2 Standards [C.2.5.1.1.2].....	1-161
1.4.5.1.3 Connectivity to Cloud Data Center [C.2.5.1.1.3] .....	1-162
1.4.5.1.4 Technical Capabilities [C.2.5.1.1.4].....	1-162

1.4.5.1.4.1 Technical Capabilities for Private Cloud  
 [C.2.5.1.1.4.1] ..... 1-162

1.4.5.1.4.2 Technical Capabilities for Data Center Augmentation with  
 Common Information Technology Service Management  
 [C.2.5.1.1.4.2] ..... 1-165

1.4.5.1.5 Features [C.2.5.1.2] ..... 1-166

1.4.5.1.6 Interfaces [C.2.5.1.3] ..... 1-166

1.4.5.1.7 Performance Metrics [M.2.1, C.2.5.1.4, G.8] ..... 1-167

1.4.5.2 Platform as a Service [L.29.2.1, C.2.5.2; C.4.4] ..... 1-167

1.4.5.2.1 Service and Functional Description [L.29.2.1, M.2.1,  
 C.2.5.2.1] ..... 1-168

1.4.5.2.1.2 Standards [C.2.5.2.1.2] ..... 1-170

1.4.5.2.1.3 Connectivity [C.2.5.2.1.3] ..... 1-170

1.4.5.2.1.4 Technical Capabilities [C.2.5.2.1.4] ..... 1-171

1.4.5.2.1.5 Features [C.2.5.2.2] ..... 1-171

1.4.5.2.1.6 Interfaces [C.2.5.2.3] ..... 1-171

1.4.5.2.1.7 Performance Metrics [M.2.1, C.2.5.2.4, G.8] ..... 1-172

1.4.5.3 Software as a Service [L.29.2.1, C.2.5.3; C.4.4] ..... 1-172

1.4.5.3.1 Service and Functional Description [L.29.2.1, M.2.1,  
 C.2.5.3.1.1] ..... 1-173

1.4.5.3.2 Standards [C.2.5.3.1.2] ..... 1-174

1.4.5.3.3 Connectivity [C.2.5.3.1.3] ..... 1-175

1.4.5.3.4 Technical Capabilities [C.2.5.3.1.4] ..... 1-175

1.4.5.3.5 Features [C.2.5.3.2] ..... 1-176

1.4.5.3.6 Interfaces [C.2.5.3.3] ..... 1-176

1.4.5.3.7 Performance Metrics [M.2.1, C.2.5.3.4, G.8] ..... 1-176

1.4.5.4 Content Delivery Network Service (CDNS) [L.29.2.1,  
 C.2.5.4; C.4.4] ..... 1-177



---

1.4.5.4.1 Service and Functional Description [L.29.2.1, M.2.1, C.2.5.4.1] .....	1-178
1.4.5.4.2 Standards [C.2.5.4.1.2] .....	1-180
1.4.5.4.3 Connectivity [C.2.5.4.1.3] .....	1-180
1.4.5.4.4 Technical Capabilities [C.2.5.4.1.4].....	1-180
1.4.5.4.5 Features [C.2.5.4.2] .....	1-182
1.4.5.4.6 Interfaces [C.2.5.4.3].....	1-183
1.4.5.4.7 Performance Metrics [M.2.1, C.2.5.4.4.1, G.8].....	1-183
1.4.6 Wireless Service [L.29.2.1, C.2.6] .....	1-183
1.4.6.1 Service and Functional Description [L.29.2.1, M.2.1, C.2.6.1].....	1-192
1.4.6.2 Standards [C.2.6.1.2] .....	1-192
1.4.6.3 Connectivity [C.2.6.1.3] .....	1-192
1.4.6.4 Technical Capabilities [C.2.6.1.4].....	1-192
1.4.6.5 Features [C.2.6.2] .....	1-193
1.4.6.6 Interfaces [C.2.6.3, 2.6.3.1].....	1-195
1.4.6.7 Performance Metrics [M.2.1, C.2.6.4, G.8].....	1-195
1.4.6.8 Private Wireless Gateway .....	1-195
1.4.7 Commercial Satellite Communications Services(CSCS) [L.29.2.1, C.2.7, C4.4].....	1-190
1.4.7.1 Service and Functional Description [L.29.2.1, M.2.1, C.2.7].....	1-192
1.4.7.2 Standards [C.2.7.1.2] .....	1-192
1.4.7.3 Technical Capabilities [C.2.7.1.3].....	1-192
1.4.7.4 Features [C.2.7.2] .....	1-193
1.4.7.5 Interfaces .....	1-195
1.4.7.6 Performance Metrics [M.2.1, C.2.7.3, G.8].....	1-195
1.4.8 Managed Service (optional).....	1-195
1.4.8.1 Web Conferencing Service [L.29.2.1, C.2.8.2; C.4.4].....	1-195
1.4.8.1.1 Service and Functional Description [L.29.2.1, M.2.1, C.2.8.2] .....	1-196

---

1.4.8.1.2 Standards [C.2.8.2.1.2] .....	1-197
1.4.8.1.3 Connectivity [C.2.8.2.1.3] .....	1-197
1.4.8.1.4 Technical Capabilities [C.2.8.2.1.4].....	1-197
1.4.8.1.5 Features [C.2.8.2.2] .....	1-199
1.4.8.1.6 Interfaces [C.2.8.2.3].....	1-200
1.4.8.1.7 Performance Metrics [M.2.1, C.2.8.2.4, G.8].....	1-200
1.4.8.2 Unified Communications Service [L.29.2.1, C.2.8.3] .....	1-200
1.4.8.2.1 Service and Functional Description [L.29.2.1, M.2.1, C.2.8.3] .....	1-202
1.4.8.2.2 Standards [C.2.8.3.1.2] .....	1-203
1.4.8.2.3 Connectivity [C.2.8.3.1.3] .....	1-203
1.4.8.2.4 Technical Capabilities [C.2.8.3.1.4].....	1-204
1.4.8.2.5 Features [C.2.8.3.2] .....	1-207
1.4.8.2.6 Interfaces [C.2.8.3.3].....	1-207
1.4.8.2.7 Performance Metrics [M.2.1, C.2.8.3.4, G.8].....	1-208
1.4.8.3 Managed Trusted Internet Protocol Service [L.29.2.1, C.2.8.4]1-Error! Bookmark not defined.	
1.4.8.3.1 Service and Functional Description [L.29.2.1, M.2.1, C.2.8.4.1, C.2.8.4.1.1] .....	1-Error! Bookmark not defined.
1.4.8.3.2 Standards [C.2.8.4.1.2] .....	1-Error! Bookmark not defined.
1.4.8.3.3 Connectivity [C.2.8.4.1.3] .....	1-Error! Bookmark not defined.
1.4.8.3.4 Technical Capabilities [C.2.8.4.1.4]1-Error! Bookmark not defined.	
1.4.8.3.4.1 MTIPS TIC Portal Capabilities [C.2.8.4.1.4.1]1-Error! Bookmark not defined.	
1.4.8.3.4.2 MTIPS Transport Collection and Distribution Capabilities [C.2.8.4.1.4.2] .....	1-Error! Bookmark not defined.
1.4.8.3.5 Features [C.2.8.4.2] .....	1-Error! Bookmark not defined.
1.4.8.3.6 Interfaces [C.2.8.4.3].....	1-Error! Bookmark not defined.
1.4.8.3.7 Performance Metrics [M.2.1, C.2.8.4.4.1, C.2.8.4.4.2, G.8]1-Error! Bookmark not defined.	
1.4.8.3.8 MTIPS Security Requirements [M.2.1, C.2.8.4.5]1-Error! Bookmark not defined.	

1.4.8.3.8.1 General Security Compliance Requirements	
[C.2.8.4.5.1].....	<b>1-Error! Bookmark not defined.</b>
1.4.8.3.8.2 Security Compliance Requirements [C.2.8.4.5;	
C.2.8.4.5.2].....	<b>1-Error! Bookmark not defined.</b>
1.4.8.3.8.3 Security Assessment and Authorization	
[C.2.8.4.5.3].....	<b>1-Error! Bookmark not defined.</b>
1.4.8.3.8.4 System Security Plan (SSP) [C.2.8.4.5.4]	<b>1-Error! Bookmark not defined.</b>
1.4.8.3.8.5 Additional Security Requirements [C.2.8.4.5.5]	<b>1-Error! Bookmark not defined.</b>
1.4.8.4 Managed Security Services [L.29.2.1, C.2.8.5]	1-247
1.4.8.4.1 Service and Functional Description [L.29.2.1, C.2.8.5.1]	<b>1-Error! Bookmark not defined.</b>
1.4.8.4.2 Standards [C.2.8.5.1.2].....	<b>1-Error! Bookmark not defined.</b>
1.4.8.4.3 Connectivity [C.2.8.5.1.3].....	<b>1-Error! Bookmark not defined.</b>
1.4.8.4.4 Technical Capabilities [C.2.8.5.1.4]	<b>1-Error! Bookmark not defined.</b>
1.4.8.4.4.1 Managed Prevention Service (MPS)	
[C.2.8.5.1.4.1].....	<b>1-Error! Bookmark not defined.</b>
1.4.8.4.4.2 Vulnerability Scanning Service (VSS)	
[C.2.8.5.1.4.2].....	<b>1-Error! Bookmark not defined.</b>
1.4.8.4.4.3 Incident Response Service (INRS) [C.2.8.5.1.4.3]	<b>1-Error! Bookmark not defined.</b>
1.4.8.4.5 Features [C.2.8.5.2].....	<b>1-Error! Bookmark not defined.</b>
1.4.8.4.6 Interfaces [C.2.8.5.3].....	<b>1-Error! Bookmark not defined.</b>
1.4.8.4.7 Performance Metrics [M.2.1, C.2.8.5.4, C.2.8.5.4.1, G.8]	<b>1-Error! Bookmark not defined.</b>
1.4.8.5 Managed Mobility Service [L.29.2.1, C.2.8.6, C.4.4]	1-263
1.4.8.5.1 Service and Functional Description [L.29.2.1, M.2.1,	
C.2.8.6].....	1-265
1.4.8.5.2 Standards [C.2.8.6.1.2].....	1-265
1.4.8.5.3 Connectivity [C.2.8.6.1.3].....	1-265
1.4.8.5.4 Technical Capabilities [C.2.8.6.1.4].....	1-265
1.4.8.5.4.1 MDM Capabilities [C.2.8.6.1.4.1].....	1-265
1.4.8.5.4.2 MAM Capabilities [C.2.8.6.1.4.2].....	1-267

---

1.4.8.5.4.3 MCM Capabilities [C.2.8.6.1.4.3] .....	1-268
1.4.8.5.4.4 Mobile Security Capabilities [C.2.8.6.1.4.4] .....	1-268
1.4.8.5.4.5 Deployment Support Capabilities [C.2.8.6.1.4.5] .....	1-270
1.4.8.5.5 Features [C.2.8.6.2] .....	1-270
1.4.8.5.6 Interfaces [C.2.8.6.3].....	1-270
1.4.8.5.7 Performance Metrics [M.2.1, C.2.8.6.4] .....	1-271
1.4.8.6 Audio Conferencing Service [L.29.2.1, C.2.8.7, C.4.4].....	1-271
1.4.8.6.1 Service and Functional Description [L.29.2.1, M.2.1, C.2.8.7] .....	1-272
1.4.8.6.2 Standards [C.2.8.7.1.2] .....	1-272
1.4.8.6.3 Connectivity [C.2.8.7.1.3].....	1-273
1.4.8.6.4 Technical Capabilities [C.2.8.7.1.4].....	1-273
1.4.8.6.5 Features [C.2.8.7.2] .....	1-274
1.4.8.6.6 Interfaces [C.2.8.7.3].....	1-275
1.4.8.6.7 Performance Metrics [M.2.1, C.2.8.7.4, G.8].....	1-275
1.4.8.7 Video Teleconferencing Service [L.29.2.1, C.2.8.8, C.4.4].....	1-275
1.4.8.7.1 Service and Functional Description [L.29.2.1, M.2.1, C.2.8.8] .....	1-276
1.4.8.7.2 Standards [C.2.8.8.1.2] .....	1-277
1.4.8.7.3 Connectivity [C.2.8.8.1.3].....	1-277
1.4.8.7.4 Technical Capabilities [C.2.8.8.1.4].....	1-277
1.4.8.7.5 Features [C.2.8.8.2] .....	1-279
1.4.8.7.6 Interfaces [C.2.8.8.3].....	1-280
1.4.8.7.7 Performance Metrics [M.2.1, C.2.8.8.4, G.8].....	1-280
1.4.8.8 DHS Intrusion Prevention Security Service [L.29.2.1, C.2.8.9; C.4.4] .....	<b>1-Error! Bookmark not defined.</b>
1.4.8.8.1 Service and Functional Description [L.29.2.1, M.2.1, C.2.8.9] .....	1-281
1.4.8.8.2 Standards [C.2.8.9.1.2] .....	1-285

---

1.4.8.8.3 Connectivity [C.2.8.9.1.3] .....	1-285
1.4.8.8.4 Technical Capabilities [C.2.8.9.1.4].....	1-286
1.4.8.8.5 Features [C.2.8.9.2] .....	1-289
1.4.8.8.6 Interfaces [C.2.8.9.3].....	1-290
1.4.8.8.7 Performance Metrics [M.2.1, C.2.8.9.4, G.8].....	1-290
1.4.8.9 Software Defined Wide Area Network Service [L.29.2.1, C.2.8.10; C.4.4] .....	<b>1-Error! Bookmark not defined.</b>
1.4.8.9.1 Service Description [L.29.2.1, M.2.1, C.2.8.10.1].....	1-281
1.4.8.9.1.1 Functional Description [L.29.2.1, M.2.1, C.2.8.10.1.1] .....	1-281
1.4.8.9.2 Standards [C.2.8.10.1.2] .....	1-285
1.4.8.9.3 Connectivity [C.2.8.10.1.3].....	1-285
1.4.8.9.4 Technical Capabilities [C.2.8.10.1.4].....	1-286
1.4.8.9.5 Features [C.2.8.10.2] .....	1-289
1.4.8.9.6 Interfaces [C.2.8.10.3].....	1-290
1.4.8.9.7 Performance Metrics [M.2.1, C.2.8.10.4, G.8].....	1-290
1.4.9 Access Arrangements [L.29.2.1, C.2.9] .....	1-301
1.4.9.1 Service and Functional Description [L.29.2.1, M.2.1, C.2.9, J.1]..	1-302
1.4.9.2 Standards [C.2.9.1.2] .....	1-303
1.4.9.3 Connectivity [C.2.9.1.3] .....	1-303
1.4.9.4 Technical Capabilities [C.2.9.1.4].....	1-303
1.4.9.5 Access Diversity and Avoidance [C.2.9.2].....	1-306
1.4.9.6 Interfaces [C.2.9.3] .....	1-306
1.4.9.7 Performance Metrics [M.2.1, C.2.9.1, C.2.9.1.4, G.3.5.3].....	1-306
1.4.10 Service Related Equipment [L.29.2.1, C.2.10, M.2.1, Section D] .....	1-307
1.4.10.1 Warranty Service [C.2.10.1] .....	1-308
1.4.10.1.1 Preservation, Packaging and Packing [D.1] .....	1-308
1.4.10.1.2 Packing List [D.2] .....	1-309
1.4.10.1.3 Initial Packing, Marking, and Storage of Equipment [D.3] ..	1-309
1.4.10.1.4 Equipment Removal [D.4] .....	1-309

---

1.4.11 Service Related Labor [L.29.2.1, C.2.11, J.5] .....	1-309
1.4.12 Cable and Wiring [L.29.2.1, C.2.12].....	1-311
1.4.13 External Traffic Routing [L.29.2.3, M.2.1 (item 4) c), C.1.8.8 (item 3)] .....	1-313
1.4.13.1 Identifying Participating Agency Traffic [L.29.2.3, M.2.1 (item 4) c)i., C.1.8.8 (item 1)].....	1-316
1.4.13.2 Traffic Control Mechanisms [L.29.2.3, M.2.1 (item 4) c)iv. and v., C.1.8.8].....	1-317
1.4.13.3 Encryption Tunnel Proxy [L.29.2.3, M.2.1 (item 4) c), C.1.8.8] .....	1-317
1.4.13.4 Smart Hands Support [L.29.2.3, M.2.1 (item 4) c)vii, C.1.8.8] .....	1-318
1.4.13.5 Performance Measurement [L.29.2.3, M.2.1 (item 4) c)viii, C.1.8.8].....	1-318
2.0 Risk Management Framework Plan [L.29.3a), C.1.8.7].....	2-1
2.1 Risk Management Framework (RMF) Approach [L.29.3.a), C.1.8.7] .....	2-1
2.2 Systems Development Life Cycle [L.29.3.a), C.1.8.7].....	2-5
2.3 Information System Boundaries [L.29.3.a), C.1.8.7] .....	2-5
2.4 Security Control Allocation [L.29.3.a), C.1.8.7] .....	2-6
2.5 The Risk Management Framework Process [L.29.3.a), C.1.8.7].....	2-6
2.5.1 Step 1: Categorize Information System [L.29.3.a), C.1.8.7].....	2-7
2.5.1.1 RMF Step 1 – Task 1-1, Security Categorization [L.29.3.a), C.1.8.7].....	2-7
2.5.1.2 RMF Step 1 - Task 1-2, Information System Description [L.29.3.a), C.1.8.7].....	2-7
2.5.2 RMF Step 2: Select Security Controls [L.29.3.a), C.1.8.7].....	2-9
2.5.3 RMF Step 3: Implement Security Controls [L.29.3.a), C.1.8.7].....	2-13
2.5.4 RMF Step 4: Assess Security Controls [L.29.3.a), C.1.8.7] .....	2-13
2.5.5 RMF Step 5: Authorize Information System [L.29.3.a), C.1.8.7] .....	2-14
2.5.6 RMF Step 6: Monitor Security Controls [L.29.3.a), C.1.8.7].....	2-14

---

2.6 Reference: FISMA Moderate (MOD) Impact Level Baseline Control Set  
 [L.29.3.a), C.1.8.7] ..... 2-15

3.0 MTIPS Risk Management Framework Plan [L.29.3.b, C.2.8.4, C.2.8.4.5,  
 C.2.8.4.5.4]..... 3-1

3.1 Step 1: Categorize Information System [L.29.3.b), C.2.8.4.5]3-**Error! Bookmark not defined.**

    3.1.1 Security Categorization, RMF Task 1-1 [L.29.3.b), C.2.8.4.5]3-**Error! Bookmark not defined.**

    3.1.2 Information System (MTIPS) Description, RMF Task 1-2 [L.29.3.b),  
 C.2.8.4.5] ..... 3-**Error! Bookmark not defined.**

    3.1.3 Information System (MTIPS) Registration, RMF Task 1-3 [L.29.3.b),  
 C.2.8.4.5] ..... 3-**Error! Bookmark not defined.**

3.2 Step 2: Select Security Controls [L.29.3.b), C.2.8.4.5]3-**Error! Bookmark not defined.**

    3.2.1 Common Control Identification, RMF Task 2-1 [L.29.3.b), C.2.8.4.5]3-**Error! Bookmark not defined.**

    3.2.2 Security Control Selection, RMF Task 2-2 [L.29.3.b), C.2.8.4.5]3-**Error! Bookmark not defined.**

    3.2.3 Monitoring Strategy, RMF Task 2-3 [L.29.3.b), C.2.8.4.5]3-**Error! Bookmark not defined.**

    3.2.4 Security Plan Approval, RMF Task 2-4 [L.29.3.b), C.2.8.4.5]3-**Error! Bookmark not defined.**

3.3 Step 3: Implement Security Controls [L.29.3.b), C.2.8.4.5]3-**Error! Bookmark not defined.**

3.4 Step 4: Assess Security Controls [L.29.3.b), C.2.8.4.5]3-**Error! Bookmark not defined.**

3.5 Step 5: Authorize Information System (MTIPS) [L.29.3.b), C.2.8.4.5]3-**Error! Bookmark not defined.**

3.6 Step 6: Monitor Security Controls [L.29.3.b), C.2.8.4.5]3-**Error! Bookmark not defined.**

3.7 Schedule [L.29.3.b), C.2.8.4.5] ..... 3-**Error! Bookmark not defined.**

**List of Figures**

Figure 1-1. Features and Benefits to the EIS Program..... 1-1

Figure 1-2. Lumen’s Network. .... 1-3

Figure 1-3. Overall CONOPS for the EIS Program. .... 1-6

Figure 1-4. The Lumen Team’s Capabilities..... 1-6

Figure 1.1-1. Overview of Lumen Network Architecture..... 1-9

Figure 1.1-2. Conceptual View of External Traffic Routing..... 1-14

Figure 1.2.1-1. Services Proposed by Lumen. .... 1-18

Figure 1.3.1.1-1. Features of Lumen VPNS ..... 1-23

Figure 1.3.1.1.1-1. Network Overview of Lumen’s VPNS. .... 1-25

Figure 1.3.1.1.1.1-1. Lumen VPNS Secure Access Architecture. .... 1-31

Figure 1.3.1.1.1.2-1. VPNS CoS Categories ..... 1-32

Figure 1.3.1.1.4-1. Sample DiffServ Queue Mappings ..... 1-35

Figure 1.3.1.1.7-1. Lumen VPNS QoS/Performance Metrics ..... 1-39

Figure 1.3.1.1.7-2. Lumen Proposes to Include Jitter as Additional KPI..... 1-39

Figure 1.3.1.2-1. Lumen’s Industry Leadership in Carrier Grade Ethernet..... 1-41

Figure 1.3.1.2-2. Features of Lumen’s ETS ..... 1-42

Figure 1.3.1.2.1-1. Overview of Lumen ETS Delivery Over an MPLS Core. .... 1-45

Figure 1.3.1.2.1-2. ETS Configurations: (a) E-LINE Point-to-Point, (b) E-LINE Point-to-Multipoint, and (c) E-LAN. .... 1-46

Figure 1.3.1.2.1-3. Enhanced Management Customer Network Report View. .... 1-47

Figure 1.3.1.2.1-4. Dynamic Capacity “Activate Now” Screen. .... 1-48

Figure 1.3.1.2.1-5. Key Features and Benefits of Lumen’s Adaptive Network Control1-48

Figure 1.3.1.2.3-1. ETS Connectivity and Interoperability ..... 1-50

Figure 1.3.1.2.4-1. Lumen’s ETS Technical Capabilities and Features per SOW  
 C.2.1.2.1.4..... 1-51

Figure 1.3.2.1-1. Features of Lumen IPVS..... 1-55

Figure 1.3.2.1-2. Lumen IPVS Solution Aligned to EIS Program Goals ..... 1-55

Figure 1.3.2.1.1-1. Lumen IPVS — Hosted Solution. .... 1-59



---

Figure 1.3.2.1.1-2. Lumen IPVS – Premise-Based Solution. ....	1-60
Figure 1.3.2.1.4-1. IPVS Technical Capabilities. ....	1-61
Figure 1.3.2.1.5-1. Hosted and Premises-Based IPVS Compliant Solution .....	1-66
Figure 1.3.2.3-1. Lumen’s SIP Trunking Functionality. ....	1-73
Figure 1.3.2.3.2-1. Lumen’s SIP Trunking Features.....	1-74
Figure 1.3.3.1-1. Features of Lumen MNS .....	1-76
Figure 1.3.3.1-2. Lumen MNS Solution Satisfies EIS Program Goals.....	1-76
Figure 1.3.3.1.1-1. Lumen Team MNS Solution Overview. ....	1-78
Figure 1.3.3.1.1-2. Lumen MNS Elements and Functions.....	1-79
Figure 1.3.3.1.4.1-1. Lumen’s MNS Design and Engineering Phases .....	1-82
Figure 1.3.3.1.4.1-2. MNS Design and Engineering Services Technical Capabilities	1-83
Figure 1.3.3.1.4.2-1. MNS Implementation, Management and Maintenance Technical Capabilities.....	1-86
Figure 1.4.1.1-1. Features of Lumen’s OWS.....	1-91
Figure 1.4.1.1.1-1. Optical Wavelength Service (OWS) Architecture Overview. <b>1-Error! Bookmark no</b>	
Figure 1.4.1.1.3-1. Lumen’s OWS Connectivity and Interoperability .....	1-93
Figure 1.4.1.1.4-1. Lumen’s OWS Technical Capabilities .....	1-94
Figure 1.4.1.1.5-1. Features of Lumen’s OWS.....	1-95
Figure 1.4.1.2-1. Features of Lumen PLS .....	1-97
Figure 1.4.1.2.1-1. Example of a Coast-to-Coast, Protected Service. ....	1-99
Figure 1.4.1.2.4-1. Lumen Compliance with PLS Categories.....	1-100
Figure 1.4.1.3-1. Feature Summary of Lumen SONETS.....	1-104
Figure 1.4.1.3.1-1. SONETS Architecture Overview. ....	1-105
Figure 1.4.1.3.4-1. Lumen Compliance with SONETS Technical Capabilities .....	1-107
Figure 1.4.1.3.5-1. Lumen’s Support of SONETS Features per SOW C.2.1.5.2 .....	1-108
Figure 1.4.1.4-1. Features of Lumen DFS.....	1-111
Figure 1.4.1.4.1-1. Dark Fiber Services Architecture Overview. ....	1-113
Figure 1.4.1.4.4-1. Lumen DFS Technical Capabilities .....	1-115
Figure 1.4.1.4.5-1. Features of Lumen’s DFS .....	1-117

---

Figure 1.4.1.5-1. Features of Lumen IPS .....	1-119
Figure 1.4.1.5.1-1. IPS Architecture Overview. ....	1-121
Figure 1.4.1.5.1-2. Lumen’s Network Extensive Peering Locations by City .....	1-121
Figure 1.4.1.5.4-1. Lumen’s Compliance with IPS Technical Capabilities.....	1-122
Figure 1.4.2.1-1. CSVS Feature Highlights .....	1-124
Figure 1.4.2.1.1-1. Lumen Circuit Switched Services. ....	1-126
Figure 1.4.2.1.4-1. CSVS Technical Capabilities .....	1-126
Figure 1.4.2.1.5-1. Lumen Compliant CSVS Features .....	1-127
Figure 1.4.2.2-1. Features of Lumen’s TFS.....	1-128
Figure 1.4.2.2.1-1. Lumen Flexible and Compliant TFS Solution. ....	1-130
Figure 1.4.2.2.4-1. TFS Technical Capabilities .....	1-131
Figure 1.4.2.2.5-1. TFS Features .....	1-132
Figure 1.4.2.2.5.1-1. TFS Feature Reports .....	1-135
Figure 1.4.2.3-1. CSDS Feature Highlights .....	1-137
Figure 1.4.2.3.4-1. CSDS Technical Capabilities .....	1-139
Figure 1.4.2.3.5-1. Lumen CSDS Features .....	1-140
Figure 1.4.3-1. Features of Lumen’s CCS.....	1-141
Figure 1.4.3.1-1. Lumen Team’s Contact Center Solution Overview. ....	1-144
Figure 1.4.3.4-1. CCS Technical Capabilities.....	1-145
Figure 1.4.3.5-1. CCS Features .....	1-147
Figure 1.4.4-1. Features Lumen CHS .....	1-150
Figure 1.4.4.1-1. Representation of Lumen Data Center Automated Failover Architecture. ....	1-152
Figure 1.4.4.4-1. Technical Capabilities of Lumen CHS.....	1-153
Figure 1.4.5-1. Summary of Lumen Team CSPs .....	1-155
Figure 1.4.5-2. Lumen Cloud Connect Solutions Portfolio. ....	1-157
Figure 1.4.5.1-1. Representative Lumen Team Member IaaS Experience.....	1-158
Figure 1.4.5.1-2. Features of Lumen Team IaaS .....	1-159
Figure 1.4.5.1.1-1. Lumen Team IaaS Architecture (Representative). ....	1-161

---

Figure 1.4.5.1.4.1-1. Technical Capabilities of Lumen Team Private Cloud per SOW  
 Section C.2.5.1.1.4.1 ..... 1-163

Figure 1.4.5.1.4.2-1. Compliant Technical Capabilities of Lumen Team Data Center  
 Augmentation with ITSM (Hybrid Cloud) per SOW C.2.5.1.1.4.2 ..... 1-166

Figure 1.4.5.1.5-1. Lumen Team Support for IaaS Features per SOW C.2.5.1.2..... 1-166

Figure 1.4.5.2-1. Feature of Lumen Team PaaS ..... 1-168

Figure 1.4.5.2.1-1. Architectural Overview of Lumen’s PaaS Solution. .... 1-170

Figure 1.4.5.2.1.4-1. Lumen Team Compliance with PaaS Technical Capabilities .. 1-171

Figure 1.4.5.3-1. Features of Lumen Team SaaS ..... 1-172

Figure 1.4.5.3.1-1. Microsoft Active Directory Architecture. .... 1-174

Figure 1.4.5.4-1. Features of Lumen CDNS ..... 1-177

Figure 1.4.5.4.1-1. Lumen's CDNS Architecture. .... 1-178

Figure 1.4.5.4.4-1. Lumen’s Compliance with Requirements for Content  
 Distribution ..... 1-180

Figure 1.4.5.4.4-2. Lumen Compliance with Requirements for Site Monitoring / Server  
 Performance Measurements ..... 1-181

Figure 1.4.5.4.5-1. Lumen Team Compliance with CDNS Technical Capabilities .... 1-182

Figure 1.4.5.4.5-2. Additional Lumen CDNS Features ..... 1-182

Figure 1.4.8.1-1.CSCS Feature Highlights ..... 1-191

Figure 1.4.7.1-1. EIS CSCS Resources. .... 1-192

Figure 1.4.8.1-1. WCS Feature Highlights..... 1-196

Figure 1.4.8.1.4-1. WCS Technical Capabilities ..... 1-197

Figure 1.4.8.1.5-1. WCS Service Features..... 1-200

Figure 1.4.8.2.-1. UCS Feature Highlights ..... 1-201

Figure 1.4.8.2.1-1. Lumen’s UCS Service Architecture. .... 1-203

Figure 1.4.8.2.4-1. Mandatory UCS Technical Capabilities ..... 1-204

Figure 1.4.8.2.4-2. Esna Cloudlink Platform. .... 1-205

Figure 1.4.8.2.4-3. Cisco IM and Presence Service. .... 1-206

Figure 1.4.8.3-1. Features of Lumen’s MTIPS ..... **1-Error! Bookmark not defined.**

---

Figure 1.4.8.3.1-1. Lumen MTIPS Schematic Depiction. **1-Error! Bookmark not defined.**

Figure 1.4.8.3.1-2. Lumen TIC Portal. .... **1-Error! Bookmark not defined.**

Figure 1.4.8.3.3-1. Lumen’s MTIPS Complies with all Connectivity Requirements**1-Error! Bookmark not defined.**

Figure 1.4.8.3.4.1-1. Compliant MTIPS TIC Portal Capabilities**1-Error! Bookmark not defined.**

Figure 1.4.8.3.4.2-1. MTIPS Transport Collection and Distribution Capabilities**1-Error! Bookmark not defined.**

Figure 1.4.8.3.5-1. Lumen Team’s MTIPS Solution Features**1-Error! Bookmark not defined.**

Figure 1.4.8.4-1. Features of Lumen’s MSS..... **1-Error! Bookmark not defined.**

Figure 1.4.8.4.1-2. Overlap of Capabilities Derived and Executed for MTIPS and MPS Features. .... **1-Error! Bookmark not defined.**

Figure 1.4.8.4.4.1-1. Lumen’s MPS Technical Capabilities Compliance**1-Error! Bookmark not defined.**

Figure 1.4.8.4.4.3-1. Lumen’s Compliance with All INRS Technical Capabilities Requirements ..... **1-Error! Bookmark not defined.**

Figure 1.4.8.4.5-1. Lumen’s Compliance with All MSS Features Requirements**1-Error! Bookmark not defined.**

Figure 1.4.8.5-1. MMS Feature Highlights..... 1-264

Figure 1.4.8.5.4.1-1. Lumen Team MMS MDM Capabilities..... 1-266

Figure 1.4.8.5.4.2-1. Lumen Team MMS MAM Capabilities..... 1-267

Figure 1.4.8.5.4.4-1. Lumen Team MMS Mobile Security Capabilities..... 1-268

Figure 1.4.8.5.4.5-1. Lumen Team MMS Deployment Support Capabilities..... 1-270

Figure 1.4.8.6-1 ACS Feature Highlights..... 1-271

Figure 1.4.8.6.1-1. ACS Architecture. .... 1-272

Figure 1.4.8.6.4-1. Lumen Compliance with ACS Technical Capabilities Requirements ..... 1-273

Figure 1.4.8.6.5-1. Lumen Team ACS Complies with Required Features..... 1-274

Figure 1.4.8.7.1-1. Features of Lumen’s VTS Solution..... 1-276

Figure 1.4.8.7.2-1. VTS Architecture. .... 1-277

Figure 1.4.8.7.4-1. Lumen Compliance with VTS Technical Capabilities ..... 1-278

Figure 1.4.7.8.5-1. Lumen Team VTS Complies with Required Features ..... 1-279

Figure 1.4.8.8.1-2. Lumen Conceptual DIPSS Architecture. .... 1-283

Figure 1.4.8.8.1-3. Lumen Conceptual DIPSS Architecture Elements Description .. 1-283

---

Figure 1.4.8.8.4-1. DIPSS Technical Capabilities ..... 1-286

Figure 1.4.8.1.5-1. DIPSS Service Features. .... 1-290

Figure 1.4.9-1. Features of Lumen’s Access Arrangements Solution..... 1-301

Figure 1.4.9.1-1. Lumen Access Arrangements. .... 1-303

Figure 1.4.9.4-1. Access Arrangement Technical Capabilities ..... 1-304

Figure 1.4.10-1. Features of Lumen’s SRE Solution ..... 1-307

Figure 1.4.11-1. Features of Lumen’s SRL Solution ..... 1-310

Figure 1.4.11-2. Service Related Positions and SOC Code with Occupational  
 Group ..... 1-310

Figure 1.4.12-1. Features of Lumen’s Cable and Wiring Solution ..... 1-311

Figure 1.4.12-2. Cable and Wiring Compliance with SOW Requirements..... 1-312

Figure 1.4.13-2. Features of Lumen’s External Traffic Routing Solution ..... 1-316

Figure 2.1-1. Lumen Risk Management Approach per NIST SP 800-37 Tiers..... 2-3

Figure 2.3-1. Conceptual Agency Data Protection Schema. .... 2-6

Figure 2.5-1. Risk Management Framework Process Steps (NIST SP 800-37)..... 2-7

Figure 2.5.2-1. FIPS 200 Security Control Families ..... 2-10

Figure 2.5.2-2. Management of Threats against Physical Assets of Lumen..... 2-11

Figure 2.5.2.3. Management of Threats against Management Elements of Lumen ... 2-12

Figure 3.0-1. The Risk Management Framework Cycle. **3-Error! Bookmark not defined.**

Figure 3.1.2-1. MTIPS Block Diagram. .... **3-Error! Bookmark not defined.**

Figure 3.1.2-2. Higher Level MTIPS Block Diagram. ... **3-Error! Bookmark not defined.**

Figure 3.1.2-3. Further Details of MTIPS per Task 1-2 Supplemental Guidance**3-Error! Bookmark not defined.**

Figure 3.2.2-1. Access Control (AC) Family of Controls Implemented for MTIPS**3-Error! Bookmark not defined.**

Figure 3.2.2-2. Awareness and Training (AT) Controls for MTIPS**3-Error! Bookmark not defined.**

Figure 3.2.2-3. Audit and Accountability (AU) Controls for MTIPS**3-Error! Bookmark not defined.**

Figure 3.2.2-4. Security Assessment and Authorization (CA) Controls for MTIPS**3-Error! Bookmark not defined.**

Figure 3.2.2-5. Security Configuration Management (CM) Controls for MTIPS**3-Error! Bookmark not defined.**

Figure 3.2.2-6. Contingency Planning (CP) Controls for MTIPS**3-Error! Bookmark not defined.**

Figure 3.2.2-7. Identification and Authorization (IA) Controls for MTIPS**3-Error! Bookmark not defined.**

- Figure 3.2.2-8. Incident Response (IR) Controls for MTIPS3-**Error! Bookmark not defined.**
- Figure 3.2.2-9. Maintenance (MA) Controls for MTIPS 3-**Error! Bookmark not defined.**
- Figure 3.2.2-10. Media Protection (MP) Controls for MTIPS3-**Error! Bookmark not defined.**
- Figure 3.2.2-11. Physical and Environmental Protection (PE) Controls for MTIPS3-**Error! Bookmark not defined.**
- Figure 3.2.2-12. Planning (PL) Controls for MTIPS..... 3-**Error! Bookmark not defined.**
- Figure 3.2.2-13. Personnel Security (PS) Controls for MTIPS3-**Error! Bookmark not defined.**
- Figure 3.2.2-14. Risk Assessment (RA) Controls for MTIPS3-**Error! Bookmark not defined.**
- Figure 3.2.2-15. System and Services Acquisition (SA) Controls for MTIPS3-**Error! Bookmark not defined.**
- Figure 3.2.2-16. System and Communications Protection (SC) Controls for MTIPS3-**Error! Bookmark not defined.**
- Figure 3.2.2-17. System and Information Integrity (SI) Controls for MTIPS3-**Error! Bookmark not defined.**
- Figure 3.2.2-18. Program Management (PM) Controls for MTIPS3-**Error! Bookmark not defined.**
- Figure 3.2.2-19. Privacy Controls for MTIPS..... 3-**Error! Bookmark not defined.**
- Figure 3.7-1. Schedule for MTIPS Development and ATO under Networx3-**Error! Bookmark not defined.**

**Abbreviation and Acronym Definitions List**

A&A	Assessment and Authorization
AA	Access Arrangements
ACD	Automatic Call Distribution
ACL	Access Control List
ACS	Audio Conferencing Service
AD	Active Directory
ADM	Add/Drop Multiplexer
ANC	Adaptive Network Control
ANSI	American National Standards Institute
API	Application Programming Interface
AQL	Acceptable Quality Levels
AS	Autonomous System
ATA	Analog Terminal Adapter

ATO	Authority to Operate
AWS	Amazon Web Services
BFD	Bi-Directional Forwarding Detection
BGAN	Broadband Global Area Network
BGP	Border Gateway Protocol
BLSR	Bi-Directional Line Switched Ring
BoD	Bandwidth on Demand
BOM	Bill of Materials
BSS	Business Support System
BYOD	Bring Your Own Device
C&W	Cable and Wiring
C2	Command and Control
CAD	Computer Aided Design
CALEA	Commission on Accreditation for Law Enforcement Agencies
CBS	Committed Burst Size
CCM	Customer Care Manager
CE	Customer Edge
CFR	Code of Federal Regulations
CFSS	Commercial Fixed Satellite Service
CHS	Colocated Hosting Service
CIR	Committed Information Rate
CM	Configuration Management
CMSS	Commercial Mobile Satellite Service
CNAM	Called ID Name
CNEC	Commander Naval European Command
CNP	Customer Network Planning
COMSATCOM	Commercial Satellite Communications

CONOPS	Concept of Operations
COOP	Continuity of Operations
CoS	Class of Service
CP	Contingency Planning
CPE	Customer Premise Equipment
CPMO	Contractor Program Management Office
CRM	Customer Relations Management
CRM	Customer Relationship Management
CSDS	Carrier Switched Data Service
CSO	Customer Support Organization
CSP	Cloud Service Provider
CSVS	Circuit-Switched Voice Service
CT	Computer Telephony
CTI	Computer Telephony Integration
CUI	Controlled Unclassified Information
DCA	Data Collection Appliance
DCIM	Data Center Infrastructure Management
DCS	Digital Cross Connect System
DF	Dark Fiber
DFS	Dark Fiber Services
DHS	Department of Homeland Security
DIA	Dedicated Internet Access
DNS	Domain Name Service
DoD	Department of Defense
DoS	Denial of Service
DR	Disaster Recovery
DTE	Data Terminal Equipment
DWDM	Dense Wavelength Division Multiplexing



EBS	Excess Burst Size
ECS	Enhanced Cybersecurity Services
EIA	Electronic Industries Alliance
EIR	Excess Information Rate
EIS	Enterprise Infrastructure Solutions
EMEA	Europe-Middle East-Asia
EMI	Electro Magnetic Interference
EN	Event Notification
ENNI	Ethernet Network to Network Interface
EOP	Executive Office of the President
EP	Emergency Preparedness
ERM	E-mail Response Management
ERP	Enterprise Resource Planning
ESF	Extended Superframe
ET	Earth Terminal
ETS	Ethernet Transport Service
EVC	Ethernet Virtual Connection
EVPL	Ethernet Virtual Private Line
FAA	Federal Aviation Administration
FCC	Federal Communications Commission
FCC CSRIC	Communications Security, Reliability and Interoperability Council
FDCCI	Federal Data Center Consolidation Initiative
FDP	Fiber Distribution Panel
FIPS	Federal Information Processing Standards
FISMA	Federal Information Security Management Act
FMS	Fiber Management System
GB	Gigabyte

GCC	Government Community Cloud
GDIT	General Dynamics Information Technology
GFP	Government Furnished Property
GIS	Geographical Information System
GoS	Grade of Service
GovNOC	Government Network Operation Centers
GovSOC	Government Security Operation Centers
GRE	Generic Routing Encapsulation
GVP	Genesys Voice Platform
HCM	Human Capital Management
HD	High Definition
HOA	Horn of Africa
HSIP	High Speed Internet Protocol
HTTP	Hyper Text Transfer Protocol
HVAC	Heating, Ventilation & Air Conditioning
IA	Information Assurance
ICB	Individual Case Basis
IDWG	Intrusion Detection Exchange Format Working Group
IEC	International Electrotechnical Commission
IEEE	Institute of Electrical Engineering
IETF	Internet Engineering Task Force
IFL	Inter-Facility Link
IGC	Intelsat Government Corporation
IM&P	Instant Messaging & Presence
INRS	Incident Response Service
IOC	Indications of Compromise
IPS	Internet Protocol Service
IPVPN	IP-based Virtual Private Network

IPVS	Internet Protocol Voice Service
ISM	In-Service Monitoring
ISP	Internet Service Provider
ISSM	Information System Security Manager
ISSO	Information System Security Officer
ITA	International Trade Administration
IT-SAC	Information Sharing and Analysis Center
ITSM	Information Technology Service Management
ITU	International Telecommunications Union
ITU-T	International Telecommunications Union
IVR	Interactive Voice Response
KPI	Key Performance Indicator
LDAP	Lightweight Directory Access Protocol
LEAF	Large Effective Area Fiber
LEC	Local Exchange Carrier
LGB	Log Database
LNP	Local Number Portability
LSP	Label Switched Path
M2M	Machine to Machine
MA	System Maintenance Policy and Procedures
MAC	Mission Assurance Category
MACD	Moving Average Convergence/Divergence
MAM	Mobile Application Management
MBS	Maximum Burst Size
MCM	Mobile Content Management
MCU	Multipoint Control Unit
MDM	Mobile Device Management
MEF	Metro Ethernet Forum

MLS	Managed LAN Service
MMS	Managed Mobility Service
MNS	Managed Network Service
MOA	Memorandum of Agreement
MOS	Mean Opinion Score
MPLS	Multi-Protocol Label Switching
MPS	Managed Prevention Service
MTIPS	Managed Trusted Internet Protocol Service
N&T SIG	Network and Telecommunications Special Interest Group
NANOG	North American Network Operators Group
NANP	North American Numbering Plan
NASS	North American Softswitch
NCAS	Non-Call Associated Signaling
NCC	National Coordinating Center for Communications
NCD	Network Call Distributor
NID	Network Interface Device
NIST	National Institute of Standards and Technology
NMS	Network Management System
NOC	Network Operations Center
NoN	Network of Networks
NS	National Security
NSP-Sec	Network Service Provider Security Association
NTP	Network Time Protocol
NTSC	National Television Standards Committee
NxGE	Nx Gigabit Ethernet
OCO	Ordering Contracting Officer
OFSTP	Optical Fiber System Test Procedure

OIF	Optical Internetworking Forum
OMB	Office of Management and Budget
OPM	Office of Personnel Management
OSP	Outside Plant
OSS	Operations Support System
OTN	Optical Transport Network
OWS	Optical Wavelength Service
PA	Participating agency
PaaS	Platform as a Service
PCI DSS	Payment Card Industry Data Security Standard
PE	Provider Edge
PIR	Peak Information Rate
PLS	Private Line Service
PM	Project Manager
PoE	Power over Ethernet
PoP	Point of Presence
PSAP	Public Service Access Point
PSTN	Public Switched Telephone Network
PtP	Point-to-Point
QoS	Quality of Service
RACC	Routing and Call Control
RADIUS	Remote Authentication Dial-In User Service
RBAC	Role-Based Access Control
RFC	Request for Comments
RFI	Radio Frequency Interference
RFP	Request for Proposal
RSVP	Resource Reservation Protocol
RTP	Real-Time Protocol

SAT	System Architecture Team
SatAA	Satellite Access Arrangements
SBC	Session Border Controller
SBU	Sensitive But Unclassified
SCAP	Security Content Automation Protocol
SCIF	Sensitive Compartmented Information Facilities
SCRM	Supply Chain Risk Management
SDL	Security Development Lifecycle
SDN	Software Defined Networking
SDP	Service Delivery Point
SE	System Engineering
SECAM	Système Electronique Couleur Avec Memoire
SED	Service Enabling Device
SES-GS	SES-Government Solutions
SHR	Self-Healing Ring
SIEM	Security Information and Event Management
SIP	Session Initiating Protocol
SIS	Satellite Internet Service
SOC	Security Operations Center
SONET	Synchronous Optical Network
SONETS	Synchronous Optical Network Services
SRE	Service Related Equipment
SRL	Service Related Labor
SSAE	Standards for Attestation Engagement
SSL	Secure Socket Layer
SSM	Synchronous Status Messaging
SVE	Service Verification Environment
TDM	Time Division Multiplexing

TF	Toll Free
TFS	Toll-Free Service
TIC	Trusted Internet Connection
TICAP	Trusted Internet Connection Access Provider
TLS	Transport Layer Security
TN	Telephone Number
TO	Task Order
ToS	Type of Service
TPID	Tag Protocol Identifier
TSP	Telecommunications Service Priority
TTR	Time to Restore
UC&C	Unified Communications and Collaboration
UIFN	Universal International Free Phone Number
UNI	User Network Interface
UPL	Unprotected Private Line
UPS	Uninterruptible Power Supplies
UPSR	Unidirectional Path Switched Ring
URL	Universal Resource Locator
VA	Veterans Affairs
VESDA	Very Early Smoke Detection Apparatus
VFI	Virtual Forwarding Instance
VLAN	Virtual Local Area Network
VM	Virtual Machine
VOIP	Voice Over Internet Protocol
VPLS	Virtual Private LAN Service
VPN	Virtual Private Network
VPNS	Virtual Private Network Service
VRF	Virtual Routing and Forwarding

VSS	Vulnerability Scanning Service
VTS	Video Teleconferencing Service
WAN	Wide Area Network
WDM	Wavelength Division Multiplexing
WFM	Workforce Management
WG	Working Group
WPS	Wireless Priority Services
XMPP	Extensible Messaging and Presence Protocol

### **Assumptions and Conditions**

Lumen has no Assumptions or Conditions for Volume 1 at this time.



**VOLUME 1 TECHNICAL**

**INTRODUCTION**

*Lumen, a U.S. based Fortune 500 company, in partnership with GSA delivers services today to more than 300 U.S. Government entities. Additionally, we provide telecommunications services to more than 50,000 business customers around the world. We partner to innovate and deliver world-class any device, anywhere solutions that are secure, reliable, scalable, and provide the greatest return on investment possible for EIS.*

*Lumen has been at the forefront of transforming the way the world communicates. The Lumen team applies our innovation and experience transforming telecommunications around the world. As an incumbent on both WITS and Networx, Lumen has partnered with GSA to transition and deliver superior services and solutions, helping our customers such as DHS, U.S. Courts and DISA to realize increased efficiencies and reduced costs through innovation. Lumen has delivered those services with a dedication to the success of the agency customers and GSA. The Lumen team continues to leverage our experience and understanding that comes with our 10-year incumbency. Our end-to-end solutions providing transport, voice, cloud and managed services are fully compliant with the technical and management requirements of the Enterprise Infrastructure Solutions (EIS) Request for Proposal (RFP).*

**Figure 1-1** summarizes key features of the Lumen Team’s EIS solution and their benefits. Our benefits ensure best value, trusted service delivery, and agency mission enablement.

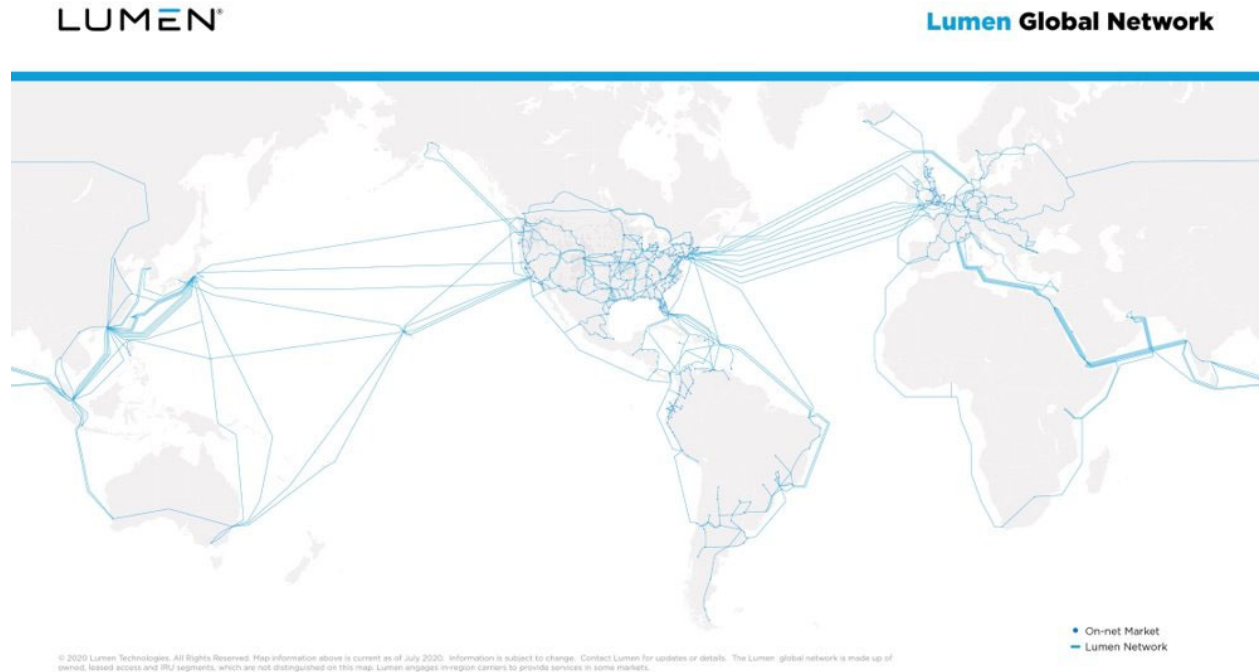
**Figure 1-1. Features and Benefits to the EIS Program**

FEATURES	BENEFITS FOR GSA
Experienced Management Team	<ul style="list-style-type: none"> <li>Led by our Program Manager, Mr. Matthew Scelza, who is well suited for our business objectives and strategy. Mr. Scelza has successfully led our NETWORKX and WITS program teams.</li> <li>Our Executive Team has substantial experience in leading the development, marketing and sale of communications services and in managing, designing and constructing metropolitan, intercity and international networks.</li> </ul>
Recognized Industry	<ul style="list-style-type: none"> <li>We have a proven track record among communication service providers for being the first to</li> </ul>

FEATURES	BENEFITS FOR GSA
Leadership	implement many new technologies, including: global MPLS network in 2001. <ul style="list-style-type: none"> <li>• First global provider with IPV6 natively deployed, first to introduce VoIP and MPLS, and the first converged IPs</li> </ul>
Global Reach of Our Network	<ul style="list-style-type: none"> <li>• We deliver services to more than 60 countries around the world on our global network.</li> <li>• Our network connects and crosses North America, Latin America, Europe and a portion of the Asia/Pacific region.</li> </ul>
A Broad Range of Communications Services	<ul style="list-style-type: none"> <li>• We provide a broad range of communications services designed to meet the needs of our customers over our network.</li> <li>• Lumen has access to products and services that are functionally equivalent to those currently available, and Enterprise-wide user agencies have access to new technology solutions</li> </ul>

Foundational to the Lumen’s Management Solutions for EIS is our global network. Lumen’s American-owned and operated global fiber network is one of the newest, highest-fiber-count networks. It includes extensive owned intercity and metro facilities in North America, including Hawaii; Latin America; and Europe; totaling more than [REDACTED] route miles. Lumen also has undersea fiber providing global reach.

Lumen-owned and operated network (**Figure 1-2**) extends to more than 60 countries. Lumen built its network from the ground up to be evolutionary and continuously upgradable, with the agility to respond and meet the ever changing demands of our customers’ missions. Holding hundreds of U.S. and international patents in telecommunications, innovation is at Lumen’s core—so much so that Lumen’s IP network was inducted into the Smithsonian Institution’s permanent archive that records the world’s ongoing evolution in information technology.



**Figure 1-2. Lumen’s Network.** *The Lumen network provides EIS access to one of the largest American-owned/operated fiber networks in the world.*

As a leader in the implementation of new technologies, Lumen was the first to deploy global Multi-Protocol Label Switching (MPLS), Virtual Private Network (VPN), and Lumen’s continuous innovation has led to the practical use of IPv6, and commercialized 100 Gbps services for cost-efficient network capabilities. We were first to support IPv6 natively network-wide. Lumen continues to invest in its network in the U.S. and abroad to provide the foundation for today’s virtual environments.

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

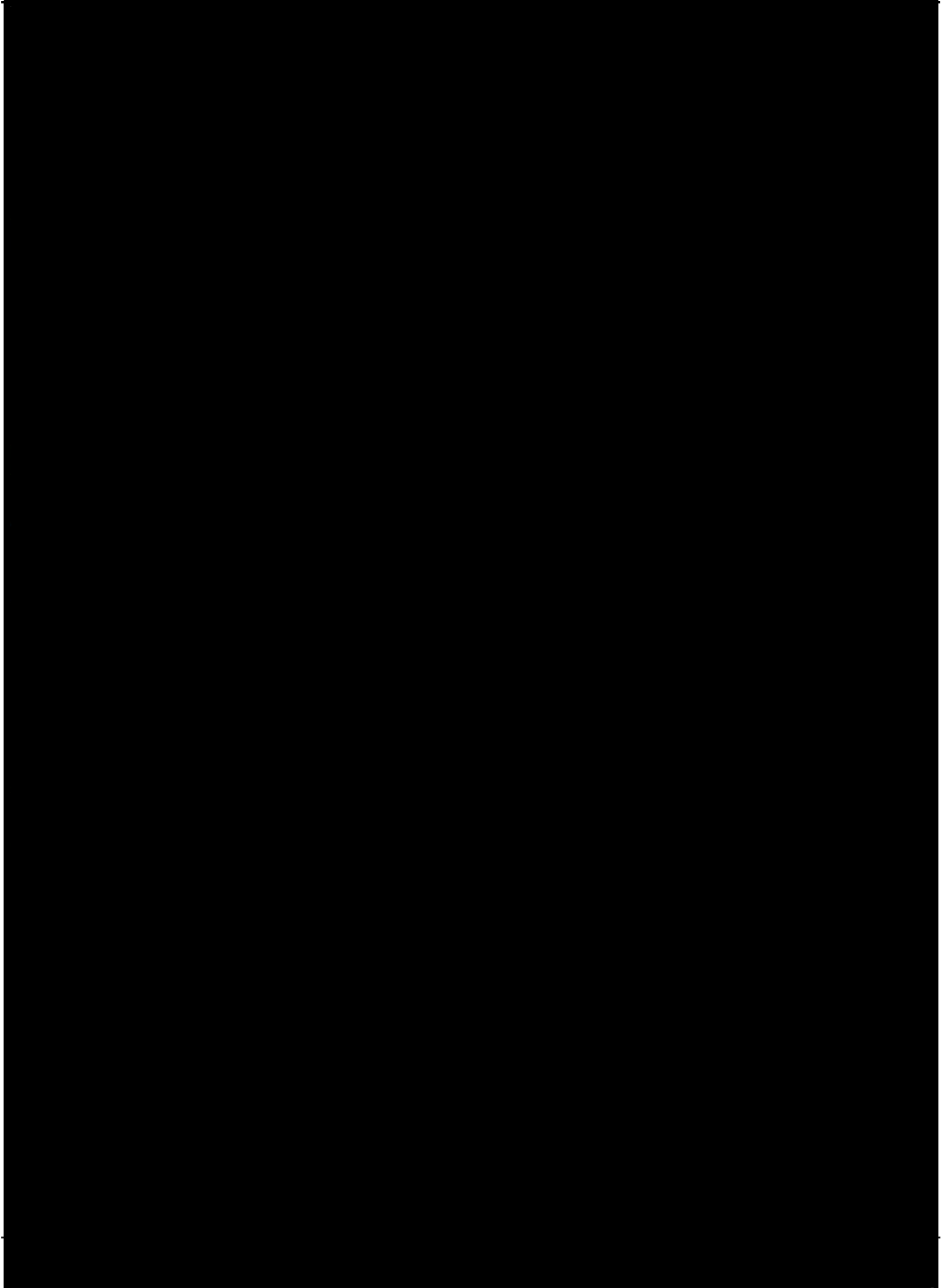
[REDACTED]

With our portfolio of infrastructure solutions and our teams' collective capabilities, Lumen is delivering innovative, hybrid solutions, combining secure access and transport for the smallest remote sites, to the largest enterprises. We provide an end-to-end, secure, managed solution on a converged communications network all the way to agency desktop users. Lumen's Large Contract Management Experience includes:

- 13 years of experience successfully running large, multi-year Federal IDIQ contracts
- Experience with GSA on Networx and WITS
- Federal customers include GSA, NASA, SEC, VA, USDA, SSA, DoD IG, DISA, Marine Corps, U.S. Courts, and DHS

**General Services Administration (GSA)**  
*Enterprise Infrastructure Solutions (EIS)*

Contract # GS00Q17NSD3006  
Mod #: P00310  
Submission #: CL01001.01a









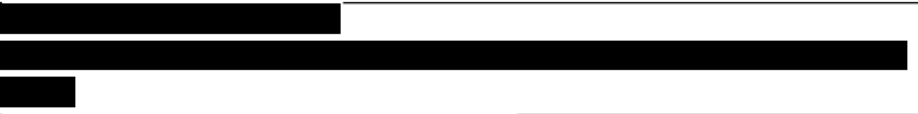




**Figure 1-3. Overall CONOPS for the EIS Program.** *Our Team’s CONOPS approach delivers a mix of highly qualified people, processes, and technical capabilities.*

**THE LUMEN TEAM**

In keeping with our management approach and commitment to best value to support EIS’ critical business and Government needs, Lumen has assembled an agile, focused, and very capable team with proven experience to partner with GSA and successfully deliver to each customer mission (**Figure 1-4**). Our Team members supplement our network coverage with terrestrial or satellite services, equipment, systems, and support solutions.

**Figure 1-4. The Lumen Team’s Capabilities**

TEAMMATE	TEAM CAPABILITIES
 Prime Contractor	Proven Federal partner with 10 years incumbency supporting GSA’s Network Enterprise, WITS 3, and multiple Local Service Agreements (LSA) Over 300 of Government entities depend on Lumen to design build and manage complex global networks and IT infrastructures. Our low-latency private, public and hybrid connectivity options help securely move voice, video and data around the world Metrics-driven, systematic continuous process improvements
	
	
	
	
	

TEAMMATE	TEAM CAPABILITIES
Cloud Services	Lumen along with select partners delivering Collocation, CDN, IaaS, PaaS, and SaaS capabilities helping to reduce the overall Federal environment footprint Lumen has relationships with companies such as [REDACTED]
Premises Infrastructure	Strategic partnerships with proven Federal incumbents including [REDACTED] for regional, national, and global support

**1.1 Network Architecture [L.29.1, C.1.6]**

The Lumen Team delivers 31 specified EIS services to include the five mandatory and 26 optional services, and looks forward to building on our 10-year partnership with GSA. We provide our EIS solution through a robust and well-integrated network architecture based upon the Lumen capacious, flexible, and adaptable global network. We support our Lumen architecture with our Government Network Operation Centers (GovNOC) and Government Security Operation Centers (GovSOC), as well as our Team’s experienced personnel and processes. The Lumen network architecture includes seamless integration of Lumen and our partner’s network elements functioning like a single entity to provide EIS services to the Government. We strategically select team partner companies to provide “best in class” EIS network service elements to complement those provided by Lumen. Our highly capable partner specialists possess extensive experience delivering EIS service elements to Government and industry.

**Lumen’s Forward-Looking Network Architecture**  
**Realizes EIS Program and Service Goals**

- Flexible, layered architecture accommodates partner services to enable our support of 31 EIS services.
- Network and security architectures satisfy DHS and OMB complex security requirements
- Lumen’s vision of IP-over-fiber yields scalability, security, and innovation platform whose advances now include SDN in the WAN.
- Redundant, dedicated GovNOCs and GovSOCs provide focused support for Government.

The Lumen network architecture supports the GSA goal to provide flexible and agile capabilities to satisfy a broad spectrum of global communications services extending over the next decade and beyond. The Lumen portfolio of service solutions in conjunction with our team’s collective capabilities deliver innovative, hybrid solutions that combine secure access and transport for the smallest remote sites, to the largest enterprises. We provide an end-to-end, secure, managed EIS solution on a converged communications network all the way to agency desktop users.

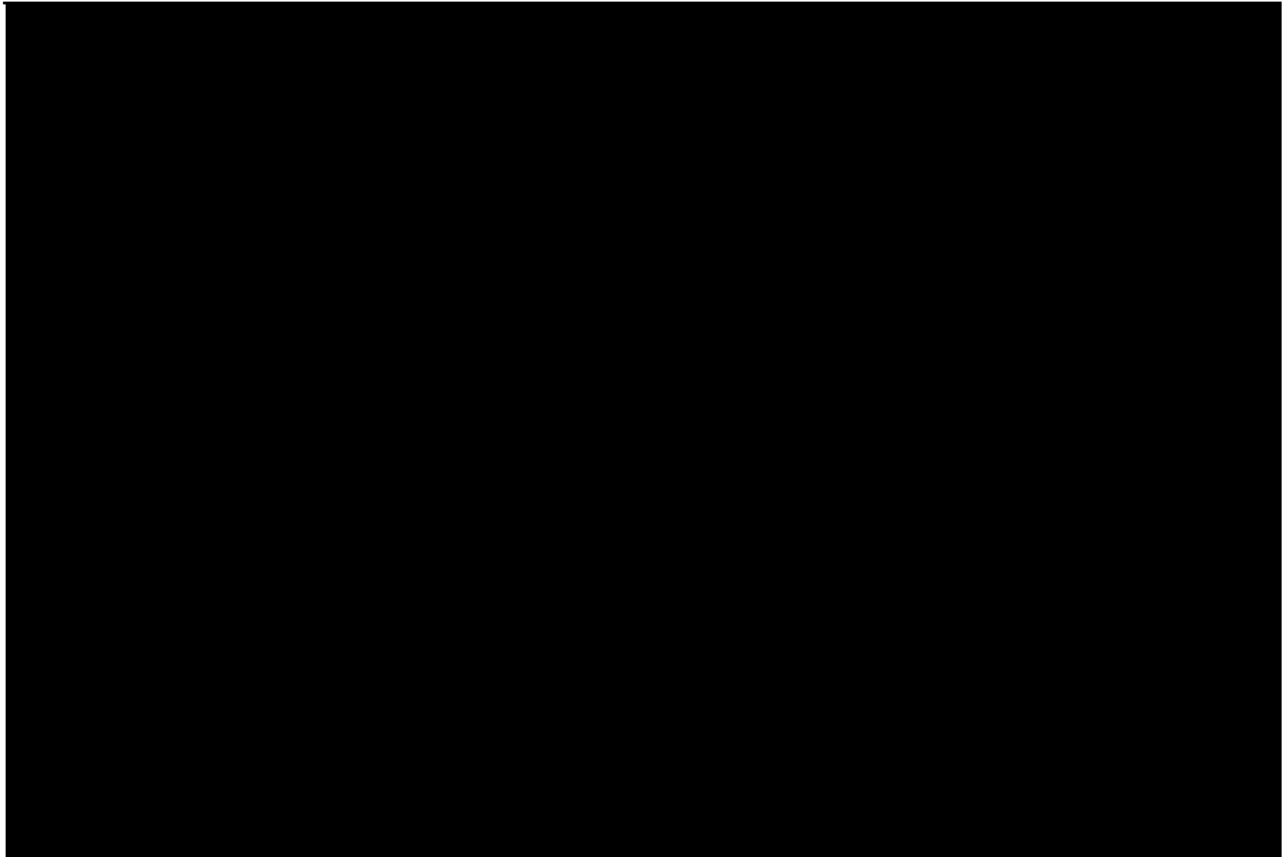
---

As a relative newcomer from a historical perspective to the telecommunications industry; legacy technologies and infrastructure reaching end of life do not encumber Lumen like those experienced by companies founded on traditional Local Exchange Carrier architectures. Although we built transitional or gateway technologies to integrate with traditional copper services, we designed and implemented our infrastructure for the post copper era with the capability to rapidly create, innovate and adopt new technology. For example, in 2015 Lumen introduced Adaptive Network Control (ANC), a feature set that gives customers immediate, *software-driven control* of Ethernet access bandwidth. *It is one of the first operational examples of Software Defined Networking (SDN) moving beyond the data center and into the WAN.*

**Figure 1.1-1** presents an overview of the Lumen network architecture. It highlights:

- The network's architectural layers and primary delivery layers for EIS services
- Integration points *for teaming* and carrier partner capabilities
- Our Government-dedicated, redundant network and security operations centers (GovNOC and GovSOC)
- Agency support by dedicated Lumen personnel





**Figure 1.1-1. Overview of Lumen Network Architecture.** *The network platform delivers EIS services worldwide with quality, scalability and security.*

Large scale networks require physical assets, and Lumen provides our fundamental network layer with our massive fiber plant and our robust optical lighting systems. Optical channels today operate at 100 Gbps. Lumen deploys fiber on a large scale – in fiber and conduit count, and in coverage in the U.S. and abroad.

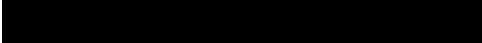
Synchronous Optical Network (SONET) remains a key technology at network layer 1, and Lumen deploys SONET worldwide. Ethernet and Optical Network Transport (OTN) technology incorporates key features of SONET technology; as such Lumen uses both to increase network coverage and reliability.

**Figure 1.1-1** shows the importance of the Data Switching layer and the many network services directly delivered by this layer. The Lumen Team members and carrier partners confidently rely on this layer for services and extended network coverage. In the Lumen network, the Data Switching layer is founded upon a high speed, high

---

capacity, and highly scalable and secure MPLS platform. MPLS, with its traffic engineering capabilities and Label Switched Paths (LSP), gives Lumen granular control on traffic routing, rerouting, prioritization, and security. We harness these capabilities to satisfy applicable EIS service transport and availability-related Key Performance Indicators (KPI). The integral MPLS in our network establishes and maintains security boundaries and any agency Trusted Domains. The figure also highlights the diverse, redundant Advanced Security Infrastructure which processes all external network traffic of subscribing agencies.

**Figure 1.1-1** also illustrates the increased IP based nature of Voice Services and Specialized Applications. As such, the network readily accommodates them and provides their requisite levels of service quality across all transport KPIs. The software driving these services and applications reside on virtualized servers, not shown in the figure, in order to achieve superior reliability and scalability. The Lumen architecture provides a robust platform with clear operational boundaries enabling our partners to provision their industry leading services.

**Figure 1.1-1** depicts Government-dedicated, redundant Lumen GovNOCs in  They provide the focal point for network operations and problem reporting and resolution. Both staffed 24/7, either one can assume full support duties. The secure GSA Customer Portal, shown in the upper left of the figure, provides the focal point for agencies to access all pertinent customer information. Our FISMA MODERATE portal will meet all the security requirements for data interchange and is based on our previous experience as an incumbent on Networx.

We based the Lumen network architecture EIS Solution upon four key factors: Understanding, Quality of Services, Service Coverage, and Security. This section describes how we considered and applied each of these four key factors in our network architecture. We provide a detailed description of individual service solutions and how these four factors satisfy the delivery of each service solution.

### **Understanding [L.29.1, M.2.1.1]**

---

Our 10-year incumbency supporting GSA provides Lumen with an enterprise-wide understanding of EIS requirements and what is required for successful service delivery. Lumen has demonstrated its ability to understand the unique challenges that Agencies face in a changing communications environment. Working together with customers such as DHS, DISA and U.S. Courts we have developed solutions that provide innovative approaches to Unified Communications, alternate bandwidth and managed security services such as Dedicated Denial of Service; all built on our Lumen Network. We bring a continued understanding to EIS and have aligned our service offerings on EIS to meet the agencies communications needs. Our Team has been assembled to provide a breadth and depth of proven customer service with partners such as GDIT and Hughes Network Systems to deliver innovation and cost savings. We applied our comprehensive understanding of Government needs and requirements for EIS services in the design of our EIS network architecture. We align our comprehensive Lumen Team infrastructure and overlying services with the proposed network architecture and services being provided for EIS. The proposed Lumen EIS services meet the program goals identified within the GSA RFP. Our highly competitive service portfolio provides GSA and the departments and agencies using EIS a strong value for the contract dollars spent.

We honed the Lumen network architecture to meet service requirements across our global customer base to include serving the unique needs of the Government and Commercial customers. Demonstrating our clear understanding of all Government requirements, our network architecture includes dedicated GovNOCs and GovSOCs, and a specialized and dedicated security infrastructure, while providing the fully compliant capability to deliver 31 mandatory and optional EIS services.

**Quality of Service [L.29.1, M.2.1.2]**

We developed our EIS network architecture with high quality of service as a key parameter. Our network architecture applies years of experience in providing services like those required to agencies and other Government entities, along with commercial customers. We offer four and five 9 SLAs to the commercial customer base providing

---

mission critical services to Government and commercial customers. Our scalable, responsive, and reliable network architecture delivers consistently compliant EIS services wherever required.

We staff the Lumen GovNOCs with seasoned technicians who possess years of experience in providing support to GSA, agencies, other Government users, and industry. Our GovNOC staff and support teams provide 24/7 proactive real-time monitoring and performance management support to help ensure that we consistently meet EIS performance requirements. The Lumen Team's extensive past performance experience with similar scope contracts results in the development of mature reporting services required for EIS.

**Service Coverage [L.29.1, M.2.1.3]**

Our network architecture supports global service coverage that significantly exceeds the minimum CBSA requirements specified in SOW C.1.3. For many of the CBSA-dependent services we cover all 929 CBSAs and *we far exceed the coverage minimum for all such services* – including an extensive native colocation offering, through which we provide service in Lumen data centers in 63 CBSAs.

The Lumen network based upon our EIS network architecture not only covers the entire U.S. mainland, but extends to 60 other countries around the globe. Our position as a wholesale carrier and our interconnections with local and regional carriers significantly expands our reach.

**Security [L.29.1, L.29.2.3, M.2.1.4]**

We created the Lumen EIS network architecture with security as a foundational and all-encompassing element. Our distinct, executive level security organization provides focus on the importance of security in Lumen. The Lumen security organization possesses deep understanding of the Government's unique security needs. Drawing from our extensive Government security experience along with our commercial industry best practices, we created GovSOCs specifically to provide agency and other Government users focused security support.

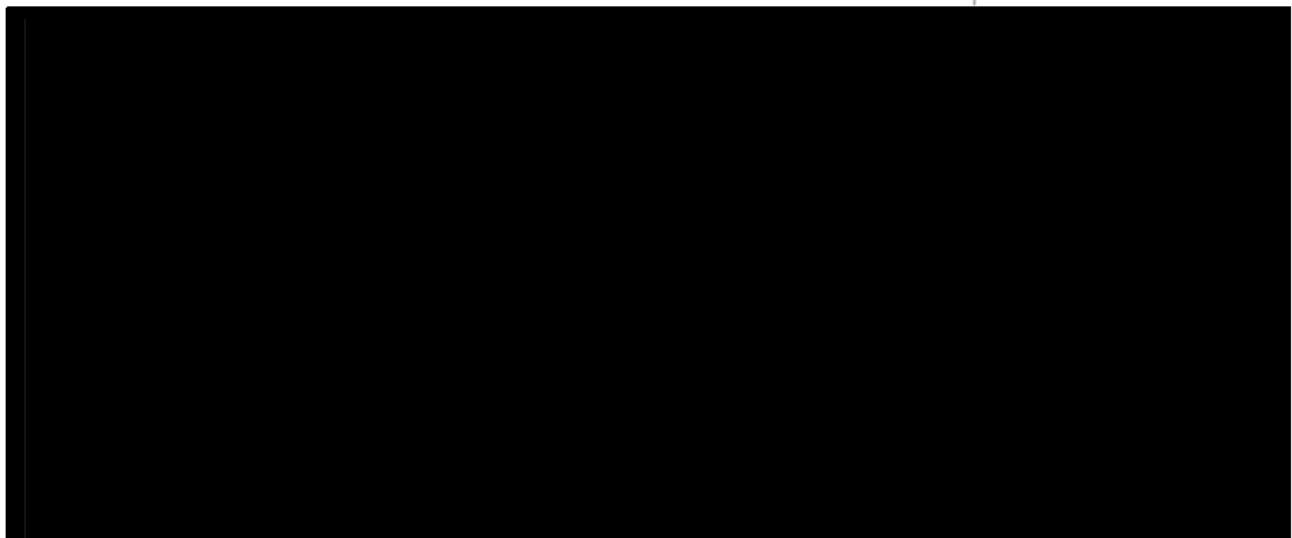
---

In providing consistent and reliable security coverage, Lumen monitors more than a billion physical and virtual security events a day; monitors sophisticated botnets and some 1,000 command and control (C2) servers Internet-wide; and each month detects several zero-day exploit attempts, based on 2<sup>nd</sup> quarter 2015 network data. As necessary, we disrupt C2 channels and work with others in our security ecosystem to do the same. Building on our security vantage point and deep expertise, Lumen offers a managed security solutions portfolio, with MTIPS, MSS and IPSS.

The Lumen security architecture includes programmatic and operational aspects. Programmatic security measures include those outlined in SOW C.1.8.7, System Security Requirements, which we address in Section 2.1 of this Technical Volume. Section 1.4.13 addresses in more detail the operational aspects of our security architecture, in reference to RFP Section L.29.2.3, External Traffic Routing Requirements. The requirements of L.29.2.3 largely stem from OMB Memorandum M-15-01 which stipulates that any EIS service transporting Internet, Extranet, and Inter-agency traffic, such as traffic crossing a Trusted Domain boundary, must identify and route this traffic through a secure DHS EINSTEIN Enclave for processing by the latest generation of EINSTEIN capabilities.

**Figure 1.1-2** shows the external traffic routing security concept and shows the routing and processing by the Enclave of all traffic crossing the Trusted Domain boundary. An external network is any logical network outside of the trusted domain. Therefore [REDACTED]

[REDACTED] Encryption and Decryption can pertain to IPsec or SSL, or the extraction traffic from an MPLS LSP tunnel.



**Figure 1.1-2. Conceptual View of External Traffic Routing.** *The Enclave processes all traffic crossing an agency Trusted Domain boundary.*

The Lumen EIS network architecture satisfies the following eight external traffic routing requirements described in SOW C.1.8.8, and L.29.2.3, and M.2.1:

■ **Traffic Identification.** As part of the bid, design and ordering process, the agency specifies elements of connectivity subject to inspection. For Layer 1 point-to-point (PtP) connectivity, for example PLS, OWS, DFS, and SONETS – including Ethernet over SONET; the Lumen design team defines the routing to pass through an Enclave. [REDACTED]

[REDACTED]

■ **Directing Traffic.** A route layout accomplishes and directs traffic to an Enclave [REDACTED]

For Layers 2 and 3 services, [REDACTED]

[REDACTED]

3. **Non-Participating Agency Traffic.** The Lumen security measures at the Enclave include the capture and subsequent examination of IP addresses for all traffic flows. [REDACTED]

[REDACTED]

[REDACTED] Also, we provide DHS access to violation information including any threat management processes applied to the unauthorized traffic.

[REDACTED] **Control Mechanisms against Bypass.** We define and fix Layer 1 PtP connectivity, [REDACTED]


[REDACTED]

5. **No Service Disruption on Failure of GFP.** [REDACTED]

[REDACTED]



*Engagement of GFP bypass is considered a significant and high-priority network event.*

6. **ANSI/TIA 942 and ICD 705-Certified Facilities.** Lumen provides and supports multiple ANSI/TIA 942 and ICD 705-Certified facilities. Facilities are available in  to support MTIPS service requirements. It is proposed that IPSS and DHS EINSTEIN enclaves are also located in these facilities.
7. **Cleared Personnel.** A feature of the Lumen ICD 705-Certified facilities is 24/7 availability of TS/SCI cleared personnel for “smart-hands” service of DHS-supplied equipment.
8. **Transport Measurement Instrumentation.** The Lumen network provides performance measuring equipment and techniques to verify transport SLA KPIs. This instrumentation measures transport parameters “to, from, and through” the Enclave, and permits subtraction of GFP-attributed processing from measurements to verify Lumen network attributable transport SLA KPIs.

### **1.2 Technical Response [L.29.2; C.2; C.1.8.6; C.1.8.9]**

For EIS, the Lumen Team provides GSA and agencies with global services delivered through our high-capacity U.S.-owned network. Our global network supports current and future service requirements at worldwide Government-designated locations. Lumen EIS support includes engineering, implementing, testing, operations, and maintenance of EIS services, in full compliance with SOW requirements. We also provide customer technical support as required for each of the EIS services.

For EIS, we provide end-to-end solutions and services supporting voice, data and video. Services we provide include the provision and support of legacy services and circuit/service transitions, from existing to new technology services. We also provide secure and reliable service management, and network security for all transmission services. Our EIS services include diversity and avoidance routing in keeping with SOW



---

requirements. We also satisfy all of the interoperability requirements of the SOW C.1.8.6, addressing interoperability for specific EIS services in this volume. Assisting Lumen in delivering and supporting our solutions are a number of capable and proven carriers, field operations companies, and systems solutions providers.

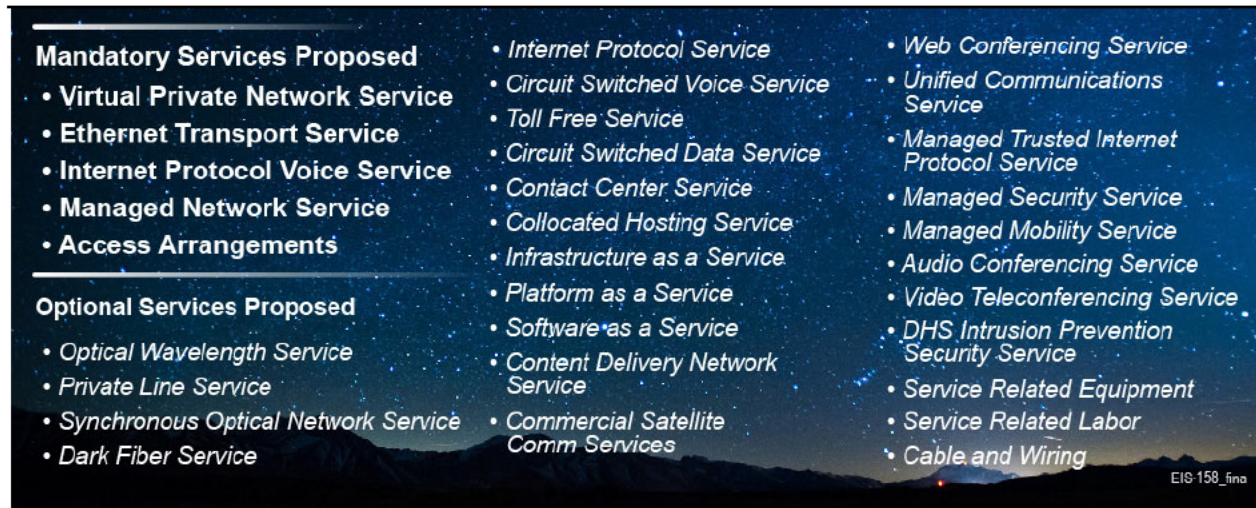
Lumen meets all Section 508 requirements of SOW C.4. Ensuring that Federal content is equally accessible and usable by all EIS users, including those with disabilities – as section 508 of the Rehabilitation Act requires – is an essential aspect of our EIS solution. As specified in SOW C.4, we comply with 508 requirements as follows:

- **Voluntary Product Accessibility Template (VPAT) [C.4.2]:** We will post the VPAT for services as identified in SOW C.4.4
- **Section 508 Applicability and Provisions Applicable to Technical Requirements [C.4.3, C.4.4]:** We comply with all of the requirements of SOW C.4.3 and C.4.4
- **Section 508 Provisions Applicable to Reporting and Training [C.4.5]:** We comply with all of the requirements of SOW C.4.5

### **1.2.1 EIS Services [L.29.2.1; M.4; C.1.2]**

**Lumen provides 31 specified EIS mandatory and optional services.** Our proposed mandatory and optional services are shown in **Figure 1.2.1-1**. A full description of each mandatory and optional service is proposed, including how features and capabilities are architecturally and technically provided, is provided in the following sections of this volume. As applicable for each mandatory and optional service, we address the following service aspects: Service and Functional Description, Standards, Connectivity, Technical Capabilities, Features, Interfaces, and Performance Metrics.

We understand that our proposal for EIS services will be evaluated by the Government for understanding, quality of service, service coverage, and security, as indicated in RFP M.2.1. To illustrate and emphasize how our solution meets these evaluation criteria, these four evaluation factors are discussed in Sections 1.2.1.1 – 1.2.1.4. Further details of how we satisfy the evaluation factors are provided in our responses for the specific services proposed.



**Figure 1.2.1-1. Services Proposed by Lumen.** *The Lumen Team has the network, facilities, processes, and experienced staff to provide the EIS services.*

**1.2.1.1 Understanding [L.29.2.1.A; M.2.1.1]**

GSA clearly identified the goals of the EIS contract in SOW C.1.1 and the hallmarks of our offering are aligned with all of those goals, reflected in this volume as our themes. We have coupled our EIS proposed themes with the EIS goals, using the icons addressed below to highlight this connection. The themes of our EIS solution are:

**Lumen Team Response Exceeds Requirements**

- All EIS mandatory and optional services, except wireless, are proposed
- 929 CBSAs proposed; well beyond the minimum of 25



**Broad Range of Communication Services** – Our proposal includes all mandatory and optional services, except wireless, provided under EIS. Lumen has grown and developed its capabilities to provide a full range of communications services through network partners, strategic acquisitions, as well as internal development of staff and facilities. The Lumen Team has highly experienced staff, and advanced and flexible equipment and facilities enabling us to provide all of the services called for by the EIS RFP.



**Global Reach of Our Network** – Our EIS proposal reflects our extensive global presence, with the Lumen owned and managed network extending to 60 countries. The reach of Lumen network capabilities is enhanced through our access to

---

facilities worldwide; giving us the ability to readily provide EIS services wherever they are required in the world.



**Leadership in Innovation** – We exert technical leadership through standards organizations such as the IETF, and through equipment and software acquisition and our own research. Our innovation is exemplified by our more than 1,000 patents and patent applications in the U.S. and around the world.



**Experienced Management Team** – Our management team leverages years of experience from Networx and WITS, as well as other Government and commercial contract efforts supplying services such as those required for EIS. Our comprehensive understanding of EIS service requirements is further demonstrated through many of the service descriptions in following sections of this volume.

**Compliance** – The Lumen Team takes no exceptions or deviations to the technical requirements found in Sections C, F, G, and J. The descriptions of the services we offer which are provided in the following sections help demonstrate compliance with EIS requirements; assisted by RFP references which correlate with the requirements of the SOW and RFP. The service architecture shown in **Figure 1-1** and described in Section 1.1 illustrates our support of all EIS requirements with our global network, facilities, staff and processes which are **scalable and flexible**. This accommodates growth and technology advances over the life of the contract.

Throughout this volume we have referenced applicable standards. Where specific versions and dates of standards are listed in the SOW of the RFP, we are compliant with that version. Otherwise, we are compliant with the latest version of the SOW standards. Lumen is standards-based in our service operations, with resulting lower risk to the Government through our provision of reliable and compatible service.

**Flexibility** – Flexibility within our network has been built in from the ground up, literally. Lumen’s backbone includes DWDM technology capable of carrying 400 Gbps of capacity on a single fiber pair at a significant cost savings, and delivers manageable and protectable SONETS/SDH and Ethernet-based services. Throughout much of our CONUS fiber optic cable network, and in much of Europe, we have extensive spare

---

ducts installed, through which we can draw new EIS dark fiber as required. Using this spare ducting, we can install new dark fiber at a lower cost and faster than would be the case for installing a completely new buried fiber capability. We also reserve some of our installed fiber to accommodate our growth and give us flexibility to respond to the evolution in service requirements.

Lumen selects innovative and proven equipment vendors for our backbone equipment. We insist on demanding criteria to introduce cost-effective conversion between optics and electronics which provides full digital access to all network-capacity-enabling advanced features, such as switching, grooming, multiplexing, bandwidth management, and performance management. Such equipment selection provides greater opportunities for leveraging other technology advances in network management and operation support infrastructure.

#### **1.2.1.2 Quality of Services [L.29.2.1.B; M.2.1.2]**

The delivery of high-quality, reliable EIS services is ensured by the Lumen Team's experience in building and maintaining world-class services, continuous monitoring against the Government's Key Performance Indicators (KPI) and Acceptable Quality Levels (AQL) in the SLA Tables provided in Section J.2 and defined in SOW C.2, and state-of-the-art network management tools and processes. We ensure that EIS Quality of Service (QoS) is maintained through the Lumen Team's skilled technicians monitoring and responding 24/7. The high quality of our network services continues to be recognized by independent rating services. **We have carefully selected our EIS partner companies for their high quality performance for services they provide.** Each of our teammates and access partners apply reliable design principals and operations which conform to industry standards, resulting in excellent quality performance.

The EIS AQLs will be routinely monitored by our Lumen GovNOC. As we are currently doing in providing Networx and WITS services, Lumen meets the Government's KPIs and AQLs through the use of our network management team's expertise and tool-sets. The Lumen NOC's Network Management System (NMS)

---

integrates network element managers, alarm aggregations, and network managers into one ubiquitous platform for greater network operations efficiency. Throughout, Lumen has deployed a number of automated tool sets to monitor the Lumen Enterprise<sup>SM</sup> network to ensure that it meets KPIs and AQLs. In addition, Lumen operations staff has in-house expertise that runs **one of the world's largest IP and transport backbones**. Combined, our people and their tool-sets provide a management environment that ensures meeting the Government's requirements. Lumen operates the network using a cross-functional team that works together closely to ensure meeting required performance levels. Within the individual EIS service delivery descriptions in this Technical Volume, we include service-specific details of how we consistently deliver high-quality EIS services that meet or exceed each of the AQLs.

#### **1.2.1.3 Service Coverage [L.29.2.1.C; M.2.1.3; C.1.3; C.1.8.5; J.1]**

The service coverage of the Lumen Team extends well beyond the minimum requirements of the mandatory services in 25 CBSAs. A listing of the CBSAs where we propose services is contained in the AcquServe portal CBSA indicator tool in accordance with RFP L.29.2.1. As many of our services are offered commercially in 60 countries, with active relationships with global carriers for local and long haul circuits, the Lumen Team is well positioned to support future Government CBSA expansion.

#### **1.2.1.4 Security [L.29.2; M.2.1.4; C.1.8.7]**

Lumen ensures that all Lumen services provided comply with Federal Information Security Management Act (FISMA), DoD, and Intelligence Community requirements where applicable. We meet the applicable Government cyber security/Information Assurance (IA) objectives and requirements for EIS confidentiality, integrity, and availability. We incorporate these principles when developing our information security program and policies for EIS and applicable TOs. Lumen currently uses the International Organization for Standardization ISO IEC 27002 standard (formerly ISO 17799) as our security policy framework.

---

### **1.3 Mandatory EIS Services [L.29(2)(a), M.2.1, C.1.2]**

The Lumen Team proposes the four mandatory EIS services described in SOW C.1.2: Virtual Private Network Service, Ethernet Transport Service, Internet Protocol Voice Service, and Managed Network Service. Details of the mandatory services Lumen provides are given in response Sections 1.3.1 through 1.3.3.1. In accordance with SOW C.1.2, Access Arrangements is also included as a mandatory component, as described in our response Section 1.4.9. As demonstrated in our response, we have the network, personnel, processes, experience, and overall capabilities to provide cost-effective and reliable mandatory services that are fully compliant with EIS requirements.

#### **1.3.1 Data Service Mandatory**

##### **1.3.1.1 Virtual Private Network Service [L.29.2.1, C.2.1.1, C.4.4]**

Lumen has successfully delivered premises- and networks-based Virtual Private Network Service (VPNS) to more than 200 Government Agencies and divisions, giving our customers secure intranet, extranet, and remote access connectivity for more than a decade. The features of our VPNS solution include flexibility in meeting bandwidth and security requirements, ensuring functionality across a diversity of hardware and software platforms.

Lumen's VPNS includes both network- and premises-based VPN services to support any access method and deliver a range of services, including dial-up voice, ISDN Internet access, and dedicated high-speed optical connections. Our network backbone supports the intranet, extranet, and remote access VPNS solutions, as described in SOW C.2.1.1.1.1. Our VPNS approach enables consistent management of network traffic to reduce costs and to prioritize time-critical and business-critical transmissions which are given higher priority. Lumen support for our VPNS includes coordination by our Contractor Program Management Office (CPMO) including our Customer Support Organization (CSO), performance monitoring by our Lumen Government NOCs, and the design, installation, maintenance, and upgrade of our services to meet the evolving needs of our customers by our engineers and technicians.

Figure 1.3.1.1-1 highlights the features to GSA and the agencies of the Lumen VPNS solution, which are aligned with the evaluation criteria.

**Figure 1.3.1.1-1. Features of Lumen VPNS**

EVALUATION CRITERIA	FEATURES OF LUMEN VPNS
Understanding [M.2.1.1]	<ul style="list-style-type: none"> <li>• More than a decade of experience providing VPNS to industry and Government, giving us insight into current and evolving customer needs and expectations</li> <li>• Our VPNS solution supports EIS goals of converged services for unified communications and collaboration across a diversity of platforms and devices</li> </ul>
Quality of Services [M.2.1.2]	<ul style="list-style-type: none"> <li>• As discussed further in paragraph 1.3.1.1.7, we meet or exceed all VPNS performance requirements, supported by quality assessment and reporting developed and enhanced through extensive past performance providing services like those required by EIS</li> <li>• Performance demonstrated on Networkx and other similar contracts</li> <li>• High availability and redundancy through many physical paths and in the Core</li> <li>• Wide range of access methods, and traffic prioritization via Class of Service (CoS)</li> <li>• We also propose jitter as an additional KPI for VPNS; jitter is an important factor in the service quality of voice and video data service and is defined as the relative variation in delay between consecutive packets</li> </ul>
Service Coverage [M.2.1.3]	<ul style="list-style-type: none"> <li>• The Lumen VPNS solution rides on globally distributed Lumen network, with integrated strategically dispersed communications switches, switching centers, and dedicated network links to eliminate latency issues and service interruptions</li> <li>• Lumen VPNS provides services to 60 countries, leveraging 74,000 terrestrial route miles in North America, 26,000 route miles in Europe, 10,000 route miles in Latin America, and 33,000 subsea route miles globally</li> </ul>
Security [M.2.1.4]	<ul style="list-style-type: none"> <li>• Maintain the integrity and privacy of VPNS content and collaboration with passwords and TLS encryption</li> <li>• We accept IPSec tunneling over our VPNS architecture</li> </ul>

**Understanding.** As an incumbent on the Networkx Enterprise, WITS3, and multiple regional GSA contracts; and as Chair of the ACT-IAC Networks and Telecommunications Special Interest Group (N&T SIG), Lumen brings an in-depth understanding of GSA’s EIS Program Goals and offers VPNS that aligns with and satisfies these goals.

**Quality of Services.** Lumen ensures VPNS performance quality across the network by carrying real-time protocol (RTP) in the highest priority IP VPN queue. This queue has SLAs of 10ms for jitter and 100% for packet delivery. As addressed in more detail in section 1.3.1.1.1.2, Lumen helps ensure meeting Quality of Service (QoS)

---

requirements by using Class of Service (CoS) levels to prioritize network traffic and manage bandwidth for Agencies.

**Service Coverage.** Lumen's solution for VPNS extends to all 929 CBSAs, well in excess of the 25 CBSAs required in SOW C.1.3. The Lumen VPNS is provided over the global Lumen network, which has integrated strategically dispersed communications switches, switching centers, and dedicated network links.

**Security.** Lumen VPNS are inherently secure on the basis of the underlying MPLS technology specified in RFC 4362. MPLS VPNs provide transport level security in the fact that the system information transiting one VPN can't be viewed by systems within another VPN. Lumen performs regular security audits of the network elements, and operational subsystems as part of the VPNS security practice. Our VPNS security approach includes physical (facility access, etc.) and logical (network-related protocols, etc.) security features. Remote access security for VPNs is provided by the Lumen Secure Access Gateways. This product supports IPsec tunnel management between the agency VPNS network and the remote user.

#### **1.3.1.1.1 Service and Functional Description [L.29.2.1, M.2.1, C.2.1.1]**

Lumen's VPNS leverages our global secure and fully meshed Multi-Protocol Label Switching (MPLS) network to create reliable and highly secure private agency paths across the Lumen backbone. MPLS technology improves traffic flows across networks, including VPN layers 2 and 3, to minimize the risk of congestion. As shown in **Figure 1.3.1.1.1-1**, our MPLS provides the ability to encapsulate many different protocols and route them securely over the routing infrastructure. An MPLS IP/VPN network allows converged services such as voice, video and data to take advantage of the same access facilities and ensures mission-critical traffic is given preferential treatment over non-critical applications.

One of the key advantages of our MPLS core is reduced fail-over time. In traditional IP networks, the routing table in each router is updated based on the dynamic communication between adjacent routers, resulting in a long convergence time. However, in an MPLS-based network, each router views the forwarding table. So, when



---

an LSP path in the forward direction fails, the router is made aware of it instantaneously with a much shorter “keep-alive” time.

The Provider Edge (PE) router is the cornerstone of the Lumen MPLS IP/VPN services on our global MPLS network. The PE routers for the global MPLS VPN network enable IP Virtual Private Network services as per Internet Engineering Task Force Request for Comments 4364 (RFC4364) — BGP/MPLS IP Virtual Private Networks.

The PE devices are uplinked via resilient OC12/OC48/GE or 10GE connections to our Core infrastructure, a converged IP routing and MPLS. The devices are served by aggregation switches for grooming of Fast Ethernet and Ethernet customer traffic via Nx Gigabit Ethernet (NxGE) circuits.



**Figure 1.3.1.1.1-1. Network Overview of CenturyLink’s VPNS.** *The reliable CenturyLink global network provides reliable and compliant EIS VPNS.*







[Redacted content]

[Redacted content]

[Redacted content]

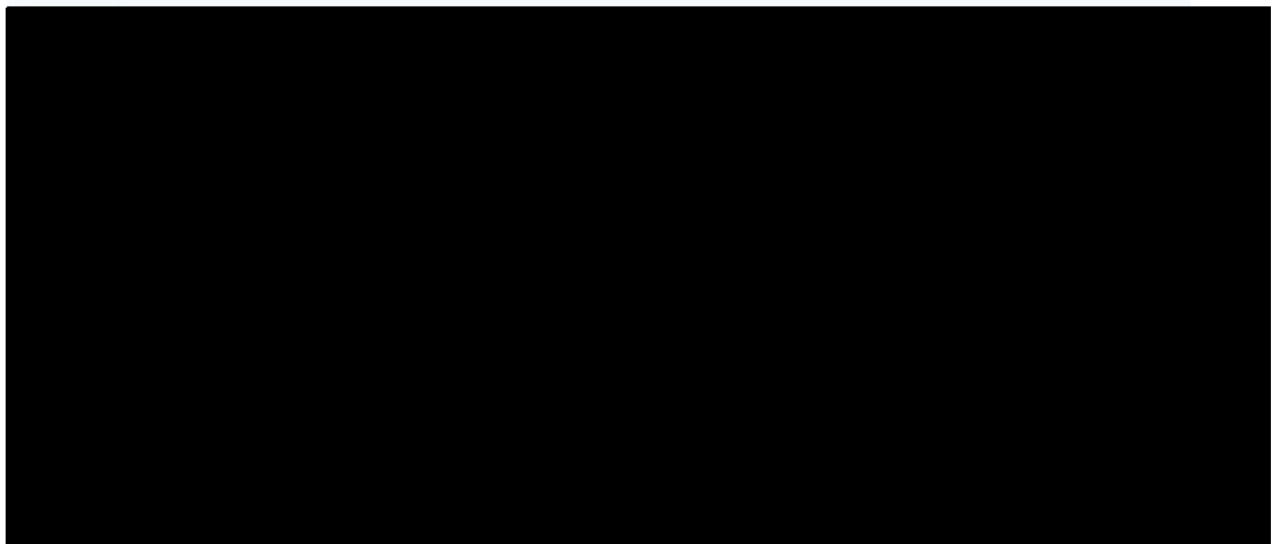
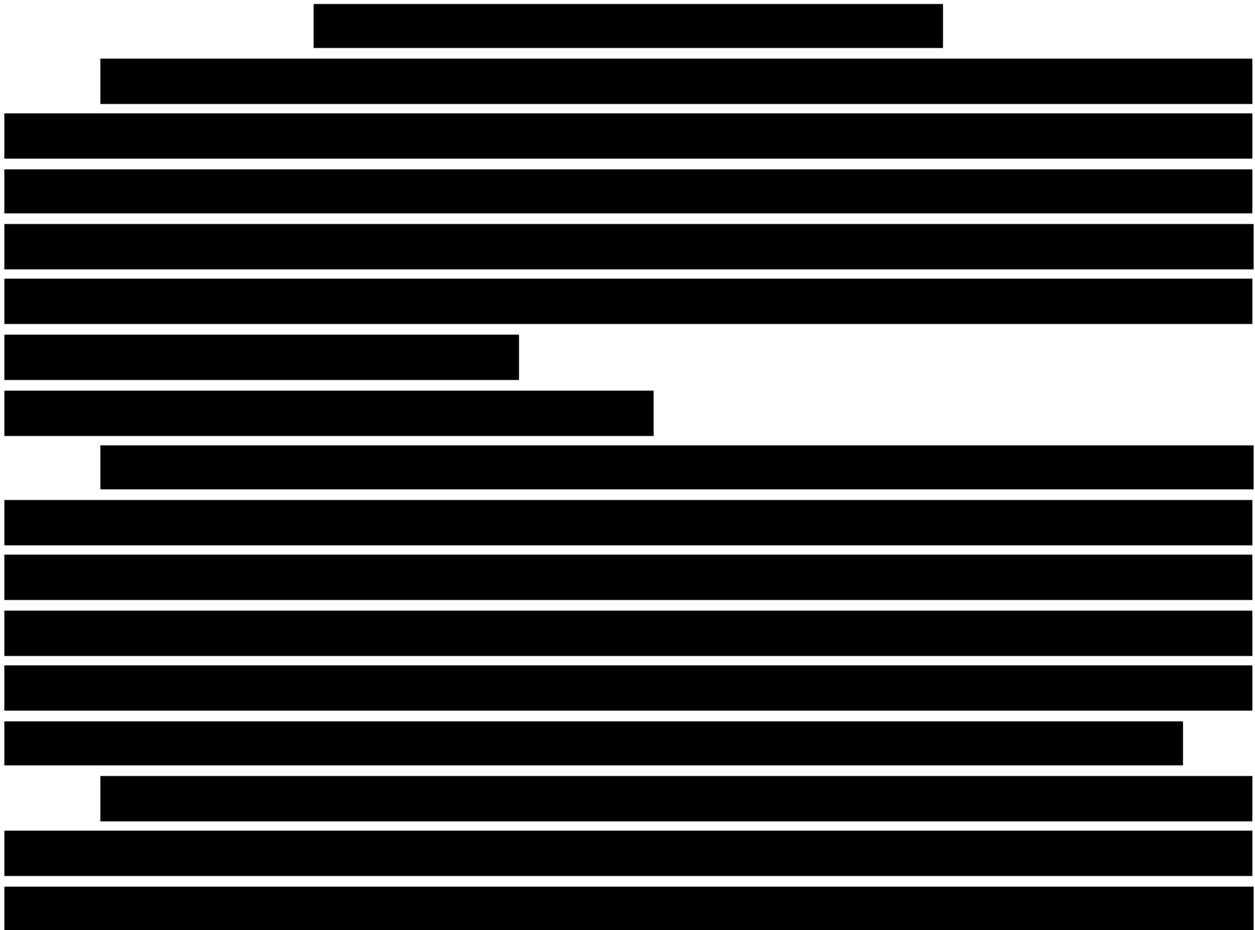


Figure 1.3.1.1.1.1-1. CenturyLink VPNS Secure Access Architecture. *Our*



[Redacted text block]

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



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

**1.3.1.1.2 Standards [L.29.2.1, M.2.1, C.2.1.1.1.2]**

Our VPNS solution complies with all the standards required in SOW C.2.1.1.1.2. Our VPNS is a network-based IP VPN service built on our converged MPLS backbone, comprising a service based on IETF RFC2547bis standard, which was co-authored by Lumen. Other aspects of our VPNS that are based on IETF specifications include certificate authorities and hard and soft tokens.

Technologies such as MPLS IETF RFC 4364 (formerly 2547) have been implemented to ensure that VPN-specific routing tables are kept private, reinforcing our VPNS security posture. VPN membership is administered on a site-to-site basis to ensure that internal IP traffic is not routed to other customers sharing the network. The MPLS technology ensures that site traffic is routed specifically to other sites on the VPN membership list. To ensure trust and reliability, our VPNS applies general MPLS standards such as RFC 3209 for RSVP-TE, RFC 4716 and RFC 4762 for BGP and LDP discovery, and RFC 6074 for auto-discovery.

We continue to incorporate IETF Working Group (WG) specifications as they mature and products supporting those RFCs become commercially available. We keep abreast of developments within the IP Security WG, IP Security Policy WG, MPLS WG, Layer 3 VPN WG, Pseudo Wire Emulation Edge to Edge WG, and IETF-TLS WG. Lumen’s network is fully IPv6-enabled for all commercial and Government customers. IPv6 and IPv4 addresses and routes can be supported within the same IPVPN and on the same IPVPN port. Agencies can migrate to IPv6 at their own pace.

---

### **1.3.1.1.3 Connectivity [L.29.2.1, M.2.1, C.2.1.1.1.3]**

The Lumen VPNS service supports a dedicated site-to-site access via leased lines. The Lumen VPNS service supports secure remote access via either dialup, DSL or Cable. The VPNS service provides for full meshing among VPN end-locations as a default configuration. Partial meshing, if required, is supported. As discussed earlier, access circuits can be on-net or off-net. Access circuits are transparent for the CoS mechanisms that operate between Lumen's PE router and the agency's GFE/CE router.

### **1.3.1.1.4 Technical Capabilities [L.29.2.1, M.2.1, C.2.1.1.1.4]**

Our VPNS solution meets all the mandatory technical capabilities and thresholds listed in PWS C.2.1.1.4. Elements of our solution are summarized in the following paragraphs:

- 1. Meet Applicable Routing Requirements.** The Lumen VPNS solution meets applicable routing requirements of SOW C.1.8.8, ensuring any encrypted tunnels are applied and proxied to enable inspection.
- 2. Provide Multiple Tunneling Standards.** The Lumen network supports 256-bit AES and 128 bit 3DES-encrypted IPSec VPN and Generic Routing Encapsulation (GRE) tunneling over IPSec. The methods describing compliance to SOW C.1.8.8 are provided in Section 1.4.13 of this Technical Volume.
- 3. Provide Various Encryption Levels.** The Lumen network supports DES and 3DES encryption from the CE router to the PE router. Secure VPNS access is supported with 3DES and AES 256 encryption standards.
- 4. Provide Authentication Services.** We can provide Windows Active Directory (AD), Lightweight Directory Access Protocol (LDAP), and RADIUS authentication services.
- 5. Support IPv4 Encapsulating and Encapsulated.** Our network supports IPv4 as both the encapsulating and encapsulated protocol.
- 6. Support IPv6 Encapsulating and Encapsulated.** We also support IPv6 as both the encapsulating and encapsulated protocol.

7. **Support QoS Modes.** Lumen supports the standardized modes as specified in SOW C.2.1.1.1.4.7.

- a) **Best Effort** traffic is supported by CoS markings. Agencies have CoS options to prioritize traffic flows between MPLS network ports. The agency selects the CoS and the distribution of bandwidth percentages by class, as shown in **Figure 1.3.1.1.4-1**. Any traffic outside such distribution percentages may be treated as Basic Traffic for the purposes of the service levels. The Lumen VPN service is fully ToS-transparent. As mentioned earlier, the customer's traffic can also be classified at the PE router by a combination of IP header information such as source and destination address and/or Layer 4 source and destination port.

**Figure 1.3.1.1.4-1. Sample DiffServ Queue Mappings**

COS	SERVICE NAME	IP DSCP MARKING (DIFFSERV)
1	Voice	EF
2	Video Signaling	CS-5
3	Video Interactive	CS-4
4	Data: Gold	AF-21, AF-22, AF-23
5	Data: Silver	AF-11, AF-12, AF-13
6	Data: Bronze	CS-0, Everything Else
	Network Control	CS-6

- b) **Aggregate CE Interface level QoS** is supported by marking all of the data entering the VPNS network with the same markings regardless of destination, essentially point-to-cloud or cloud-to-point.
- c) **Site-to-Site Level QoS** is supported by each pair of connected VPN endpoints having their own QoS per endpoint pair. This is similar to an EVC point-to-point that could have its own QoS/CoS. Lumen also allows multiple VRFs per port connection that have their own QoS schema.

- 
- d) **Intserv (RSVP)-signaled QoS.** Lumen supports IntServ using Resource Reservation Protocol (RSVP) to explicitly signal the QoS needs of an application's traffic in the end-to-end path through the network. This provides a way to deliver the end-to-end QoS that real-time applications require by explicitly managing network resources to provide QoS to specific user packet streams (flows).
- e) **Diffserv.** Our VPN core provides a transparent Differentiated Services domain. When an agency uses their own Diffserv policies, Lumen's VPN network transports those markings transparently through the network. This is achieved by using the MPLS EXPerimental field in the Lumen VPN, leaving the agency IP header (ToS/IP Precedence) intact.
8. **Support QoS on Access.** Lumen supports QoS on the following access networks:
- a) **802.1p Prioritized Ethernet.** Lumen network equipment recognizes agency Ethernet frames whose Tag Protocol Identifier (TPID) value, in the outermost 802.1q header, is 0x8100.
- b) **MPLS-based Access.** Our MPLS is independent of access technologies and delivers scalable end-to-end IP services with simple configuration and provisioning for users and providers, supported by a range of platforms; users with differing access links can be combined on an MPLS edge without changing their current environments.
- c) **Multilink Multiclass PPP.** Lumen VPN ports support multilink PPP encapsulation.
- d) **QoS-Enabled Wireless.** The Lumen Team provides both LTE and wireless 802.11x access.
- e) **Cable High-Speed Access (DOCSIS 1.1).** Lumen Secure Access Site service allows fixed remote locations (branch sites or home offices) to securely connect for safe access to the network anywhere, anytime; eliminating the need for all sites to have a direct connection to the VPN. Key

---

service features include high availability and diverse path redundancy using cable, DSL or 3G/4G. Hughes ActiveQoS™ provides superior traffic management on “best efforts” broadband access to prioritize mission-critical applications and related traffic during “rush hour” congestion.

- f) **QoS-Enabled Digital Subscriber Line (DSL).** Lumen offers Secure Access services to extend the security policies of the agency VPN to mobile users and other/remote agency sites not directly connected to the VPN network. This service leverages the agency’s existing Internet access or other DSL/Cable circuit to provide secure access to their VPN.

**QoS-Enabled Satellite Broadband Access.** The Lumen Team provides QoS-enabled satellite broadband access through [REDACTED]

9. **Support QoS Objectives for Intserv and/or Diffserv.** Lumen supports Differentiated Services (Diffserv). Our VPN core provides a transparent Diffserv domain. This means that, should the agency use their own Diffserv policies, Lumen's VPN network transports those markings transparently through the network. This is achieved by using the MPLS EXPerimental field in the Lumen VPN, leaving the agency IP header (ToS/IP Precedence) intact.
10. **Provide Traffic Isolation and Layered Security Architecture.** Technologies such as MPLS IETF RFC 4364 (formerly 2547) have been implemented to ensure that VPN specific routing tables are kept private. VPN membership is administered on a site-to-site basis to ensure that internal IP traffic is not routed to other Agencies sharing the network. MPLS does not allow traffic from a site to be routed to a site not on the VPN membership list. Beyond the security inherent to MPLS, other layers of our security architecture include the methods and procedures, discussed earlier, for physical access, equipment login access, and function-limited access.

- 
11. **Temporary Access to VPNs.** Lumen supports multiple VPNs by allowing both permanent and temporary access to one or more VPNs for authenticated users across a broad range of access technologies.
  12. **Provide Secure Routing Services.** The native MPLS technology does not allow traffic from a site to be routed to a site not on the VPN membership list. Lumen has implemented technologies such as MPLS IETF RFC 4364 to ensure that VPN specific routing tables are kept private. VPN membership is administered on a site-to-site basis to ensure that internal IP traffic is not routed to other customers sharing the network.
  13. **Support Encryption, Decryption, and Key Management Profiles.** Our VPNS supports encryption through DES or 3DES from the Customer Edge to the Provider Edge. Secure VPNS access is supported with 3DES and AES 256 encryption standards.
  14. **Support Agency Internal Security Mechanisms.** Lumen supports an agency deploying its own internal security mechanisms which are in addition to those we employ in support of VPNS, to secure specific applications or traffic more precisely than on a site-to-site basis.
  15. **Allow Agency Alternatives for Temporary Authentication.** Lumen allows an agency to choose from Windows Active Directory (AD), LDAP or RADIUS for authentication of temporary access users.

#### **1.3.1.1.5 Features [L.29.2.1, M.2.1, C.2.1.1.2]**

Our VPNS includes the SOW-specified mandatory features, as described below:

- **High-availability Options for CPE:** Provides high availability and diverse path redundancy using cable, DSL or 3G/4G
- **Interworking Services:** Lumen provides interworking services for an agency's VPN to transparently access agency locations that use Lumen's Ethernet Service--Multiservice port/Ethernet access

**1.3.1.1.6 Interfaces [L.29.2.1, C.2.1.1.3]**

Lumen’s VPNS supports the mandatory and optional interfaces specified in SOW C.2.1.1.3.

**1.3.1.1.7 Performance Metrics [L.29.2.1, M.2.1, C.2.1.1.4, G.8]**

As shown in **Figure 1.3.1.1.7-1**, Lumen’s VPNS meets or exceeds all VPNS performance quality requirements, as demonstrated by our performance on Network and other recent or ongoing contracts similar in scope and complexity.

**Figure 1.3.1.1.7-1. Lumen VPNS QoS/Performance Metrics**

KPI	SERVICE LEVEL	PERFORMANCE STANDARD	AQL	LUMEN AVERAGE
Latency (CONUS)	Routine	70 ms	<=70 ms	<=50 ms
Latency (OCONUS)	Routine	150 ms	<= 150 ms	Trans-Atlantic: <= 95 ms Trans-Pacific: <= 150 ms
Av (VPN)	Routine	99.9%	>=99.9%	99.9%
	Critical	99.99%	>=99.99%	99.99% (On-Net Availability)
Time to Restore	Without Dispatch	4 hours	<= 4 hours	4 hours
	With Dispatch	8 hours	<= 8 hours	8 hours

Lumen proposes jitter as an additional KPI for VPNS. Jitter is an important factor in the service quality of voice and video data service and is defined as the relative variation in delay between consecutive packets. To measure jitter, samples are taken every 500 milliseconds and consecutive samples are compared for variation in delay.

Jitter is reported as a network average and does not include local access loops or GFE/CE. The KPI value varies according to the class of service required by the agency, shown in **Figure 1.3.1.1-2**, which provides the jitter classes of service we propose for VPNS.

**Figure 1.3.1.1.7-2. Lumen Proposes to Include Jitter as Additional KPI**

KPI	CLASS OF SERVICE	PERFORMANCE STANDARD	AQL	LUMEN AVERAGE
-----	------------------	----------------------	-----	---------------

KPI	CLASS OF SERVICE	PERFORMANCE STANDARD	AQL	LUMEN AVERAGE
Jitter	Gold	10 ms	<=10 ms	Intra U.S.: 3 ms EU – U.S.: <10 ms
	Silver	15 ms	<=15 ms	<=15 ms
	Bronze	N/A	N/A	N/A

**1.3.1.2 Ethernet Transport Service [L.29.2.1, C.2.1.2, C.4.4]**

The telecommunications industry is in the midst of a lengthy migration from services and access based on Time Division Multiplexing (TDM) to those based on Ethernet. Government and industry alike are taking part in this migration driven by, among other reasons, Ethernet’s overall superiority in bandwidth efficiency, granularity, protection bandwidth, topologies supported, operational simplicity, and lower cost. These factors are highly relevant to agencies which face both funding restrictions and funding uncertainty, hence Government’s overall embrace of Ethernet Transport Service (ETS).

**Lumen’s Industry-Leading ETS**

- Expansive geographic availability with more than 35,000 on-net buildings in the U.S. and network presence in more than 60 countries
- MEF CE 2.0 Compliance
- SDN-driven Adaptive Network Control with Enhanced Management and Dynamic Capacity for superb visibility and near real time bandwidth scaling
- Secure, reliable, and responsive network that supports high-performance voice, video, and data applications with up to 99.999% network uptime

Expanding Ethernet coverage represents the strategic direction of Lumen. Much of Lumen’s investments in time and money continue to be directed at expanding and improving our Ethernet coverage and service. For example, announced in mid-2015 and in active roll-out worldwide, Adaptive Network Control, particularly its Dynamic Capacity feature – both discussed below, is indicative of the innovative spirit that distinguishes Lumen ETS from nearly all other carriers worldwide. Lumen Ethernet service and innovation continues to garner recognition by leading industry analysts as highlighted in **Figure 1.3.1.2-1**.



Not just industry analysts, the Government itself has recognized and responded to Lumen’s leadership in ETS. As of 3Q15, under Networx and WITS, Lumen is providing:

- Approximately 270 dedicated access arrangements, more than 70% of which are at or above 50 Mbps
- Approximately 120 point-to-point E-LINE circuits or variants of dedicated ETS, almost 70% of which are at or above 1 Gbps

This track record includes an excellent history of quality of service performance. In short, Lumen is experienced and demonstrably adept at providing and supporting a feature-rich, secure ETS to agencies.

Lumen ETS is fully compliant with all EIS ETS requirements and supports all of the optional features named under ETS. We discuss these below and some distinct Lumen capabilities in product features and support.



**Ethernet Excellence Awards:**

- ★ Retail Service Provider of the Year" award for Global, Caribbean and Latin America (CALA), North American regions, 2014
- ★ Wholesales Provider of the Year" award for North America, 2014
- ★ Best Carrier Ethernet Wholesale and Business Application, CALA region, 2013
- ★ "Service Provider of the Year" for Ethernet services in CALA, 2011
- ★ Best Business Ethernet Service, 2011

**Gartner** Challenger, 2015 Magic Quadrant for Global Network Services (including Ethernet WAN)



- Network Performance Excellence Award, 2013
- Brand Carrier Excellence Award, 2013



- Pilot House Award for Top Provider Ethernet Services, 2012
- "Carrier Ethernet has emerged as a more robust and flexible alternative to traditional WAN services. Level 3's stellar customer rating score moved them to the lead amongst all providers." —Henry Svendblad, Principal Analyst, Nemertes Research

**Figure 1.3.1.2-1. Lumen’s Industry Leadership in Carrier Grade Ethernet.**

**Figure 1.3.1.2-2** highlights the features of the Lumen ETS solution aligned with the evaluation criteria.

**Figure 1.3.1.2-2. Features of Lumen’s ETS**

EVALUATION CRITERIA	FEATURES OF LUMEN ETS
Understanding [M.2.1.1]	<ul style="list-style-type: none"> <li>• Indicative of Lumen’s strength in ETS and understanding of the GSA environment, today we are providing approximately 120 E-LINE “circuits”, almost 70% of which are at or above 1 Gbps! – as well as some 270 Ethernet based dedicated access arrangements.</li> <li>• Lumen chairs the ACT-IAC Networks and Telecommunications Special Interest Group which keeps us current with Ethernet’s evolution and application in service provider environments.</li> </ul>
Quality of Service [M.2.1.2]	<ul style="list-style-type: none"> <li>• Satisfies all KPIs, plus Lumen has a strong track record of performance on ETS under Networkx.</li> <li>• Delivered over a carrier class MPLS infrastructure to satisfy service restoration KPIs.</li> <li>• Leverages its core network based on adherence to Metro Ethernet Forum (MEF).</li> <li>• Managed from redundant GovNOCs in Broomfield, CO and Atlanta, GA.</li> <li>• Lumen’s use of a Network Interface Device (NID) to terminate Ethernet connections on agency sites gives us greater visibility and control, and results in better service quality and higher user satisfaction.</li> </ul>
Service Coverage [M.2.1.3]	<ul style="list-style-type: none"> <li>• Via Lumen’s Ethernet network and Ethernet Network to Network Interfaces (ENNI)s with almost 40 partners, Lumen ETS is available in all 929 CONUS and OCONUS CBSAs.</li> <li>• Lumen’s Ethernet network is now directly in 136 CBSAs, including 68 of the 100 CBSAs named in SOW J.1.4.1.</li> <li>• OCONUS, Lumen ETS is available in more than 60 countries.</li> </ul>
Security [M.2.1.4]	<ul style="list-style-type: none"> <li>• ETS is implemented within the secure, private Lumen network.</li> <li>• Lumen’s architecture, ETS over MPLS, offers an additional level of inherent security through the proven application of the Virtual Forwarding Instance (VFI), within which agency ETS traffic is uniquely tagged for segregation within unique, secure groups.</li> <li>• ETS supports routing of applicable traffic through an EINSTEIN Enclave per OMB Memo. M-15-01.</li> </ul>

**Understanding.** As an incumbent on the Networkx Enterprise, WITS3, and multiple regional GSA contracts; and as Chair of the ACT-IAC Networks and Telecommunications Special Interest Group (N&T SIG), Lumen brings an in-depth understanding of GSA’s EIS Program Goals and offer an ETS that satisfies these goals. Most indicative of this understanding is our practical experience with ETS and agencies – namely, the approximately 120 E-LINE “circuits” and some 270 Ethernet-based dedicated access arrangements.

**Quality of Services.** Lumen achieves ETS performance quality across the network by implementing it over our MPLS platform, which provides traffic engineering and superbly manages CoS and QoS across the network. In addition, Lumen terminates Ethernet connections on a customer site with a Lumen Network Interface Device (NID).

---

Virtually without exception, we do this for all Ethernet connections around the world regardless of whether the facility is owned or leased by Lumen. Monitored by our GovNOCs, the NIDs give us greater visibility and control, and result in better service quality and higher user satisfaction.

**Service Coverage.** Lumen's solution for ETS extends to all 929 CBSAs, well in excess of the requisite 25 CBSAs. To achieve this coverage, we draw upon our Ethernet presence in 136 CBSAs, including 68 of the 100 CBSAs named in SOW J.1.4.1, and supplement local (access) coverage via ENNIs with approximately 40 carrier partners. Of course, as a global player, ETS is available in more than 60 countries. As noted, Lumen NIDs terminate virtually all ETS connections, regardless of local carrier.

**Security.** Lumen ETS is implemented using the secure, private Lumen network. Lumen's architecture, ETS over MPLS, offers an additional level of inherent security through the proven application of the Virtual Forwarding Instance (VFI), wherein agency ETS traffic is uniquely tagged for segregation within unique, secure groups. If, for coverage extension, Lumen draws upon another carrier via an ENNI, we note that there is VFI continuity across the interface – meaning that a VFI tag one on side of the ENNI is directly mapped to a VFI across the network boundary. Additionally, for overall security, Lumen SOCs continuously monitor the threat landscape and take action as needed.

#### **1.3.1.2.1 Service and Functional Description [L29.2.1, M.2.1, C.2.1.2.1, C.2.1.2.1.1]**

Available throughout the U.S and in more than 60 countries, Lumen ETS solutions deliver carrier-class metro and WAN connectivity over our secure, private infrastructure. The core of this infrastructure is a 100 G backbone, with resilient OC-48, 10GE or 100G uplinks. This network is always expanding, enabling Lumen to meet customers' never-ending demands for scale and scope.

Leveraging this high speed core is Lumen's MPLS architectural platform, which underlies our ETS. MPLS delivers proven, reliable service performance and scalability, and enables carrier-grade Quality of Service (QoS) to be managed over the entire

---

network. Secure, diverse MPLS Label Switched Paths (LSP) are defined and configured at the entry point to the core network. Consequently, Lumen is able to provision all on-net ETS Ethernet Virtual Connections (EVC) with network-protection by default. Another advantage of an MPLS core is reduced fail-over time as each internal router views the forwarding table. Hence, when an LSP path in the forward direction fails, the router is made aware of it instantaneously, with a much shorter keep-alive time.

Lumen Metro Ethernet Forum 2.0 Carrier Ethernet (MEF 2.0 CE)-compliant ETS E-LINE and E-LAN configuration options provide EVCs over our global core MPLS network.

This enables agencies to transport voice, data, multimedia, and collaboration applications among two or more agency-designated locations. E-LINE and E-LAN service offer granular bandwidth increments on physical interfaces of Ethernet, Fast E, NxFast E, Gig E, NxGig E, 10G, and 40G.

**ETS Configurations.** The E-LINE point-to-point and point-to-multipoint configurations, shown in **Figure 1.3.1.2.1-2 (a) and (b)** allow agencies to connect two or more locations via an EVC and send Ethernet traffic transparently across the Lumen network. E-LAN, illustrated in **Figure 1.3.1.2.1-2 (c)**, is a multipoint-to-multipoint EVC-based configuration in which agencies connect multiple sites in a fully meshed, single-bridged Ethernet domain. The Lumen network default is to discard Layer 2 control protocol frames. E-Tree, not depicted, is another type of point-to-multipoint configuration.



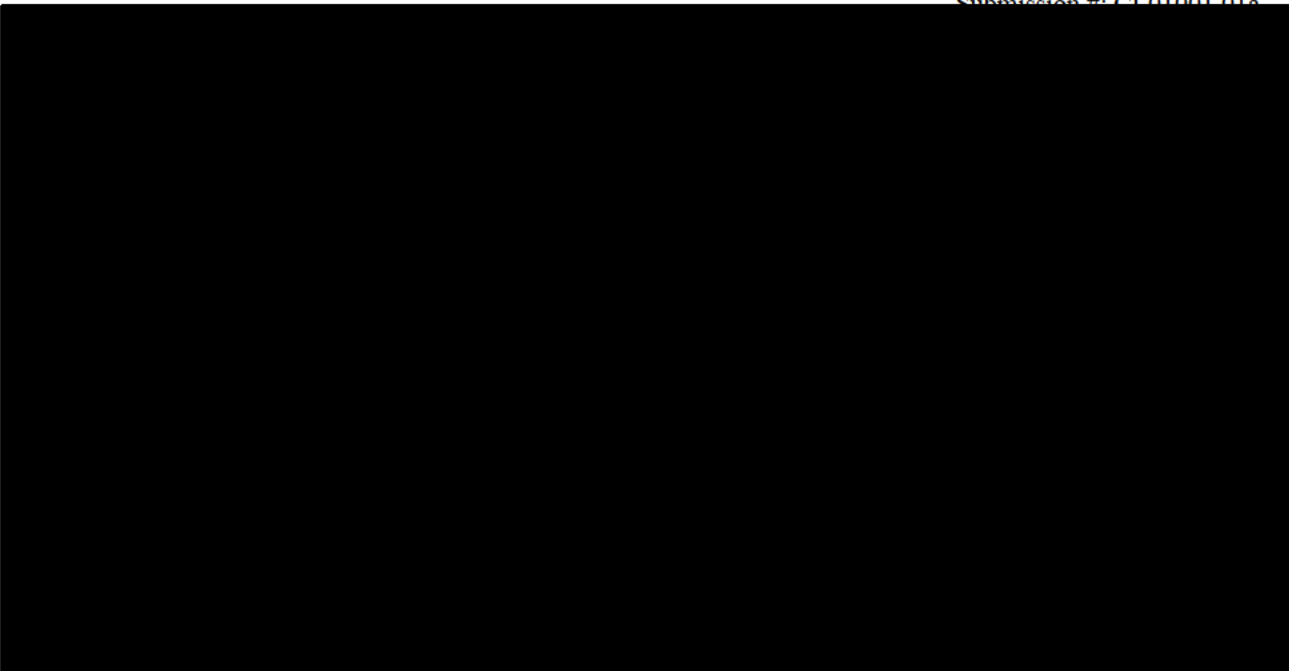
**Figure 1.3.1.2.1-1. Overview of CenturyLink ETS Delivery Over an MPLS Core.**

*Underlying MPLS enhances performance, scalability and end-to-end QoS of ETS.*

**VLAN and Port Mapping.** A single VLAN or VLAN range can be mapped to an EVC. A VLAN mapping to a single EVC can connect to a separate E-LAN VPN, if, for example, more than one VPN were established or multiple services were being delivered over a single access circuit. In port mapping, all VLANs on the port are mapped to a single EVC. Port mapping typically is applied in a strict point-to-point configuration where no service multiplexing is required.

**Class of Service.** For E-LINE and E-LAN, respectively, three and six Class of Service (CoS) levels are available. This includes a CoS level (available to E-LINE and E-LAN) that is used to carry real-time voice and video. Typically, Ethernet “p” bits (IEEE 802.1p) are used to signal CoS, although static treatments are also used. In the latter, an EVC is managed as carrying a single CoS across the network.

As Lumen ETS leverages the power of an underlying MPLS architecture, CoS is mapped to MPLS EXP values.



**Figure 1.3.1.2.1-2. ETS Configurations: (a) E-LINE Point-to-Point, (b) E-LINE Point-to-Multipoint, and (c) E-LAN.** *All create simplifying, single-bridged Ethernet domains.*

### **Lumen ETS Adaptive Network Control and Bursting**

In May 2015, Lumen announced Adaptive Network Control (ANC), one of the industry's first realizations of Software Defined Networking (SDN) across the WAN. Applicable for Lumen ETS, ANC Solutions – Enhanced Management and Dynamic Capacity - offer unmatched levels of control, real-time visibility and a cost-management flexibility in circuit capacity. Enhanced Management adds network intelligence, visibility, and insight to the agency network to assist with troubleshooting, network planning, bandwidth adjustments, and CoS. *Dynamic Capacity provides bursting control and flexibility for agencies by providing 2x or 3x times their bandwidth as needed in near real-time. It does so by giving agencies the ability to actually increase a site's Committed Information Rate (CIR)!* Dynamic Capacity can be invoked by pre-defined utilization thresholds, through scheduling, or on an ad hoc basis. The agency is in control of how long the additional bandwidth is available and can view all events in historical reports. Costs are known before each event occurs, and there's even a

monthly rate cap. Dynamic Capacity is available on all ETS configurations. E-LAN also offers a bursting capability via a commit with usage basis.

Figures 1.3.1.2.1-3 and 1.3.1.2.1-4 are examples of ANC screen shots that reflect the ease of harnessing Lumen’s SDN ANC capability.

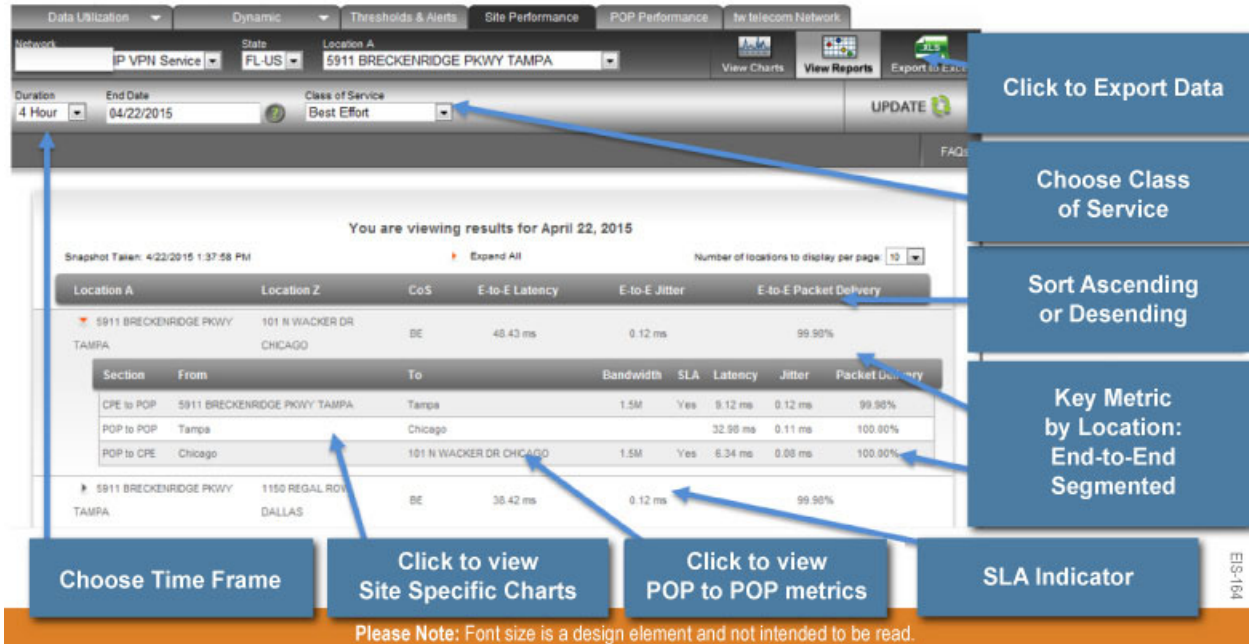
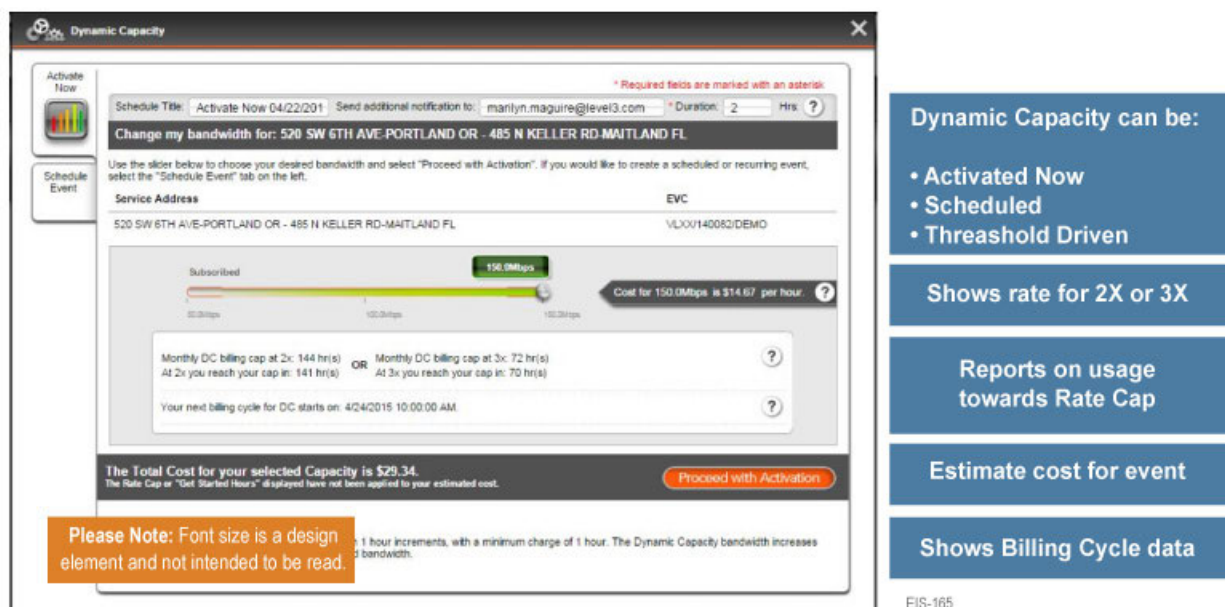


Figure 1.3.1.2.1-3. Enhanced Management Customer Network Report View. ANC reporting is facilitated through the Lumen ETS solution.



**Figure 1.3.1.2.1-4. Dynamic Capacity “Activate Now” Screen.** *Dynamic Capacity is a key feature of the Lumen ETS.*

**Figure 1.3.1.2.1-5** summarizes key features and benefits of Lumen’s industry leading ANC SDN technology.

**Figure 1.3.1.2.1-5. Key Features and Benefits of Lumen’s Adaptive Network Control**

FEATURES	BENEFITS
Dynamic Capacity -2X or 3X	<ul style="list-style-type: none"> <li>• Immediate access to additional bandwidth</li> <li>• Hourly usage charges</li> <li>• Rate cap per billing cycle - 144 hours at 2X and 72 hours at 3X</li> </ul>
Dynamic Capacity – Threshold driven events	<ul style="list-style-type: none"> <li>• Network driven events provide capacity when needed</li> <li>• Cost control through hourly billing</li> </ul>
Enhanced Management – Segment by Segment view	<ul style="list-style-type: none"> <li>• Greater visibility into network connections</li> <li>• Threshold settings with alerts watches the network for the agency</li> </ul>

**Smart Demarcation.** Lumen ETS includes Smart Demarcation as a standard ETS component for all agency sites in the U.S. and, as available, globally. Smart Demarcation is provided via a Lumen-owned Network Interface Device (NID) located at the agency premises/SDP that serves as the Lumen network point of demarcation. NIDs provide loopback capabilities, test traffic generation, fault detection, verification, isolation and discovery at Layer 2 as well as historical information on availability and port utilization. Therefore, benefits of Smart Demarcation include simplified test and turn-up, faster trouble resolution, and agency end-to-end visibility of service performance. It also ensures RFC 2544 compliance.

Lumen ETS is managed from the redundant GovNOCs in [REDACTED]. In addition collected data from NIDs, Lumen uses a Service Assurance Agent to monitor various performance metrics, including delay, loss, and jitter. Measurements are continuous, with all site-to-site combinations tested 3,000 times per hour.

**Security of Lumen ETS**

Security of Lumen ETS is derived from factors including an inherent level of security afforded to ETS by operating on the private, secure Lumen network; an added inherent level of security conferred by the Ethernet over MPLS implementation; and the



---

additional security measures executed by Lumen in accordance with SOW C.1.8.8, consistent with OMB Memorandum M-15-01 regarding Internet, Extranet and Inter-agency traffic – i.e., External Networks.

E-LINE ETS is provided in a secure point to point environment between two endpoints. An agency-specific E-LINE connection is generally expected to fall within the agency's security boundary. If there are no External Network connections in an E-LINE (or E-LAN) configuration, then that ETS instance is operating within the agency's security boundary. However, as noted above, if an E-LINE endpoint resides on an External Network, special routing will be invoked to route the E-LINE EVC through an EINSTEIN enclave. *The same considerations apply for E-LAN sites on External Networks.*

Regarding Ethernet over MPLS, in the shared physical network environment of E-LAN (a VPN), customer traffic separation is realized via the VFI. The VFI is defined and discussed in several Internet Engineering Task Force (IETF) Request for Comments (RFC) specifications, notably RFCs 4761 and 4762. In this proven technology, a unique tag is assigned to the traffic of a given agency/ customer so that traffic of different customers can be segregated on distinct logical networks within the Lumen network. *Therefore, each customer (or customer network) is completely isolated from other customers' domains, resulting in a high level of security through the traffic separation within the ETS environment.* Should an agency site be a member of more than one VFI, there is no VFI awareness at the SDP; the VFI is only used and defined within the core network.

As noted previously, when Lumen extends ETS coverage via an ENNI, VFI continuity is maintained across the interface as part of the ENNI agreement and implementation. This means that a VFI tag one on side of the ENNI is directly mapped to a VFI across the network boundary. Therefore, traffic segregation and security are maintained.

**1.3.1.2.2 Standards [L.29.2.1, C.2.1.2.1.2]**

SOW C.2.1.2.1.2 calls for compliance with a number of standards and documents of: 1) the MEF, 2) the ITU, 3) the IEEE and 4) IETF RFCs for Acceptance Testing. *Consistent with Lumen’s leadership in ETS, we are in compliance with all of them, including the optional one - support for Jumbo Ethernet frames.* Particularly as Lumen personnel are active in a variety of industry forums and working groups related to Ethernet and ETS, per item 5), Lumen will review new versions, amendments, and modifications to the above documents and standards for compliance as future technology advancements occur. An example of this would be draft standards such as G.8011.3/Y.1307.3 and G.8011.4/Y.1307.4.

**1.3.1.2.3 Connectivity [L.29.2.1, C.2.1.2.1.3]**

Lumen’s ETS solution meets the connectivity and interoperability requirements described in SOW C.2.1.2.1.3. Our approach to meeting these requirements is summarized in **Figure 1.3.1.2.3-1**.

**Figure 1.3.1.2.3-1. ETS Connectivity and Interoperability**

LUMEN COMPLIES	SOW C.2.1.2.1.3 ELEMENT	LUMEN COMPLIANT SOLUTION
✓	Intra-agency LAN-LAN Connectivity	<ul style="list-style-type: none"> <li>With our focus on deploying Ethernet as a near ideal means to interconnect LANs and the global extent of our network, Lumen ETS provides LAN-to-LAN connectivity between sites of the same agency. This connectivity applies to agency sites in the more than 60 countries served by the Lumen network. Such interconnectivity can occur on either an E-LINE or E-LAN basis. At one layer, interconnected sites would be part of the same Virtual Forwarding Instance (VFI) within the Lumen network.</li> </ul>
ü	Inter-agency LAN-LAN Connectivity	<ul style="list-style-type: none"> <li>Lumen provides secure Ethernet service supporting inter-agency LAN-LAN connectivity through local VLAN connections. Traffic from each agency site is uniquely identified across the shared network using VLAN tags, implemented through the use of EVC connections. These logical connections not only virtually separate one customer’s traffic from that of another, but they also provide security in such a way that each customer’s traffic is securely delivered only to that customer’s ports or UNIs.</li> <li>In compliance with OMB Memorandum M-15-01, agencies must identify such connectivity as inter-agency traffic must be routed through an EINSTEIN Enclave for security processing. (Lumen EINSTEIN Enclaves are discussed in Section 1.4.8.3, MTIPS, of this Technical Volume.) Using the VLAN tags, Lumen will identify such traffic and route it through an EINSTEIN Enclave. In some cases, traffic may be identified on a port/UNI basis. This special handling may need to accommodate the need for route information exchange (Layer 3) across the agency-agency boundary, something that would be incorporated in the security routing design.</li> </ul>

1.3.1.2.4 Technical Capabilities [L.29.2.1, C.2.1.2.1.4]

Lumen’s full compliance with ETS technical capabilities is summarized in **Figure**

1.3.1.2.4-1.

**Figure 1.3.1.2.4-1. Lumen’s ETS Technical Capabilities and Features per SOW C.2.1.2.1.4**

LUMEN COMPLIES	SOW C.2.1.2.1.4 REQUIREMENT	LUMEN COMPLIANT SOLUTION
✓	1. Routing and security	• To enable agencies to comply with OMB Memorandum M-15-01, Lumen will route any Internet, Extranet, and inter-agency traffic through a secure DHS EINSTEIN Enclave for processing by the latest generation of EINSTEIN capabilities. Agencies will identify connectivity requirements that must be so routed, and, for ETS, Lumen will identify such traffic using VLAN tags or on a port/UNI basis.
✓	2. Geographical coverage	• In a word, the metro-to-global Lumen network renders moot both location and distance. We can provide ETS a) within a city – or b) between cities - in CONUS, OCONUS and Non-Domestic as well as between cities. Based on Lumen’s direct Ethernet presence in 136 CBSAs, and ENNs with 40 partners, we can offer ETS in all 929 CONUS and OCONUS CBSAs. ETS is available in more than 60 countries.
ü	3. Ethernet UNI	• The Ethernet UNI inherently operates and supports Layer 2 interfaces. Clients supporting higher level protocols packets still present an Ethernet UNI, but the higher levels in the protocol stack are supported in that they are not considered by the UNI.
✓	4. EVC support	• EVC support is inherent in an MEF CE 2.0 compliant network such as that of Lumen.
✓	5. ETS Delivery at SDP via UNI	• A basic requirement of ETS, and supported by Lumen in general and currently done so under Networx and WITS.
✓	6. Circuit Emulation	• As required, Lumen supports Circuit Emulation and does so according to details specified at the TO level.
✓	7. Ethernet Virtual Circuits	• Lumen supports all configurations, point-to-point, multipoint-to-multipoint, and rooted multipoint Ethernet Virtual Circuits (EVC). These are common in ETS.
✓	8. EVC Multiplexing	• EVC multiplexing is a basic capability within Lumen ETS.
✓	9. Rate-Limited Throughput Access Links	• Rate limiting on access links, e.g., limiting a physical 1 Gbps access circuit to, say, 200 Mbps, is a routine practice of Lumen. In the short term, it can be more economical for the customer, while offering the potential of a rapid upgrade of the speed because of the physical headroom.
✓	10. Rate Limiting Support	• Rate limiting is performed at the SDP (item 9, above), typically on access. In addition, it is not often done, and almost unknown at egress, but Lumen can apply rate limiting on an individual VLAN at ingress and egress.
✓	11. Privacy and Security	• Technology feature built into 802.3 standard and support is specified at the TO level.
✓+	12. Service	• Lumen ETS supports the physical interfaces (mandatory <i>and all optional</i> ) listed in SOW C.2.1.2.3.

LUMEN COMPLIES	SOW C.2.1.2.1.4 REQUIREMENT	LUMEN COMPLIANT SOLUTION
	Attributes	These are recapped below in section 1.3.1.2.6 of this Technical Volume.
✓+	13. Traffic Profiles	<ul style="list-style-type: none"> <li>Lumen ETS is certified compliant with MEF CE 2.0. As such, it supports traffic profiles:                             <ol style="list-style-type: none"> <li>Committed Information Rate (CIR), minimum amount of bandwidth guaranteed for an ETS.</li> <li>Committed Burst Size (CBS), the size up to which subscriber traffic is allowed to burst and still be in-profile and not discarded or shaped.</li> <li>Peak Information Rate (PIR), the rate above the CIR that traffic is allowed into the network for a given burst interval defined by the MBS. In MEF CE 2.0 terms, this is called the Excess Information Rate (EIR).</li> <li>Maximum Burst Size (MBS). In MEF CE 2.0 terms, this is called the Excess Burst Size (EBS).</li> </ol> </li> <li>As noted above, with Lumen’s remarkable Dynamic Capacity feature element of Adaptive Network Control, when an event-driven or scheduled process or authorized agency user calls up more bandwidth on a given access arrangement, what the Lumen network system does is actually increase the CIR, affected immediately. CIR can be increased by 2x or 3x as needed or over a specified time period. Changing the CIR also adjusts the CBS, EIR (PIR), and EBS (MBS).</li> </ul>
✓+	14. Performance Parameters	Lumen ETS supports the Performance Parameters listed in SOW C.2.1.2.4. These are recapped below in section 1.3.1.2.7 of this Technical Volume.
✓	15. Service Frame Delivery options	Lumen ETS supports the commonly seen Service Frame Delivery options of a) Unicast Frame Delivery, b) Multicast Frame Delivery, per RFC 4604, and c) Broadcast Frame Delivery, per IEEE 802.3
ü+	16. VLAN tag support	Lumen ETS supports VLAN tag: a) preservation, b) translation, and c) stacking. In addition, <i>we support optional d) VLAN aggregation across a common physical connection</i>
✓	17. Service Multiplexing	A basic feature of Ethernet, Lumen ETS supports the ability for multiple EVCs to be connected/ supported via a single UNI. Each EVC can be configured to support One-to-One Mapping (one VLAN to one EVC), All-to-One Mapping (all VLANs to one EVC, also called Port Mapping), or VLAN ID Bundling. For the latter, the EVC is “VLAN-aware” and supports multiple VLAN IDs (item 18, below).
✓	18. VLAN ID Bundling	Lumen ETS supports VLAN ID Bundling, the ability for multiple VLAN ID to be connected/supported via a single EVC. As noted above, that EVC is deemed “VLAN aware”.
✓	19. Security Filters	Lumen supports security filters as they are specified at the TO level.
✓+	20. Performance Monitoring (optional)	<ul style="list-style-type: none"> <li>As part of an enhanced package, Lumen provides Performance Monitoring that can include:                             <ol style="list-style-type: none"> <li>Signal failure, b) Signal degradation, c) Connectivity or Loss of connectivity, d) Frame loss, e) Errored frames, f) Looping, and g) Denial of Service (DoS), h) Misinserted frames, i) Maintenance parameters. Anti-DoS (or anti-DDoS) measures could be part of a security package.</li> </ol> </li> </ul>
✓	21. Maintenance Functions	Lumen ETS supports maintenance functions including: a) Alarm suppression, b) Loopbacks (intrusive and non-intrusive (transparent to on-going connections)), and c) Protection switching, restoration, etc. Loopbacks to the SDP are supported by the NID at the SDP with which Lumen terminates all Ethernet circuits.
✓	22. Network	Lumen ETS supports network topologies including a) Point-to-point, b) Rooted Multi-point, and c)

LUMEN COMPLIES	SOW C.2.1.2.1.4 REQUIREMENT	LUMEN COMPLIANT SOLUTION
	Topologies	Multi-point-to-Multi-point (i.e., mesh). Incidentally, rings are not a formally defined configuration but are readily supported through configuration should the need for them arise.
✓	23. Geographical Diversity	• Diversity is a strength of Lumen because of our distinct orientation toward building and deploying new facilities. Our network core is inherently constructed for diversity. On access, if we don't have sufficient diversity, we often construct diverse laterals to achieve it. As the situation warrants, an agency may buy a geographically diverse route from a different contractor.
✓	24. Bridging	• Lumen ETS supports bridging in compliance with IEEE 802.1 (2014).
✓	25. Virtual Connection Sizes	• Lumen ETS supports Virtual Connection sizes up to 40 Gbps for a) point-to-point Ethernet connections, and b) multipoint-to-multipoint connections.
✓	26. Quality of Service (QoS)	• Lumen ETS supports QoS and provides options so that an agency can have its traffic managed and prioritized as suits its needs. QoS support is discussed below in some depth, in short, Lumen supports 6 Classes of Service (CoS). Class distinctions are signaled to the network according to how the agency sets the 802.1p bits and other rules defined at set-up.
✓	27. Traffic Reconfiguration	• Lumen ETS supports traffic reconfiguration enabling an agency to modify a specific service connection subsequent to the establishment of the connection. Such reconfigurations are reasonably straightforward when there is no physical equipment or circuit changes. We note that in some instances Lumen's Dynamic Capacity feature, which is very easy to invoke, may suffice for traffic reconfiguration.

**1.3.1.2.5 Features [L.29.2.1, C.2.1.2.2]**

Not applicable. ETS features are shown as "Reserved" in the SOW.

**1.3.1.2.6 Interfaces [L.29.2.1, C.2.1.2.3]**

As an industry leader in Ethernet, Lumen ETS supports all the interfaces specified in SOW C.2.1.2.3, *including all of the optional ones, thereby exceeding EIS requirements.*

**1.3.1.2.7 Performance Metrics [L.29.2.1, M.2.1(c), C.2.1.2.4]**

Lumen complies with all performance levels and Acceptable Quality Level (AQL) of Key Performance Indicators (KPI) for ETS specified in SOW C.2.1.2.4.

**Industry Leadership and Global Footprint for a Best-Value IPVS Solution**

- The **most extensive** Tier-1 Internet carrier backbone services, North American Softswitch (NASS) service and the Public Service Access Point (PSAP) connectivity of any carrier
- The **largest** CLEC operating in the US with **over 2M voice trunks** interconnecting the PSTN
- Local voice services in over **120 metropolitan areas and 2,300 rate centers** nationwide from our installed base of 61 class-5 switching offices
- Voice network carrying **over 13B minutes** of traffic and **5B calls per month**

---

We also note that for all KPIs: Availability (Routine for single connections and Critical for double connections), Latency for CONUS and OCONUS connectivity, Packet Jitter, Packet Delivery Grade of Service (GoS) for Routine and Critical situations, Time to Restore (TTR) with and without dispatch, and GoS pertaining to Fail Over Time for Routine and Critical situations are measured in accordance with the pertinent SOW C.2.1.2.4 notes.

### **1.3.2 Voice Service (Mandatory)**

#### **1.3.2.1 Internet Protocol Voice Service [L.29.2.1, M.2.1, C.2.2.1]**

Lumen's Internet Protocol Voice Service (IPVS) solution is built on a converged voice and data network infrastructure. Our IPVS solution is part of our unified communications strategy, and offers a reliable, secure, and cost-efficient alternative to legacy PBX systems by providing built-in applications like voice mail, call center, automated attendant, call detail recording, and network management.

Our IPVS solution is proven to work, having been successfully deployed and maintained at more than 20,000 enterprises worldwide, including top U.S. Government Agencies such as DHS, NASA, and the U.S. Coast Guard. We deliver a rich suite of voice communications features over a fully managed IP infrastructure built for reliability, diversity, and failure recovery. For DHS, we transformed traditional voice circuits from their original carrier to an end-to-end IPVS solution connecting more than 40 DHS sites.

The IPVS we provide includes:

- Premises-based and network-based (hosted) IP-PBX solutions for IP voice
- Session Initiation Protocol (SIP) Trunk Service – Lumen SIP Trunking to communicate with internal and external users over IP, including calls to traditional PSTN networks.
- Managed LAN services to monitor and maintain IPVS premise components

**Figure 1.3.2.1-1** highlights the features to GSA and the Agencies of the Lumen IPVS solution, which are aligned with the evaluation criteria. Additional details of how the Lumen IPVS solution features satisfy Section M.2.1 evaluation criteria are provided following the figure.

**Figure 1.3.2.1-1. Features of Lumen IPVS**

EVALUATION CRITERIA	FEATURES OF LUMEN IPVS
Understanding [M.2.1.1]	<ul style="list-style-type: none"> <li>Lumen is an incumbent on the Network Enterprise, WITS3, and multiple regional GSA contracts</li> <li>Lumen capitalizes on years of experience in delivering IPVS to Government and industry to provide high quality and reliable IPVS to the Agencies in full compliance with requirements</li> <li>Lumen can seamlessly upgrade agency IPVS users to Unified Communications Service if the upgrade is required by the Government.</li> </ul>
Quality of Services [M.2.1.2]	<ul style="list-style-type: none"> <li>We meet or exceed all IPVS performance requirements, supported by quality assessment and reporting developed and enhanced through extensive past performance providing services like those required by EIS</li> <li>Proven deployment to over 20,000 enterprises, including Government agencies</li> <li>Lumen ensures voice quality across the network by carrying real-time protocol (RTP) in the highest priority IP VPN queue.</li> </ul>
Service Coverage [M.2.1.3]	<ul style="list-style-type: none"> <li>The Lumen IPVS solution is comprised of both Voice over Internet Protocol (VOIP) and Time Division Multiplexing (TDM) components to provide global reach</li> <li>Our Enterprise VOIP covers over 80% of the U.S., with plans for expansion into Western Europe in 2016</li> <li>Our international Local Inbound and international Toll Free services cover 29 and 100 countries, respectively.</li> </ul>
Security [M.2.1.4]	<ul style="list-style-type: none"> <li>Our IPVS is delivered over our IP VPN, which is secure and meets the Denial of Service requirement</li> <li>Our IPVS include a secure authentication scheme for any calls originating on the network, providing intrusion protection</li> <li>Lumen and our subcontractors perform security operations in accordance with industry best practices and standards supporting Cyber, Personnel and Physical Security</li> </ul>

**Understanding.** As an incumbent on the Network Enterprise, WITS3, and multiple regional GSA contracts; and as Chair of the ACT-IAC Networks and Telecommunications Special Interest Group (N&T SIG), Lumen brings an in-depth understanding of GSA's EIS Program Goals and offers IPVS that aligns with and satisfies these goals, as shown in **Figure 1.3.2.1-2**.

**Figure 1.3.2.1-2. Lumen IPVS Solution Aligned to EIS Program Goals**

EIS GOAL	CHALLENGE FOR EIS IPVS	LUMEN SOLUTION
Service Continuity	Downed equipment and servers with no backup in place; built-in failover capability may not be available in PBXs. Voice communications are mission-critical for our customers, so any	<ul style="list-style-type: none"> <li>IPVS systems have demonstrated value to large enterprises in disaster recovery. Lumen's hosted IPVS supports continuity of operations through its inherently distributed IP software model. On-net backup sites at other locations are unaffected. Off-net backup sites can be quickly established as users gain access to remaining</li> </ul>

EIS GOAL	CHALLENGE FOR EIS IPVS	LUMEN SOLUTION
	disruption of service is unacceptable	LAN/WAN assets with full voice station functionality.
Highly Competitive Prices	Telecom budget constraints limit ability to maintain legacy equipment	<ul style="list-style-type: none"> <li>Lumen IPVS, which requires less equipment and fewer human resources to monitor and manage is more cost-efficient than PBX/Centrex applications</li> <li>Lumen-hosted VoIP service features unlimited local and long-distance calling anywhere in the U.S. and Canada; international calls are billed at competitive per-minute rates with any carrier.</li> </ul>
High-Quality Service	Maximize operational uptime by eliminating single points of failure and building in redundancies for servers, routers, and switches	<ul style="list-style-type: none"> <li>Lumen's fault tolerant architecture means there are no single points of failure and our IPVS solution is designed to function with the loss of a server, a cluster of servers, a database or an entire data center without interruption. All servers, routers and switches are also dual redundant, with dual power supplies such that a virtual PBX has a hot standby server (located in a different data center) and databases are completely mirrored.</li> </ul>
Operations Support	Minimize or eliminate service interruptions when adding new or enhanced features	<ul style="list-style-type: none"> <li>Enhanced features can be added on the fly, and are more advanced. Example, collaboration tools, soft phones/clients; mobility of end user.</li> </ul>

**Quality of Services.** Lumen ensures voice quality across the network by carrying real-time protocol (RTP) in the highest priority IP VPN queue. This queue has SLAs of 10ms for jitter and 100% for packet delivery. Lumen meets the Mean Opinion Score (MOS) of 4.0 for agency-to-agency calls and calls within Lumen's Core and IP VPN networks using a G.711 codec. In addition, we support the G.722 codec for on-net IP-to-IP calls to provide high-definition (HD) voice quality.

Lumen performs quality measurements through on-net and off-net to on-net analysis tools. On-net quality is measured using probes that determine voice quality across the Lumen network. These devices generate MOS voice quality estimations, providing real-time feed-back on network voice quality. These devices also actively monitor packet loss, jitter, and latency. Lumen can also provide statistically significant data on calls traversing the hosted VoIP Softswitch in near-real time.

Six CoS levels are carried through the Lumen network and subsequently delivered to customers. IPVS, being real-time traffic, is carried at the highest CoS level.



---

The CoS mappings at the edge ensure that SLAs with respect to jitter, packet loss, and latency are maintained and that customers receive the QoS appropriate to the class of traffic being transmitted. To deliver on the agreed QoS, queuing mechanisms such as Weighted Random Early Detection and intelligent buffer management are employed to assure output queues deliver traffic with defined service level attributes appropriately.

In addition to redundant, no single point-of-failure systems, the hosted IPVS solution in the core data centers provides a third layer of redundancy so that if all connectivity to the buildings fail, the system can be set to automatically re-route calls to out-of-network phones (whether back-up facilities, individual cell phones, etc.). The voicemail system also remains active and can be accessed from either PSTN phones, web browsers, or iPhone/Android devices via a free application provided with our hosted VoIP service.

**Service Coverage.** Lumen's solution for IPVS extends to all 929 CBSAs, well in excess of the 25 CBSAs required in SOW C.1.3. The Lumen IPVS is provided over the global Lumen network, which has integrated strategically dispersed communications switches, switching centers, and dedicated network links. Lumen IPVS supports DTMF, and PRI signaling to IXCs and end offices as a certified CLEC in all 50 states. Lumen's local network covers 93% of the U.S. population and is also connected to all U.S. SS7 Tandem switches and many End Offices to support its IXC traffic.

**Security.** Lumen IPVS employs security measures such as building redundancy into the data network, locking down IP Telephony servers and performing regular security audits as part of the IPVS we provide. If the IP phone system supports voice-over-wireless connections, access to the wireless link as well as the link itself is secured with a combination of authentication and encryption. For Agencies deploying a hosted IPVS solution, Lumen recommends archiving voicemail messages, company contacts and directory information.

Lumen applies the following safeguards to ensure the security of our IPVS, which is delivered over our secure IP VPN:

- **Denial of service (DoS):** Voice traffic is kept distinct and secure by our session border controllers that prevent attacks by hacker, worms, or viruses from denying legitimate users access to network services. Our solution provides global protections from distributed DoS attacks between voice and data (the data network DDOS is prevented from impacting voice and, similarly, voice DDOS is prevented from impacting the data network).
- **Intrusion:** Our edge proxy servers have the originating end-points predefined, which prevents unauthorized call origination. In addition, our service includes a secure authentication scheme for any calls originating on the network. This protects the network from attempts by foreign or other unknown devices pursuing access to the network.
- **Invasion of privacy:** Our Core network is private and protected, as a Lumen-owned and operated network that is not accessible to the public.

*Section 2.1 Information Security* of this volume provides specific details on Lumen's approach to Information Security requirements listed in the RFP.

### 1.3.2.1.1 Service and Functional Description [L.29.2.1, M.2.1, C.2.2.1.1]

Lumen offers a feature-rich, flexible, and cost-effective IPVS solution to meet EIS program requirements and accommodate future growth. Our IPVS architecture supports domestic and non-domestic connectivity and gateways for interoperability with the traditional PSTN, wireless carrier networks, satellite-based voice networks, and other agency IPVS networks. Lumen's EIS IPVS includes the following:

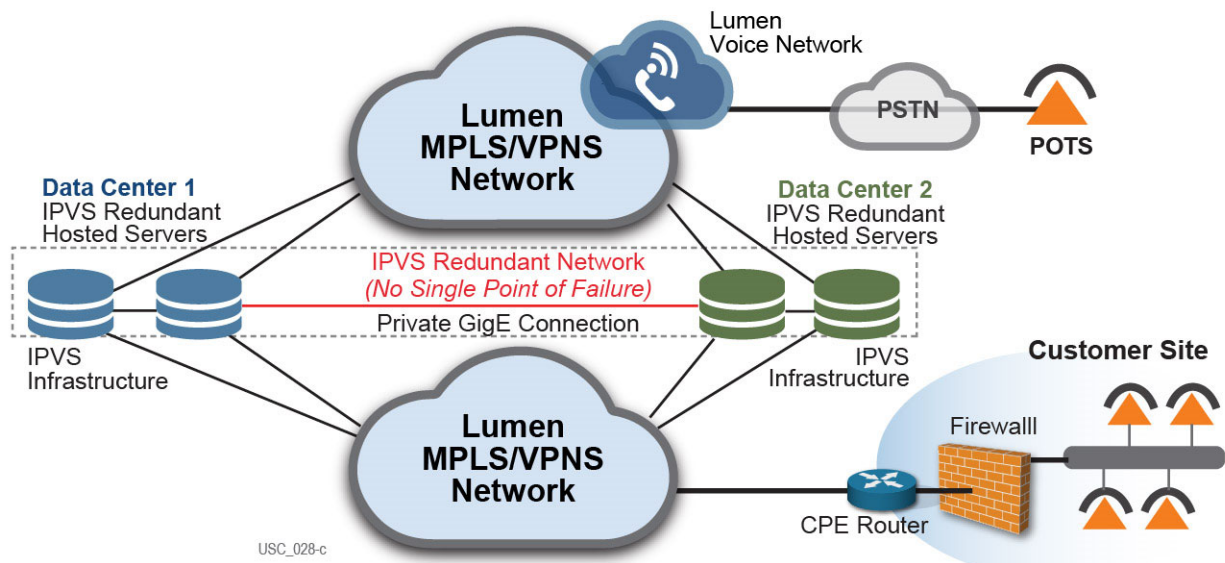
- **Hosted Solution:** Similar to a traditional Centrex offering, Lumen's hosted solution provides a call application server over our global IP/MPLS network, with only user handsets required on site. Our solution leverages SIP trunking and, coupled with

#### State-of-the-Art Hosted IPVS Solution

- The Lumen hosted VoIP communications solutions are delivered from mirrored, fully redundant, and geographically diverse state-of-the-art data centers.
- In addition to being interconnected with private connections, each data center is connected to the Internet through multiple redundant links from Tier 1 and major Internet service providers, each capable of handling the entire data center traffic
- Each data center is connected to more than 7 PSTN carriers to deliver the best possible call quality Lumen customers

our managed LAN services, ensures that all aspects of the system are monitored 24/7. **Figure 1.3.2.1.1-1** shows our hosted solution.

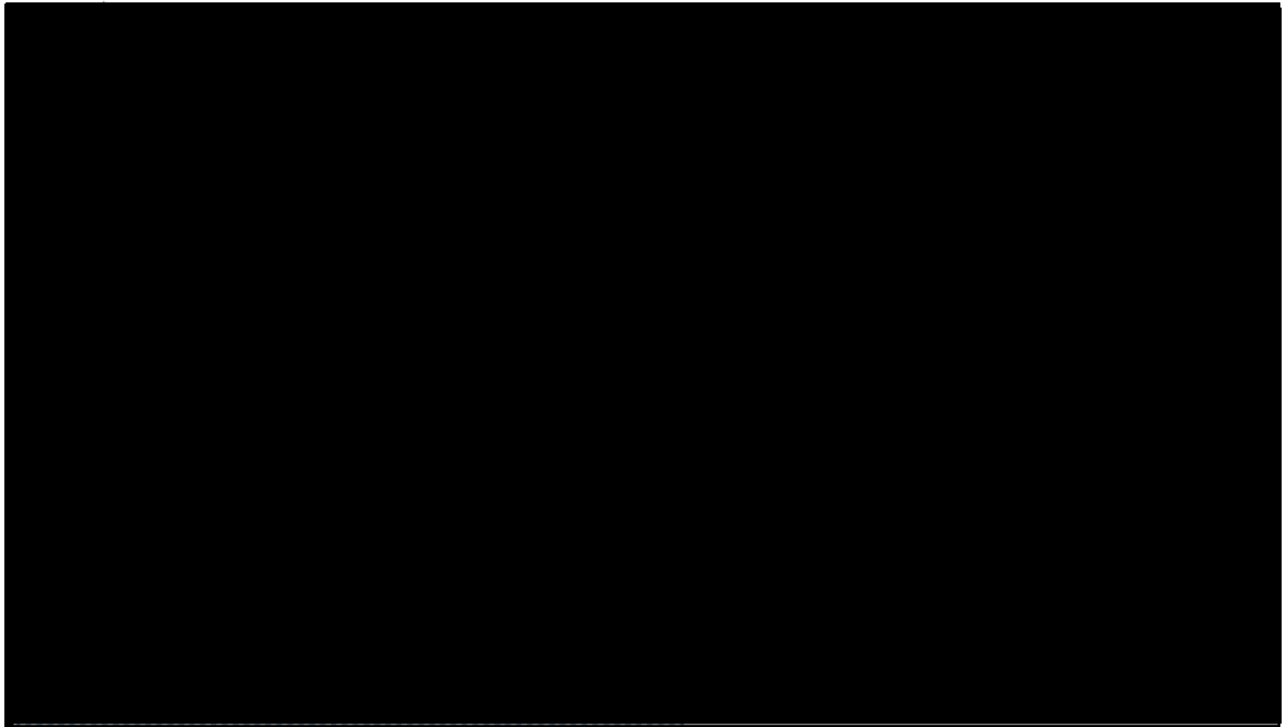
- **Premises-based solution:** A scalable architecture that allows us to deliver services to organizations with less than five subscribers to those with more than 20,000 subscribers. Our IP-based on-premise solution ensures that all aspects of the system are continuously monitored. A diagram of our premise-based solution is provided in **Figure 1.3.2.1.1-2**.



**Figure 1.3.2.1.1-1. CenturyLink IPVS — Hosted Solution.** We leverage our SIP trunking and managed LAN services in providing IPVS.

A Communications Manager (Unified CM) at the central site facilitates connectivity to remote offices via the IP WAN, connectivity to the PSTN (via SIP or legacy Telco connections), and, if required, connectivity to the Internet. Calls outside of the EIS agency network are transported via Lumen MPLS networks to Lumen's extensive North American Softswitch (NASS) architecture with many POPs and nationwide co-carrier trunking facilities for hand-off to the PSTN or other EIS carriers.

The Lumen IPVS solution employs QoS enabled IP access connections that may be integrated with other agency data, or may be used only for voice. A single access connection carries all voice traffic: on-net, local off-net, and long distance off-net traffic.



**Figure 1.3.2.1.1-2. Lumen IPVS – Premise-Based Solution.** *Lumen provides premise-based IPVS to premises with less than five subscribers to those with more than 20,000 subscribers.*

Our offering is augmented by a variety of Service Enabling Devices (SED) including managed routers and LAN switches for IP connectivity at the agency voice LAN, VoIP station equipment and Analog Terminal Adapters (ATA). ATAs enable Agencies to continue using existing analog FAX machines, key systems, and phones over the VoIP network.

**1.3.2.1.2 Standards [L.29.2.1, M.2.1, C.2.2.1.1.2]**

Lumen's TFS offering is compliant with the standards listed in SOW C.2.2.1.1.2. Our IPVS offering supports all FCC-mandated regulations including E911 and CALEA.

**1.3.2.1.3 Connectivity [L.29.2.1, M.2.1, C.2.2.1.1.3]**

The Lumen IPVS solution provides connectivity and interoperability with the PSTN, Internet and/or private IP networks, other EIS contractors' voice service networks, and satellite-based voice networks. Within the hosted environment, the

---

Lumen IPVS solution includes a public (IPS) or private (VPNS) IP service connection to the hosted VoIP data centers. VPNS service has built-in privacy, availability, and performance management features. IPVS provides managed onsite communications among both VoIP station endpoints and analog terminal adaptors suitable for analog telephone sets or legacy fax machines. We provide feature transparent services between agency locations via the Lumen IP/MPLS backbone infrastructure, which includes extended connectivity to remote offices.

Lumen's IPVS administrator features provide secure browser-based access with authentication to perform IPVS administration capabilities, configuration management, and retrieve management reports. Administrators can make real-time or scheduled administrative changes to the system, including enforcing or changing the class of service per station; blocking selected numbers; viewing subscriber line status for single or multiple users; retrieving IPVS reports (real time or historical); activating/de-activating call forwarding; administering dial plans; directory updates; and account password management.

#### **1.3.2.1.4 Technical Capabilities [L.29.2.1, M.2.1, C.2.2.1.1.4]**

Lumen's IPVS solution offers a sophisticated suite of personalized settings for features and capabilities. Through secure browser-based access, subscribers can manage their personal calling preferences, messages, and view call status in real time. They can control available user telephony functions, screen and route calls, block selected numbers; activate/de-activate call forwarding; change ring preferences; view call history log; manage personal directory/address books; manage abbreviated dialing lists; select display format; manage individual subscriber password(s); view subscriber line status; manage routing of incoming calls and messages; view caller ID information; manage voice mail messages; and provide message waiting indications.

**Figure 1.3.2.1.4-1** shows how the Lumen EIS IPVS fully complies with all SOW technical capabilities requirements.

#### **Figure 1.3.2.1.4-1. IPVS Technical Capabilities.**

**General Services Administration (GSA)**  
**Enterprise Infrastructure Solutions (EIS)**

Contract # GS00Q17NSD3006  
 Mod #: P00310  
 Submission #: CL01001.01a

LUMEN COMPLIES	SOW REQUIREMENT (C.2.2.1.1.4)	NETWORK-BASED	PREMISE-BASED	LUMEN COMPLIANT SOLUTION
✓	Unlimited on-net to on-net	✓	✓	<ul style="list-style-type: none"> <li>The Lumen IPVS solution provides unlimited on-net to on-net calling. This applies to the customers' end-points connected via a customer private WAN/LAN. No PSTN access is required.</li> </ul>
✓	Unlimited on-net to CONUS off-net calling	✓	✓	<ul style="list-style-type: none"> <li>Our IPVS provides calling to CONUS locations that are NOT connected via a customer private WAN / LAN</li> </ul>
✓	Support for off-net calling	✓	✓	<ul style="list-style-type: none"> <li>The Lumen IPVS supports off-net calling to CONUS, OCONUS, and Non-Domestic locations</li> </ul>
✓	Establish and receive telephone calls between on-net locations and the PSTN	✓	✓	<ul style="list-style-type: none"> <li>Our IPVS includes various PSTN-to-VoIP (and vice versa) gateways that connect Lumen PSTN and local exchange terminations for inbound and outbound calling</li> </ul>
P	Remote access capability	✓	✓	<ul style="list-style-type: none"> <li>Our IPVS supports flexible call routing using our VoIP remote office features, which enables users to bridge calls to remote or home office numbers</li> </ul>
✓	<b>Mandatory and Optional Capabilities</b>			
✓	1. Real-time transport of voice, facsimile, and TTY communications.	✓	✓	<ul style="list-style-type: none"> <li>Our IPVS solution supports the Real-time Transport Protocol (RTP) as a network protocol for delivering audio over an IP networks. RTP is designed for end-to-end, real-time, transfer of streaming media. The protocol provides facilities for jitter compensation and detection of out of sequence arrival in data, which are common during transmissions on an IP network.</li> </ul>
✓	2. Real time delivery of caller ID (ANI) information	✓	✓	<ul style="list-style-type: none"> <li>The Government can choose a Caller ID Name (CNAM) or simply apply a calling line ID number for all outbound calls. Delivery of CNAM &amp; Number are loaded into a national database and passed during the call set up (SIP signaling) so, if caller ID is passed, it is delivered in real time.</li> </ul>
✓	3. Interoperate with NANP and IU-E.164	✓		<ul style="list-style-type: none"> <li>Lumen supports E.164 as the standard for specifying global phone numbers contained in SIP Universal Resource Locators (URL) for Telephone Calls. SIP URLs can contain either local or global phone numbers. E.164 defines the number structure and functionality for three categories of numbers used for international public</li> </ul>

**General Services Administration (GSA)**  
**Enterprise Infrastructure Solutions (EIS)**

Contract # GS00Q17NSD3006  
 Mod #: P00310  
 Submission #: CL01001.01a

LUMEN COMPLIES	SOW REQUIREMENT (C.2.2.1.1.4)	NETWORK-BASED	PREMISE-BASED	LUMEN COMPLIANT SOLUTION
				telecommunication. These three categories of numbers are used for identifying geographic areas, global services, and Networks. E.164 also details the components of the numbering structure and the digit analysis required to successfully route calls in each of the three categories of numbers.
✓	4. Interoperate with private network dial plans and support direct dialing.	✓	✓	<ul style="list-style-type: none"> <li>The Lumen IPVS supports direct dialing, and interoperates with private network dial plans. Private dial plans are on-net applications that, in most cases, do not require PSTN access and are supported by most PBX manufacturers, as well as hosted providers</li> </ul>
✓	5. Interoperate with non-commercial, agency-specific 700 numbers. (Optional)	P	✓	<ul style="list-style-type: none"> <li>The Lumen IPVS provides this optional capability. Our IPVS interoperates with non-commercial, agency-specific 700 numbers. This can be accomplished by routing the calls to the appropriate Class 5 or Tandem switch from Lumen's PSTN network or by routing via a private IP dial plan if these numbers are accessible via an IP gateway with SIP capability.</li> </ul>
P	6. Provide access to public directory and operator assistance services.	✓	✓	<ul style="list-style-type: none"> <li>Operator assistance to users connected to a hosted- or premise-based PBX is standard and may be accessed via a portal or IP telephone,</li> </ul>
✓	7. Provide unique directory numbers and support existing Government numbers	✓	✓	<ul style="list-style-type: none"> <li>The Lumen IPVS solution supports this requirement. When customers order SIP or TDM voice services, Lumen can provide unique telephone numbers to be used as a directory listing for Government locations, as well as, list existing Government owned telephone numbers.</li> </ul>
✓	8. Provide capability to initiate automatic cal back	✓	✓	<ul style="list-style-type: none"> <li>The Lumen solution retains the called number and provides a callback to the retained number when a line and/or service becomes available.</li> </ul>
✓	9. Support 3-way calling	✓	✓	<ul style="list-style-type: none"> <li>The Level IPVS is configured to support 3 way calling via the terminal (end point), the network, or both.</li> </ul>
Gateway Functionality				

LUMEN COMPLIES	SOW REQUIREMENT (C.2.2.1.1.4)	NETWORK-BASED	PREMISE-BASED	LUMEN COMPLIANT SOLUTION
✓	1. Subscriber gateway interoperability for non-IP telephone devices	✓	✓	<ul style="list-style-type: none"> <li>The Lumen IPVS provides the ability for analog devices to leverage an Ethernet based network by converting the TDM signaling to SIP signaling via an analog adapter gateway. The analog adapter may be premise based or network based, or a combination of both.</li> </ul>
✓	2. PSTN gateway with transparent access to, and interwork with, the domestic and non-domestic PSTNs	✓	✓	<ul style="list-style-type: none"> <li>Lumen IPVS provides transparent access to and interworking with domestic and non-domestic PSTNs. PSTN Gateway functions are implemented using the Lumen Media Gateway, which is a standard element within Lumen's IPVS service architecture.</li> </ul>
P	Station mobility support	✓	✓	<ul style="list-style-type: none"> <li>Ability to relocate a device to a different physical location/port without impacting calling plans, dial plans, and in some instances, 911; mobility may also encompass "hoteling" which allows multiple user profiles to be maintained on a single device</li> </ul>
✓	Traverse and interoperate with firewalls and security layers	✓	✓	<ul style="list-style-type: none"> <li>The Lumen IPVS TURN servers and Session Border Controllers (SBC) provide NAT and firewall traversal capabilities.</li> </ul>
Security Practices and Safeguards				
✓	1. Denial of service security practices and safeguards	✓	✓	<ul style="list-style-type: none"> <li>Denial of Service (DoS): Voice traffic is kept distinct and secure by our session border controllers that prevent attacks by hacker, worms, or viruses from denying legitimate users access to network services.</li> <li>Our solution provides global protections from distributed DoS attacks between voice and data (the data network DDOS is prevented from impacting voice and, similarly, voice DDOS is prevented from impacting the data network).</li> </ul>
✓	2. Intrusion security practices and safeguards	✓	✓	<ul style="list-style-type: none"> <li>Our edge proxy servers have the originating end-points predefined, which prevents unauthorized call origination. In addition, our service includes a secure authentication scheme for any calls originating on the network. This protects the network from attempts by foreign or other unknown devices pursuing access to the network.</li> </ul>



LUMEN COMPLIES	SOW REQUIREMENT (C.2.2.1.1.4)	NETWORK-BASED	PREMISE-BASED	LUMEN COMPLIANT SOLUTION
✓	3. Invasion of Privacy security practices and safeguards	✓	✓	<ul style="list-style-type: none"> <li>Our Core network is private and protected, as a Lumen-owned and operated network inaccessible to the public.</li> </ul>
✓	Emergency services, including 911 and E911 services, and PSAP support	✓	✓	<ul style="list-style-type: none"> <li>We support and provide for all FCC-mandated regulations, including Augmented 911/E911 services; some restrictions exist on E911 services for users telecommuting outside of the National Capital Region.</li> </ul>
✓	FCC LNP compliance	✓	✓	<ul style="list-style-type: none"> <li>Our LNP process complies with FCC regulations.</li> </ul>

More key capabilities and features of our IPVS solution are described in the following paragraphs.

**Unlimited local calling for IPVS subscribers.** Unlimited Local, inter-agency, on-net to on-net, and on-net to CONUS off-net calling is included in Lumen’s IPVS service.

**Interconnectivity.** Hosted IPVS service provides on-site communications among both VoIP station end points and analog telephone sets. Hosted IPVS provides feature transparent services between agency locations via the Lumen MPLS backbone network. This includes extended connectivity to remote office/home office arrangements, where permitted by Lumen’s E911 coverage. Intra-agency intersite traffic may, at the Agencies discretion, be encrypted using IPsec.

**Number Porting.** Lumen’s IPVS is fully compliant with the Federal Communications Commission (FCC) Local Number Portability (LNP) requirements. Allocation of DID numbers is included and available as part of the solution. Number Portability is also included as with standard Voice services. Lumen has a dedicated team of people associated with number porting. We provide templates for customer to fill out jointly with our project

**Lumen IPVS Global Capabilities**

- First Carrier to develop VoIP Softswitch capabilities 12 years ago.
- Network and telephone numbers in rate centers serving over 87% of US households
- Voice network carrying over 13B minutes of traffic and 5B calls/month
- Over 1.7M voice-capable trunks connecting the Lumen network to PSTN
- International local inbound presence in 26 countries

managers and request a LOA to make the porting request. Lumen manages more than 2,000 number ports per month and has best practices it can share to ensure numbers are ported in a timely fashion.

**Integration with existing analog / digital voice services.** Lumen can integrate with analog fax services by using an ATA (analog terminal adapter) to make the fax service an integrated part of the IP based solution. All long distance calling anywhere in the U.S. and Canada are included in the Lumen standard offering for any number ported to the Lumen service.

**Custom Dial Plans.** Lumen can support a custom dial plan across multiple locations and can support five (5) digit or higher dial plans. We can emulate what you use today or help create something new to streamline dialing between locations.

**Automatic Call Distribution (ACD).** Lumen’s patented ACD routing with service level optimization aligns contact priority to specific service level agreement and matches priority with appropriately experienced agents. This enables the system to automatically set the appropriate service levels for each type of incoming communication – call, email or chat – simplifying configuration, utilizing agents more effectively, and ultimately providing better customer service.

**1.3.2.1.5 Features [L.29.2.1, M.2.1, C.2.2.1.2]**

Lumen provides the features specified in SOW C.2.2.1.6. **Figure 1.3.2.1.5-1** shows how the Lumen EIS IPVS fully complies with all SOW features requirements.

**Figure 1.3.2.1.5-1. Hosted and Premises-Based IPVS Compliant Solution**

LUMEN COMPLIE	SOW C.2.2.1.2 REQUIREMENT	HOSTED	PREMISES -BASED	LUMEN COMPLIANT SOLUTION
✓	Voice Mail Capability	✓	✓	<ul style="list-style-type: none"> <li>Lumen's Voice Mailbox capability meets or exceeds the minimum requirements described in SOW C.2.2.1.2.</li> <li>Lumen's IPVS supports Unified Messaging (UM) with voicemails sent as WAVE (.wav) file attachments to designated email to programs such as MS Exchange or Google mail.</li> <li>Users are able to remotely access voice mail services via secure access using a password or PIN. As a standard IP PBX capability, users can record multiple custom voice mail greetings (one for no</li> </ul>

**General Services Administration (GSA)**  
**Enterprise Infrastructure Solutions (EIS)**

Contract # GS00Q17NSD3006  
 Mod #: P00310  
 Submission #: CL01001.01a

LUMEN COMPLIE	SOW C.2.2.1.2 REQUIREMENT	HOSTED	PREMISES -BASED	LUMEN COMPLIANT SOLUTION
				answer and a separate greeting for phone busy)
✓	Auto Attendant	✓	✓	<ul style="list-style-type: none"> <li>Our solution allows callers to dial a single number for high volume call areas and to select from up to nine (9) options to be directed to various attendant positions, external phone numbers, mailboxes or to dial by name or extension at a minimum.</li> </ul>
✓	Augmented 911/E911 Service	✓	✓	<ul style="list-style-type: none"> <li>We support and provide for all FCC-mandated regulations, including Augmented 911/E911 services; some restrictions exist on E911 services for users telecommuting outside of the National Capital Region. Our web portal enables the Government to update profiles, as required. Users or administrators are responsible to manage their E-911 address if they move their phone from the original physical address previously assigned. The E-911 database is automatically updated within minutes to ensure a 911 call would be routed to the proper PSAP. If the agency is using our SIP trunking service in conjunction with a PBX, changes can be done via a portal and updates to the ALI database are near real time.</li> </ul>
Standard Features				
✓	1. Caller ID	✓	✓	<ul style="list-style-type: none"> <li>Caller name and number ID is supported by the Lumen solution</li> </ul>
✓	2. Conference Calling	✓	✓	<ul style="list-style-type: none"> <li>Station with the ability to connect to up to three unique devices/ telephone numbers. In addition, Lumen's audio conferencing solution allows each user to have up to 20 people on a bridge.</li> </ul>
✓	3. Do Not Disturb	✓	✓	<ul style="list-style-type: none"> <li>Block inbound calls and/or re-route to voice mail</li> </ul>
✓	4. Call Forward – All	✓	✓	<ul style="list-style-type: none"> <li>All calls forwarded to a pre-determined destination</li> </ul>
✓	5. Call Park	✓	✓	<ul style="list-style-type: none"> <li>Incoming call is answered and put on a form of hold. This call can then be picked up on any other device that is on the same network as then initial device receiving the call.</li> </ul>
✓	6. Hotline	✓	✓	<ul style="list-style-type: none"> <li>Red Phone for end-to-end encryption app for voice calls</li> </ul>
✓	7. Call Forward – Busy	✓	✓	<ul style="list-style-type: none"> <li>Calls forwarded to a pre-determined destination when called party number is busy</li> </ul>
✓	8. Call Pickup	✓	✓	<ul style="list-style-type: none"> <li>Lumen IPVS solution supports call pickup</li> </ul>
✓	9. Hunt Groups	✓	✓	<ul style="list-style-type: none"> <li>We can link multiple users in a hunt group so that, when the first</li> </ul>

LUMEN COMPLIE	SOW C.2.2.1.2 REQUIREMENT	HOSTED	PREMISES -BASED	LUMEN COMPLIANT SOLUTION
				number is busy, the call is delivered to the next user-defined number in the hunt group, a process that is repeated until the call is answered or the last available number is reached. The call loop can be restarted from the last number.
✓	10. Call Forward – Don't Answer	✓	✓	<ul style="list-style-type: none"> <li>If called party does not answer, call is forwarded to a pre-determined destination</li> </ul>
ü	11. CoS Restriction	✓	✓	<ul style="list-style-type: none"> <li>We can assign priorities to specific calls based on packet payloads</li> </ul>
✓	12. Multi-Line Appearance	✓	✓	<ul style="list-style-type: none"> <li>A phone that can support more than one inbound call</li> </ul>
✓	13. Call Hold	✓	✓	<ul style="list-style-type: none"> <li>Our solutions includes call-hold capability</li> </ul>
✓	14. Distinctive Ringing	✓	✓	<ul style="list-style-type: none"> <li>We offer a variety of rings to suit user needs and preferences</li> </ul>
✓	15. Directory Assistance	✓	✓	<ul style="list-style-type: none"> <li>Lumen directory assistance is Web-based and via IP phone</li> </ul>
✓	16. Call Transfer	✓	✓	<ul style="list-style-type: none"> <li>The call transfer capability provided by the Lumen IPVS allows the transfer of calls to an on-net or off-net location. Call transfers can be blind or consultative. A blind transfer is one in which the transferring extension connects the caller to a destination extension before ringback begins. A consultative transfer is one in which the transferring party either connects the caller to a ringing phone (ringback heard) or speaks with the third party before connecting the caller to the third party.</li> </ul>
✓	17. Call Waiting	✓	✓	<ul style="list-style-type: none"> <li>Lumen IPVS enables a user to answer a call while already engaged in another call. To answer the waiting call, the user initiates a flash hook mechanism. The user connects with the waiting party and holds the original party. By initiating a flash hook capability, the user reconnects to the original party and holds the waiting party. The feature completes when any party hangs up. Users can activate/deactivate the Call Waiting service for all incoming calls via a feature code or Web interface.</li> </ul>
✓	18. Speed Dial	✓	✓	<ul style="list-style-type: none"> <li>Speed dialing is programmable, to allow one button dialing</li> </ul>
✓	19. Call Number Suppression	✓	✓	<ul style="list-style-type: none"> <li>Lumen IPVS enables a user to block delivery of his/her identity to the called party. The user controls the service via a feature code or</li> </ul>

LUMEN COMPLIANT	SOW C.2.2.1.2 REQUIREMENT	HOSTED	PREMISES-BASED	LUMEN COMPLIANT SOLUTION
				Web interface, which provides the ability to activate and deactivate the service. If activated, all calls made by the user have the user's identity blocked. If this service is activated, users can still choose to allow the delivery of their Calling Line ID on a specific call by entering the respective feature access code for Calling Line ID Delivery per Call. Once the call is over, Calling Line ID Blocking is restored.
ü	20. Specific Call Rejection	✓	✓	<ul style="list-style-type: none"> <li>Lumen enables users or administrators to block specified incoming calls to their company, department, and/or individual users. In addition to being able to configure which types of calls each user is restricted from receiving, a user or group administrator can regulate incoming calling by restricting specific digit patterns.</li> </ul>
✓	21. Last Number Dialed	✓	✓	<ul style="list-style-type: none"> <li>Our solution provides speed dialing of last number dialed</li> </ul>
✓	22. IP Telephony Manager (Admin)	✓	✓	<ul style="list-style-type: none"> <li>Lumen IPVS allows an administrator using the web interface to perform functions, such as, add, modify, or delete group administrators, department administrators, and schedules. Also, modify calling plans, manage utilities such as the common phone lists and feature codes, and perform advanced administrative functions.</li> </ul>
✓	23. IP Telephony Manager (Subscriber)	✓	✓	<ul style="list-style-type: none"> <li>The user web interface allows (and limits) users to access their profile, which is mapped to the users telephone number. The user has the capability to manage applications such as call waiting, calling line ID blocking (all or per call), and external/internal calling ID delivery.</li> </ul>

**1.3.2.1.6 Interfaces [L.29.2.1, M.2.1, C.2.2.1.3]**

Lumen meets the interface requirements shown in the IPVS Interfaces table in SOW C.2.2.1.3. The Lumen IPVS supports a wide variety of subscriber devices, including analog phones, facsimile devices, IP phones, and PC client soft phones, whether downloadable and web- or flash-based. We also support the required IPVS interface at the SDP, identified as UNI Type #1: Router or LAN Ethernet port: RJ-45 (using standard IEEE 802.3) in SOW C.2.2.1.3.

**1.3.2.1.7 Performance Metrics [L.29.2.1, M.2.1(c), C.2.2.1.4]**

Lumen meets all of the IPVS performance metrics shown in the IPVS Performance Metrics table in SOW C.2.2.1.4. Lumen’s GovNOCs manage all aspects of the IPVS service 24/7. The entire service is monitored for uptime and quality. Our GovNOCs have the ability to failover to alternate servers or datacenters to ensure maximum availability for our customers as we are fully aware that phone service is a critical business function and must be highly reliable. This enables us to pinpoint geographic areas or even individual customers where service appears to be degrading, enabling Lumen to proactively address issues before the problem has even become noticeable to the customer.

**1.3.2.2 Managed LAN Service [L.29.2.1, M.2.1, C.2.2.1.5]**

Lumen’s Managed LAN Service (MLS) includes a full suite of professional services to support the EIS program requirements described in SOW C.2.2.1.5 for hosted and premises-based IPVS solutions. **Figure 1.3.2.2-1** shows how the Lumen IPVS complies with MLS requirements shown in SOW C.2.2.1.5.

**Figure 1.3.2.2-1. Lumen Complies with MLS Requirements**

LUMEN COMPLIES	SOW C.2.2.1.5 REQUIREMENT	LUMEN COMPLIANT SOLUTION
✓	Provide and manage all LAN networking components (hardware and licensing)	<ul style="list-style-type: none"> <li>Lumen will provide wired LAN networking equipment fulfillment, including all of the hardware and licensing necessary to extend the IPVS site demarcation point to the terminating device, including all equipment on site in support of the IPVS service</li> </ul>
✓	Equipment provided must support Power over Ethernet	<ul style="list-style-type: none"> <li>Lumen equipment supports Power over Ethernet (PoE) to provide power needed by IP phones and other Power over Ethernet (PoE) devices.</li> </ul>
✓	Provide, manage, maintain, and repair or replace all necessary Managed LAN Service equipment	<ul style="list-style-type: none"> <li>Our MLS include monitoring, management, maintenance (repair/replace), for all Layer 2 devices, routers, switches, and other devices related to the IP Voice service, including hardware and software to support the on-premise call processing and handset requirements.</li> </ul>
Technical Capabilities, C.2.2.1.6(1) through (11)		
✓	1. Provide necessary hardware and licensing	<ul style="list-style-type: none"> <li>Our approach is described earlier in the first row of this figure.</li> </ul>
✓	2. Interoperability with subscribing agency’s VoIP-ready cabling infrastructure	<ul style="list-style-type: none"> <li>IPVS CPE fulfillment, pre-configuration, inside wiring, and staging to ensure (and flag as necessary) interoperability with agency IPVS-ready cabling infrastructure</li> </ul>

**General Services Administration (GSA)**  
**Enterprise Infrastructure Solutions (EIS)**

Contract # GS00Q17NSD3006  
 Mod #: P00310  
 Submission #: CL01001.01a

LUMEN COMPLIES	SOW C.2.2.1.5 REQUIREMENT	LUMEN COMPLIANT SOLUTION
✓	3. Ongoing maintenance and upgrades of contractor-owned equipment	<ul style="list-style-type: none"> <li>Preventive and corrective Maintenance and upgrades for all Lumen-owned hardware/software used to provide IPVS services to the agency</li> </ul>
✓	4. Installation time intervals	<ul style="list-style-type: none"> <li>In response to specific TO requirements, Lumen will propose installation time intervals for additional user devices at facilities already using MLS.</li> </ul>
ü	5. Managed LAN Service wireless devices or components	<ul style="list-style-type: none"> <li>The Lumen MLS won't include wireless devices or components on the LAN unless the wireless elements are requested and approved by the OCO.</li> </ul>
✓	6. Managed LAN Service shall not support other services	<ul style="list-style-type: none"> <li>The MLS Lumen provides will not support other services such as video and data, unless the OCO requests and approves having the MLS provide such support</li> </ul>
✓	7. Ensure only authorized subscriber devices	<ul style="list-style-type: none"> <li>Lumen will use the management and accounting processes we have developed and used in providing Network and other Government contract support over many years to ensure that only ordering agency authorized devices operate on the MLS we provide.</li> </ul>
✓	8. Monitor manage and restore	<ul style="list-style-type: none"> <li>Lumen will manage the MLS and provide restoral as needed on a 24/7 basis through the Lumen EIS NOCs.</li> </ul>
✓	9. Specify LAN management activities	<ul style="list-style-type: none"> <li>Our configuration management (CM) approach is divided into user- and device-level changes, each with their own protocols.</li> <li>Lumen provides GSA insight into the performance of Lumen's EIS elements using Web-based tools accessible through the GSA Customer Portal.</li> <li>Our Moving Average Convergence/Divergence (MACD) process provides a model for managing and executing the moving, adding, changing and removing of hardware and software configuration items (and configurations) in the agency environment.</li> <li>As required, Lumen schedules and dispatches qualified technical resources for replacement and installation and RMA of failed equipment</li> <li>The Lumen Web-based, real-time monitoring of network connectivity minimizes downtime and provides fast fault resolution without you having to initiate support requests; proactive notification and resolution to any network outages; automatic trouble ticketing and email notification.</li> </ul>
✓	10. Provide proactive notification of major and minor alarms to the Managed LAN Service	<ul style="list-style-type: none"> <li>We manage integrated service elements such as service/alarm monitoring and fault management; ticket creation; proactive notification of alarms, issue resolution, and issue updates to designated agency contacts (via calls by service desk agents and/or auto-generated email notifications); and trouble isolation and resolution.</li> <li>We send alarm notifications (through email) to designated agency users within 15 minutes of alarm detection.</li> </ul>
✓	11. Define the escalation path	<ul style="list-style-type: none"> <li>Lumen's 24/7 Service Desk provides Tier 1 support and escalates incidents to Tier</li> </ul>

LUMEN COMPLIES	SOW C.2.2.1.5 REQUIREMENT	LUMEN COMPLIANT SOLUTION
	for trouble tickets for both network and hardware issues	2/3 according to pre-defined SLAs; at any point in the incident management process, an agency may request escalation via the Service Desk Supervisor to address concerns about the handling of the incident. <ul style="list-style-type: none"> <li>• If service restoration requires activities by a third-party provider, we initiate and manage the process as described in the table above. For High Severity incidents, our Service Desk initiates immediate Tier 2/engineer engagement. Designated agency representatives are provided ongoing status updates till ticket is resolved/closed.</li> </ul>

**1.3.2.3 Session Initiating Protocol Trunk Service [L.29.2.1, M.2.1, C.2.2.1.6]**

Lumen’s Session Initiating Protocol (SIP) Trunking is a VoIP-based, PSTN access service for TDM and IP telephony customer premises equipment. Our SIP trunking voice service offering is designed to support SIP and traditional voice (TDM/ISDN) equipment. The service operates on Tier 1 voice backbone, one of the largest and most advanced in the world.

**Industry-Leading SIP Footprint**  
 Commander Naval European Command (CNEC) chose Lumen to help provide telecommunications service to its member institutions, resulting in a cost reduction of up to 20% with our VoIP-enhanced local and SIP Trunking services.

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

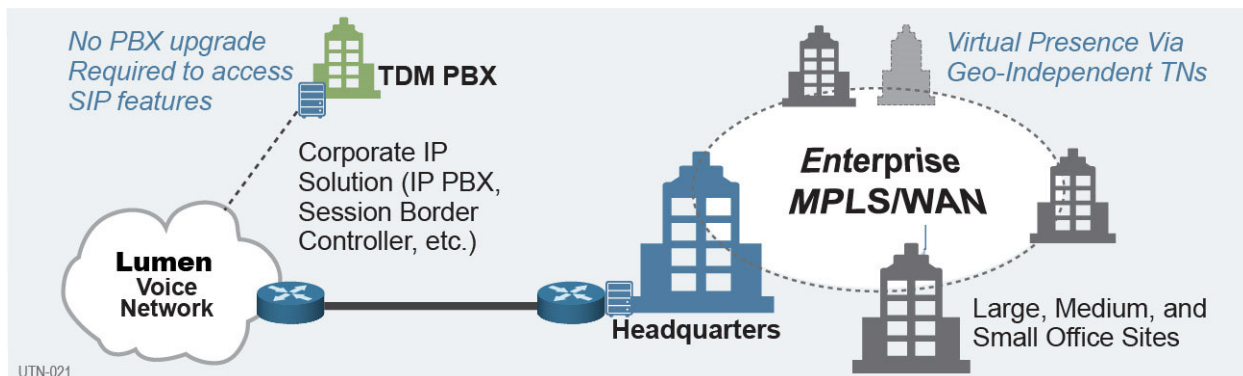
[REDACTED]

Our SIP trunking is offered to the EIS agency’s LAN/WAN over Lumen-provided dedicated IP connections. All voice traffic remains on Lumen’s premium IP backbone until it needs to communicate with other PSTN partners, helping to improve overall



service quality and easing problem resolution. Our solution is built to enhance service quality through infrastructure redundancy. It supports configurable call management and routing failover capabilities, while at the same time allowing customers to leverage their investments in legacy TDM equipment as they make the transition to an end-to-end SIP-signaled environment.

Lumen offers SIP Trunking over dedicated IP connections or native PRI (TDM) hand-offs to the customer LAN/WAN on which the IP PBX/PBX/SBC resides, as shown in **Figure 1.3.2.3-1**. Multiple access options are available, including T-1, NxT-1, DS-3, ISDN PRI hand-off and metro Ethernet for the flexibility to meet connectivity requirements for all sites, including branches, regional offices, headquarters, and data centers.



**Figure 1.3.2.3-1. CenturyLink's SIP Trunking Functionality.** We offer SIP Trunking over dedicated IP connections or native PRI (TDM) hand-offs to customer LANs/WANs on which the IP PBX/PBX/SBC resides.

Lumen can converge the SIP-signaled trunking packets with data traffic onto the same access facility, allowing the traffic to use our IP Virtual Private Network (VPN) infrastructure's available bandwidth when it is not needed for voice traffic. This ability does not apply to native PRI hand-offs in which the circuit has to be dedicated to the SIP trunk. This is supported through our extensive MPLS QoS and CoS capabilities.

Lumen offers two deployment models to our EIS customer agencies:

- **IP-PBX model:** the customer deploys an IP-PBX at its location. The IP-PBX provides call control, on-site switching, features, voice mail, and the other typical

functions of a PBX, using a VoIP interface to control IP phones. It can be connected to the Lumen voice network for PSTN access using either TDM or IP trunks. Often times customers will have the carrier deliver SIP trunks to the IP PBX and the customer will “trunk” out to remote sites on their corporate WAN thus consolidating remote locations onto the single Voice Complete solution and eliminate local branch telephony infrastructure such as smaller PBXs, key systems, PRIs, POTS (Plain Old Telephone Service) lines, etc.

- **Hosted PBX model:** the customer connects to the Lumen network over IP connections. The Lumen network provides call control, features, voice mail, and PSTN access using a network-based solution. In this model, there is no on-site switching – simply VoIP phones interacting directly with the Lumen network.

**1.3.2.3.1 SIP Trunking Technical Capabilities [L.29.2.1, M.2.1, C.2.2.1.6.1]**

Supporting our unified communications approach, our SIP VoIP trunking service consolidates voice and data onto a single secure, reliable network, optimizing network capacity and flexibility for calls between on-net locations and the PSTN. Our service also reduces voice communication costs, and, being IP-based, improves reliability and disaster recovery capability. Our SIP Trunking service works with a diversity of devices and applications.

**1.3.2.3.2 SIP Trunking Features [L.29.2.1, M.2.1, C.2.2.1.6.2]**

Lumen’s Managed LAN Service solution provides the mandatory SIP Trunk Service features listed in SOW C.2.2.1.6.2, and described in **Figure 1.3.2.3.2-1**.

**Figure 1.3.2.3.2-1. Lumen’s SIP Trunking Features**

LUMEN COMPLIES	SOW C.2.2.1.6 REQUIREMENT	LUMEN COMPLIANT SOLUTION
✓	1. Automatic call routing	<ul style="list-style-type: none"> <li>• Our DID/DDI call routing options handle potential call congestion or outage conditions, emergency planning, load balancing, and internal network optimization to ensure that their internal calls are handled effectively and efficiently.</li> <li>• Our solution provides automatic call routing and trunk group routing. Location routing provides customers with different realms or IP trunk groups on different Lumen IP Session Directors. Lumen will route calls to the appropriate realm or IP trunk group based on predefined customer</li> </ul>

LUMEN COMPLIES	SOW C.2.2.1.6 REQUIREMENT	LUMEN COMPLIANT SOLUTION
		instruction. Calls can be routed based on a round robin scheme of traditional hunt which can also support an out of service condition within the Lumen network. For Trunk Group routing, "option pings" are used to ensure traffic is being sent to a functional customer termination point. In the unlikely event a location cannot accept calls, the call is routed to the next available customer-defined termination point.
✓	2. Bandwidth QoS management	<ul style="list-style-type: none"> <li>Lumen's network analysis tools, including our Adaptive Network Control Solutions suite of network management applications, enable us to effectively manage bandwidth quality for SIP trunking</li> <li>Our NOCs have technicians and tools that leverage traffic analytics technologies to provide real-time end-to-end, site-to-site visibility into network bandwidth performance</li> </ul>
✓	3. Trunk bursting	<ul style="list-style-type: none"> <li>We provide call bursting options with unlimited, fixed, and pre-determined burst capacities; Lumen monitors network availability 24/7/365 and produces daily reports for tracking our network trunking and system alarms, and a proactive process to alert account teams when a network problem is detected</li> </ul>
✓	4. Telephone number blocks	<ul style="list-style-type: none"> <li>Lumen SIP Trunking service offers telephone number blocks with flexible pricing for large number blocks</li> </ul>

### 1.3.3 Managed Service (Mandatory)

#### 1.3.3.1 Managed Network Service [L.29.2.1, M.2.1, C.2.8.1, C.1.8.7]

Government Agencies today are growing increasingly dependent on networked applications and mission critical business communications over complex global infrastructures. Lumen's Managed Network Service (MNS) helps alleviate these challenges by providing a single point of contact in designing, building, and ultimately managing the end-to-end communication network. Delivered

**24/7 Support for Lumen Networks Worldwide**

- Lumen currently manages the operation of four Network Operations Centers (NOC) and field service support for approximately 400 campus network sites and roughly 2,800 remote sites.
- Available globally in North America, Latin America, EMEA, and APAC

around the corner or across the globe for federal and commercial enterprises, our industry-recognized MNS portfolio helps Agencies optimize IT investments, control costs, and improve operational and network efficiencies.

**Figure 1.3.3.1-1** highlights the features to GSA, and the Agencies, of the Lumen MNS solution. This figure also aligns key features with the evaluation criteria to illustrate how the Lumen MNS Solution meets the Government's needs.

**Figure 1.3.3.1-1. Features of Lumen MNS**

EVALUATION CRITERIA	FEATURES
Understanding [M.2.1.1]	<ul style="list-style-type: none"> <li>Expert design teams design solutions to agency communication and mission needs</li> <li>Expertise across multiple facets including CPE, voice, data, security, and data center networking</li> <li>Collaborative solutions design that incorporates key agency network information</li> <li>Networking experts to handle growing network complexities and optimize network</li> </ul>
Quality of Services [M.2.1.2]	<ul style="list-style-type: none"> <li>We meet or exceed all EIS performance requirements</li> <li>Secure, 24/7 reporting tools enable the assessment of services.</li> <li>Extensive past performance experience with similar scope contracts has resulted in the development of mature reporting services required for EIS MNS</li> <li>Fill Program Management responsibility for Quality of Services</li> </ul>
Service Coverage [M.2.1.3]	<ul style="list-style-type: none"> <li>Lumen and our partners provide a global footprint of MNS for our EIS agency customers covering the entire range of CBSAs</li> </ul>
Security [M.2.1.4]	<ul style="list-style-type: none"> <li>Our state-of-the-art Government Security Operations Center (GovSOC) monitors the complete threat landscape with a continuous cycle of protection.</li> <li>Lumen and our subcontractors perform security operations in accordance with industry best practices and standards supporting cyber, personnel, physical, network, and EIS systems security</li> </ul>

**Understanding.** Today’s Government communications environment offers unique challenges that demand the need for an EIS service provider who understands underlying issues and develops solutions that offer best value to the Government. As an incumbent on the Networx Enterprise, WITS3, and multiple regional GSA contracts; and as Chair of the ACT-IAC Networks and Telecommunications Special Interest Group (N&T SIG), Lumen brings an in-depth understanding of GSA’s EIS Program Goals and offers Managed Network Services positioned to meet and exceed these goals, as illustrated by **Figure 1.3.3.1-2**.

**Figure 1.3.3.1-2. Lumen MNS Solution Satisfies EIS Program Goals**

EIS PROGRAM GOAL	CHALLENGE FOR EIS MNS SERVICES	LUMEN SOLUTION
Service Continuity	Vendor software or hardware issues occur (including maintenance, uptime, capacity, throughput, extensibility) affecting availability statistics.	Lumen’s MNS provides 24x7/365 remote monitoring, incident detection and remediation services. These services include patch management and vendor management to ensure software and hardware problems are resolved swiftly. All managed equipment configurations are backed up so they can be applied quickly in the event of replacing a failed piece of hardware. Software patches and updates are

**General Services Administration (GSA)**  
**Enterprise Infrastructure Solutions (EIS)**

Contract # GS00Q17NSD3006  
 Mod #: P00310  
 Submission #: CL01001.01a

EIS PROGRAM GOAL	CHALLENGE FOR EIS MNS SERVICES	LUMEN SOLUTION
		evaluated and applied based on the specific EIS agency's network and configuration.
Highly Competitive Prices	Cost savings and productivity gains: Reduce the agency's capital outlay for hardware costs and control headcount/IT staff needs by leveraging a single carrier to provide a turn-key service that includes design, procurement, installation, configuration, implementation, management and 24/7 monitoring & maintenance can be challenging.	Lumen's MNS provides integrated turn-key service that includes design, procurement, installation, configuration, implementation, management and 24/7 monitoring & maintenance. We utilize as many, or as few, of these turn-key features to meet agency goals and manage costs as appropriate to meet all requirements. Because we support multiple customers, we are able to spread the support costs and offer very competitive pricing.
High-Quality Service	Right-of-way access or other logistical issues prevents or delay delivery of new capacity.	Lumen is one of the few carriers that can boast of a highly reliable and robust end-to-end network not only in the long haul/WAN environment, but also in the metro and regional footprint. Lumen MNS offers multiple contact methods to ensure customers have easy access to our Service Delivery Centers. Our 1-800 contact number is answered by a live technician and triaged and escalated according to the priority and impact of the incident. Lumen MNS customers also have the ability to escalate the priority level of an incident to ensure it receives the relevant attention.
Full Service Vendors	Cable companies do not have the global reach themselves. They could partner and integrate, but again it is similar to managing 3rd party networks where significant visibility into the infrastructure is lost. Similarly, System Integrators and smaller carriers may have to build from scratch and add on additional flexibilities and capabilities as they go. They don't have the prebuilt processes, expertise, flexibility and add-ons pre-defined and structured.	Lumen provides Managed MPLS/IP VPN & Internet Services in 60 countries and 500 markets worldwide. This lessens the need for multiple providers and reduces customer administrative overhead.
Operations Support	Vendor software or hardware issues occur (including maintenance, uptime, capacity, throughput, extensibility) affecting availability statistics.	Lumen MNS offers support 24/7/365: ♦ Service Desk (troubleshooting/resolution); ♦ Monitoring; ♦ Client Portal; ♦ Standard Reports; ♦ Change Management; ♦ Move, Add, Change, Delete (MACD); ♦ Problem Management; ♦ Patch Management; ♦ Dispatch Service; ♦ Carrier Case Management.
Transition Assistance and Support	Transitioning any EIS service can impact agency mission if not carefully planned.	Seamless migration supported by the Lumen CPMO - Makes the transition easier with the Lumen service

EIS PROGRAM GOAL	CHALLENGE FOR EIS MNS SERVICES	LUMEN SOLUTION
		delivery team coordinating the implementation as defined by agency needs and timelines. As an added benefit, this frees up agency resources to focus on their core mission.

**Quality of Services.** The Lumen GovNOC is manned by seasoned technicians with years of experience providing support to GSA, agencies, other Government users, and industry. Our GovNOC staff and support teams provide 24/7 proactive real-time monitoring and performance management support to help ensure that MNS performance requirements are consistently met. The Lumen Team has extensive past performance experience with similar scope contracts which has resulted in the development of mature reporting services required for EIS MNS.

**Service Coverage.** Lumen and our partners provide a worldwide footprint of MNS for our EIS agency customers covering the entire range of CBSAs. The Lumen MNS is provided over the global Lumen network, which has integrated strategically dispersed communications switches, switching centers, and dedicated network links.

**Security.** Lumen establishes and maintains DHS EINSTEIN enclaves where required, in accordance with the National Policy requirements specified in SOW C.1.8.8. Lumen also satisfies the requirements of SOW C.2.8.1.2.4, in accordance with applicable security standards and requirements, in keeping with the specifications of individual TOs.

**1.3.3.1.1 Service and Functional Description [L.29.2.1, M.2.1,**

Managed Network Services	Data		Managed Router
	Data and Voice		Managed IAD
		Full Mgmt	Physical Mgmt
• Service Elements/ Management Options	✓	✓	
• Design and Engineering	✓	✓	
• Equipment Procurement	✓	✓	
• Implementation Management	✓	✓	
• Equipment Installation	✓	✓	
• Operations Management	✓	✓	
• Proactive Monitoring	✓	✓	
• Lifecycle Management	✓	✓	
• Software Level 1 Troubleshooting	✓	✓	
• Hardware Break/Fix	✓	✓	
<b>MSLS/IPVPN and DIA Network Services</b>			

**Figure 1.3.3.1.1-1. Lumen Team MNS Solution Overview.** *The Lumen MNS solution architecture provides all of the functionality required to completely satisfy agency requirements.*

---

**C.2.8.1]**

Lumen MNS fulfills the mandatory service requirements for WCS contained in SOW C.2.8.1. This section presents a technical description of our offering, demonstrating our capabilities in the following areas: Standards, Connectivity, Technical Capabilities, Features, Interfaces, and Performance Metrics.

Lumen MNS consists of full-service management and on-site support of customer end-to-end networks including, as required, Customer Premise Equipment (CPE). **Figure 1.3.3.1.1-1** illustrates the architecture of our MNS approach, which includes the provision of Full-Service Management and Physical Management, as described below.

**Full-Service Management** includes design, procurement, installation, configuration, monitoring, management and maintenance of CPE including routers and IADs. agency's may choose to utilize all, or a subset, of these services when creating a managed solution.

**Physical Management** is a component of the Lumen MNS that includes procurement, installation and maintenance of the CPE. This managed solution allows agency users to keep more control over their day-to-day configuration, monitoring, and management and is readily supported within the Lumen MNS capabilities.

Our MNS encompasses all access/transport User Network Interfaces (UNI) under the EIS contract (see Section 1.3.3.1.6). Lumen's network management and proactive real time monitoring services enable rapid troubleshooting and service restoration. Lumen Network Operations Center staff, remote, and field support services teams are geared toward ensuring that customer Agencies realize the seamless connectivity, availability, and reliability parameters defined in the EIS contract. Lumen MNS solutions, the supporting teams, and the reporting tool sets are all available 24/7 to support agency mission critical needs.

**Figure 1.3.3.1.1-2** shows the elements and functions of the Lumen MNS provided 24/7/365.

**Figure 1.3.3.1.1-2. Lumen MNS Elements and Functions**

ELEMENT	FUNCTION
Service Desk	<ul style="list-style-type: none"> <li>The service desk is the central point of contact between the agency and Lumen MNS on a day-to-day basis. It is also a focal point for reporting Incidents (disruptions or potential disruptions in service availability or quality) and for Clients making service requests.</li> <li>This service element covers troubleshooting calls into the Lumen MNS Service Delivery Centers (SDC) for P1 through P4 service calls. The Lumen Team takes on overall ownership of resolving incidents. This service desk activity is used to troubleshoot hardware, software and tools issues that are applicable to the specific service offered Client.</li> <li>Where applicable for third-party devices and products Lumen collaborates with the specific Vendor to resolve the issue for the Client.</li> </ul>
Monitoring	<ul style="list-style-type: none"> <li>Monitoring events from each device or component, defined as Configuration Item (CI) under management and notification of specific events to agency users. Key events include outages, performance bottlenecks (via thresholds) and security incidents (for security services).</li> </ul>
MNS Client Portal	<ul style="list-style-type: none"> <li>Online web portal providing access to open a service ticket, track ticket status, generate reports and view of managed device performance.</li> </ul>
Standard Reporting	<ul style="list-style-type: none"> <li>Online access to standard reports is available through self-service portal for Government users. Sample reports include uptime/availability, performance and usage information. Specific reports are outlined in services appendix.</li> </ul>
Change Management	<ul style="list-style-type: none"> <li>Changes fall into three categories: Standard, Planned, and Emergency. Lumen follows the applicable Government Change Management Process and this includes RFC and service requests which can be handled remotely. If the Government does not have a formal Change Management process, we implement our standardized process.</li> </ul>
MACD Dispatch	<ul style="list-style-type: none"> <li>Change Management is inclusive of MACD for hardware and software and fall into two categories: User and device level changes.</li> </ul>
Dispatch	<ul style="list-style-type: none"> <li>Scheduling and dispatch of qualified technical resources for replacement and installation and RMA of failed equipment.</li> </ul>
Problem Management	<ul style="list-style-type: none"> <li>In certain troubleshooting situations it may be necessary to not only fix the issue but identify the root causes of the issues. Problem analyses are limited to only incidents with high impact severity.</li> </ul>
Carrier Case Management	<ul style="list-style-type: none"> <li>Operational handling of third-party data and telecommunications carriers. This Service Element empowers the Lumen Team to open and manage trouble tickets for MNS with service providers with executed Letter of agency (LOA).</li> </ul>
Patch Management	<ul style="list-style-type: none"> <li>Application of a patch is at the discretion of the Lumen Team and is applied for MNS users to address vulnerability (Select) or to resolve an incident or problem (Essential or Select). Vulnerabilities are investigated by the Lumen Team when released by the vendor and applied when they affect the installed customer CI.</li> </ul>

**1.3.3.1.2 Standards [C.2.8.1.1.2]**

Lumen’s MNS offering is compliant with the standards addressed in SOW C.2.8.1.1.2, and satisfies standards and recommendations specified in applicable TOs. Members of our Team are active in a variety of industry forums and working groups, including serving as Chairman of the ACT-IAC Networks and Telecommunications



---

Special Interest Group (N&T SIG), and are committed to implementing future standards as technology is developed, standards are defined and commercially availability occurs.

#### **1.3.3.1.3 Connectivity [C.2.8.1.1.3]**

The MNS provided by Lumen interfaces with, uses, and interoperate with the underlying global Lumen network which supports EIS services worldwide. We use the most appropriate EIS services, such as VPNS, Ethernet, and Private Line Services, to ensure seamless connectivity to, and optimal performance with, agency networking environments.

#### **1.3.3.1.4 Technical Capabilities [C.2.8.1.1.4]**

In delivering MNS, Lumen provides all of the technical capabilities specified by the SOW. The capabilities we provide in support of MNS include Design and Engineering Services, as well as Implementation, Management and Maintenance.

##### **1.3.3.1.4.1 Design and Engineering Services [C.2.8.1.1.4.1]**

Lumen provides MNS design and engineering services that fully satisfy agency requirements. The right people and a proven process form the cornerstones of Lumen's MNS design and engineering services.

**The Right People.** The Lumen Team provides subject matter experts and end-to-end project management for design, implementation, installation, access coordination, provisioning, equipment configuration, hardware testing, and service activation. Lumen's design and engineering services under the EIS contract includes subject matter experts carefully matched to agency and project needs with:

- Agency-based focus and understanding, combined with the ability to rapidly respond to evolving agency needs
- Work with agency requirements and make design recommendations such as performance levels and network capacities
- Highly professional technical backgrounds, with certifications in relevant systems

**Proven Methodology and Processes.** Lumen's design objectives are based on customer needs and specifications when providing MNS, and incorporate the following

overall objectives to the extent possible: high network availability; increased network performance; network architecture scalability; lower total cost of ownership; enterprise control and visibility; and industry best practices.

**Figure 1.3.3.1.4.1-1** illustrates our MNS design and engineering phases to be performed in accordance with the specific requirements of TOs. During design and engineering, Lumen will rely on our EIS Supply Chain Risk Management (SCRM) Plan for MTIPS to assess risks and areas of vulnerability and determine mitigation plans to overcome risks identified.

**Figure 1.3.3.1.4.1-1. Lumen’s MNS Design and Engineering Phases**

DESIGN AND ENGINEERING PHASES	DESCRIPTION	OUTPUT
Requirements Gathering	Lumen assesses mission, business, and operational requirements and collaborates with Agencies to map them to technical requirements that impact design, including Key Performance Indicators (KPI) and Acceptable Quality Levels (AQL)	Scope Of Work / Requirements Document
Preliminary Architecture Development	This phase involves decisions impacting architecture, including server locations, redundancy, site size/applications/access, DMZ/firewall layout, etc.	Selection of hardware
Site Survey	Assessment of site specific details such as: <ul style="list-style-type: none"> <li>• Inside/Outside plant (ISP/OSP) cable diagrams</li> <li>• Existing network or communications equipment</li> <li>• Facilities layouts</li> <li>• Heating, Ventilation &amp; Air Conditioning (HVAC)</li> <li>• Power requirements</li> <li>• Existing circuit information</li> <li>• Condition of any existing network infrastructure</li> </ul>	Site survey report
Engineering and Design	<ul style="list-style-type: none"> <li>• Network logical diagram indicating the connection types and speed</li> <li>• Specifications including protocols, redundancy, traffic filtering, and traffic prioritization.</li> <li>• Infrastructure workbook providing all details on the connection types by closet by device</li> <li>• Draft Bill Of Materials (BOM) identifying all required network components, hardware, firmware, and related software for the delivery of EIS service(s).</li> <li>• Racking and uninterruptible power supplies</li> <li>• Patch panel connection matrix</li> </ul>	Master Design Specification that includes (but is not limited to): <ul style="list-style-type: none"> <li>• Architecture (including details of physical and logical interfaces and technologies provided)</li> <li>• Site-specific as-built</li> <li>• Traffic patterns</li> <li>• Availability of space</li> <li>• Network address management</li> <li>• Naming conventions</li> <li>• Protocols</li> </ul>

DESIGN AND ENGINEERING PHASES	DESCRIPTION	OUTPUT
	<ul style="list-style-type: none"> <li>ISP drawings showing new cabling</li> <li>OSP drawings showing new cabling</li> <li>Assessing and addressing security concerns including email content filtering, virus/worm/Trojan detection and prevention, intrusion detection and prevention, and internal/external access rights</li> </ul>	<ul style="list-style-type: none"> <li>Fault resilience</li> <li>Power</li> <li>Ventilation</li> <li>Fire prevention</li> </ul> <p>Includes a draft management plan for how the network is to be maintained and managed once any design changes are implemented.</p>

All Lumen design files and architecture documents are quality checked – once by a peer review and again by a technical review board. This validation is intended to ensure customer requirements are met and the solution is the best possible solution for the desired result. Once the design specifications pass our internal Quality Assurance (QA), we generate a final Bill of Materials (BOM) for internal review and approval, paying special attention to ensure adaptability and scalability for future needs.

The agency is then presented with the BOM and project plan for review. Once approved, Lumen places equipment orders and schedules any additional cable plant or passive equipment modification. If all elements are in place, implementation takes place according to the project plan. Our project plan is sensitive to ensuring minimal disruption to current networking environment, and includes coordination of all installation activities with the agency.

**Figure 1.3.3.1.4.1-2** provides specific details pertaining to each of the three MNS Design and Engineering Services SOW required elements, showing how the Lumen MNS fully complies with SOW Design and Engineering Services requirements.

**Figure 1.3.3.1.4.1-2. MNS Design and Engineering Services Technical Capabilities**

LUMEN COMPLIES	SOW C.2.8.1.1.4.1 REQUIREMENT	LUMEN COMPLIANT SOLUTION
✓	1. Identify hardware, firmware, and related software required	<ul style="list-style-type: none"> <li>As required, Lumen identifies hardware, firmware, and software that is needed to provide MNS services.</li> </ul>

LUMEN COMPLIES	SOW C.2.8.1.1.4.1 REQUIREMENT	LUMEN COMPLIANT SOLUTION
✓	2. Identify network components, protocols, and traffic factors – making recommendations	<ul style="list-style-type: none"> <li>In providing MNS design and engineering services, Lumen use our extensive experience and well-honed skills to recommend network capacities and performance levels as they apply. Lumen determines and identify traffic prioritization and filtering requirements, determining protocols and redundancy needed, and identifying network components.</li> </ul>
✓	3. Provide project management	<ul style="list-style-type: none"> <li>Lumen provides complete project management for our MNS design and engineering services. As applicable, we manage the design, configuration, implementation, installation, provisioning, testing, and activation of MNS equipment, software, and connectivity. To minimize the impact on the current networking environment, we coordinate installation and testing activities with the agency.</li> </ul>

**1.3.3.1.4.2 Implementation, Management and Maintenance [C.2.8.1.1.4.2]**

Lumen provide all necessary implementation, management and maintenance needed to deliver MNS meeting agency requirements.

**Implementation.** Lumen’s implementation services include full project management responsibility for installation of site networks to fulfill the requirements of an agency’s site design of all network structures and components. When implementing new connectivity, equipment, or software, the Lumen Team conducts a site survey, which includes an analysis of agency network, facilities, equipment, and software to be used or interfaced with as part of the MNS implementation. The result of the survey is a document detailing the existing protocols, architecture, traffic patterns, availability of space, network address management, naming conventions, fault resilience, power, ventilation, fire prevention, and other related factors. Details concerning physical and logical interfaces and the services provided for those by the Lumen Team are specified in this document. This document,

**Addressing Agency Needs**

Lumen provides agencies *customized reports* as required by agencies, allowing them to choose what performance or incident data they wish to see. The reporting data can include (but is not limited to):

- Outage durations
- Number of incidents
- Response times
- End to end performance
- Quality of Service statistics
- Traffic loads and relative capacity indicators
- Port utilization
- Packet errors

---

along with all customer deliverable documents, undergoes a review by an internal QA team prior to being presented to the agency. Post-implementation quality assurance processes ensure design integrity.

**Management.** This service can be performed either at Lumen's GovNOCs or at an agency-specified NOC at an agency facility. In the latter case, a separate site survey and analysis is required at the designated NOC to ensure it supports all necessary activities. Our Network Management System (NMS) proactively monitors the agency environment for breaks in service resulting from equipment failure, misconfigured equipment, and policy violations. The NMS covers all premises equipment at both ends of the wide area network as well as all customer equipment attached to the network that complies with the SNMP protocol (IETF RFC1157 and related). Based on the defined performance metrics, we deploy appropriate tools to measure relevant indicators such as latency, packet loss, jitter, utilization, and availability. Lumen provides agency-specific NOCs to manage the agency network 24/7 and provide integrated management of services provided by Lumen and other contractors.

**Maintenance.** Lumen technicians provide Agencies maintenance support as required by the RFP. Maintenance activities include hardware repair and maintenance, software maintenance, cable replacement, ongoing configuration changes, and the physical moves/adds/changes of equipment. Our MNS maintenance also includes repair/replacement of Government Furnished Property (GFP) as applicable. To ensure timely updates, agency users can subscribe to email notifications on maintenance activities and trouble tickets. Lumen supports two types of network maintenance activities: Scheduled and Unscheduled:

- **Scheduled Maintenance.** Scheduled maintenance includes any foreseen/predictable need to make a change to the network, including upgrades and augments. If the scheduled maintenance activity is expected to produce any service interruption, advanced notification via email is provided to Agencies. Lumen makes every effort to schedule all scheduled maintenance during off-peak hours (between midnight and 6:00 am in local time zones). All scheduled

maintenance is planned with a back-out contingency plan, as needed, prior to scheduling.

- Unscheduled Maintenance.** Unscheduled maintenance is defined as an unplanned and immediate need to make changes to the network. Such an environment demands prompt action to restore a high-risk condition or failure status to normal operating status. The need for unscheduled maintenance is directly related to an outage, potential outage, or degradation of service. Agency stakeholders are notified via e-mail of any emergency network impairment repair activities as soon as the network defect is determined.

Figure 1.3.3.1.4.2-1 provides specific details pertaining to each of the 13 MNS Implementation, Management and Maintenance SOW requirements elements, showing how the Lumen MNS fully complies with SOW implementation, management and maintenance requirements.

**Figure 1.3.3.1.4.2-1. MNS Implementation, Management and Maintenance Technical Capabilities**

LUMEN COMPLIES	SOW C.2.8.1.1.4.2 REQUIREMENT	LUMEN COMPLIANT SOLUTION
✓	1. Develop, implement, and manage comprehensive solutions	<ul style="list-style-type: none"> <li>Lumen develops, implement, and manage comprehensive solutions using components of EIS services. This includes providing : ♦ Transport solutions that provide high reliability, redundancy and diversity; ♦ Access solutions to ensure connectivity at required performance levels; ♦ Customer premise solutions with required equipment hardware, software, and interface; and ♦ agency-specific security considerations and solutions including email content filtering, virus/worm/Trojan detection and prevention, intrusion detection and prevention, and internal/external access rights.</li> </ul>
ü	2. Supply and manage hardware, firmware, and related software	<ul style="list-style-type: none"> <li>The Lumen Team manages covered hardware and software as identified by the agency. The agency is required to maintain a current manufacturer maintenance contract (e.g., Cisco SMARTnet) to ensure Lumen MNS has access to software patches, updates and hardware replacements (RMA) for failed hardware.</li> </ul>
✓	3. Provide Tools	<ul style="list-style-type: none"> <li>The Monitoring Service requires installation of the Lumen MNS Data Collection Appliance (DCA) on the Client network. Each DCA contains a complete copy of Lumen MNS monitoring tools, including the core monitoring framework software, a local collection database, and over 140 different probes. The DCA is installed on the Client premises on a single subnet configured with Secure Socket Layer (SSL) tunnel to the</li> </ul>

LUMEN COMPLIES	SOW C.2.8.1.1.4.2 REQUIREMENT	LUMEN COMPLIANT SOLUTION
		<p>Lumen MNS Monitoring Framework. It is recommended that the DCA be installed within the Client data center at the network core. The DCA provides the complete hardware, software, and a suite of management applications required for service delivery.</p> <p>Additional Lumen MNS appliances may be required, depending on the services the Client purchased and the number, type, and location of monitored devices and systems.</p>
✓	4. Manage network in real-time on a 24/7 basis	<ul style="list-style-type: none"> <li>The Lumen Team manages the applicable agency network/s in real-time, on a 24/7 basis. We monitor utilization and packet loss and errors in intervals of 15 minutes or less to ensure proper operation and performance. We support remote network management, including monitoring, troubleshooting and fault/problem resolution, testing, maintenance, and equipment configuration, via the Lumen NOC.</li> </ul>
✓	5. Permit SNMP read-access data feeds	<ul style="list-style-type: none"> <li>The Lumen Team MNS solution supports Simple Network Management Protocol (SNMP) data feeds used to provide managed equipment information to the agency, as applicable. We also track and remain very cognizant and involved in the development of future/emerging protocols which may be subsequently incorporated into the managed environment.</li> </ul>
✓	6. Manage network configuration activities	<ul style="list-style-type: none"> <li>We perform and track all required configuration changes, as required by the SOW. There are two primary classes of changes – physical and logical. Logical changes fall into three classes – basic, moderate, and advanced. The GSA Customer Portal, available 24/7/365, allows Agencies, or Lumen Team members acting on behalf of Agencies, to submit basic and moderate logical changes. Advanced logical changes and physical changes use a MACD form and undergo a review process to make sure they do not negatively impact EIS performance.</li> </ul>
✓	7. Provide IP Address Management as applicable	<ul style="list-style-type: none"> <li>The Lumen Team provides IP Address Management as applicable. In doing this, we supply registered IP addresses as required, and also assist in translating non-registered private IP addresses into public addresses for routing purposes.</li> </ul>
ū	8. Monitor and control access to equipment	<ul style="list-style-type: none"> <li>We monitor and control access to equipment under our control. Our controls include implementing passwords and permissions and limiting access to authorized personnel, as directed and approved by the agency.</li> </ul>
✓	9. Perform off-site equipment configuration backups	<ul style="list-style-type: none"> <li>The Lumen Team performs regular backups of off-site equipment configurations to ensure the availability of configuration data as may be required for restoration. We provide secure access to backup logs to the agency.</li> </ul>
✓	10. Perform necessary upgrades, updates, patches and bug fixes	<ul style="list-style-type: none"> <li>The Lumen Team performs all necessary hardware and software updates, upgrades, patches, and bug fixes as soon as they are available. Lumen implements updates in coordination with, and upon approval by, the agency. Prior to implementation we test new releases to resolve any security concerns and ensure compatibility within the agency environment to maintain equipment functionality and minimize service disruptions.</li> </ul>
✓	11. Provide preventative	<ul style="list-style-type: none"> <li>The Lumen MNS addresses preventative and corrective maintenance through patch</li> </ul>

LUMEN COMPLIES	SOW C.2.8.1.1.4.2 REQUIREMENT	LUMEN COMPLIANT SOLUTION
	and corrective maintenance	<p>management. Patch application to remediate incidents and reduce known vulnerabilities is at the discretion of Lumen MNS. Patches are evaluated to ensure the current environment stability is maintained. Patches to remediate an incident or problem identified by Lumen MNS are handled as a Standard Change. Vulnerabilities are defined as a defect reported by a manufacturer that has a potential to affect the overall security of the device, and typically resolved with software workaround or a patch issued by the manufacturer. Client-requested patches for obtaining additional features or functions are out of scope and must be handled as a separate agreement.</p> <ul style="list-style-type: none"> <li>• As part of the Patch process, Lumen MNS:               <ul style="list-style-type: none"> <li>○ Reviews manufacturer field notices to determine impact and urgency to the Client system and existing software levels.</li> <li>○ Remotely applies updates to affected CIs following approved Change Management process.</li> </ul> </li> <li>• Lumen MNS provides a Change Management process for submitting and managing Standard, Planned, and Emergency Change Requests for patch activities. Approved changes are coordinated, planned, and monitored via the incident management system and the Service Delivery Centers. This allows coordination of activities to determine how to best schedule activities to minimize the potential for negative impact. The Engineer ensures relevant stakeholders, including the Client, are notified the change is complete and tested. When evaluation and notification are completed, the change is closed. If the Patch application requires an upgrade in revision level or impacts dependent technologies, the effort is evaluated and may be subject to a separate agreement. Covered equipment with software where the software maintenance has reached end of support is not covered by the Patch Management element.</li> </ul>
ü	12. Proactively detect problems, respond, and report	<ul style="list-style-type: none"> <li>• Using our 24/7 NOC resources, Lumen proactively detects performance problems and promptly respond to restore service performance to proper levels. We provide prompt notification to the impacted agency of alarms, network issues, and service interruption that adversely affect network performance. The notifications are provided by email, telephone, or otherwise, as directed by the agency.</li> </ul>
✓	13. Provide real-time access to schedule, performance information, security logs, and reporting/tracking	<ul style="list-style-type: none"> <li>• The Lumen MNS solution provides to the agency real-time access to: ♦ Network performance information and statistics, ♦ Installation schedule detailing the progress of activities, ♦ Trouble reporting and ticket tracking tools, ♦ Security logs.</li> </ul>
✓	14. Provide inventory tracking tool(s)	<ul style="list-style-type: none"> <li>• The Lumen Team provides an inventory tracking tool with our MNS solution that tracks all agency transport service, circuit, and equipment inventory information.</li> </ul>
✓	15. Provide secure access to current and	<ul style="list-style-type: none"> <li>• Lumen provides to the agency secure access to current and historical information to include but not be limited to what is prescribed in SOW C.2.8.1.1.4.2.15.</li> </ul>



LUMEN COMPLIES	SOW C.2.8.1.1.4.2 REQUIREMENT	LUMEN COMPLIANT SOLUTION
	historical information	

**1.3.3.1.5 Features [C.2.8.1.2]**

Lumen provides the following three features required by SOW C.2.8.1.2:

**1. GFP Maintenance.** Lumen maintains and repairs GFP and SRE.

**2. Agency Specific Network Operations**

**Center (NOC) and Security Operations**

**Center (SOC).** Lumen provides agency specific NOC, SOC, and Help Desk support, as required by applicable TOs.

**3. Network Testing.** Lumen develops Test plans for any changes to the agency’s network. These are structured in

collaboration with the agency and also address the agency’s potential need to test equipment, software, and applications on the Lumen network prior to purchase and deployment. Our test plans take into account the impact on Virtual Local Area Networks (VLAN), routing, traffic patterns, time of day, continuity of operations and disaster recovery issues; and include a restoration/rollback to the prior configuration if needed. After approval by our internal QA group, we collaborate with the customer agency and a schedule proposed for implementation. All proposed changes are tested in a production mockup network prior to introduction to the production environment.

**4. Traffic Aggregation Service (DHS Only).** Lumen establishes and maintains DHS EINSTEIN Enclaves where DHS-furnished equipment can be deployed. We provide network connectivity from the applicable DHS EINSTEIN Enclave to the required DHS data centers, routing all traffic in accordance with the National Policy requirements specified in SOW C.1.8.8. We satisfy all of the other

**Network Testing Support**

- We perform “proof of concept” testing, certification and training when deploying a new network or new architecture on behalf of an agency
- Supported networks include Optical, Ethernet, MPLS and IP, Voice; On-net WAN or Metro with off-net access

requirements of SOW C.2.8.1.2.4, and all applicable security standards and requirements, in keeping with the specifications of individual TOs.

#### **1.3.3.1.6 Interfaces [C.2.8.1.3]**

Lumen meets the interface requirements shown in SOW C.2.8.1.3, supporting all UNIs for all underlying EIS access and transport services.

#### **1.3.3.1.7 Performance Metrics [M.2.1.2, C.2.8.1.4, G.8]**

Lumen meets all of the MNS performance metrics specified in applicable TOs, as specified in SOW C.2.8.1.4. The Lumen GovNOC monitors all Lumen Enterprise services provided using our network.

#### **1.4 Optional EIS Services [L.29.2.1-3, M.4, C.1.2]**

The Lumen Team proposes all of the optional EIS services described in C.1.2. Details of the optional services Lumen provides are given in sections 1.4.1 through 1.4.12 of this Technical Volume, in the order the requirements for each service are provided in the SOW. As demonstrated in our response, Lumen has the network, personnel, processes, experience, and overall capabilities to provide cost-effective optional services that are fully compliant with EIS requirements.

#### **1.4.1 Data Services**

##### **1.4.1.1 Optical Wavelength Service [L.29.2.1, C.2.1.3]**

For a range of high volume, mission-critical applications, Agencies use Optical Wavelength Service (OWS) from Lumen to transparently connect locations across town, the nation, or the globe. OWS' wide range of speeds (1Gbps to 100 Gbps), protocol transparency, reliability, security, and dedicated nature allows Agencies to satisfy high bandwidth requirements across a range of applications including data center connectivity, storage, networking, imaging, back-up and recovery, and off-site data mirroring. *Indicative of Lumen's strength in*

##### **Optical Wavelengths Service**

- Provides an ultra-high bandwidth, scalable, flexible solution without the expense of owning and operating network infrastructure
- Extreme security and privacy
- Managed by agency or Lumen
- Proven: Lumen provides ~60 OC-192/10 Gbps waves today under Networkx

OWS, today we are providing approximately 60 OC-192 (10 Gbps level) wavelengths to Agencies under the Networx contract.

Figure 1.4.1.1-1 highlights features of the Lumen OWS solution aligned with the evaluation criteria.

**Figure 1.4.1.1-1. Features of Lumen’s OWS**

EVALUATION CRITERIA	FEATURES OF LUMEN OWS
Understanding [M2.1.1]	<ul style="list-style-type: none"> <li>Indicative of Lumen’s strength in OWS and understanding of the GSA environment, today we provide approximately 60 OC-192 (10 Gbps level) wavelengths under the Networx contract and are in alignment with EIS service requirements.</li> </ul>
Quality of Service [M.2.1.2]	<ul style="list-style-type: none"> <li>Satisfies all KPIs, and Lumen has a demonstrably strong track record of quality of service performance on OWS under Networx.</li> <li>Managed by experienced operations teams from redundant GovNOCs in Broomfield, CO and Atlanta.</li> <li>Scales up to 100 Gbps</li> <li>Lumen infrastructure provides high availability enabling us to meet time-to-restore requirements.</li> <li>Available protected and unprotected service options, and available custom routing</li> <li>Lumen’s extensive facilities based, owned and operated network can provide highly customized route designs with high availability to avoid overlapping routes.</li> <li>Available low-latency routes and latency guarantees</li> </ul>
Service Coverage [M.2.1.3]	<ul style="list-style-type: none"> <li>Lumen’s large global network features approximately 110,000 intercity, 64,000 metro, and 33,000 undersea fiber route miles</li> <li>Extent of service availability provides a high degree of confidence of the availability of intercity OWS between any required CBSA pair</li> <li>OWS availability extends to a number of international and OCONUS markets as well. Lumen’s underlying backbone OWS services are offered in over 40 countries globally</li> </ul>
Security [M.2.1.4]	<ul style="list-style-type: none"> <li>As a point-to-point, Layer 1 service, OWS enjoys certain inherent security features. agency circuit information is secured, and transport facilities are in secured locations, including deeply buried fiber.</li> <li>Lumen monitors status and performance parameters on more than 200,000 fiber miles globally</li> <li>Lumen and our subcontractors perform security operations in accordance with industry best practices and standards supporting Cyber, Personnel and Physical Security</li> </ul>

**1.4.1.1.1 Service and Functional Description [L.29.2.1, M.2.1, C.2.1.3.1]**

Lumen OWS is a bi-directional, point-to-point offering that enables Agencies to interconnect sites with dedicated wavelength-based channels. Lumen is a recognized leader in providing OWS to Government, commercial industry, and other carriers. This leadership is derived from our flexible underlying Wave Division Multiplexed (WDM)

---

technology, the scope of Level 3 network and fiber facilities plant, and our practiced support for OWS. By virtue of Lumen's end-to-end network deployment model, Agencies can deploy a seamless OWS spanning metro to national to global end points.

**Figure 1.4.1.1.1-1** shows an overview of the architecture of Lumen's OWS. OWS is managed from our Broomfield, CO and Atlanta GovNOCs. It is one of several services founded upon the Lumen Network Architecture presented in section 1.1 of this Technical Volume.

Some of the more notable features of Lumen's OWS offering include:

- A standards-based, 100% homogenous network design and architecture, allowing delivery of the highest quality OWS service
- Underlying advanced long-haul optronics that simplify our solution and allow for unparalleled flexibility to support Agencies' capacity requirements
- Reliability derived from a backbone network with fully diverse paths everywhere and no spurs or collapsed paths; many Lumen on-net buildings feature diverse fiber access
- Protected and unprotected solution options; available custom routing and transparent network design; and protected and unprotected solution options.
- The "future proof" Lumen network - with extra conduits in place on many routes and ownership of the necessary real estate to accommodate forthcoming generations of fiber and optical equipment, we offer a compelling migration path for future services

The attributes and conformance of Lumen OWS with all SOW requirements are discussed below.

#### **1.4.1.1.2 Standards [C.2.1.3.1.2]**

Lumen OWS over WDM complies with the standards specified in SOW C.2.1.3.1.2, as applicable for ITU and Telcordia. While not formally defined as Standards, Optical Internetworking Forum (OIF) Implementation Agreements (IA) are largely considered and followed as such. For OWS, although they are optional Lumen

follows the OIF IAs named in SOW C.2.1.3.1.2 (items 8 – 13). In addition, Lumen complies with all new versions, amendments, and modifications made to the supported documents and standards.

**1.4.1.1.3 Connectivity [C.2.1.3.1.3]**

OWS is delivered at the Service Delivery Point (SDP) via UNIs as specified in SOW C.2.1.3.3.

Point-to-point, bi-directional, duplex services are connected from the SDP to the OTN via a fiber pair.

The wavelengths ordered by the Agencies can connect to and interoperate with: 1) Lumen’s metro and long haul networks, 2) the agency’s Intranet, and 3) other agency networks, as expanded upon in **Figure 1.4.1.1.3-1**.

**Figure 1.4.1.1.3-1. Lumen’s OWS Connectivity and Interoperability**

LUMEN COMPLIES	SOW C.2.1.3.1.3 REQUIREMENT	LUMEN COMPLIANT SOLUTION
✓	1. Metro and Long Haul Networks	<ul style="list-style-type: none"> <li>Services connected from the SDP to Lumen’s OTN via fiber pairs.</li> <li>More than 35,000 on-net buildings in North America make it more likely that agencies can easily and cost-effectively connect and interoperate with Lumen’s OTN.</li> </ul>
✓	2. Agency’s Intranet	<ul style="list-style-type: none"> <li>Agencies’ intranets can be interconnected within metro markets, across cities or internationally. Few other suppliers can match the comprehensiveness of Lumen’s scope on OWS.</li> </ul>
✓	3. Other Agency Networks	<ul style="list-style-type: none"> <li>As OWS is a point-to-point service operating at Layer 1, with agencies in agreement, Lumen OWS can interconnect them between two points on Lumen’s OTN.</li> <li>If such connectivity should be subject to OMB Memorandum M-15-01, Lumen has the network infrastructure to route the OWS circuit through an EINSTEIN Enclave.</li> </ul>

**1.4.1.1.4 Technical Capabilities [C.2.1.3.1.4]**

Lumen is not only in full compliance with the mandatory technical capabilities requirements for OWS, *but also the optional ones*. All are addressed in **Figure 1.4.1.1.4-1**.

**Figure 1.4.1.1.4-1. Lumen’s OWS Technical Capabilities**

LUMEN COMPLIES	SOW C.2.1.3.1.4 REQUIREMENT	LUMEN COMPLIANT SOLUTION
<b>Connection Types</b>		
✓	1. Non-domestic Wavelengths (Optional)	<ul style="list-style-type: none"> <li>OWS available on a non-domestic basis via Lumen’s network which extends to 60 countries. It includes almost 10,000 route miles in foreign metropolitan markets and ~33,000 route miles of subsea optical cable systems. Coverage can be supplemented by qualified foreign carriers as needed.</li> </ul>
✓	2. Domestic Wavelengths	<ul style="list-style-type: none"> <li>In N. America alone, the Lumen network is comprised of some 74,000 intercity and 55,000 metropolitan route miles with presence in more than 200 North American markets. Therefore, we can easily provide OWS on an intercity basis within CONUS – certainly between two agency sites in different states - and some OCONUS domestic locations, for example, Lumen has a strong presence in Hawaii. Availability in U.S. territories is determined at the TO level.</li> </ul>
✓	3. Metro Wavelength Services	<ul style="list-style-type: none"> <li>Lumen provides OWS within metro markets, including between agency sites in the same city.</li> <li>Metro level OWS is offered over metropolitan fiber networks in ~350 markets worldwide containing approximately 64,000 route miles: 55,000 in North America, 3,200 in Europe, and 6,200 in Latin America.</li> </ul>
<b>Capabilities</b>		
✓	1. Transmission Rates (including Optional rates)	<ul style="list-style-type: none"> <li>OWS speeds supported include mandatory wavelengths at 1, 2.5, and 10 Gbps, plus optional wavelengths at 40 and 100 Gbps. Lumen maintains a proactive focus on technological evolution and is positioned to support optional transmission rates beyond 100 Gbps when these higher rates are commercially realizable. The predominant fiber types used for Lumen’s intercity and metro segments, respectively Corning LEAF and Corning SMF-28 family, are extremely well-suited for very high speed transport.</li> </ul>
✓	2. Clock Transparency	<ul style="list-style-type: none"> <li>Asynchronous transport and Synchronous Status Messaging (SSM) supported</li> </ul>
✓	3. Protocol Transparency - Metro	<ul style="list-style-type: none"> <li>Metro networks support wavelengths that are rate and protocol independent.</li> </ul>
✓	4. Protocol Transparency – Domestic and Non-Domestic (Optional)	<ul style="list-style-type: none"> <li>Rate and protocol independent wavelengths are supported in Domestic and Non-Domestic locations. Exact Domestic and Non-Domestic coverage will be determined at the TO level.</li> </ul>
✓+	5. Byte Transparency	<ul style="list-style-type: none"> <li>For metro, domestic and non-domestic locations, Lumen provides byte transparency at all supported wavelengths - 1 Gbps to 100 Gbps - exceeding the SOW’s requirements for bandwidths. Per the SOW, the A1 and A2 bytes, and B0 and J1 are exempted.</li> </ul>
✓	6. Concatenation	<ul style="list-style-type: none"> <li>Standard and virtual concatenation is supported for framed wavelengths.</li> </ul>
✓	7. (Optional) Channelization	<ul style="list-style-type: none"> <li>Channelized UNIs are supported for framed wavelengths.</li> </ul>
ü	8. Wavelength Delivery	<ul style="list-style-type: none"> <li>Lumen delivers two fibers over two ports for bi-directional wavelengths with terminations based on the agency’s needs.</li> </ul>

LUMEN COMPLIES	SOW C.2.1.3.1.4 REQUIREMENT	LUMEN COMPLIANT SOLUTION
✓	9. Access Methods	<ul style="list-style-type: none"> <li>In accordance with items a, b, and c, a variety of access methods for an end-to-end OWS are available. General Access arrangements are discussed in section 1.4.9 of this Technical Volume.</li> </ul>
✓	10. GFP/SRE	<ul style="list-style-type: none"> <li>Multi-vendor interoperability supporting UNIs for cases a, b and c are available.</li> </ul>
✓	11. Efficient Transport	<ul style="list-style-type: none"> <li>Maximizing ROI, a single wavelength can carry multiple disparate protocols</li> </ul>

1.4.1.1.5 Features [C.2.1.3.2]

Figure 1.4.1.1.5-1 presents the features of Lumen OWS and notes Lumen’s full compliance with all mandatory *and all optional* requirements of SOW C.2.1.3.2.

Figure 1.4.1.1.5-1. Features of Lumen’s OWS

LUMEN COMPLIES	SOW C.2.1.3.2 REQUIREMENT	LUMEN COMPLIANT SOLUTION
✓	1. Customer Network Management (CNM) – Level 1 (Optional)	<ul style="list-style-type: none"> <li>Provisioned through the GSA Customer Portal</li> </ul>
✓	2. Customer Network Management (CNM) – Level 2 (Optional)	<ul style="list-style-type: none"> <li>Provisioned through the GSA Customer Portal</li> </ul>
✓	3. Equipment Protection 1:1 – GFE/SRE	<ul style="list-style-type: none"> <li>Described in note on equipment protection below</li> </ul>
✓	4. Equipment Protection 1+1 – Network Side	<ul style="list-style-type: none"> <li>Described in note on equipment protection below</li> </ul>
✓	5. Equipment Protection – Network Side	<ul style="list-style-type: none"> <li>Described in note on equipment protection below</li> </ul>
✓	6. Geographical Diversity Wavelengths	<ul style="list-style-type: none"> <li>A multitude of diversity options are available to Agencies, including route, location, path and equipment diversity. Lumen’s System Architecture Team (SAT) and Systems Engineering (SE) groups are available to custom-design diversity to address unique requirements defined at the TO level.</li> </ul>
✓	7. Protected Non-Domestic and OCONUS Wavelength (Optional)	<ul style="list-style-type: none"> <li>Lumen architects work the agency to deliver the protection required, utilizing BPSR or equivalent protection switching over submarine transmission networks in less than 4 seconds per single failure.</li> <li>Unprotected point-to-point wavelengths also are available if the agency needs it. This reduces costs of operation in cases where protected wavelengths are not necessary or where redundancy is (for example) provided via a second non-protected route.</li> </ul>
ü	8. Protected CONUS Wavelength (Optional)	<ul style="list-style-type: none"> <li>For protected wavelengths up to 2,500 kilometers within CONUS, protection switching is less than 300 ms for a single failure</li> </ul>
✓	9. Protected Metro Wavelength	<ul style="list-style-type: none"> <li>Unidirectional Path Switched Ring (UPSR) protection is used. Restoration times for protected wavelengths in the metro area is less than 60 ms for a single failure</li> </ul>

**Note on Equipment Protection.** When required, Lumen provides protected and diverse OWS. Lumen's network design provides 1:1 and 1+1 protection to meet the needs of the Government on both the CPE (compatible GFE and SRE) and the network sides. Redundant transport equipment combined with a network that has been constructed to eliminate route overlaps yields a service that is fully redundant and diverse in metro areas and on intercity routes.

#### **1.4.1.1.6 Interfaces [C.2.1.3.3]**

Exceeding EIS requirements, Lumen complies with all mandatory *and all optional* OWS interface requirements specified in SOW C.2.1.3.3.

#### **1.4.1.1.7 Performance Metrics [M.2.1, C.2.1.3.4, G.8]**

##### **1.4.1.1.7.1 Framed Wavelength Performance**

Wavelengths based on SONET framing comply with performance requirements as stated in SOW C.2.1.5.1.4 (7) through (8).

##### **1.4.1.1.7.2 Transparent Wavelength Performance**

Fully transparent wavelengths are supported with equipment using G.709 wrapper-based technology. The G.709 standard defines how Performance Metrics (PM) are collected and circuit quality is monitored. It is similar to SONET but instead of using the PM fields in the SONET frame, it uses the ones in the wrapper frame. ES and SES are monitored for wrapper frames, with AQL monitored through these parameters.

##### **1.4.1.1.7.3 In-Service Monitoring**

Lumen supports In-Service Monitoring (ISM) and does not rely on performance observed and measured at higher layers of the network.

##### **1.4.1.1.7.4 Performance Levels**

Lumen complies with OWS Performance Levels and AQL of KPIs specified in SOW

#### **Lumen's Private Line Service**

- Mature, field-proven transport service with high reliability, security, and privacy
- Wide geographical coverage (metro, inter-city, and international), on Lumen -owned fiber
- Built on SONET/SDH and leverages this technology's inherent self-healing properties
- Customized diversity options to address unique agency availability requirements
- Proven experience: Lumen provides almost 200 PLS circuits under the Networx and WITS contracts today



C.2.1.3.4. We also note that all KPIs named, Availability, Time to Restore, and Grade of Service, are measured in accordance with the SOW C.2.1.3.4 notes 1 through 3 respectively.

**1.4.1.2 Private Line Service [L.29.2.1, C.2.1.4; C.4.4]**

Lumen’s Private Line Service (PLS) offers Agencies a highly reliable, dedicated, secure, and scalable network service for transport of their mission-critical data, voice, and video. Lumen is a highly experienced provider of PLS, offering this service since its first days of operation almost 20 years ago. Lumen has been offering PLS on the Network contract for years *and currently has some 200 PLS circuits in operation under the Network and WITS contracts.*

Figure 1.4.1.2-1 shows features of the Lumen PLS solution aligned with evaluation criteria.

**Figure 1.4.1.2-1. Features of Lumen PLS**

EVALUATION CRITERIA	FEATURES
Understanding [M2.1.1]	<ul style="list-style-type: none"> <li>Lumen is a highly experienced provider of PLS, having been offering this service since its first days of operation almost 20 years ago.</li> <li>Lumen provides PLS on the Network contract and we currently have some 200 PLS circuits in operation under the Network and WITS contracts - this reflects our understanding of the GSA/EIS environments as EIS requirements for PLS are virtually the same as under Network.</li> </ul>
Quality of Service [M2.1.2]	<ul style="list-style-type: none"> <li>Affording resilience and reliability Lumen's PLS offers fully protected point-to-point services built on SONET Self-Healing Rings (SHR).</li> <li>Also for resilience and reliability, the intercity PLS is supported with 4-fiber bi-directional line switched ring (BLSR) protection technology, the best available for long haul.</li> <li>Lumen PLS satisfies all KPIs, plus Lumen has a strong, track record of quality of service performance on PLS under Network and WITS</li> <li>Managed by experienced operations teams from redundant GovNOCs in Broomfield, CO and Atlanta</li> <li>Lumen PLS is in compliance with the Multipoint Connection and Special Routing (i.e., Transport Diversity and Transport Avoidance).</li> </ul>
Service Coverage [M2.1.3]	<ul style="list-style-type: none"> <li>Lumen PLS is available in all 929 CBSAs based on our extensive national presence and interconnection agreements with relevant local carriers to supplement our native coverage.</li> <li>International PLS is provided from Lumen’s global network with supplemental coverage provided through interconnections with approved foreign carriers.</li> </ul>
Security [M2.1.4]	<ul style="list-style-type: none"> <li>As a point-to-point, Layer 1 service, PLS enjoys certain inherent security features. agency circuit information is secured, and transport facilities are in secured locations, including deeply buried fiber.</li> <li>Based on the size and scope of our network, Lumen PLS supports the routing of applicable circuits/</li> </ul>

EVALUATION CRITERIA	FEATURES
	traffic through an EINSTEIN Enclave per OMB Memo.M-15-01. <ul style="list-style-type: none"> <li>• Lumen monitors status and performance parameters on more than 200,000 fiber miles globally</li> <li>• Lumen and our subcontractors perform security operations in accordance with industry best practices and standards supporting Cyber, Personnel and Physical Security</li> </ul>

**1.4.1.2.1 Service and Functional Description [L.29.2.1, M.2.1, C.2.1.4.1.1]**

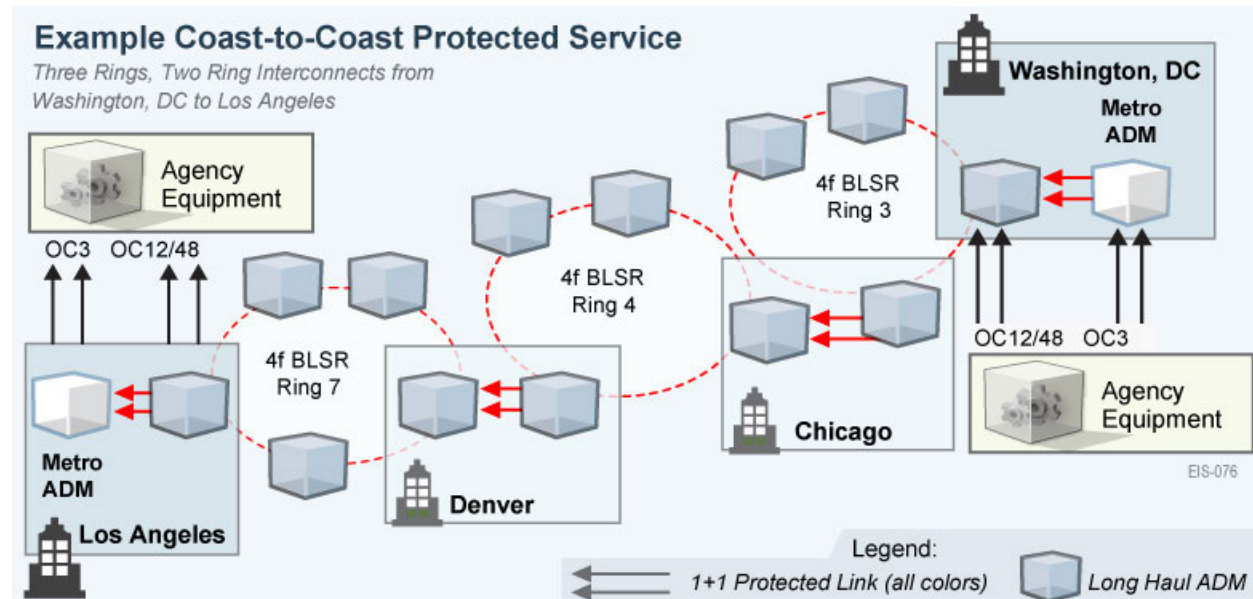
The scope of Lumen PLS includes metro, intercity and international circuits. Lumen's PLS offers fully protected point-to-point services built on SONET Self-Healing Rings (SHR). The intercity PLS is supported with 4-fiber bi-directional line switched ring (BLSR) protection technology, the best available for long haul. Metro PLS is supported with 1+1, 2 fiber-BLSR and Unidirectional Path Switched Ring (UPSR) protection, depending upon agency requirements and the number of nodes on the ring. Multiple Digital Cross Connect Systems (DCS) are used for aggregation and protection of low rate (OC-3 and below) signals. All Lumen private lines are full-duplex, with standards-compliant interfaces at each endpoint. Speeds from 64 Kbps to OC-768 (40 Gbps) are offered.

Although not part of this response, we note that Lumen offers Unprotected Private Lines (UPL) as an option for Agencies that wish to control their own networks at a finer level than supported by standard PLS. UPL provides OC-3, OC-12, OC-48 capacity on a specified route.

In Section 1.1 of this Technical Volume, we provided a description of the Lumen Network Architecture upon which PLS is supported.

**Figure 1.4.1.2.1-1** depicts a typical end-to-end PLS circuit, here a protected circuit across the U.S. PLS uses standard industry Add/Drop Multiplexers (ADM) and Wavelength Division Multiplexing (WDM) equipment, with the appropriate interfaces (e.g., DS1, DS-3, OC-3, OC-12, OC-48, and OC-768). In most cases metro area fiber loops are employed to reach an agency site. Lumen deploys a metro ADM at the agency site with the appropriate interface card(s) to support the service(s). The metro ADM is connected to the long-haul ADM, if it is an intercity circuit, or to another metro

ADM if it is a metro area circuit. The end-to-end circuit is highly reliable, as it is deployed over SONET infrastructure with inherent self-healing mechanisms and switchover times within rings of less than 50 ms.



**Figure 1.4.1.2.1-1. Example of a Coast-to-Coast, Protected Service.**

*The bidirectional SONET ring structure provides high service availability.*

The attributes and conformance of Lumen PLS with all SOW requirements are discussed below.

#### **1.4.1.2.2 Standards [C.2.1.4.1.2]**

As applicable, Lumen PLS complies with all of the ANSI, Telcordia, and ITU standards noted in SOW C.2.1.4.1.2. Additionally, Lumen complies with new versions, amendments, and modifications to the documents and standards of this SOW when offered commercially and as applicable.

#### **1.4.1.2.3 Connectivity [C.2.1.4.1.3]**

As is routinely done today on the roughly 200 PLS circuits delivered under Networkx and WITS, Lumen PLS connects to and interoperates with Government-specified terminations and does so with all other networks including those of other EIS contractors where additional coordination between networks is required for interoperability.

**1.4.1.2.4 Technical Capabilities [C.2.1.4.1.4]**

Lumen private lines are fully compliant with all of the requisite technical capabilities and categories. Perhaps the most challenging requirement, meeting the routing requirements of OMB Memorandum M-15-01 (named in SOW C.1.8.8) to pass applicable traffic through an EINSTEIN Enclave for inspection, can be readily managed by Lumen. To do so, Lumen draws upon the size and scope of its network to implement the connectivity needed to route the private line to and through the Enclave. For inspection, Lumen will only remove encryption that it has applied and not any agency-applied encryption.

Lumen private lines are transparent to any protocol used by Government Furnished Property (GFP), and data is handled transparently for all bit sequences transmitted by GFP through the SDP.

Lumen supports all of the PLS categories (i.e., data rates) – including *the optional sub-T1 items, lines 13, 14 and 15* - outlined in SOW C.2.1.4.1.4 and summarized in **Figure 1.4.1.2.4-1**.

We note that while PLS essentially is defined on a TDM/SONET (or SDH) basis, Lumen is seeing demand for circuits having PLS characteristics, but whose interfaces are defined on an Ethernet basis. These may be considered a dedicated Ethernet private line. *Lumen is well-suited to provide such circuits and currently provides more than 10 of them under Networx at speeds up to 1 Gbps.*

**Figure 1.4.1.2.4-1. Lumen Compliance with PLS Categories**

LUMEN COMPLIES	SOW C.2.1.4.1.4 REQUIREMENT	LUMEN COMPLIANT SOLUTION
✓	1. DS0	• 56 Kbps to 64 Kbps
✓	2. T1	• 1.544 Mbps, channelized and un-channelized
✓	3. T3	• 44.736 Mbps, channelized and un-channelized
✓	4. E1	• 2.048 Mbps, channelized and un-channelized
✓	5. E3	• 34.368 Mbps, channelized and un-channelized
✓	6. (Optional) SONET OC-1	• Can support 49.536 Mbps information payload, and 51.840 Mbps line rate on a TO basis
✓	7. (Optional) SONET OC-1 Virtual Tributary (VT)	• Can support 51.840 Mbps line rate, seven VT groups over a single SONET OC-1 interface on a TO basis

LUMEN COMPLIES	SOW C.2.1.4.1.4 REQUIREMENT	LUMEN COMPLIANT SOLUTION
✓	8. SONET OC-3	• 155.520 Mbps line rate, channelized OC3 or un-channelized OC-3c
✓	9. OC-12	• 622.080 Mbps line rate, channelized OC-12 or un-channelized OC-12c
✓	10. OC-48	• 2.488 Gbps line rate, channelized OC-12 or un-channelized OC-12c
✓	11. SONET OC-192	• 10 Gbps line rate, channelized OC-192 or un-channelized OC-192c
✓	12. SONET OC-768	• 40 Gbps line rate, channelized OC-768 or un-channelized OC-768c
✓	13. (Optional) Subrate DS0	• <i>Information payload data rates of 4.8, 9.6, and 19.2 Kbps</i>
✓	14. (Optional) Analog Line	• <i>4 kHz bandwidth</i>
✓	15. (Optional) Fractional T1	• <i>Two, four, six, eight, or twelve adjacent DS0 clear channels over an interface of T1 with a line rate of 1.544 Mbps</i>
✓	16. (Optional) Fractional T3	• <i>Two adjacent T1 clear channels over an interface of T3 with a line rate of 44.736 Mbps.</i>

**1.4.1.2.5 Features [C.2.1.4.2]**

Lumen PLS is in compliance with the two-feature requirements, Multipoint Connection and Special Routing (i.e., Transport Diversity and Transport Avoidance), detailed in SOW C.2.1.4.2. These PLS features are currently provided by Lumen under the Networx contract and are discussed in the following sections.

**1.4.1.2.5.1 Multipoint Connection**

Lumen PLS can interconnect three or more subscribers’ premises in both Branch-Off and Drop-and-Insert Modes. In the former, all SDPs are treated as one shared medium and each point can autonomously send and receive data. The CPE application ensures master/slave mode of operation. In Drop-and-Insert mode, previously specified channels of a channelized T1, T3, SONET OC-3 or OC-12 service category can be dropped off, and new channels can be simultaneously picked up or inserted.

**1.4.1.2.5.2 Special Routing**

Lumen’s specialized and highly experienced Customer Network Planning (CNP) team designs diverse transport paths and special routing such as transport avoidance. (Transport Diversity and Avoidance and discussed below.) Such special routing features are common in many Lumen-provided commercial and Government networks. The CNP team makes use of Lumen’s geocoded network mapping tool that shows all fiber paths

---

throughout the Lumen network with GPS-enabled accuracy. This tool enables them to observe the level of diversity achievable for any given set of circuits. If available, other service providers' geographic network data is also displayed.

Supporting **Transport Diversity**, Lumen can supply two or more physically separated routes for PLS circuits between connecting POPs. These diverse routes do not share common telecommunications facilities or offices. Lumen notes that each pair of circuits that must be diverse from each other constitutes a relationship pair. Lumen maintains a minimum separation of 30 feet throughout all diverse routes.

If diversity is not available or the compromised diversity is not acceptable to the Government, Lumen and the Government will negotiate an arrangement on an individual case basis.

To ensure **Transport Avoidance**, Agencies can order circuits along any of the paths available on the Lumen network, bypassing any area or route they intend to avoid. Lumen's provisioning system assigns a "Do-Not-Change-Route" flag to the selected route which controls route modifications.

Should it prove that either Transport Diversity or Transport Avoidance is not available, Lumen can exert best efforts to propose an acceptable arrangement along with documentation describing the basis for the compromise.

Lumen provides, within 30 calendar days of the implementation of transport diversity or avoidance, and again thereafter whenever a change is made, a graphical representation of transport circuit routes to show where diversity or avoidance has been implemented. Lumen provides, at least 30 calendar days in advance of implementation, written notification to the agency (with a copy to the PMO) requesting Government approval of any proposed reconfiguration of routes that were previously configured for transport diversity or avoidance.

#### **1.4.1.2.6 Interfaces [C.2.1.4.3]**

Lumen complies with all mandatory PLS interface requirements specified in SOW C.2.1.4.3. In addition, Lumen is prepared to comply with the four optional UNIs (9, 10,

19 and 20). Support for UNIs 9 and 10 (OC-1 and STS-1) will require finding satisfactory industry support for these interfaces.

#### **1.4.1.2.7 Performance Metrics and Quality of Service [M.2.1, C.2.1.4.4, G.8]**

Lumen complies with PLS Performance Levels and AQL of KPIs specified in SOW C.2.1.4.4. We also note that all KPIs named, POP-to-POP and SDP-to-SDP Availability, and Time to Restore, are measured in accordance with the SOW C.2.1.4.4 notes 1 and 2 respectively.

#### **1.4.1.3 Synchronous Optical Network Services [L.29.2.1, C.2.1.5; C.4.4]**

Agencies benefit from Lumen's proven leadership in Synchronous Optical Network Services (SONETS), a reliable, secure and high bandwidth service with the inherent built-in protection afforded by a self-healing architecture. Wide geographic coverage on Lumen's owned infrastructure and SONET/SDH interoperability enables Agencies to interconnect their networks across town, CONUS, or around the globe.

##### **Synchronous Optical Network Services (SONETS) Highlights**

- Mature, field-proven transport service
- Inherent reliability with 50 millisecond self-healing and restoration around failures
- High security and privacy
- Wide geographical coverage (metro, inter-city, and international) on owned fiber
- SONET-SDH Gateway enables interconnection of agency SONET rings in the U.S. with SDH rings internationally

SONETS continues to set reliability/availability standards for transport services. As a result, many transport services rely on SONETS for underlying connectivity.

Using Lumen SONETS, Agencies can build optical transport networks that are high bandwidth, with a high level of reliability and traffic isolation. SONETS provides proactive performance monitoring and enables self-healing functions with robust network management.

SONET is a mature, proven technology and Lumen has been offering SONETS to Agencies on the Networx contract for years. *We currently provide considerable SONETS connectivity at the OC-3 level under Networx and WITS.*

**Figure 1.4.1.3-1** highlights features of the Lumen SONETS solution aligned with the evaluation criteria.

**Figure 1.4.1.3-1. Feature Summary of Lumen SONETS**

EVALUATION CRITERIA	FEATURES OF LUMEN SONETS
Understanding [M.2.1.1]	<ul style="list-style-type: none"> <li>• Having been offering this service since our first days of operation almost 20 years ago, Lumen is a highly experienced provider of SONETS and it remains a core service of ours.</li> <li>• Lumen provides SONETS on the Networkx contract and currently we are providing a considerable level of SONETS connectivity at the OC-3 (155 Mbps) level under the Networkx and WITS contracts - this reflects our understanding of the GSA/EIS environments as EIS requirements for SONETS are virtually the same as under Networkx.</li> <li>• Lumen is a leading wholesale provider to other carriers who rely upon our SONETS.</li> </ul>
Quality of Service [M.2.1.2]	<ul style="list-style-type: none"> <li>• Lumen SONETS' native self-healing ring architecture – featuring a standard recovery time of less than 50 milliseconds - inherently provides resilience and reliability.</li> <li>• Also for resilience and reliability, on intercity routes, an add/drop multiplexer (ADM) network employs four-fiber BLSR self-healing rings.</li> <li>• The Lumen infrastructure provides overall high availability that supports our ability to meet specified time-to-restore requirements.</li> <li>• Lumen SONETS satisfies all KPIs, plus Lumen has a strong, track record of quality of service performance on SONETS under Networkx and WITS.</li> <li>• Managed by experienced operations teams from redundant GovNOCs in Broomfield, CO and Atlanta.</li> </ul>
Service Coverage [M.2.1.3]	<ul style="list-style-type: none"> <li>• Lumen's extensive network in the U.S. has PLS-relevant POPs in hundreds of locations. Therefore, from these locations and through interconnection agreements with relevant local carriers to supplement our own coverage, Lumen provides PLS in all 929 CBSAs.</li> <li>• As the Lumen network extends to 60 countries, and we have interconnections with local carriers around the world, Lumen provides PLS from nearly all non U.S. locations.</li> </ul>
Security [M.2.1.4]	<ul style="list-style-type: none"> <li>• As essentially a point-to-point, Layer 1 service, SONETS enjoys certain inherent security features. agency circuit information is secured, and transport facilities are in secured locations, including deeply buried fiber.</li> <li>• Lumen monitors status and performance parameters on more than 200,000 fiber miles globally</li> <li>• Lumen and our subcontractors perform security operations in accordance with industry best practices and standards supporting Cyber, Personnel and Physical Security</li> </ul>

**1.4.1.3.1 Services and Functional Description [L.29.2.1, M.2.1, C.2.1.5.1.1]**

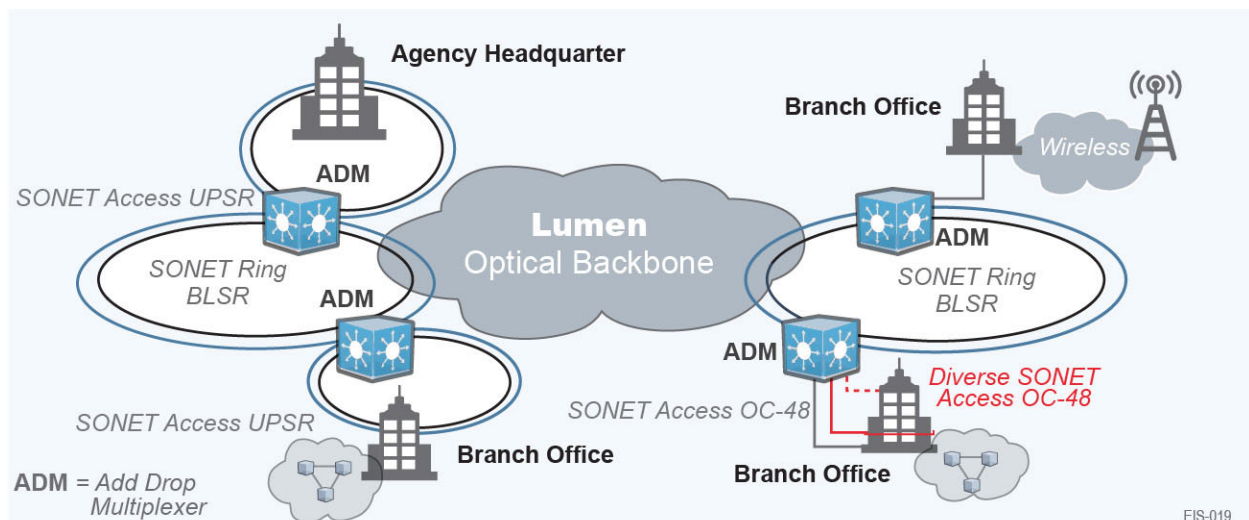
SONETS is a core service of Lumen and we are a leading wholesale provider of it to other carriers. As a consequence, it is extremely well understood and supported by us. Lumen offers the full range of transmission rates for SONET (and SDH).

A point of distinction of Lumen SONET is its wide availability in the U.S. – including coverage in Hawaii – and around the world. In Section 1.1 of this Technical Volume, we provided a thorough description of the Lumen Network Architecture. One of



the fundamental technologies of this Architecture is SONET, upon which the Service, SONETS is built. A high level view of Lumen's SONETS architecture is shown in **Figure 1.4.1.3.1-1**.

Lumen SONETS is delivered using standard industry Add and Drop Multiplexer (ADM) and Wavelength Division Multiplexing (WDM) equipment with the appropriate interfaces (e.g., OC-3, OC-12). For long-distance connections, a dedicated long-haul ADM network employs four-fiber Bi-directional Line-switched Ring (BLSR) self-healing rings around CONUS. The standard recovery time is less than 50 milliseconds, with no noticeable disruption in service. The physical length of the ring and the number of switching nodes determine the recovery time. Under normal operation data only travels the minimum distance to the destined traffic node. Lumen's intercity network protection is revertive, meaning that it switches back to the normal (shortest) path once the fault is isolated and repaired.



**Figure 1.4.1.3.1-1. SONETS Architecture Overview.** Agencies benefit from Lumen's proven leadership in SONETS, a reliable, secure and high bandwidth service with protection built-in from the ground up.

To reach the agency sites, metropolitan (metro) area fiber rings are employed. Lumen deploys a metro ADM at the agency site with the appropriate interface card(s) to support the service(s). The metro ADM is connected to the Lumen facility using 1+1

---

protection, Unidirectional Path Switched Ring (UPSR) protection, or two-fiber BLSR protection, as appropriate for the demand of the agency site. The metro ADM is connected to the long-haul ADM if it is a long-distance circuit or another metro ADM if it is a metro-area circuit. After equipment installation, the circuit is provisioned according to the Government order (e.g., as an OC-12 or OC-12c). The agency connection is either protected (four-fiber handoff) or unprotected (two-fiber handoff) according to the agency order.

The interfaces are supported through the commercially available interface cards installed in the ADMs at the agency site. The circuits are then provisioned according to the Government order (e.g., as an OC-12 or an OC-12c). International connectivity is provided through the use of SONET to SDH gateways.

The attributes and conformance of Lumen SONETS with all SOW requirements are discussed in the following sections.

#### **1.4.1.3.2 Standards [C.2.1.5.1.2]**

SONETS is a mature service and Lumen SONETS complies with all of the mandatory Telcordia, ANSI, ITU-T, IEEE, and OIF standards noted in SOW C.2.1.5.1.2 as well as many of the optional ones. In addition, Lumen complies with new versions, amendments, and modifications to the documents and standards of this SOW.

#### **1.4.1.3.3 Connectivity [C.2.1.5.1.3]**

As is routinely done today, Lumen SONETS connects to and interoperates with Government-specified terminations and does so with all other networks including other EIS contractors' networks, where additional coordination between networks is required for interoperability.

Note that if there should be a requirement for SONETS connectivity that is subject to OMB Memorandum M-15-01 (SOW C.1.8.8), Lumen can manage this drawing on the size and scope of our network. It will be executed by routing the SONETS connectivity to and through the EINSTEIN Enclave, where proxies facilitate traffic inspection in both directions.

**1.4.1.3.4 Technical Capabilities [C.2.1.5.1.4]**

Lumen SONETS is fully compliant with all of the requisite technical capabilities outlined in SOW C.2.1.5.1.4 as summarized in **Figure 1.4.1.3.4-1**. The figure applies *special notation to the many optional technical capabilities also routinely supported by Lumen as well as those which can be accommodated at the TO level.*

**Figure 1.4.1.3.4-1. Lumen Compliance with SONETS Technical Capabilities**

LUMEN COMPLIES	SOW C.2.1.5.1.4 REQUIREMENT	LUMEN COMPLIANT SOLUTION
✓	1. Geographic Coverage	<ul style="list-style-type: none"> <li>Lumen’s global network includes numerous metro markets, with a significant amount in CONUS. Lumen satisfies all mandatory and optional coverage requirements. Lumen is one of an elite group of carriers whose network scope is so broad as to completely satisfy all of the SOW’s mandatory and optional geographic coverage requirements.</li> </ul>
✓	2. Gateway Functionality (Optional)	<ul style="list-style-type: none"> <li>Supports SONET-to-SDH and SDH-to-SONET conversions. With a network presence in 65 countries on 6 continents, Lumen is very experienced with such gateway functionality.</li> </ul>
✓	3. Network Topologies	<ul style="list-style-type: none"> <li>Supports linear, ring, and meshed topologies.</li> </ul>
✓	4. Protection Methods	<ul style="list-style-type: none"> <li>Supports all a) Tributary Side (i-iii), and b) Network Side (i-vi) protection methods as defined. We note that the commercial viability of Network Side (ii) Mesh Protection remains marginal.</li> </ul>
✓	5. Transmux Capability	<ul style="list-style-type: none"> <li>Supports all mandatory Transmuxing requirements, items b –d, and optional items a and e.</li> </ul>
✓	6. Concatenation Methods (Optional)	<ul style="list-style-type: none"> <li>Supports a) Standard Concatenation mandatory items i and ii, and optional items iii and iv at the TO level.</li> <li>Supports b) Virtual Concatenation items i-v at the TO level.</li> <li>Supports c) i. High order concatenation and ii. Low order concatenation.</li> </ul>
✓	7. Performance Monitoring	<ul style="list-style-type: none"> <li>Complies with Performance Monitoring parameters specified by GR-253 and the requirements for monitoring, recording, and storing the performance parameters.</li> <li>Parameters a) Error Seconds (ES) and b) Severe Error Seconds (SES) are monitored and measured (per AQL) as specified and performance requirements for all EIS users are met.</li> </ul>
✓	8. Synchronization and Timing Methods	<ul style="list-style-type: none"> <li>Supports a) External Timing and b) Internal Timing.</li> </ul>
	9. Reserved	
✓	10. Next Generation SONET (Optional)	<ul style="list-style-type: none"> <li>Can be supported at the TO level.</li> </ul>
✓	11. Framing and Concatenation	<ul style="list-style-type: none"> <li>Support for all i) Generic Framing Procedures (1 and 2), ii,) Link Adjustment Capacity Scheme for Virtual Concatenation (ANSI T1.105 and G.797), iii) (optional) Virtual Concatenation.</li> </ul>
✓	12. Data Communications	<ul style="list-style-type: none"> <li>Can be supported at the TO level.</li> </ul>

LUMEN COMPLIES	SOW C.2.1.5.1.4 REQUIREMENT	LUMEN COMPLIANT SOLUTION
	Channel (Optional)	
✓	13. Integrated Control Plane (Optional)	<ul style="list-style-type: none"> <li>Can be supported at the TO level.</li> </ul>

**1.4.1.3.5 Features [C.2.1.5.2]**

Delivered under Network today, Lumen SONETS is a proven, feature-rich SONET solution. As such, it supports the all of the mandatory as well as *many of the optional* SONETS Service Features specified in SOW C.2.1.5.2 as summarized in **Figure 1.4.1.3.5-1**. Lumen supports all mandatory SONETS Features and many of the optional ones.

**Figure 1.4.1.3.5-1. Lumen’s Support of SONETS Features per SOW C.2.1.5.2**

LUMEN COMPLIES	SOW C.2.1.5.2 REQUIREMENT	LUMEN COMPLIANT SOLUTION
✓	1.* Channelization	<ul style="list-style-type: none"> <li>Lumen supports SONET interfaces to the CPE to seamlessly interface with its SONET network for data transport. By virtue of its global network, Lumen supports the six channelized arrangements named in SOW C.2.1.5.2, Channelization Features (e.g., 1. STS-1 payload with VT1.5, VT2). They are standard features of the ADMs used by Lumen.</li> </ul>
✓	2.* DS1 Rate Synchronization Service	<ul style="list-style-type: none"> <li>Available under Network today, Lumen provides this feature so that agency Stratum 2 or Stratum 3 clocks at the agency location can synchronize to a Stratum 1 clock at a Lumen location. The DS1 to be used for synchronization is delivered using external timing.</li> </ul>
✓	3. SONET Performance	<ul style="list-style-type: none"> <li>As today under Network, all SONET services delivered by Lumen comply with the Performance Metrics included in SOW C.2.1.5.4 and the following performance indicators:               <ol style="list-style-type: none"> <li>Jitter, at all SDPs, as specified in GR-253 and measured as outlined in SOW C.2.1.5.2.</li> <li>Restoration Time, as specified by GR-253 for Automatic Protection Switching and by GR-1230, Section 6.1.1. Traffic is re-routing to restore the SONETS (over redundant path) before the failure is repaired. Lumen reconfigures affected services for Rings &lt; 1200 KM as:                   <ol style="list-style-type: none"> <li>For Routine Users, in less than 100 ms, when preemption of extra traffic is required</li> <li>For Critical Users, in less than 60 ms including detection time (10ms)</li> </ol> </li> </ol> <li>These restoration times are afforded by the SONETS (and SDH) standards-compliant ADM and DCS that must pass these specifications to be used by Lumen.</li> </li></ul>
✓	4. Equipment Protection – Network Side	<ul style="list-style-type: none"> <li>As it does under Network, Lumen SONETS provides protection to the client interfaces at the SDP, where the protection channel is bridged to the failed working channel. Three scenarios are shown below, all of which are supported by the ADM equipment.               <ol style="list-style-type: none"> <li>Equipment Protection 1:1 – CPE: Lumen provides protection to user-to-network interfaces at the</li> </ol> </li> </ul>

LUMEN COMPLIES	SOW C.2.1.5.2 REQUIREMENT	LUMEN COMPLIANT SOLUTION
		SDP, where the protection channel is bridged to the failed working channel 2. Equipment Protection 1+1 – CPE: Lumen provides protection to user-to-network interfaces at the SDP, where the protection channel is permanently bridged to the working channel 3. Equipment protection – Network side: Lumen provides two channels facing the network for full redundancy and equipment protection at the SDPs
ü	5. Framing for Electrical Interfaces	<ul style="list-style-type: none"> <li>Lumen supports all mandatory framing formats, as appropriate, for the particular electrical interface (e.g., DS-1, DS-3). following framing formats for electrical interfaces: 1. M-frame with C-parity. 2. Binary, 8 zero substitution line code. 3. ANSI Extended Superframe (ESF) (ANSI T1403, 1995).</li> </ul>
✓	6. Geographic Diverse Protection	<ul style="list-style-type: none"> <li>As is the case under Networkx, Lumen can ensure a minimum separation of 25 feet between the diverse circuits end-to-end and, if applicable, flag them to prevent disconnection during network grooming work, based on the A and Z locations identified in the Task Order.</li> <li>Additionally, Lumen supports two geographically diverse delivery channels from SDP1 to SDP2 based on the Task Order request and the location of SDP1 and SDP2. Physically diverse paths enable for immediate restoration on a protect path in the event that a fault occurs on the working path. This is as important for a network operations facility as it is for a POP or a protected-circuit route.</li> <li>The vast majority of Lumen fiber facilities have complete physical route and path diversity in the network. We have designed our networks with four-fiber BLSR and UPSR protection. This core SONETS technology protects against fiber cuts and port or equipment failures with a 50ms restoration capability. A service provider showing physical layer diversity on its network, but not using facilities to provide dedicated and diverse protection routes, run a working and protection path for managed transport services on the same physical path. This combination of working and protection paths in the same physical route is called a “collapsed ring”, which does not offer protection against fiber cuts.</li> </ul>
✓	7. Local and Remote Node Multiplexing	<ul style="list-style-type: none"> <li>Provided by Lumen under Networkx today, this feature is enable the multiplexing of different low-speed circuits onto a high-speed SONET signal.</li> </ul>
* Optional		

**1.4.1.3.6 Interfaces [M.2.1, C.2.1.5.3, G.8]**

For SONETS, a wide variety of UNIs are required (Per SOW C.2.1.5.3) at the SDP. Lumen SONETS is fully compliant with all mandatory and all optional SONETS interfaces, thereby exceeding EIS requirements.

**1.4.1.3.7 Performance Metrics [M.2.1, C.2.1.5.4, G.8]**

Lumen complies with all performance levels and Acceptable Quality Level (AQL) of Key Performance Indicators (KPI) for SONETS specified in SOW C.2.1.5.4. We also note that all KPIs named, Availability (SDP-to-SDP) and Time to Restore, are measured in accordance with the pertinent SOW C.2.1.5.4 notes.

**1.4.1.4 Dark Fiber Services [L.29.2.1, C.2.1.6, C.4.4]**

With Lumen Dark Fiber Services (DFS) Agencies to have total control and management over their end-to-end communication paths with minimal intervention from a telecommunications service provider. As a result, Agencies can manage and control scalability, security, network management, technology evolution at the service delivery points, while managing latency very tightly for their mission-critical applications. With its massive fiber infrastructure in the U.S. and abroad, Lumen is uniquely suited to provide DFS to Agencies under EIS. *Indeed, Lumen already is one of the largest providers of DFS to the Government, providing it more than [REDACTED] route miles in CONUS.*

**Figure 1.4.1.4-1** highlights the features of the Lumen DFS solution aligned with the evaluation criteria.

**Dark Fiber Services**

- Gives Agencies total control and management of ultra-high bandwidth applications
- Agency optronics can be located at agency site or collocated at Lumen POP(s)
- 130,000 dark fiber route-miles with more than 35,000 on-net buildings in North America
- Ultimate security and privacy
- Flexible configuration and diversity options
- Built-in scalability through spare fibers, multiple conduits, and demonstrated willingness of Lumen to build to new agency sites

**Figure 1.4.1.4-1. Features of Lumen DFS**

EVALUATION CRITERIA	FEATURES OF LUMEN DFS
Understanding [M.2.1.1]	<ul style="list-style-type: none"> <li>• Lumen has a massive fiber infrastructure in the U.S. and abroad and today is one of the largest providers of DFS to the Government, providing it more than [REDACTED] route miles in CONUS including “remote hands” support.</li> <li>• Based on our DFS experience to the Government itself and to high-end commercial customers, Lumen has an excellent understand of agencies’ DFS needs and expectations.</li> <li>• Lumen meets all EIS DFS requirements and, although not specified as a technical requirement, Lumen – as the owner of the underlying facilities - provides DFS to agencies under special, long term lease arrangements.</li> </ul>
Quality of Service [M.2.1.2]	<ul style="list-style-type: none"> <li>• DFS can be provided with diverse, alternate routes to improve resilience and reliability.</li> <li>• Our facilities were designed with ample space, power, environmental controls and security features to accommodate growth, evolution in service requirements and advances in technology.</li> <li>• To maintain service excellence, Lumen continues to invest in its online, geographical information system (GIS) and fiber management system (FMS). These systems enable faster delivery and implementation, flexibility in customer network designs, communication of scheduled and unscheduled maintenance events, and protection of the physical layer of the network.</li> <li>• Lumen DFS satisfies all KPIs, plus Lumen has a strong, track record of quality of service performance on other DFS contracts within the Government.</li> <li>• Although managed at a different level than most other services, DFS is yet managed by experienced operations teams from redundant GovNOCs in Broomfield, CO and Atlanta.</li> </ul>
Service Coverage [M.2.1.3]	<ul style="list-style-type: none"> <li>• Although DF availability varies with capacity availability, with fiber deployed in some 170 U.S. cities, Lumen is confident that at any given time, it can provide DF in [REDACTED] CBSAs named in SOW section J.1.4.1.</li> <li>• Lumen owns and operates one of largest facilities-based networks in the world and is regarded as having one of the largest reserves of DF in the U.S., [REDACTED] route miles of intercity and metro DF, respectively.</li> <li>• Lumen’s major backbone routes were built for scalability as multiple conduit duct banks were installed along these routes. This allows Lumen to pull additional fiber along the routes without having extensive excavation. This reduces cost and speed to completion. Lumen is also prepared to invest capital to build new routes where appropriate opportunities exist to service the EIS contract.</li> </ul>
Security [M.2.1.4]	<ul style="list-style-type: none"> <li>• As a point-to-point, Layer 1 service, DFS enjoys certain inherent security features. Agency circuit information is secured, and transport facilities are in secured locations, including deeply buried fiber.</li> <li>• Lumen monitors status and performance parameters on more than [REDACTED] fiber miles globally</li> <li>• Lumen and our subcontractors perform security operations in accordance with industry best practices and standards supporting Cyber, Personnel and Physical Security</li> </ul>

**1.4.1.4.1 Service and Functional Description [L.29.2.1, M.2.1, C.2.1.6.1.1]**

Lumen has constructed extensive metropolitan fiber optic networks in numerous cities throughout CONUS and OCONUS. With DFS, Lumen provides Agencies with

---

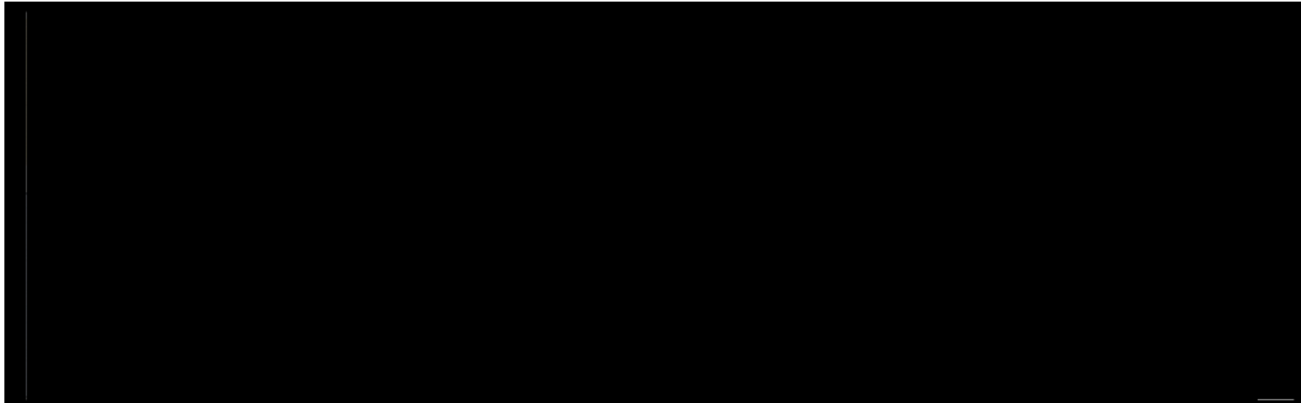
special, long term lease arrangements for the Dark Fiber (DF) on these networks. Our facilities were designed with ample space, power, environmental controls and security features to accommodate growth, evolution in service requirements and advances in technology. Reasons that Lumen is the premier provider of DFS include:

- **Experience:** Lumen has delivered [REDACTED] fiber route miles
- **Product Support:** DFS is a routine offering from Lumen to the Government with all of the systems and personnel in place from design through operations
- **Network:** Route diverse with multiple conduits available for expansion, plus Lumen is constantly expanding the network and adding new buildings on-net to satisfy customer-specific needs for DFS
- **Bury Depth and Right of Way (ROW):** The Lumen Network is buried at least 42” to the top of the conduit bank wherever possible. Lumen fiber is mostly along railroad, highway and pipeline ROW, which reduces fiber cuts, thereby increasing reliability
- **Running Line Site (i.e., Hut) Spacing:** Lumen’s nominal intercity route hut spacing of 100 km leads to fewer active elements subject to failure, thus increasing reliability
- **Facilities:** Lumen’s secure facilities are designed to accommodate growth for DFS customers’ equipment with ample space and power
- **Expansion:** Lumen is constantly expanding its network with new construction for customer-specific DFS requests and the addition of new buildings to the network

In addition, Lumen offers for remote field services and these technician services can be purchased to support “remote hands” requirements. In and EIS context, these would be under Managed Network Services, likely on an Individual Case Basis (ICB).

The high level overview of Lumen’s service architecture for DFS is shown in **Figure 1.4.1.4.1-1**. DFS is one of several services founded upon the Lumen Network Architecture presented in Section 1.1 of this Technical Volume.





**Figure 1.4.1.4.1-1. Dark Fiber Services Architecture Overview.**

*DFS from Lumen provides Agencies a secure and private fiber infrastructure for ultra-high bandwidth, as well as back up and disaster recovery applications.*

A fundamental element of our architecture is the fiber itself. In both CONUS and non-domestic locations, Lumen uses best-in-class Non-Zero Dispersion-Shifted Single-Mode (NZ-DFS) Corning Large Effective Area Fiber (LEAF) for intercity routes and Corning SMF-28 (series) for metro networks. Corning LEAF fiber exhibits very low attenuation at the critical 1550 nm wavelength – just 0.19 dB/km compared with the 0.25 dB/km acceptable value in the DFS Performance Metrics (SOW C.2.1.6.4). Over a span of just 50 km, the 3 dB difference in accumulated fiber attenuation for these two values represents a doubling of the loss of signal strength. Ultimately, this translates to either more wavelengths carried and/or longer spacing between repeaters – both lower cost positions for an agency.

To maintain service excellence, Lumen continues to invest in its online, Geographical Information System (GIS) and Fiber Management System (FMS). These systems enable faster delivery and implementation, flexibility in customer network designs, communication of scheduled and unscheduled maintenance events, and protection of the physical layer of the network. The attributes and conformance of Lumen DFS with all SOW requirements are discussed in the following sections.

---

#### **1.4.1.4.2 Standards [C.2.1.6.1.2]**

As one of the world's largest providers of DFS, Lumen is committed to support for industry standards. Lumen complies, as applicable, with the standards outlined in SOW C.2.1.6.1.2. These include standards issued by:

- Electronic Industry Alliance/Telecommunications Industry Association (EIA/TIA), namely EIA/TIA-559 and Optical Fiber System Test Procedures (OFSTP) including OFSTP: -2, -3, -7, -14 and -11
- Telcordia, namely GR-: 20-CORE, 63-CORE, 253-CORE and 326-CORE
- American National Standards Institute (ANSI), namely ANSI Z136.2-1998
- International Electrotechnical Commission (IEC), namely IEC 60825-1 and -2
- Code of Federal Regulations (CFR), namely 21 CFR 1040
- International Telecommunications Union (ITU-T), namely ITU-T: G.655 (10/2000), G.652 (10/2000), G.694.1, K.25 (02/2000), and L.35 (10/1998)

Consistent with our delivery of a considerable and expanding level of DFS to the Government today, Lumen and any Team members are responsible for all permits, easements, and rights of way, to include Host Nation agreements/approvals, and are responsible for complying with local Government regulations. If obstacles that negatively affect an agency's schedule are found during the process, Lumen can coordinate solutions with the Government.

Lumen complies with all new versions, amendments, and modifications made to the supported documents and standards as applicable.

#### **1.4.1.4.3 Connectivity [C.2.1.6.1.3]**

As largely demonstrated by our DFS currently delivered to the Government, Lumen DFS connects and interoperates with:

- Inter-agency or Intra-agency LANs within the same vicinity such that an agency can interconnect via Inter-agency or Intra-agency LAN to selected locations situated within the same metro area. Note that inter-agency connectivity may be subject to the routing requirements of OMB Memorandum M-15-01 (named in SOW C.1.8.8) to pass applicable traffic through an EINSTEIN Enclave for

inspection. If this applies, Lumen may be uniquely positioned to address it on the basis of the amount and extent of the dark fiber available, and the Enclaves. It will be executed by routing the DFS fiber path to and through the Enclave, where proxies facilitate traffic inspection in both directions.

- Lumen’s Long Haul or Metro networks such that an agency can connect its locations(s) to the nearest Lumen wire center, LEC wire center, Hut, IXC POP, or CLEC collocation facility as applicable.
- Reliability-enhancing redundant paths to support agency’s transport infrastructure.
- Lumen terminates fiber(s) in the existing Fiber Distribution Panel (FDP) or the FDP specified by the agency using connectors specified by industry’s standards for a) multi-tenant buildings, and b) single tenant buildings.

**1.4.1.4.4 Technical Capabilities [C.2.1.6.1.4]**

Lumen’s full compliance with the technical capabilities requirements for DFS are outlined in **Figure 1.4.1.4.4-1** with details of Lumen’s geographic coverage following.

**Figure 1.4.1.4.4-1. Lumen DFS Technical Capabilities**

LUMEN COMPLIES	SOW C.2.1.6.1.4 REQUIREMENT	LUMEN COMPLIANT SOLUTION
✓	1. Geographical Coverage	• Lumen specifies the coverage of its DFS in a) CONUS, b) (Optional) Non-domestic, and c) (Optional) OCONUS when required as part of a TO. Lumen substantial network assets – excellent metro and intercity market coverage in the U.S, Europe and Latin America; an extensive plant of conduits, high quality fiber and regeneration/ amplification huts; and some [REDACTED] facilities around the world – today make it a one of the nation’s leading providers of DFS in commercial, carrier, and Government markets. A discussion of our coverage is presented below this summary table.
✓	2. Configuration Options	• Supports all Configuration Options: a) Point-to-Point, b) Route Diversity/Single Drops, c) Route Diversity/Dual Drops, d) Star Configuration, and e) Hybrid Configuration
✓	Note: Numbers Restart 1. Fiber Service Delivery Point (FSDP)	• As required by the agency, Lumen supports the SDP at either the fiber patch panel where the fibers terminate at a Government location, or the collocation facility where the agency has installed its optonics. a) Optical Fiber. Lumen optical fibers meet or exceed all applicable standards specified in SOW C.2.1.6.1.2. Lumen provides the fiber count as specified by the agency.
✓	2. Ducting	• Lumen provides numbers and other details regarding the ducts connecting locations including number of fibers in the duct(s).

LUMEN COMPLIES	SOW C.2.1.6.1.4 REQUIREMENT	LUMEN COMPLIANT SOLUTION
✓	3. (Optional) Future Growth	<ul style="list-style-type: none"> <li>When available, Lumen includes an additional duct for future growth. New buildouts almost always include additional ducting so that growth, particularly unexpected growth, can be accommodated. If the network design involves a Lumen lateral pull or new construction, we typically install a larger count cable than is required (typically, 24 or more fibers). If all fiber in an existing cable is consumed, a new cable is pulled through one of our multiple empty conduits.</li> </ul>
✓	4. Channel Count	<ul style="list-style-type: none"> <li>Supports minimum of 80 DWDM wavelengths or user data spacing as specified in ITU-T G.694.1. Fibers capable of operating in the “C”, “L” and “S” bands. The Corning LEAF NZ-DFS fiber that Lumen uses for intercity routes, with its effective large core area and tailored attenuation and dispersion properties, is designed for DWDM applications.</li> </ul>
✓	5. Gateways	<ul style="list-style-type: none"> <li>Gateways are Lumen locations where agency traffic can be added and/or dropped. a) Lumen gateways have external generators and uninterruptible power conditioning and management systems that include a battery plant that can provide backup power for at least 8 hours without interruption. Generators and on-site fuel storage are designed to run for 24 hours at maximum capacity without refueling. b) Lumen provides locked cabinets, with the Government’s choice of either 19- or 23-inch mounting rails. Locked private suites are also available. c) Authorized personnel have 24/7 access to the gateway’s collocation area. d) Gateway locations are equipped with surveillance and high-security systems, and f) are monitored remotely, including for g) environmental conditions. Lumen continues to expand as the demand requires. e) Gateway expansion, both in terms of building out existing space and, when justified, acquiring new space is possible for most Lumen Gateways and gateway markets.</li> </ul>
ü	6. Service Components	<ul style="list-style-type: none"> <li>DFS components include a) trunks, b) laterals (agency-funded as noted in SOW), and c) building entrances. DFS components also include running line facilities (e.g., huts and amplifiers)</li> </ul>

**Discussion of Geographical Coverage for Dark Fiber Services**

With a deep commitment to building fundamental telecommunications infrastructure, Lumen ranks among a handful of leaders in providing DFS around the world. For example, in non-domestic locations, we offer DFS across Europe - notably in the UK, Germany, France, Belgium and the Netherlands.

Lumen’s network is continually expanding, but as of December 31, 2014, in North America, a network snapshot showed approximately [redacted] route miles and facilities-based, metropolitan networks in [redacted] markets. More than 95% of these route miles are in CONUS as are more than [redacted] markets. The same snapshot for Europe [Latin America] showed [redacted]

route miles and facilities-based, metropolitan networks in markets. The network serves one metro market in Asia.

While Lumen has an extensive dark fiber plant, the availability of DFS varies and it is not necessarily available on all route miles at all times.

**1.4.1.4.5 Features [C.2.1.6.2]**

Figure 1.4.1.4.5-1 presents the features of Lumen DFS and notes Lumen’s full compliance with all mandatory *and all optional* requirements of SOW C.2.1.6.2.

**Figure 1.4.1.4.5-1. Features of Lumen’s DFS**

LUMEN COMPLIES	SOW C.2.1.6.2 REQUIREMENT	LUMEN COMPLIANT SOLUTION
✓	1. Colocation Service	Enabling Agencies to manage their own DF networks and control their costs, Lumen provides the ability to add/drop traffic by allocating space in the POPs, repeater, and regenerator huts along the fiber route. As needed, Agencies provide the equipment necessary for optical regeneration and amplification.
✓	2. (Optional) Duct	Lumen DFS supports the number of ducts specified by the agency for new deployments per the Task Order request. Lumen showed great foresight in having deployed spare ducting over many years, even when commercial conditions at the time did not seem to warrant such action.
✓	3. (Optional) Dark Fiber Local Loop	Lumen provides DF connection between the agency’s location and the applicable Lumen wire center or outside plant (running line or regeneration location).
✓	4. (Optional) Diverse Loop Single Drop	For higher availability, Lumen provides diverse paths on the network. A single add/drop location/network element with automatic protection switching capabilities could provide the required switching. In DFS, this typically would be GFE, but could be provided by Lumen under a Professional Services agreement.
✓	5. (Optional) Diverse Route Dual Drop	To further enhance availability, where specified by the Government, Lumen provides diverse paths end-to-end. If it is required and cannot be provided by Lumen, Lumen works with a second contractor to satisfy this diversity requirement.
✓	6. (Optional) Inter-city connectivity	Lumen provides DF connections between an agency’s locations in metro areas in CONUS, OCONUS and non-Domestic locations. An advantage of Lumen is that it has deployed fiber in metro and long haul markets in many international markets, not just U.S. ones.
✓	7. (Optional) Multiple Duct	Lumen can upgrade to multiple ducts as required, typically on an Individual Case Basis (ICB). We note that Lumen already has multiple ducts in-place in many locations.
✓	8. Splicing	Supports joining of two or more lengths of fiber cable when necessary using either fusion or mechanical splicing.
✓	9. Off-net laterals	Off-net laterals are built to agency locations on an ICB with agency funding.

#### **1.4.1.4.6 Interfaces [C.2.1.6.3]**

The interfaces for DFS are the fiber terminations at the FSDP. Lumen supports SC and LC connectors as standard, but other types of commercially available connectors are also tested and supported as identified at the TO level.

#### **1.4.1.4.7 Performance Metrics [M.2.1, C.2.1.6.4]**

Lumen complies with all DFS Performance Levels and AQL of KPIs specified in SOW C.2.1.6.4 and measured in accordance with the notes of that section.

We note that AQL values for Connectors Loss and Fusion Splicing Loss are specified on an individual connection or splice basis. For connectors and splices in place, Lumen satisfies these on an average basis across a given span and over that space meets a requisite total (insertion) loss as opposed to parsing the loss requirements for each individual element in that span. For example, in the architectural description in Section 1.4.1.4.1, we noted the cumulative positive impact on potential cost (more wavelengths carried and/or longer spacing between repeaters) derived from the superb attenuation characteristics offered by Corning LEAF fiber at 1550 nm – an attenuation coefficient of just 0.19 dB/km compared with the 0.25 dB/km acceptable value in the SOW.

#### **1.4.1.5 Internet Protocol Service [L.29.2.1, C.2.1.7; C.4.4]**

Agencies can connect to the public Internet or interconnect their intranets from anywhere in the world using Lumen's Internet Protocol Service (IPS). A world leader in Internet connectivity, Lumen is directly interconnected with more than 4,200 Autonomous Systems (AS) that represent the core of the Internet. Lumen's global serving capacity is more than 42 Tbps, which includes more than 21 Tbps of private peering capacity.

Under Networx and WITS today, Lumen provides IPS to more than 125 locations and

##### **Lumen Internet Protocol Service**

- Lumen is a worldwide leader in providing connectivity to the Internet from more than 500 markets in more than 60 countries
- Directly interconnected with more than 4,200 networks (autonomous systems)
- Lumen offers a unique global services platform, anchored by Lumen -owned fiber networks
- Currently providing IPS to more than 125 locations under Networx and WITS

continues to ensure secure and high performance IP connectivity for Agencies under EIS.

Figure 1.4.1.5-1 highlights the features of the Lumen IPS solution aligned with the evaluation criteria.

**Figure 1.4.1.5-1. Features of Lumen IPS**

EVALUATION CRITERIA	FEATURES OF LUMEN IPS
Understanding [M.2.1.1]	<ul style="list-style-type: none"> <li>• A world leader in Internet connectivity, Lumen is directly interconnected with more than 4,200 Autonomous Systems (AS) that represent the core of the Internet.</li> <li>• Indicative of our understanding of IPS and the GSA environment, under Networkx and WITS today, Lumen is providing IPS to more than 125 locations.</li> </ul>
Quality of Service [M.2.1.2]	<ul style="list-style-type: none"> <li>• One of the most important component networks comprising the Internet, today Lumen’s demonstrably scalable, global serving capacity is more than 42 Tbps, which includes more than 21 Tbps of private peering capacity.</li> <li>• Lumen IPS is renowned for its many access options, high performance, exceptional connectivity (i.e., low network hop count to reach a given network), and overall service management.</li> <li>• Within its full compliance with EIS requirements, Lumen IPS satisfies all KPIs, plus Lumen has a strong, track record of quality of service performance on IPS under Networkx and WITS.</li> <li>• Lumen IPS supports IPv4 and IPv6 and Agencies with their own Autonomous System (AS) numbers can connect using Border Gateway Protocol (BGP).</li> <li>• Managed by experienced operations teams from redundant GovNOCs in Broomfield, CO and Atlanta.</li> </ul>
Service Coverage [M.2.1.3]	<ul style="list-style-type: none"> <li>• Lumen IPS is available in all 929 CBSAs based on our extensive national presence and interconnection agreements with relevant local carriers to supplement our native coverage for access circuits to IPS.</li> <li>• The network spans more than 60 countries and 500 markets globally. Agencies deploying IPS connect to the nearest Lumen POP Provider Edge (PE) router by using a Customer Edge (CE) router on their premises.</li> </ul>
Security [M.2.1.4]	<ul style="list-style-type: none"> <li>• By OMB mandate, all agency Internet traffic must be processed through a TIC Portal which is offered by Lumen (MTIPS, Section 1.4.8.3 of this Technical Volume). In addition, Lumen’s anti-DDoS solution is available to Trusted Internet Connection Access Providers (TICAPs).</li> <li>• Our state-of-the-art Security Operations Center (SOC) monitors the complete threat landscape with a continuous cycle of protection works closely with our Government SOC (GovSOC) teams.</li> <li>• Lumen and our subcontractors perform security operations in accordance with industry best practices and standards supporting Cyber, Personnel and Physical Security</li> </ul>

**1.4.1.5.1 Service and Functional Description [L.29.2.1, M.2.1, C.2.1.7.1.1]**

Stemming from our expansive network and standout Internet presence, IPS continues to be one of the defining services of Lumen. Lumen IPS is renowned for its

---

many access options, high performance, exceptional connectivity (i.e., low network hop count to reach a given network), and overall service management.

Lumen IPS supports IPv4 and IPv6 in a dual stacked environment. Agencies may utilize their own Autonomous System (AS) numbers and can connect to IPS using Border Gateway Protocol (BGP). OSPF and static routing are also supported by IPS, as are DNS and multicast. Of note regarding IPv6, Lumen was one of the first IPS providers to support network, end-to-end IPv6. Lumen IPS is available nationwide and internationally from all markets served by Lumen.

IPS is implemented on Lumen's robust IP network, supported by a highly resilient, scalable and secure optical network. The network spans more than 60 countries and 500 markets globally. Agencies deploying IPS connect to the nearest Lumen POP Provider Edge (PE) router by using a Customer Edge (CE) router on their premises. The PE/CE connection can use a range of interfaces and media. An agency can choose to provide all, some, or none of the required network equipment necessary to interface with the Lumen network.

**Figure 1.4.1.5.1-1** provides an overview of Lumen's IPS including its peering arrangements and its place as part of the Internet.





**Figure 1.4.1.5.1-1. IPS Architecture Overview.** *Lumen is among the Internet's most interconnected networks.*

**Figure 1.4.1.5.1-2** shows the networks peering locations by city, many of which are outside the U.S. With multiple peering locations in some cities, the total number of actual peering locations [REDACTED]

**Figure 1.4.1.5.1-2. Lumen's Network Extensive Peering Locations by City**

[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
* Multiple locations								

The attributes and conformance of Lumen IPS with all SOW requirements are discussed below.

**1.4.1.5.2 Standards [C.2.1.7.1.2]**

As applicable, Lumen IPS complies with all of the standards noted in SOW C.2.1.7.1.2. In addition, Lumen complies with new versions, amendments, and

modifications to the documents and standards called out in that SOW when offered commercially and as applicable.

**1.4.1.5.3 Connectivity [C.2.1.7.1.3]**

Lumen IPS is fully compliant with all of the requisite connectivity requirements outlined in SOW C.2.1.7.1.3. These include connecting Government locations including mobile and remote users to the Internet over a wide range of equipment. In addition, IPS connects Government locations to other networks, including those of other EIS contractors.

For the IPS that Lumen is providing today under Networx and WITS, network connectivity includes DSL and fixed circuits up to 10 Gbps.

**1.4.1.5.4 Technical Capabilities [C.2.1.7.1.4]**

Lumen IPS is fully compliant with all of the requisite technical capabilities outlined in SOW C.2.1.7.1.4 as summarized in **Figure 1.4.1.5.4-1**.

**Figure 1.4.1.5.4-1. Lumen’s Compliance with IPS Technical Capabilities**

LUMEN COMPLIES	SOW C.2.1.7.1.4 REQUIREMENT	LUMEN COMPLIANT SOLUTION
✓	1. SOW C.1.8.8 Routing Requirements (National Security Policy)	<ul style="list-style-type: none"> <li>By OMB mandate all Internet traffic must be processed through a TIC which includes an EINSTEIN Enclave and inspection, including with proxies when needed. In the basic definition of Lumen IPS, there is a presumption that IP traffic crossing the Lumen/agency handoff is processed by a TIC per a separate agency arrangement. If not, then Lumen can provide the necessary inspection, although the service definition may evolve to MTIPS. Otherwise, in a manner to be defined at the TO level, Lumen can establish a special routing mechanism between the agency’s location and its designated TIC.</li> </ul>
✓	2. IPS ports at peak data rates	<ul style="list-style-type: none"> <li>Provides IPS ports at the peak data rates specified by Agencies.</li> </ul>
✓	3. Access Methods	<ul style="list-style-type: none"> <li>Supports appropriate access services (e.g., DSL, PLS, satellite) to connect agency SDPs to Lumen IPS. Lumen today supports agency interconnections using a range of access methods from low speed DSL connections up to 10 Gbps circuits. We expect that our Ethernet access will become the predominant form of fixed line access.</li> </ul>
✓	4. Peering Arrangements	<ul style="list-style-type: none"> <li>a) As a Tier 1 global ISP, Lumen is publically peered (i.e., directly interconnected) with more than 4,200 networks (unique AS numbers).</li> <li>b) Lumen maintains private peering connections with more than 50 of the world’s largest Internet carriers. More than 90% of our interconnection traffic runs through these connections. Such connections are nearly always redundant and physically diverse. There are more [REDACTED]</li> </ul>



**1.4.2 Voice Service (Optional)**

**1.4.2.1 Circuit Switched Voice Service [L.29.2.1, C.2.2.2]**

Even as Government agencies migrate to more IP-based communication methods, Circuit-Switched Voice Service (CSVS) remains important. Lumen’s voice products provide a robust suite of voice services that give EIS program customers direct, global connectivity. We process over 12B minutes for 5B carrier switched calls per month on our network.

Our CSVS includes domestic and international outbound long distance for IP- and CS-based calls across multiple platforms including mobiles, laptops, tables, and traditional telephones. Lumen’s CSVS solution, as part of Voice Complete, meets all of GSA’s requirements for EIS. **Figure 1.4.2.1-1** highlights how the features of the Lumen CSVS solution satisfy the evaluation criteria.

**Figure 1.4.2.1-1. CSVS Feature Highlights**

EVALUATION CRITERIA	FEATURES OF LUMEN CSVS
Understanding [M.2.1.1]	<ul style="list-style-type: none"> <li>Lumen’s far-reaching and integrated Circuit-Switched network ensures that all EIS customers using CSV continue to receive voice service and support, that the entire U.S. public sector community has seamless voice connectivity, and that all U.S. citizens, private sector firms, and foreign entities with whom the U.S. Government does business can be reliably reached</li> </ul>
Quality of Service [M.2.1.2]	<ul style="list-style-type: none"> <li>Compliant—Voice Complete, as described in this section, fully complies with the functional and performance requirements and adheres to all applicable standards</li> <li>Scalable—Network is built on vendor-neutral, standards-based technologies that enable a modular approach to network expansion</li> <li>Reliable—Government Network Operation Centers (GovNOC) in Broomfield, CO, Atlanta, GA, and Herndon, VA provide real-time, 24/7/365 traffic management for the Lumen network, resolve network outages, and apply pre-planned or automated network controls to minimize an adverse event’s network impact</li> <li>Resilient—Appropriate network redundancy and safeguards while maintaining efficiency are designed to ensure service continuity through a variety of events that include cyber-attacks and natural disasters</li> </ul>
Service Coverage [M.2.1.3]	<ul style="list-style-type: none"> <li>Includes coverage of [REDACTED] CBSAs specified in Section J.1 and over [REDACTED] of the U.S. population. Non-domestic coverage to over 60 countries and more through international carrier agreements (J.1.3).</li> <li>E-911 network connects to over 6000+ Public Service Answering Points covering over 90% of the U.S. population</li> </ul>
Security [M.2.1.4]	<ul style="list-style-type: none"> <li>Provides the Government with encrypted voice that complies with federal security standards</li> </ul>

#### 1.4.2.1.1 Service and Functional Description [L.29.2.1, M.2.1, C.2.2.2]

Lumen's voice services consist of dedicated, circuit-switched, virtual circuit-switched, and IP voice services, enabling Government customers to leverage the power of our TDM and VoIP networks to deliver reliable and scalable solutions that increase productivity and reduce expenses without compromising quality. Our dedicated and switched access methods ensure standards-based connectivity to optimize and leverage the Government's existing telecommunications systems.

Our CSVS is integrated into our suite of enterprise voice technologies, which combines dedicated long distance, local, SIP, and ISDN-PRI services. We coordinate with best-in-class vendors, both domestically and abroad, for the highest-performing and lowest-cost solutions for a seamless wireline-wireless converged service architecture and optimal bridge solutions between legacy circuit-switched and IP-based services.

Among the features of our approach, the TDM local voice offers a reliable, easy-to-use voice service delivered over Lumen's nationwide coverage network. TDM local voice provides local access service for PBXs and may be customized to meet specific subscriber requirements. A summary of our circuit switched services and features are provided in **Figure 1.4.2.1.1-1**.



**Figure 1.4.2.1.1-1. Lumen Circuit Switched Services.** *Our circuit switched services provides our Government customers with reliable voice services over our national coverage network.*

**1.4.2.1.2 Standards [C.2.2.2.1.2]**

Lumen’s CSVS solution complies with all applicable industry standards for voice services.

**1.4.2.1.3 Connectivity [C.2.2.2.1.3]**

Lumen’s CSVS solution provides maximum connection and interoperability with customer-specified terminations, PSTNs, other contractor VS networks, and satellite phones and terminals, as stipulated in SOW C.2.2.2.1.3.

**1.4.2.1.4 Technical Capabilities [C.2.2.2.1.4]**

Lumen’s CSVS solution meets the capability requirements and thresholds described in SOW C.2.2.2.1.4. **Figure 1.4.2.1.4-1** summarizes elements of our CSVS solution for each technical capability.

**Figure 1.4.2.1.4-1. CSVS Technical Capabilities**

LUMEN COMPLIES	SOW C.2.2.2.1.4 REQUIREMENT	LUMEN COMPLIANT SOLUTION
✓	1. Numbering Plan	<ul style="list-style-type: none"> <li>Lumen CSVS supports ITU-TSS Integrated Services Digital Network (ISDN) E.164 uniform numbering and address plan</li> </ul>
✓	2. Network Intercept	<ul style="list-style-type: none"> <li>We route calls to intercept announcements for disconnected numbers, time-out during dialing, network congestion, denial of access to off-net and on-net calls, denial of access to features, and other conditions</li> </ul>
✓	3. User-to-User Signaling (Optional)	<ul style="list-style-type: none"> <li>Lumen provides optional non-call associated signaling (NCAS), which allows users to communicate by means of user-to-user signaling without setting up circuit-switched connection</li> </ul>
✓	4. Voice Quality	<ul style="list-style-type: none"> <li>G.711 is an ITU standard for converting analog signals (voice, into PCM 64 kbps digital signals, ensuring that we provide high quality calls over our circuit-switched network</li> </ul>
✓	5. Emergency Service	<ul style="list-style-type: none"> <li>Lumen is compliant with 911 and E911 service requirements, Commission on Accreditation for Law Enforcement agencies (CALEA) requirements, mission-critical Government requirements</li> <li>Our digital network is stable and resilient, and can identify locations of originating-call stations and route them to appropriate public safety answering points</li> </ul>

**1.4.2.1.5 Features [C.2.2.2.2]**

Lumen’s CSVS solution provides the entire range of functionality described in SOW C.2.2.2.2. **Figure 1.4.2.1.5-1** highlights elements of our approach to providing required CSVS features.

**Figure 1.4.2.1.5-1. Lumen Compliant CSVS Features**

LUMEN COMPLIES	SOW C.2.2.2.2 REQUIREMENT	LUMEN COMPLIANT SOLUTION
✓	1. Agency-Recorded Message Announcements	<ul style="list-style-type: none"> <li>Maintains the message system (from VOIP and CS) a messaging solutions that meets each of the thresholds described, including authentication, recording numbering, message length, access/accessibility, and storage capacity.</li> </ul>
✓	2. Authorization Codes/Calling Cards (Optional)	<ul style="list-style-type: none"> <li>Lumen provides optional Network Authorization System that enables the Government to set and manage call authorization based on prepaid and post-paid access codes on calling cards as required.</li> </ul>
✓	3. Caller Identification (ID)	<ul style="list-style-type: none"> <li>SS7 network fully supports delivery of all available caller ID information.</li> </ul>
✓	4. Call Screening for Users	<ul style="list-style-type: none"> <li>Network services enable the Government to manage call authorization, based on a specified CoS.</li> </ul>
✓	4.2 Code Block (Optional)	<ul style="list-style-type: none"> <li>We provide optional Code Block capability through which Customers can specify CoS access restrictions for users, stations, and trunks to be automatically blocked.</li> </ul>
ü	5. Customized Network Announcement Intercept Scripts (Optional)	<ul style="list-style-type: none"> <li>Gives the Government optional capability to manage, monitor, and record announcements.</li> </ul>
✓	6. Internal agency Accounting Code (Optional)	<ul style="list-style-type: none"> <li>Lumen provides optional direct dial service that, when used with VNS, furnishes this capability to the Government, including additional digits and CDR details.</li> </ul>
✓	7. Directory Assistance	<ul style="list-style-type: none"> <li>Voice network allows for the dialing of all NPA-555-1212 directory assistance and support of 8XX calls.</li> </ul>
✓	8. Suppression of Calling Number Delivery	<ul style="list-style-type: none"> <li>VNS features can provide this functionality with per-line and per-call blocking options.</li> </ul>
✓	9. Voice Mail Box	<ul style="list-style-type: none"> <li>Includes enhanced voice services such as Voice Mailbox that delivers the required functionality.</li> </ul>
✓	10. Basic Subscriber Line: Multi Appearance Directory Number (Optional)	<ul style="list-style-type: none"> <li>Lumen provides the optional CSVS capability to assign the same telephone number to more than one telephone.</li> </ul>
✓	11. ISDN PRI: Backup of Shared-D Channel (Optional)	<ul style="list-style-type: none"> <li>Provides optional backup of shared D-Channels in order to maintain active calls in the event of a D-Channel failure.</li> </ul>
✓	12. ISDN BRI: Multi Appearance Directory Number (Optional)	<ul style="list-style-type: none"> <li>Lumen CSVS solution provides the optional capability to assign multi appearance directory numbers on an ISDN BRI.</li> </ul>
✓	13. MLPP (Optional)	<ul style="list-style-type: none"> <li>Lumen CSVS call manager software is configurable to allow properly validated</li> </ul>

LUMEN COMPLIES	SOW C.2.2.2.2 REQUIREMENT	LUMEN COMPLIANT SOLUTION
		users to place priority calls and, if necessary, preempt lower-priority phone calls to targeted stations or through fully subscribed TDM trunks.

**1.4.2.1.6 Interfaces [C.2.2.2.3]**

Lumen’s flexible CSVS solution accommodates the 14 interface types described in SOW C.2.2.2.3.

**1.4.2.1.7 Performance Metrics [M.2.1, C.2.2.2.4, G.8]**

Lumen meets all of the CSVS performance standards and thresholds listed in the CSVS Performance Metrics table in SOW C.2.2.2.4. The Lumen GovNOCs proactively monitor all Lumen Enterprise services so that we can quickly respond to any quality of service routing issues. Lumen uses monitoring tools that provide comprehensive visibility of numerous network elements and the ability to accurately measure AQLs for the applicable KPIs.

**1.4.2.2 Toll Free Service [L.29.2.1, C.2.2.3; C.4.4]**

With the scale and depth of the Lumen network, along with the advanced features, routing capabilities and flexibility of our solution Lumen provides the agency with comprehensive and compliant Toll-Free Service (TFS). The TFS we offer is a feature-rich solution that includes transfer, multiple carrier routing, standard and custom DNIS and ANI capabilities.

**Compliant TFS Performance**

- Global reach provides scalable solutions driven by consistent network platforms for efficiency
- Secure, high-quality, carrier-grade connections via private IP backbone network
- Full-featured services enable better tracking, cost management, and billing

Our EIS TFS has real-time customer-controlled Enhanced Routing capabilities that enable multiple routing configurations at a Toll Free (TF) number level.

**Figure 1.4.2.2-1** highlights the features to GSA and the Agencies of the Lumen TFS solution, which are aligned with the evaluation criteria.

**Figure 1.4.2.2-1. Features of Lumen’s TFS**



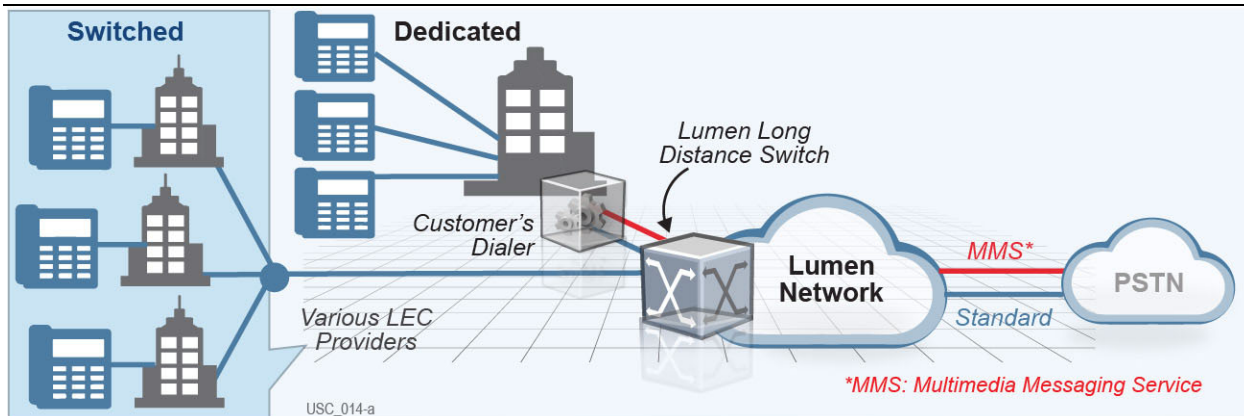
EVALUATION CRITERIA	FEATURES OF LUMEN TFS
Understanding [M.2.1.1]	<ul style="list-style-type: none"> <li>The TFS we offer is a feature rich solution that includes transfer, multiple carrier routing, and standard and custom DNIS and ANI capabilities, in alignment with EIS requirements</li> <li>The Lumen TFS delivers the technical capabilities, features and feature reports required by the Government</li> </ul>
Quality of Services [M.2.1.2]	<ul style="list-style-type: none"> <li>We meet or exceed all TFS performance requirements, supported by quality assessment and reporting developed and enhanced through extensive past performance providing services like those required by EIS</li> <li>The Lumen GovNOC monitors and manages TFS services provided to help ensure that all applicable AQLs for the applicable KPIs are met</li> </ul>
Service Coverage [M.2.1.3]	<ul style="list-style-type: none"> <li>The Lumen TFS solution rides on globally distributed Lumen network, with integrated strategically dispersed communications switches, switching centers, and dedicated network links to eliminate latency issues and service interruptions</li> <li>Lumen offers service to over 100 countries in the Americas, Europe, and Asia</li> <li>Lumen carries over 12 B minutes per month over more than 5 B calls</li> </ul>
Security [M.2.1.4]	<ul style="list-style-type: none"> <li>Our state-of-the-art GovSOC monitors the complete threat landscape with a continuous cycle of protection</li> <li>Lumen and our subcontractors perform security operations in accordance with industry best practices and standards supporting Cyber, Personnel and Physical Security</li> </ul>

**1.4.2.2.1 Service and Functional Description [L.29.2.1, M.2.1, C.2.2.3]**

The Lumen TFS solution fulfills the mandatory service requirements for TFS contained in SOW C.2.2.3. This section presents a technical description of our offering, demonstrating our TFS Standards, Connectivity, Technical Capabilities, Features, Interfaces, Performance Metrics, and Service Coverage.

The Lumen TFS solution rides on the globally distributed Lumen network, which has integrated, strategically dispersed communications switches, switching centers, and dedicated network links to eliminate latency issues and service interruptions.

As illustrated in **Figure 1.4.2.2.1-1**, Lumen lets you choose from dedicated or switched TFS solutions, which deliver a powerful complement to advanced routing services and features.



**Figure 1.4.2.2.1-1. Lumen Flexible and Compliant TFS Solution.**

#### **1.4.2.2.2 Standards [C.2.2.3.1.2]**

Lumen's TFS offering is compliant with the standards listed in SOW C.2.2.3.1.2. We comply with new versions, modifications, and amendments to the standards listed in SOW C.2.2.3.1.2. Members of our Team are active in industry forums and working groups related to toll free services, and are committed to implementing future standards when applicable, as technologies are developed and new standards are defined and become commercially practicable.

#### **1.4.2.2.3 Connectivity [C.2.2.3.1.3]**

Our TFS solution rides on the globally distributed Lumen network, with integrated strategically dispersed communications switches, switching centers, and dedicated network links to eliminate latency issues and service interruptions. This infrastructure provides overall availability of 99.99% and allows Lumen to meet required Time-to-Restore requirements.

#### **1.4.2.2.4 Technical Capabilities [C.2.2.3.1.4]**

**Figure 1.4.2.2.4-1** shows how the Lumen EIS TFS fully complies with all SOW C.2.2.3.1.4 technical capabilities requirements. All of the technical capabilities addressed are mandatory.

Figure 1.4.2.2.4-1. TFS Technical Capabilities

LUMEN COMPLIES	SOW C.2.2.3.1.4 REQUIREMENT	LUMEN COMPLIANT SOLUTION
✓	1. Act as responsible organization (Resp Org)	<ul style="list-style-type: none"> <li>Lumen acts as Resp Org for the assignment and maintenance of TF numbers if requested by a ordering agency.</li> </ul>
✓	2. Support TF number portability	<ul style="list-style-type: none"> <li>We support TF number portability. The Lumen Customer Care Manager (CCM) and Lumen Project Manager (PM) coordinate with the EIS user and the Resp Org in moving TF numbers to the Lumen-provided TFS.</li> </ul>
✓	3. Accommodate presently assigned TF numbers	<ul style="list-style-type: none"> <li>Lumen accommodates presently assigned toll-free numbers. We work with any current carrier on the customer's behalf to gain ownership of the presently assigned TF number. TF numbers may be reserved at any time through the Lumen TFS Portal.</li> </ul>
✓	4. Offer Universal International TF Number service	<ul style="list-style-type: none"> <li>Lumen provides Universal International TF Number service as required. Lumen's Universal International Free Phone Number (UIFN) Service provides TF numbers where the same number can be used to originate calls from different participating countries.</li> </ul>
ü	5. Provide TF number capabilities	<ul style="list-style-type: none"> <li>Lumen provides the termination capabilities required. Lumen's TFS supports seamless routing of inbound calls to multiple locations. Calls terminate at customer-specified locations based on the caller's area code, area code and exchange, or the caller's 10-digit telephone number.</li> </ul>
✓	6. Provide busy signal or recorded announcement	<ul style="list-style-type: none"> <li>Lumen provides a busy signal or recorded announcement for all calls terminating egress congestion or facing network congestion. Lumen TFS Route Advance sends TF calls to another trunk group if the first trunk group is busy.</li> </ul>
✓	7. Provide network intercept to recorded announcements	<ul style="list-style-type: none"> <li>As a TFS function, Lumen provides a network intercept to recorded announcements as an inherent network capability. The generic announcements provided by Lumen are at a minimum be those specified in the SOW.</li> </ul>
✓	8. Provide capability for customized network intercept recorded announcements	<ul style="list-style-type: none"> <li>As a function of EIS TFS, Lumen provides the capability for customized network intercept recorded announcements. This function allows users to create and upload network intercept recorded announcements to the TFS platform and have the ability to route calls to these announcements as termination points.</li> </ul>
✓	9. Provide recording in English and Spanish	<ul style="list-style-type: none"> <li>The TFS provided by Lumen includes the capability to have all announcements recorded in both English and Spanish by Lumen or GSA Administrators.</li> </ul>
✓	10. Provide referral message to callers	<ul style="list-style-type: none"> <li>Lumen provides a referral message to callers of a disconnected TF number, as required by the SOW. If so designated by the Government, an agency-provided referral telephone number is provided in the disconnect message.</li> </ul>
✓	11. Provide Dialed Number Identification Service (DNIS)	<ul style="list-style-type: none"> <li>The Lumen EIS TFS DNIS enables the routing and unique identification of multiple TF numbers on a shared trunk group. Upon agency request, we transmit DNIS digits prior to delivery of a TFS call to identify the dialed TF number uniquely. The number of DNIS digits range from 3 to a maximum of 10.</li> </ul>
✓	12. Automatic Number	<ul style="list-style-type: none"> <li>The Lumen EIS TFS identifies and provides calling parties Automatic Number</li> </ul>

LUMEN COMPLIES	SOW C.2.2.3.1.4 REQUIREMENT	LUMEN COMPLIANT SOLUTION
	Identification (ANI)	Identification, allowing the Government to identify calling parties as their call is delivered, to assist with the identification of emergency or malicious calls.

**1.4.2.2.5 Features [C.2.2.3.2]**

Lumen provides all of the mandatory features specified in SOW C.2.2.3.2. The features we provide can be used individually or in any combination, as required by specific TOs. **Figure 1.4.2.2.5-1** shows how the Lumen EIS TFS fully complies with all SOW features requirements.

**Figure 1.4.2.2.5-1. TFS Features**

LUMEN COMPLIES	SOW C.2.2.3.2 REQUIREMENT	LUMEN COMPLIANT SOLUTION
✓	1. Agency-Based Routing Database	<ul style="list-style-type: none"> <li>The Lumen solution provides the ability to route TFS calls or provide information based on queries to a database located at the ordering agency premises, in compliance with SOW requirements. We deliver this solution through comprehensive Computer Telephony Integration (CTI) with the Government legacy CTI implementation or using Lumen-provided web service APIs for EIS users who do not have, or wish to leverage, a legacy CTI solution.</li> </ul>
✓	2. Alternate Routing	<ul style="list-style-type: none"> <li>Lumen provides alternate routing to terminate dedicated inbound traffic when the targeted dedicated facility is either in an all-circuits busy condition or is out of service. If none of the alternate routing terminations are able to receive a call, the Call Referral Recording capability we provide lets the Government prerecord and play an announcement to the caller, or our TFS engine provides a busy signal, at the ordering agency's option.</li> </ul>
✓	3. ANI	<ul style="list-style-type: none"> <li>Lumen provides transmission of a TFS caller's ANI in real time. Using this feature, EIS TFS users receive the calling party's 10-digit telephone number as the call is delivered to allow caller identification.</li> </ul>
✓	4. ANI Based Routing	<ul style="list-style-type: none"> <li>The Lumen TFS solution enables the routing of TFS calls based upon the ANI of the caller. We provide default routing defined by the ordering agency when ANI is not used or available.</li> </ul>
✓	5. Announced Connect	<ul style="list-style-type: none"> <li>Lumen supports the Whisper functionality specified in the SOW for ANI or digits captured through Interactive Voice Response (IVR).</li> </ul>
✓	6. Announcements	<ul style="list-style-type: none"> <li>Lumen provides announcements as prescribed by the SOW. Our Network Announcement capability fully supports all required functionality. Network</li> </ul>

**General Services Administration (GSA)**  
**Enterprise Infrastructure Solutions (EIS)**

Contract # GS00Q17NSD3006  
 Mod #: P00310  
 Submission #: CL01001.01a

LUMEN COMPLIES	SOW C.2.2.3.2 REQUIREMENT	LUMEN COMPLIANT SOLUTION
		Announcements can be recorded in English, Spanish, and optionally in three other languages by Lumen or GSA Administrators.
✓	7. Call Menu Routing	<ul style="list-style-type: none"> <li>Lumen provides the capability to provide information messages to TFS callers, and route the callers via speech or information entered by DTMF signals. The Call Menu Routing feature provides all of the capabilities specified in the SOW.</li> </ul>
✓	8. Call Redirection	<ul style="list-style-type: none"> <li>The Lumen TFS solution enables TFS calls to be transferred by our network, using at the agency's discretion any of the following transfer modes: blind transfer, verification then transfer, and three-way conference then transfer. There is no double billing for call redirection transfers. There also is the ability to put the caller on hold and provide abbreviated dialing codes, with two music options as specified in the SOW.</li> </ul>
✓	9. Computer Technology Integration (CTI)	<ul style="list-style-type: none"> <li>Lumen provides the CTI messaging capability required by the SOW. Our TFS CTI capability provides a seamless experience between self-service and live interactions.</li> </ul>
✓	10. Custom Call Records	<ul style="list-style-type: none"> <li>We provide Custom Call Records capability as required by the SOW in our TFS solution. Our TFS reporting includes the capability to have a full definition of all data elements in detailed call data records and reports. All standard and custom reports provided through our TFS platform can be built in html, .csv, and .xls.</li> </ul>
ü	11. Day of Week Routing	<ul style="list-style-type: none"> <li>Lumen's TFS Day of Week Routing allows the routing of a TF number to different applications or terminations based on the day of the week.</li> </ul>
✓	12. Day of Year Routing	<ul style="list-style-type: none"> <li>The Lumen TFS supports agency configurable routing by time of day, day of week, day of year, NPA/NXX, and a number of other criteria. Lumen provides 20 dates that are eligible for day of year routing during any 12 month period.</li> </ul>
✓	13. In Route Announcements	<ul style="list-style-type: none"> <li>Lumen provides In Route Announcements as required by the SOW. In Route Announcements, recorded in either English or Spanish and three optional other languages allow callers to hear an announcement during call setup without affecting the final destination of the call.</li> </ul>
✓	14. Interactive Voice Response (IVR)	<ul style="list-style-type: none"> <li>Lumen provides mandatory and optional Interactive Voice Response (IVR) capabilities as required by the SOW. The Lumen IVR platform supports the latest speech recognition functionality, including yes/no and numeric input, and our application development team can implement the user interface in a manner to ensure the highest recognition rates. Our speech recognition capabilities include support for both English and Spanish input.</li> </ul>
✓	15. Make Busy Arrangement	<ul style="list-style-type: none"> <li>The Lumen TFS supports the Make Busy Arrangement requirements of the SOW. The Lumen TFS enables customers to control routing on TF and Local Inbound telephone numbers, and to configure transfer destinations as well as any network announcements.</li> </ul>
✓	16. Network Call Distributor	<ul style="list-style-type: none"> <li>Lumen supports all Network Call Distributor (NCD) capabilities and functions required by the SOW. Our NCD functions use real-time Active Call Directory (ACD) operating status information to access the best resource or location to deliver inbound calls. The</li> </ul>

LUMEN COMPLIES	SOW C.2.2.3.2 REQUIREMENT	LUMEN COMPLIANT SOLUTION
		Lumen TFS NCD is provided as a managed service that is optionally contractor-provided and contractor-based or contractor-provided and agency-based.
✓	17. Network Queuing (Optional)	<ul style="list-style-type: none"> <li>The Lumen TFS solution for this optional feature satisfies the SOW Network Queuing requirements. The TFS Network Queuing capability provides the capability to queue calls in the network, and enhances the ability to manage incoming call traffic.</li> </ul>
✓	18. NPA/NXX Routing	<ul style="list-style-type: none"> <li>Inbound toll TF calls are sent to different locations based on the NPA, or NPA-NXX, or country code of the caller. Users can seamlessly route inbound calls to an unlimited number of terminating locations. When NPA/NXX isn't available, we route calls to an agency-defined default location.</li> </ul>
✓	19. Percentage Call Allocation	<ul style="list-style-type: none"> <li>Lumen provides the Percentage Call Allocation capability required by the SOW. With this capability, calls can be routed to destinations based on customer-defined allocations. Customers can have up to 100 active terminating destinations assigned to a TF or Local Inbound number, with each destination receiving call allocations in 1% increments.</li> </ul>
ü	20. Real Time Reporting	<ul style="list-style-type: none"> <li>The Lumen TFS Real Time Reporting capability provides to Agencies the ability to monitor and report on detail and summary data related to TFS call status on a near real-time basis, as required by the SOW. All standard and custom reports can be built and delivered in html, .csv, or .xls, and be available on a daily, weekly, or monthly basis.</li> </ul>
✓	21. Routing Control	<ul style="list-style-type: none"> <li>Lumen provides Routing Control meeting SOW requirements, with sufficient security and auditing capability, via our TFS feature uCommand. uCommand gives EIS users near real-time control of enhanced TF routing, without tying them to a specific PC or proprietary application software. Through uCommand, users can set up a routing plan for each different way they want to route their calls.</li> </ul>
✓	22. Service Assurance Routing	<ul style="list-style-type: none"> <li>The Lumen TFS solution has the capability to route toll TF to a predetermined alternate termination or an announcement within five minutes of a Government request due to an emergency request or service disruption. Rerouting is completed within 30 minutes of receipt of the Government request for this action.</li> </ul>
✓	23. Speech Recognition	<ul style="list-style-type: none"> <li>The EIS TFS provided by Lumen has network-based natural speech recognition capability to recognize English and Spanish, as well as optionally other languages spoken words and digits, as required by the SOW and applicable TOs.</li> </ul>
✓	24. Tailoring Call Coverage	<ul style="list-style-type: none"> <li>Inbound TF calls originating from specific locations (state/country), telephone numbers (based on the NPA, NPA-NXX, ANI), or call source (such as from payphones) can be restricted through our TFS solution. Restricted callers hear a courteous message indicating that TF service is not available from their area/phone.</li> </ul>
✓	25. Time of Day Routing	<ul style="list-style-type: none"> <li>Lumen's TFS Time of Day Routing allows the routing of one TF number to an unlimited number of locations based on the time of day, as required by the SOW. Our Time of Day Routing solution provides the capability to route in one minute intervals.</li> </ul>

LUMEN COMPLIES	SOW C.2.2.3.2 REQUIREMENT	LUMEN COMPLIANT SOLUTION
✓	26. Language Interpretation	<ul style="list-style-type: none"> <li>Lumen's TFS provides language translation services for near-real time communications between callers speaking different languages.</li> </ul>
✓	27. Virtual Queue	<ul style="list-style-type: none"> <li>Lumen provides the capability for callers to choose to continue to wait online for an attendant or to receive a call back in turn.</li> </ul>
✓	28. Vanity Number	<ul style="list-style-type: none"> <li>The Lumen TFS provides vanity toll-free numbers if requested by the agency.</li> </ul>

**1.4.2.2.5.1 Feature Reports [C.2.2.3.2.1]**

Lumen TFS provides Feature Reports that satisfy SOW requirements. Feature Reports will indicate an Eastern Time presentation using a 24-hour clock or a 12-hour clock with an AM/PM indication. We provide the optional capability for Feature Reports to indicate the time zone of the TFS terminating location.

Each report will contain standard information including:

1. Title of Report
2. Date of Report
3. Period covered by the Report
4. Name of ordering agency
5. Toll free number(s) included in the Report

These reports are made available by electronic means, providing the ordering agency with information concerning the status of calls placed to each TF number and/or termination. **Figure 1.4.2.2.5.1-1** shows how the Lumen EIS TFS fully complies with all SOW TFS Feature Reports requirements.

**Figure 1.4.2.2.5.1-1. TFS Feature Reports**

LUMEN COMPLIES	SOW C.2.2.3.2.1 REQUIREMENT	LUMEN COMPLIANT SOLUTION
✓	1. Call Status Report - TFS	<ul style="list-style-type: none"> <li>Lumen provides a Call Status Report – TFS for any given TF number which includes the information required by the SOW. TFS reporting is derived through our TFS reporting engine, via the Routing and Call Control (RACC) Portal.</li> </ul>
✓	2. Call Status Report – Alternate Routing	<ul style="list-style-type: none"> <li>In accordance with SOW requirements, Lumen provides Call Status Reports – Alternate Routing, containing the required information, for any TF number with</li> </ul>

LUMEN COMPLIES	SOW C.2.2.3.2.1 REQUIREMENT	LUMEN COMPLIANT SOLUTION
		alternate routing. In preparing these reports, we use CDRs which depict each entire call, to include multiple legs as a result of being transferred one or more times and re-routing.
✓	3. Call Status Report - Announcement	<ul style="list-style-type: none"> <li>Lumen provides a Call Status Report – Announcement for any given TF number using Terminating or In-Route Announcements, which includes the information required by the SOW.</li> </ul>
✓	4. Call Status Report – Call Prompter	<ul style="list-style-type: none"> <li>Lumen provides a Call Status Report – Call Prompter for any given TF number using Call Prompter Access, which includes the information required by the SOW. Using the Lumen TFS Build Excel reporting feature this Report can be downloaded for every call into the Call Prompter, and from that information averages and percentages can be calculated.</li> </ul>
✓	5. Call Status Report - IVR	<ul style="list-style-type: none"> <li>Lumen provides a Call Status Report – IVR for any given TF number using IVR, which includes the information required by the SOW. Our TFS Topline Report capability tallies calls by call outcome. The outcomes for an IVR are set by the IVR.</li> </ul>
ü	6. Caller Information Report	<ul style="list-style-type: none"> <li>Lumen provides a Caller Information Report for all ANI information of all callers to a specified TF number, with the information required by the SOW. We provide the NPA or NPA-NXX of the caller, as available, when the caller's ANI is not available, substituting Zeroes in place of any missing digits.</li> </ul>
✓	7. Caller Profile Report	<ul style="list-style-type: none"> <li>Lumen provides Caller Profile Reports with the information required by the SOW.</li> </ul>
✓	8. Call Redirection Report (Optional)	<ul style="list-style-type: none"> <li>The Lumen TFS solution for the optional Call Redirection Report satisfies SOW requirements. Call Redirection Reports provide a summary of call redirection activity by TF number and abbreviated dial code if available.</li> </ul>

**1.4.2.2.6 Interfaces [C.2.2.3.3]**

The Lumen TFS solution meets all of the interface requirements shown in the TFS Interfaces table in SOW C.2.2.3.3.

**1.4.2.2.7 Performance Metrics and Quality of Services [M.2.1, C.2.2.3.4, G.8]**

The Lumen TFS solution meets all of the TFS performance metrics shown in the TFS Performance Metrics table in SOW C.2.2.3.4.

The Lumen GovNOC monitors all Lumen Enterprise services provided using our network.

**1.4.2.3 Circuit Switched Data Service [L.29.2.1, C.2.2.4]**

**Lumen CSDS Highlights**

- Robust geographic availability with service to all 50 states and the District of Columbia, to U.S. territories, and internationally
- High-quality service in conjunction with digital network that carries both voice and data
- Proven record of successful support, having provided CSDS for multiple Government agencies, including FEMA and U.S. District Courts



Lumen’s Carrier Switched Data Service (CSDS) solution extends dial-up capability through our synchronous, full-duplex, transparent, and all-digital circuit-switched networks from SDP to POP.

Our Circuit Switched networks support speeds ranging from DS0 to DS1 to on-net ad off-net locations. **Figure 1.4.2.3-1** highlights how the features of the Lumen CSDS solution satisfy the evaluation requirements.

**Figure 1.4.2.3-1. CSDS Feature Highlights**

Evaluation Criteria	Features of Lumen CSDS
Understanding [M.2.1.1]	<ul style="list-style-type: none"> <li>Lumen draws on experience providing CSDS to agencies such as FEMA and U.S. District Courts to meet Government requirements for traditional dial-up digital connectivity for both specialized applications and locations where infrastructure does not support newer options for digital data communication.</li> </ul>
Quality of Service [M.2.1.2]	<ul style="list-style-type: none"> <li>Compliant—Meets all functional and performance requirements in order to ensure that all EIS customers with specialized needs for CSDS receive the highest quality service.</li> <li>Scalable—Our expansive network makes our CSDS scalable to the changing needs of EIS customers. The recent merger between Lumen and tw telecom provides EIS customers thousands of new building-to-building connections with a higher quality, more reliable on-net experience. Our CSDS is integrated with our Toll-Free Services (TFS) platform, enabling alternative access methods.</li> <li>Reliable—Carries CSDS calls over the same digital network used for our voice service, with the same performance and quality standards.</li> <li>Resilient—Carries CSDS over the same digital network used for our voice service, with appropriate network redundancy and safeguards that ensure resiliency through a variety of conditions and events.</li> </ul>
Service Coverage [M.2.1.3]	<ul style="list-style-type: none"> <li>With more than 200,000 fiber route miles and 33,000 subsea route miles connecting more than 500 markets worldwide, global backbone provides CSDS services from the United States to more than 60 countries, facilitating video conferencing, bulk data transfer, and dial-up backup circuits.</li> <li>Applies industry best capabilities so that Government customers have end-to-end, digital circuit-switched communications, providing access through switched or dedicated facilities for greater flexibility and increased service coverage.</li> </ul>
Security [M.2.1.4]	<ul style="list-style-type: none"> <li>Lumen’s E-Line and E-LAN services provide agency networks the level of security and privacy similar to ATM or Frame Relay. Supported by a private SONET backbone dedicated bandwidth, our E-Line services ensure security and privacy.</li> <li>Integrates security measures through the use of authorization codes, routing calls to a switch that connects the user to the access authorization system for proper authorization before completing the connection.</li> </ul>

**1.4.2.3.1 Service and Functional Description [L.29.2.1, M.2.1, C.2.2.4]**

To enable access alternatives, our CSDS is integrated with our TFS, part of our overall solution to meet customer needs with flexible, scalable, and reliable service. To connect to the public phone network, our CSDS complies with Telcordia, ANSI T-1 and

---

ITU-TSS standards for ISDN and SS7, and encompasses all connectivity and transport requirements. We connect to and interoperate with a variety of switched data compatible equipment including PBX, Video CODECs, the Public Switched Telephone Network (PSTN) and all other EIS program CSDS contractors' networks. Key features include:

- **Dial-in, toll-free numbers for off-net locations.** Our CSDS is integrated with our TFS platform, enabling alternative access methods
- **User-to-user signaling via ISDN D-Channel.** Lumen CSDS provides this feature in accordance with ANSI T-1 and ITU-TSS standards for ISDN and SS7; CSDS can transfer ISDN signaling information transparently through the network between two SDPs, a functionality supported with minimal configuration changes
- **Performance reports.** Our monitoring and reporting features include metrics for availability, post-dial delay, and grade of service. Many of the performance indicators are available through authorized access on the myLevel3.com portal

Lumen's CSDS service offers dial up, bandwidth-on-demand service that allows customers to transmit in speeds at 1.54 Mbps. CSDS access is provided off-net through our partnerships with Local Exchange Carriers (LEC). We have interconnect arrangements with all major U.S. carriers; where LEC-switched access is currently unavailable, we arrange to establish the required access.

For switched access, we support a uniform numbering plan for all on-net Government locations. We assign a unique directory number to each station receiving service so that CSDS users can call each other without having to schedule calls.

#### **1.4.2.3.2 Standards [C.2.2.4.1.2]**

Lumen's CSDS solution complies with all applicable industry standards, including American National Standards Institute (ANSI) X3.189, International Telecommunications Union (ITU) E.72, International Telecommunications Union-Telecommunications Service Sector (ITU-TSS) and Electronic Industries Alliance (EIA) standards for Data Terminal Equipment (DTE) interfaces.

**1.4.2.3.3 Connectivity [C.2.2.4.1.3]**

Lumen’s CSDS solution provides maximum connection and interoperability with customer-specified terminations, the PSTN where available, all other EIS CSCS contractor’s EIS CSDS networks, and satellite phones and terminals. Our high-speed digital connectivity provides accurate CSDS transmissions while optimizing usage minutes, reducing usage-based costs.

**1.4.2.3.4 Technical Capabilities [C.2.2.4.1.4]**

Lumen’s CSDS solution meets the technical capability requirements and thresholds described in SOW C.2.2.4.1.4. **Figure 1.4.2.3.4-1** highlights elements of our compliant CSDS solution for each technical capability.

**Figure 1.4.2.3.4-1. CSDS Technical Capabilities**

LUMEN COMPLIES	SOW C.2.2.4.1.4 REQUIREMENT	LUMEN COMPLIANT SOLUTION
✓	1. Unified Numbering Plan	• Supports the ITU-TSS ISDN E.164 numbering system and addressing plan
✓	2. Authorization Codes for CSDS	• Supports the same authorization codes as those offered in voice services
✓	3. Bandwidth Limitations	• Switch technology accommodates a wide variety of bandwidths; agency users can dial up in 56 Kbps or 64 Kbps increments of digital bandwidth, up to a full switched T-1 (about 1.54 Mbps)
✓	4. Calling Capability without Scheduling	• A unique directory number is provided for each station receiving service, so that CSDS users can call each other without having to schedule calls
✓	5. Network-derived Clocking	• Accommodates network clocking platforms for data termination equipment or PBX/Multiplexer (MUX) at the SDP, ensuring synchronized network operation for delay-sensitive data types
✓	6. Data/Bit Transparency & Integrity	• Can transfer ISDN signaling information transparently through the network between two SDPs, a functionality supported with minimal configuration changes; after a call is established, all data bit sequences are transmitted transparently
✓	7. Dialable Bandwidth Categories: DS0, DS1, and Multirate DS0	• Tools accommodate multiple categories (DS0, DS1, and Multirate DS0) of EIS-required dialable information-payload bandwidth
✓	8. Bandwidth Category: Multirate DS0	• Network offers appropriate dial sequences and transport of all bit sequences associated with signaling and transport.
✓	1. – 2. Bandwidth Category: Multirate DS1 & DS3 (Optional)	• Lumen CSDS satisfies the optional multirate DS1 and DS3 bandwidth category requirements

LUMEN COMPLIES	SOW C.2.2.4.1.4 REQUIREMENT	LUMEN COMPLIANT SOLUTION
✓	3. – 5. SONET Categories: Levels I, II, and III (Optional)	<ul style="list-style-type: none"> <li>The Lumen CSDS solution meets the SONET Level -1, -II, and -III category requirements of the SOW. Lumen SONET/SDH network provides optimal capacity and performance</li> </ul>

**1.4.2.3.5 Features [C.2.2.4.2]**

Lumen’s CSDS provides the optional features specified in SOW C.2.2.4.3.

Figure 1.4.2.3.5-1 highlights the features of our compliant CSDS solution.

**Figure 1.4.2.3.5-1. Lumen CSDS Features**

LUMEN COMPLIES	SOW C.2.2.2.2 REQUIREMENT	LUMEN COMPLIANT SOLUTION
✓	1. Dial-in (Optional)	<ul style="list-style-type: none"> <li>Lumen provides optional connection via our all-digital switching systems and customized call handling and toll-free call support; with private numbering plans, screening tools, and authorization codes for added security and accountability</li> <li>Lumen has network connectivity with the PSTN and TFS infrastructure, independent of carrier, enabling dial-in flex bility. With switched access, both Toll-Free and PSTN numbers can be used for dial ii; dedicated access method for Toll-Free only numbers</li> </ul>
✓	2. User-to-User Signaling via ISDN D-Channel (Optional)	<ul style="list-style-type: none"> <li>Lumen provides optional user-to-user signaling through ISDN D-channel during a call. This signaling is separate from B-channel transmissions and supported in accordance with ANSI T1 and ITU-TSS standards</li> </ul>

**1.4.2.3.6 Interfaces [C.2.2.4.3]**

Lumen’s CSDS solution accommodates all the mandatory and optional interface types for EIS, as described in SOW C.2.2.4.3.

**1.4.2.3.7 Performance Metrics [M.2.1, C.2.2.4.4]**

Lumen meets all of the CSDS performance standards and thresholds listed in the CSDS Performance Metrics table in SOW C.2.2.4.4 by using industry standard monitoring tools that deliver a comprehensive visibility of numerous network elements and the ability to accurately measure AQLs for the applicable KPIs. Our GovNOCs

ensure that all CSDS network elements meet or exceed performance requirements for the EIS program.

**1.4.3 Contact Center Service [L.29.2.1, C.2.3]**

The Lumen Team’s CCS offering integrates best-in-class solutions from leading software vendors and unifies them into a holistic, cost-saving service model.

Lumen has partnered with [REDACTED]

**Lumen Team Contact Center Highlights**

- Developed on the Genesys platform - winner of the Gartner Magic Quadrant for Contact Center Infrastructure the past seven (7) years
- FedRAMP-Compliant; FISMA Moderate
- Pay-Per-Use Pricing Model

[REDACTED] The Lumen Team solution provides GSA and agencies flexible CCS capabilities that unify knowledge and case management, dashboard reporting, and multi-modal service channels into a single highly scalable solution for all inbound and outbound contact operations. **Figure 1.4.3-1** highlights the features to GSA for CCS.

**Figure 1.4.3-1. Features of Lumen’s CCS**

EVALUATION CRITERIA	FEATURES OF LUMEN CCS
Understanding [M.2.1.1]	<ul style="list-style-type: none"> <li>• The Lumen Team’s CCS offering integrates best-in-class solutions from leading software vendors and unifies them into a holistic, cost-saving service model</li> <li>• We provide GSA and Agencies flexible CCS capabilities that unify knowledge and case management, dashboard reporting, and multi-modal service channels into a single highly scalable solution for all inbound and outbound contact operations</li> </ul>
Quality of Services [M.2.1.2]	<ul style="list-style-type: none"> <li>• Our Team’s solution enables GSA and Agencies’ callers to communicate via a variety of web and mobile channels – interacting with customers via channels such as e-mail, chat, co-browse, SMS (text), Web Call Through, and Web Callback</li> <li>• Our teammate GDIT offers eServices that enable cross channel conversations which deliver a consistent customer experience for all customers, through one conversation over time, across phone, web, and mobile channels</li> </ul>
Service Coverage [M.2.1.3]	<ul style="list-style-type: none"> <li>• Geographically dispersed Lumen Team Contact Center facilities are interconnected to the Virtual Contact Center</li> <li>• The Lumen Team’s CCS is built on the proven, industry leading Genesys Customer Interaction Platform, which has an outstanding track record for availability</li> <li>• The Genesys routing engine offers best-in-class contact center functionality, providing the ability for each customer to reach the optimal CCS staff member based on the rules that make the most sense in support of agency requirements</li> <li>• Embedded analytics provide complete visibility into customer interactions, helping Lumen to deliver the most responsive customer experience</li> </ul>

EVALUATION CRITERIA	FEATURES OF LUMEN CCS
Security [M.2.1.4]	<ul style="list-style-type: none"> <li>• Our state-of-the-art GovSOC monitors the complete threat landscape with a continuous cycle of protection</li> <li>• Lumen monitors the status, traffic and data performance parameters on more than 200,000 fiber miles and globally</li> <li>• Lumen and our subcontractors perform security operations in accordance with industry best practices and standards supporting Cyber, Personnel and Physical Security</li> </ul>

**1.4.3.1 Service and Functional Description [L.29.2.1, M.2.1, C.2.3]**

Leveraging the technology of our CCS solution, GSA and Agencies are able to obtain a full suite of contact center services at our Team’s locations and agency facilities, or a combination of both, with flexible staffing models to ensure service coverage anytime and anywhere.

Our Team’s solution enables GSA and Agencies’ callers to communicate via a variety of web and mobile channels -- interacting with customers via channels such as e-mail, chat, co-browse, SMS (text), Web Call Through, and Web Callback. The Lumen CCS solution fulfills the mandatory service requirements for CCS contained in SOW C.2.3. This section presents a technical description of our offering, which consists of a virtual contact center architecture with contact center agents that are geographically dispersed to optimally provide 24/7 CCS support.

**Lumen Team CCS Quality Performance**

Our CCS solution is designed for 99.9% system availability and we are delivering at 99.9% and above based on customer requirements. For example, during the most recent peak season of January 1<sup>st</sup>- March 2<sup>nd</sup> 2015 for a current Contact Center customer (Federal Student Aid Information Center - FSAIC), we operated during the entire mission-critical peak period with 100% critical service-level availability; and consequently, exceeded the contractual FSAIC requirement of 99.8% availability (and the GSA EIS requirement of 99.9% availability) during the agency’s most crucial delivery period.

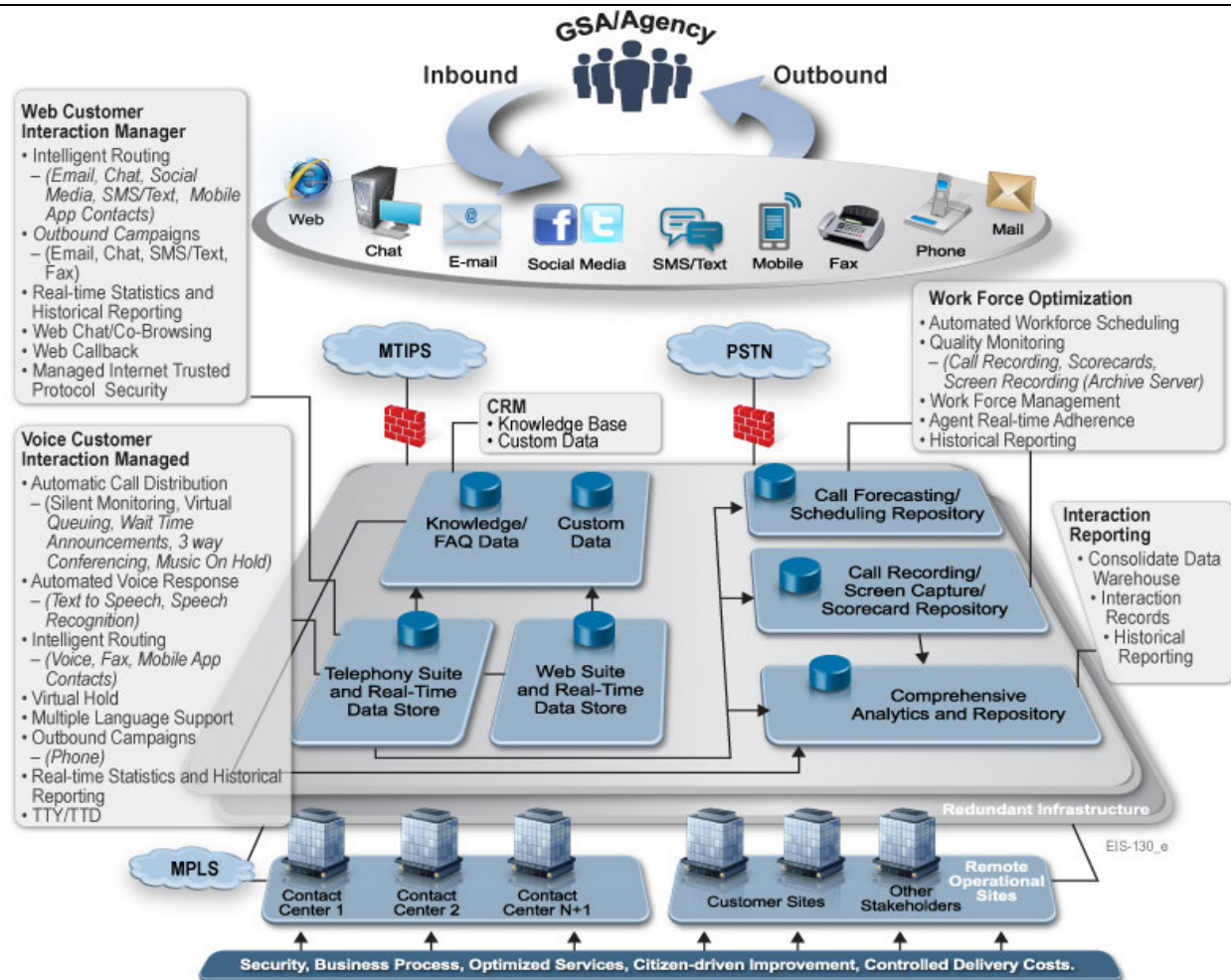
The Lumen Team’s CCS is built on the proven, industry leading Genesys Customer Interaction Platform, which has an outstanding track record for availability. The architecture of our technical approach is organized into three logical sub-systems: Customer Interaction Channel, Virtual Contact Center, and Contact Center Staff Facilities. Each is described below and illustrated in **Figure 1.4.3.1-1**.

---

**Customer Interaction Channel:** As shown at the top of **Figure 1.4.3.1-1**, The Lumen CCS accommodates inbound and outbound communications with customers seeking CCS support, through the internet and PSTN interaction channels.

**Virtual Contact Center:** Illustrated in the center portion of **Figure 1.4.3.1-1**, our Virtual Contact Center functions as the central mechanism which manages and provides the tools for us to provide compliant and very responsive CCS support. As shown in **Figure 1.4.3.1-1**, the Virtual Contact Center is a fully integrated, redundant and highly reliable cloud-based capability consisting of the following functional elements: Web Customer Interaction Manager, Voice Customer Interaction Manager, Customer Relations Management (CRM) Database, Work Force Optimization, and Interaction Reporting.

**Contact Center Staff Facilities:** As shown in the lower portion of **Figure 1.4.3.1-1**, CCS staff is located in geographically dispersed Lumen Team Contact Center facilities which are interconnected to the Virtual Contact Center cloud functions through redundant Lumen MPLS trunks. Staff at these facilities performs all contact center functions, using the cloud-based Virtual Contact Center resources and capabilities.



**Figure 1.4.3.1-1. Lumen Team's Contact Center Solution Overview.** *The Lumen CCS solution architecture provides all required functionality.*

### 1.4.3.2 Standards [C.2.3.1.2]

Lumen's CCS offering is compliant with the mandatory standards listed in SOW C.2.3.1.2. We comply with optional standards listed in SOW C.2.3.1.2 as applicable, in accordance with TO requirements. Members of our Team have considerable years of training, applicable certifications, are active in a variety of industry forums and working groups. We are also committed to implementing future standards as technologies are developed and standards are defined and become commercially available.



**1.4.3.3 Connectivity [C.2.3.1.3]**

The Lumen network provides all of the CCS connectivity required. The Lumen Team’s CCS connects and interoperates with the PSTN. Our Team’s has widespread experience working with both commercial telephony services and federal Network providers to establish connectivity to the PSTN. We leverage this experience to support connectivity to the PSTN through the full range of available options from high capacity aggregated traditional Time Division Multiplexed (TDM) and VoIP trunks through individual regular business lines.

**1.4.3.4 Technical Capabilities [C.2.3.1.4]**

Figure 1.4.3.4-1 shows how the Lumen EIS CCS fully complies with all SOW technical capabilities requirements. All technical capabilities addressed are mandatory.

**Figure 1.4.3.4-1. CCS Technical Capabilities**

LUMEN COMPLIES	SOW C.2.3.1.4 REQUIREMENT	LUMEN COMPLIANT SOLUTION
✓	C.2.3.1.4.1 CCS Delivery Methods	<ul style="list-style-type: none"> <li>The Lumen Team is fully compliant to the requirements.</li> </ul>
✓	1. Host Based Call Management Service	<ul style="list-style-type: none"> <li>The Lumen Team provides the hardware, software, inside wiring, power, and all other components required to deliver Host Based Call Management Service at our contractor-provided location.</li> </ul>
ü	2. Premises Based Call Management Service	<ul style="list-style-type: none"> <li>Our Team provides all components required for CCS Premises Based Call Management Service, including hardware and software. Our technicians and engineers install, configure, and maintain the CCS equipment, using agency power and inside wiring, at agency-provided location/s.</li> </ul>
✓	3. Premises Based Call Answering Service	<ul style="list-style-type: none"> <li>The Lumen Team provides personnel to perform Premises Based Call Answering Service at an agency provided location. The service we provide includes Premises Based Call Management.</li> </ul>
✓	4. Host Based Call Answering Service	<ul style="list-style-type: none"> <li>Our Team provides Host Based Call Answering Service at our contractor provided location. The service we provide includes Host Based Call Management. In providing Host Based answering service, we use Lumen work space, furniture, hardware and software, and building utilities.</li> </ul>
✓	C.2.3.1.4.2 CCS Call Management Service	<ul style="list-style-type: none"> <li>The Lumen Team is fully compliant to the requirements.</li> </ul>
✓	1. Provide capability for a network call queue	<ul style="list-style-type: none"> <li>Our CCS routing engine funnels all incoming multi-media channels to a single universal queue (or to multiple queues, if required by the agency). We manage the routing and distribution of contacts from a variety of multi-media sources, including voice, email, facsimile, and an agency Web site.</li> </ul>

**General Services Administration (GSA)**  
**Enterprise Infrastructure Solutions (EIS)**

Contract # GS00Q17NSD3006  
 Mod #: P00310  
 Submission #: CL01001.01a

LUMEN COMPLIES	SOW C.2.3.1.4 REQUIREMENT	LUMEN COMPLIANT SOLUTION
✓	2. intelligent routing and distribution of contacts	<ul style="list-style-type: none"> <li>We provide intelligent routing and distribution of contacts in accordance the real-time operating status of ordering agency contact center/s and their business rules.</li> </ul>
✓	3. Interoperate with the ordering Agencies' CCS communications channels	<ul style="list-style-type: none"> <li>Our CCS interoperates with the ordering Agencies' CCS communications channels to seamlessly orchestrate and manage interactions through email, voice, facsimile, and Websites to create a dynamic and personalized customer experience.</li> </ul>
✓	4. Traverse and interoperate with firewalls and layers	<ul style="list-style-type: none"> <li>Our CCS solution can be configured to operate with and traverse agency firewalls and various security layers.</li> </ul>
✓	5. Support service observation	<ul style="list-style-type: none"> <li>We provide the capability for support service observation of both local and remote agents that is secure and is only available to authorized local and remote agency individuals. This capability also allows agents to invite their supervisors to calls when dealing with customers.</li> </ul>
✓	6. Capability to manage queues, algorithms, agent profiles, and reports	<ul style="list-style-type: none"> <li>The CCS we provide gives ordering Agencies that ability to manage call routing algorithms, network queues, reports, and contact center agent profiles. We provide the administrative capabilities specified in the SOW, allowing authorized agency individuals to make real time and scheduled changes.</li> </ul>
✓	7. Provide reports as required by the OCO	<ul style="list-style-type: none"> <li>Our CCS provides reports as they are required by the OCO.</li> </ul>
✓	8. Provide access to reporting of queue status	<ul style="list-style-type: none"> <li>Our CCS dashboard allows ordering agency access to real-time graphical reports of the CCS queue status. Our dashboard allows flexible customization of views and reporting.</li> </ul>
✓	9. Provide the capability to inform the caller of the queue status	<ul style="list-style-type: none"> <li>Our solution has the capability to provide queue status and estimated wait time to callers, as well as provide Agencies the ability to change/customize recorded announcements.</li> </ul>
ü	10. Transmit and deliver music on hold (or recordings)	<ul style="list-style-type: none"> <li>Our solution delivers the capability for music on hold or recordings to be provided to originating callers. Our solution allows for agency provided or Lumen provided music or recordings.</li> </ul>
✓	11. Supply terminal devices	<ul style="list-style-type: none"> <li>Our Team provides terminal devices such as circuit switched phones, IP phones, and softphones required for provision of CCS if required. Terminal devices provided support caller ID, and optionally name/message displays.</li> </ul>
✓	12. Provide the capability to accommodate agency contact center closings	<ul style="list-style-type: none"> <li>Our solution provides intelligent routing which is fully capable of accommodating contact center closings, providing announcements and re-routing of incoming contacts using customizable pre-recorded or hot insert messages.</li> </ul>
✓	C.2.3.1.4.3 CCS Call Answering Service	<ul style="list-style-type: none"> <li>The Lumen Team is fully compliant to the requirements.</li> </ul>
✓	1. Provide a CCS call answering service	<ul style="list-style-type: none"> <li>The Lumen Team delivers the required CCS Call Answering Service, using technology, processes and staffing that are exemplified by past performance and industry recognition.</li> </ul>
✓	2. Call answering service requirements	<ul style="list-style-type: none"> <li>Lumen meets the following minimum CCS Call Answering Service requirements.</li> </ul>

LUMEN COMPLIES	SOW C.2.3.1.4 REQUIREMENT	LUMEN COMPLIANT SOLUTION
✓	2.a). Receive and respond to caller inquiries	<ul style="list-style-type: none"> <li>We are well prepared to receive caller inquiries through the Genesys CIM platform during agency operating hours, within agreed upon KPIs.</li> </ul>
✓	2.b). Manage caller inquiries	<ul style="list-style-type: none"> <li>We apply our reliable and capable CCS technology and processes to manage and respond to calls during non-operational hours and holidays.</li> </ul>
✓	2.c). CSS interoperation	<ul style="list-style-type: none"> <li>We ensure that the CCS is interoperable with the ordering Agencies' identified databases and back office systems if required under specific TOs, delivering customer service functions as specified, at agreed upon performance levels.</li> </ul>
✓	2.d). Accommodate all CCS callers	<ul style="list-style-type: none"> <li>The Lumen Team provides the capability to accommodate all CCS callers, including those with foreign language requirements and disabilities.</li> </ul>
✓	2.e). Capability to quickly increase capacity	<ul style="list-style-type: none"> <li>The Lumen Team applies our extensive CCS experience in providing the most expeditious and reliable CCS capacity increase. As a practice we size the solution so it can quickly prepare or adapt for unforeseen demand on the system. Providing additional language support is also easily managed through the Language Line service.</li> </ul>
✓	3. Provide call answering resources as needed	<ul style="list-style-type: none"> <li>The Lumen Team provides the basic call answering resources specified in SOW Table C2.3.1.4.4 as needed to meet the requirements of agency TOs.</li> </ul>

**1.4.3.5 Features [C.2.3.1.5]**

Lumen CCS provides 14 mandatory features specified in SOW C.2.3.1.5. **Figure 1.4.3.5-1** shows how the Lumen EIS CCS complies with SOW features requirements.

**Figure 1.4.3.5-1. CCS Features**

LUMEN COMPLIES	SOW C.2.3.1.5 REQUIREMENT	LUMEN COMPLIANT SOLUTION
✓	1. Call Recording and Monitoring	<ul style="list-style-type: none"> <li>Lumen provides the call recording and monitoring functions and capabilities specified by the SOW. Our Team's digital recording and monitoring solution provides the ability to capture and retrieve inbound and outgoing customer contacts and experience through voice, email, or through web self-service channels, as well as associated interaction data (screen capture).</li> </ul>
✓	2. Collaborative Browsing	<ul style="list-style-type: none"> <li>Our collaborative browsing solution allows bi-directional sharing of web pages between the contract center agent and the caller. It supports requests for co-browse sessions and is capable of highlighting text, navigating to specific areas of a web page, pushing web pages, and allowing seamless transfer to another agent without losing focus. Actions that the participants in a co-browsing session can perform together are navigate web sites; conduct online transactions; fill out web forms; interact with Web-based software applications; download files, playing audio, or watching video streams.</li> </ul>
✓	3. Computer Technology Integration	<ul style="list-style-type: none"> <li>We provide Computer Telephony Integration (CTI) capability enabling the transfer of caller information, agency specified data and systems, IVR inputs, and other data to the agent</li> </ul>

LUMEN COMPLIES	SOW C.2.3.1.5 REQUIREMENT	LUMEN COMPLIANT SOLUTION
	(CTI)	directly associated with the inbound call. Our solution supports agency applications such as, intelligent routing, keyboard dialing, third party call control, pop/splash, and multi-channel call blending.
✓	4. Customer Contact Application	<ul style="list-style-type: none"> <li>Our CCS solution provides the capability to track, document, and manage the CCS customer contacts across multiple contact channels. The agent desktop records caller contact, account, call history, inquiry status, nature of inquiry, date and time information, call disposition, and agent detail. The desktop creates cases for every inquiry by channel and has robust workflows and business rules to assign and escalate cases to the best resource. Our solution also provides management reports, and the capability to created and provide scripted responses for contact center agents.</li> </ul>
✓	5. Email Response Management	<ul style="list-style-type: none"> <li>Our E-mail Response Management (ERM) solution provides all of the capabilities required by the SOW. Through our ERM capability, a tracking ID is assigned to each email, allowing the handling and routing of email communication according to agency specified business rules.</li> </ul>
✓	6. Interactive Voice Response (IVR)	<ul style="list-style-type: none"> <li>Our CCS solution includes Interactive Voice Response (IVR) capabilities that allow callers to gain information based upon DTMF keypad entries or via speech recognition. We provide all of the capabilities specified in SOW</li> <li>C.3.1.2.6. The Genesys Voice Platform (GVP) we use enables the quick and easy delivery of integrated speech or touch-tone applications to automate caller self-service transactions.</li> </ul>
✓	7. IVR – Agency Based Database (Host Connect)	<ul style="list-style-type: none"> <li>We provide the capability to route calls or provide information based on queries into single or multiple ordering agency databases, located at the ordering agency premises. Our sophisticated IVR capability is able to retrieve, review and modify information from agency databases that are either hosted on a mainframe or are server based. Our solution can access data from legacy mainframe or non-relational DBMSs by utilizing a built-in, remote procedure call to enterprise-specific applications.</li> </ul>
ü	8. Reserved	<ul style="list-style-type: none"> <li>No requirement is stated in the SOW.</li> </ul>
✓	9. IVR – Speech Recognition	<ul style="list-style-type: none"> <li>Lumen provides IVR natural speech recognition capabilities in both American English and American Spanish dialects, with an accuracy of 95% or greater, as required by SOW C.2.3.1.2.9.</li> </ul>
✓	10. Language Interpretation Service	<ul style="list-style-type: none"> <li>Lumen provides telephone language interpretation services, delivering on-demand three-way conferencing capability with a foreign language caller, the contact center agent, and our language service professional, who provides language interpretation within one minute of request. With our solution, we provide interpretation service for over 200 languages, including English, Spanish, and all of the other most common major languages of the world.</li> </ul>
✓	11. Outbound Dialer	<ul style="list-style-type: none"> <li>Lumen provides all of the outbound dialing capabilities specified in SOW C.2.3.1.2.11. The dialing service we provide supports either centralized or distributed contact center environments as required by ordering Agencies.</li> </ul>

LUMEN COMPLIES	SOW C.2.3.1.5 REQUIREMENT	LUMEN COMPLIANT SOLUTION
✓	12. Text Chat (Web Chat)	<ul style="list-style-type: none"> <li>Our CCS solution provides the capability for contact center agents to conduct real time web text chat with callers in compliance with the requirements of SOW C.2.3.1.2.12.</li> </ul>
✓	13. Web Call Back	<ul style="list-style-type: none"> <li>Our solution enables customers to select an immediate or scheduled callback at the number of their choosing, offering the ability to see status and cancel a callback request. Our solution automatically routes call back requests to the most appropriate available agent.</li> </ul>
✓	14. Web Call Through	<ul style="list-style-type: none"> <li>Our solution provides a click to talk solution that is fully integrated into the CCS technology, which allows callers to directly initiate a voice conversation with agents directly from websites, without the need to install an additional third-party application.</li> </ul>
✓	15. Workforce Management	<ul style="list-style-type: none"> <li>Our solution provides a workforce management (WFM) system that automates and optimizes call center personnel scheduling based on historical data to provide a more accurate forecast of call volumes and to effectively schedule resources across all interaction types, agent skills, skill levels and shifts, for single or multiple sites and blended applications.</li> </ul>
✓	16. Virtual Queue	<ul style="list-style-type: none"> <li>Our CCS solution provides automated callback capability. The solution calculates and quotes the expected wait time if there are calls in the queue. The caller will be provided with a choice to either remain on the line for the next available and best skilled agent to answer their inquiry, or to receive a callback in the same amount of time as if they had waited on hold, or to schedule a callback for a more convenient time.</li> </ul>

**1.4.3.6 Interfaces [C.2.3.1.6]**

The Lumen CCS meets the interface requirements in SOW C.2.3.1.6. The CCS we provide rides on our robust, reliable, and capacious Lumen global network.

**1.4.3.7 Performance Metrics and Quality of Services [M.2.1, C.2.3.1.4, G.8]**

Lumen meets all of the CCS performance metrics shown in the CCS Performance Metrics table in SOW C.2.3.1.4. The Lumen GovNOC monitors all Lumen Enterprise services provided using our network.

**Colocated Hosting Service**

- Lumen operates 126 colocation data centers in the U.S. and another 27 around the world.
- Lumen data centers offer high power densities, and feature concurrently maintainable power and cooling, high security, and outstanding connectivity to meet the most demanding colocation requirements.
- Data centers are located directly on the Lumen network backbone, featuring virtually unlimited capacity.

**1.4.4 Colocated Hosting Service [L.29.2.1,**

**C.2.4, C.4.4]**

Lumen offers compliant Colocated Hosting Service (CHS) in more than [REDACTED] [REDACTED] locations around the world in more than 15 countries. Approximately [REDACTED] [REDACTED] are in the U.S. Lumen data centers offer exceptional connectivity – all of them are located on the Lumen backbone and many feature multiple carrier options.

**Figure 1.4.4-1** highlights the features of the Lumen CHS solution aligned with the evaluation criteria.

**Figure 1.4.4-1. Features Lumen CHS**

EVALUATION CRITERIA	FEATURES OF LUMEN CHS
Understanding [M.2.1.1]	<ul style="list-style-type: none"> <li>Lumen is a recognized, established worldwide provider of CHS with 153 data center locations around the world, 126 of which are in the U.S.</li> </ul>
Quality of Service [M.2.1.2]	<ul style="list-style-type: none"> <li>Lumen CHS data centers feature concurrently maintainable power and cooling systems, which results in the high levels of reliability and resilience required to support agencies' mission critical applications.</li> <li>All Lumen data centers are located directly on the Lumen backbone.</li> <li>Lumen's DCIM, Alerton, can provide Agencies information in real time about data center conditions and specific information about an agency's colocated systems.</li> </ul>
Service Coverage [M.2.1.3]	<ul style="list-style-type: none"> <li>Lumen offers CHS from 126 data centers in 63 CBSAs, including 112 such facilities in 50 of the Top 100 CBSAs named in SOW J.1.4.1.</li> </ul>
Security [M.2.1.4]	<ul style="list-style-type: none"> <li>All Lumen data centers are located in physically secured buildings with minimal and strictly controlled access, often with biometric bases.</li> <li>Lumen and our subcontractors perform security operations in accordance with industry best practices and standards supporting Cyber, Personnel and Physical Security.</li> </ul>

**1.4.4.1 Services and Functional Description [L.29.2.1, M.2.1, C.2.4.1, G.8]**

Lumen's 153 data centers offering CHS feature concurrently maintainable power and cooling systems, which results in the high level of availability required to support mission-critical applications. Lumen provides the Government and its representatives 24x7 access to leased space and GFP at co-location facilities. Key attributes of Lumen CHS data centers include:

- Lumen managed IT (support and maintenance of applications and servers)
- High power densities - up to 75 watts/square foot and up to 5 KW/rack inside a suite with select locations offering up to 200 watts/square foot and up to 10 KW/rack inside a suite

- 
- Redundant, concurrently maintainable power and cooling systems (N+1 AC power, N+1 cooling)
  - High facility security with strictly controlled access

Lumen data centers in Ashburn, VA and Denver, CO are designated as facilities to serve as DHS EINSTEIN Enclaves capable of hosting DHS GFP. Like all Lumen CHS sites, these locations feature exceptional network connectivity.

Lumen has developed [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

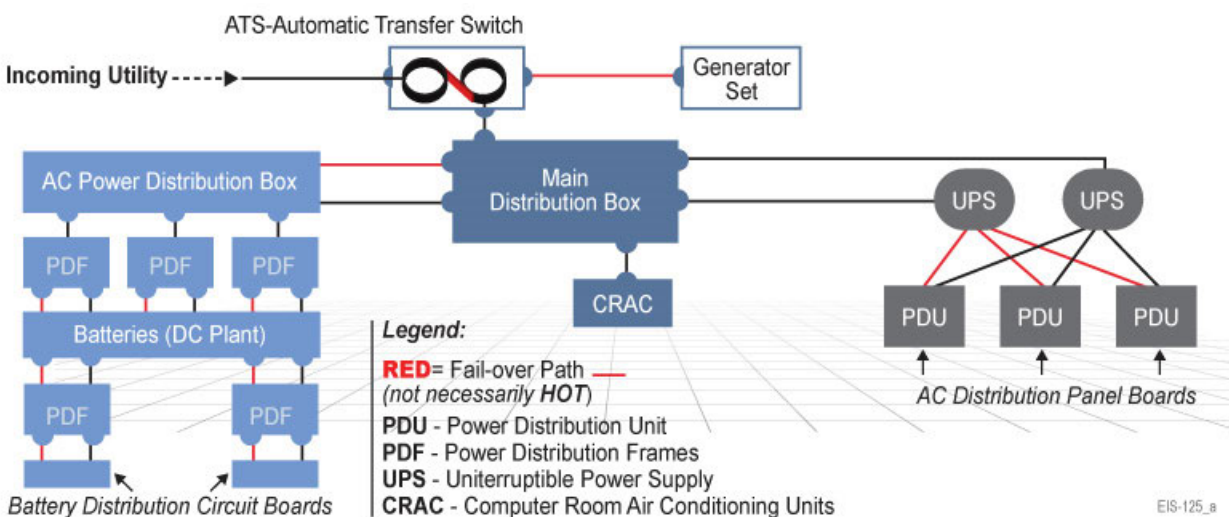
All Lumen data centers are located directly on the Lumen backbone. This reduces metro access costs, reduces latency, provides virtually unlimited capacity levels, and greatly simplifies connectivity to cloud services from your collocated equipment. All data centers remain carrier neutral. Offering maximum flexibility, collocation options range from the sub-rack level to custom cages, and suites. Rapidly deployable, pre-built collocation cabinets (28"W x 36"D x 85"H) offer pre-configured power. The fully enclosed and lockable metal cabinets and provide visual isolation and a high level of security. They can accommodate 19" or 23" racks. Private cages and suites in Lumen data centers offer the ability to tailor space to meet specific technical and security requirements.

For power, a range of amperages are available for 120 VAC (single phase) and 208 VAC (single or three phase). Other options can be provided.

All Lumen data centers are located in physically secured buildings with minimal and strictly controlled access, often with biometric bases. Facilities typically are supplied by at least two utility power feeds, and are designed with redundancy in the critical power and cooling systems. The critical power chain includes Uninterruptible Power Supplies (UPS) which can accept either the utility feed or a generator-sourced power. In our U.S. facilities, HVAC units are equipped to support typical computer room

applications with humidifiers and electric re-heat coils to control humidity. Raised floor construction with perforated floor tiles creates hot and cold aisles in the data center.

All facilities feature smoke detection (Very Early Smoke Detection Apparatus, VESDA) and fire suppression systems designed for application in data centers (e.g., dry pipe systems). **Figure 1.4.4.1-1** is representative of a Lumen data center's automated failover architecture for one incoming feed of utility power and one generator. The battery back-up plant attached to the UPS is designed to carry the full AC-powered load for 15 minutes, although generators are typically engaged and operational in less than 30 seconds. The back-up plant for DC systems, rated for 8-hour reserve time at 100% load, is also shown.



**Figure 1.4.4.1-1. Representation of Lumen Data Center Automated Failover Architecture. Redundancy and automatic failover are key to availability.**

Nearly all Lumen CHS data centers are colocation service-certified for Statement on Standards for Attestation Engagements (SSAE) 16 Type 1 or Type 2, and Payment Card Industry Data Security Standard (PCI DSS) Version 2.0 or 3.0 or they are in the certification process.

Note that Lumen has some 100 additional data center facilities – not presented for CHS – that nevertheless meet the needs of telecommunications network equipment. For example, such facilities may be suitable to house Government optical network



equipment. The attributes and conformance of Lumen CHS with all SOW requirements are discussed in the following sections.

**1.4.4.2 Standards [L.29.2.1, M.2.1, C.2.4.2, G.8]**

Lumen CHS data centers comply with TIA-942, Telecommunications Infrastructure Standard for Data Centers, typically at the Tier 3 level.

NIST SP800-53 Rev 4, Security and Privacy Controls for Federal Information Systems and Organizations, almost fully applies to information systems housed in a data center. However, there are a few controls, largely within the Contingency Planning (CP), System Maintenance Policy and Procedures (MA), and Physical and Environmental Protection (PE) control areas that do relate to the pertinent data center and its operations. Examples of these are CP-8, Telecommunications Services; MA-5, Maintenance Personnel; and PE-3, Physical Access Control. Lumen data centers satisfy such security and privacy controls.

Compliance with ICD 705, 26 May 2010, Sensitive Compartmented Information Facilities (SCIF), is TO specific and satisfied at the TO level.

**1.4.4.3 Connectivity [L.29.2.1, M.2.1, C.2.4.3, G.8]**

As noted, all Lumen data centers are located directly on the Lumen backbone. Therefore, for CHS Lumen is well positioned to provide external connectivity as defined at the TO level.

**1.4.4.4 Technical Capabilities [L.29.2.1, M.2.1, C.2.4.4, G.8]**

Lumen’s compliance with the technical capabilities requirements for CHS outlined in SOW C.2.4.4 are summarized in **Figure 1.4.4.4-1**, below. Detailed customer requirements can be listed at the TO level.

**Figure 1.4.4.4-1. Technical Capabilities of Lumen CHS**

LUMEN COMPLIES	SOW C.2.4.4 REQUIREMENT	LUMEN COMPLIANT SOLUTION
✓	1. General procedures and support	<ul style="list-style-type: none"> <li>• Lumen CHS is compliant with all items, a) through f).</li> <li>a) Requirements, duties, and responsibilities outlined in this section for data centers are common in nearly all well run data centers, including those of Lumen.</li> <li>b) Site preparation including security measures, equipment receipt and storage are offered by</li> </ul>

LUMEN COMPLIES	SOW C.2.4.4 REQUIREMENT	LUMEN COMPLIANT SOLUTION
		Lumen at its data centers. Details are specified at the TO level. c) Relocation of GFE, details are specified at the TO level. d) Final preparation for site installation with physical space, environmental systems, and network connectivity to be available on a 24/7 basis (unless mutually agreed upon and specified) is supported by Lumen at its data centers. Some details may have to be specified at the TO level. e) Facilitation of GFE setup (or takedown) as well as the expedient determination of inter-compatibility and inter-operability are supported by Lumen. f) Lumen ensures that all Lumen and Lumen contractor personnel have the required national citizenship, security clearances, training, and technical certifications to receive, use, maintain, manage, operate, package, transport, or ship sensitive and secure GFP.
✓	2. Access to GFE by authorized personnel	<ul style="list-style-type: none"> <li>Assuming they are following pertinent procedures, granting authorized users access to their equipment is a routine matter in Lumen data centers. Therefore, authorized Government personnel and third-parties shall have access to GFP at specified times, in specified locations, as mutually agreed upon between the Government and Lumen, subject to Lumen's applicable Acceptable Use Policy (AUP), except where the AUP conflicts with Government policy, or other Government executive orders, regulations or laws.</li> </ul>
ü	3. Service management remote monitoring	<ul style="list-style-type: none"> <li>Lumen's [REDACTED] can capture and present status information to the user in real-time to monitor the facility and equipment.</li> </ul>
✓	4. Service management alarms	<ul style="list-style-type: none"> <li>[REDACTED] can capture and present alarms to the user in real-time for facility and communications failures. Often users' own management systems alert them to communications failures, the source of which can be their equipment, possibly beyond what Lumen can see.</li> </ul>
✓	5. Service management updates	<ul style="list-style-type: none"> <li>[REDACTED] can collect and report data on cooling, temperature, smoke detection, connectivity and rack (breaker level) power. Updates on entry/exit log data are defined at the TO level as this information can be collected in several different ways, which could require different [REDACTED] interfaces.</li> </ul>

**1.4.4.5 Features [L.29.2.1, M.2.1, C.2.4.5, G.8]**

As required, Lumen provides CHS in a SCIF per ICD 705 according to details to be specified at the TO level.

**1.4.4.6 Interfaces**

None specified for CHS.

**1.4.4.7 Performance Metrics [L.29.2.1, M.2.1, C.2.4.5.1, G.8]**

Lumen complies with all CHS Performance Levels and AQL of KPIs specified in SOW C.2.4.5.1 and measured in accordance with the notes of the SOW. In addition, Lumen offers SLAs on several key elements of its data center colocation service. These service levels include: colocation installation, cross connection installation, and power availability. The latter, which is applicable for sites with Lumen conditioned power, suggests an AOL of  $\geq 99.999\%$  (exclusive of excused outages).

**1.4.5 Cloud Services [L.29.2.1, C.2.5; C.4.4]**

Whether directly because of mandates such as the OMB Cloud First Policy or secondarily through those such as the Federal Data Center Consolidation Initiative (FDCCI), a number of forces are driving agencies to migrate to cloud services. Regardless of the driving factor, the reliance on cloud-based services continues to increase. Yet despite cloud services' already prominent role, they in fact still represent a new, rapidly changing industry.

**Lumen Team Cloud Services**

- As a Cloud Broker Lumen can tailor cloud solutions across a needs spectrum.
- Cloud Team members contribute a range of attributes and assets to our cloud solutions.
- For security and security flex bility, cloud traffic will be processed as required by one of Lumen's TICs or the CSP's own overlay TIC.
- Lumen's Cloud Connect Solutions plus Dynamic Capacity offer unique advantages in security, capacity surge management and cost control.

In light of this rate of change, Lumen draws on its partner-management strengths and takes a teaming or cloud service brokering approach to delivering cloud solutions. All Lumen Team Cloud Service Providers (CSP) satisfy the five essential characteristics and four deployment models of cloud services defined in NIST SP 800-145. **Figure 1.4.5-1**, below, summarizes the Lumen Team CSPs and their offerings in this response.

**Figure 1.4.5-1. Summary of Lumen Team CSPs**

CLOUD SERVICE PARTNER	CAPABILITIES SUMMARY	IASS	PAAS	SAAS
[REDACTED]	[REDACTED]		✓	✓
[REDACTED]	[REDACTED]	✓		
[REDACTED]	[REDACTED]	✓	✓	✓
[REDACTED]	[REDACTED]	✓		✓
[REDACTED]	[REDACTED]			

---

In addition, all Lumen Team members are FedRAMP certified or well into the process (discussed in Section 1.4.5.1) and all cloud traffic subject to security processing is processed by either Lumen's cloud service TIC(s) (the basis of Lumen MTIPS, Section 1.4.8.3) or, for those that have them, the CSP's overlay TIC. As TIC operation and certification is extremely complicated, Lumen's ability to provide a TIC for cloud services can widen the field of potential CSPs and/or assure a maximum level of security.

Given that certain work-loads and applications might perform better in one Cloud Service Provider (CSP) environment versus another, under our flexible approach, Lumen can offer a solution tailored to the specific needs of a given TO. The flexibility of our approach extends to other contracting issues. For example, some of our cloud service partners could satisfy requirements for small business set-asides.

As discussed in the following sections, regardless of the particular cloud service or deployment model, the Lumen Team supports all requirements including all services and capabilities, all standards, all features and connectivity options, all interfaces, and all performance metrics defined within the C.2.5 sections of the SOW.

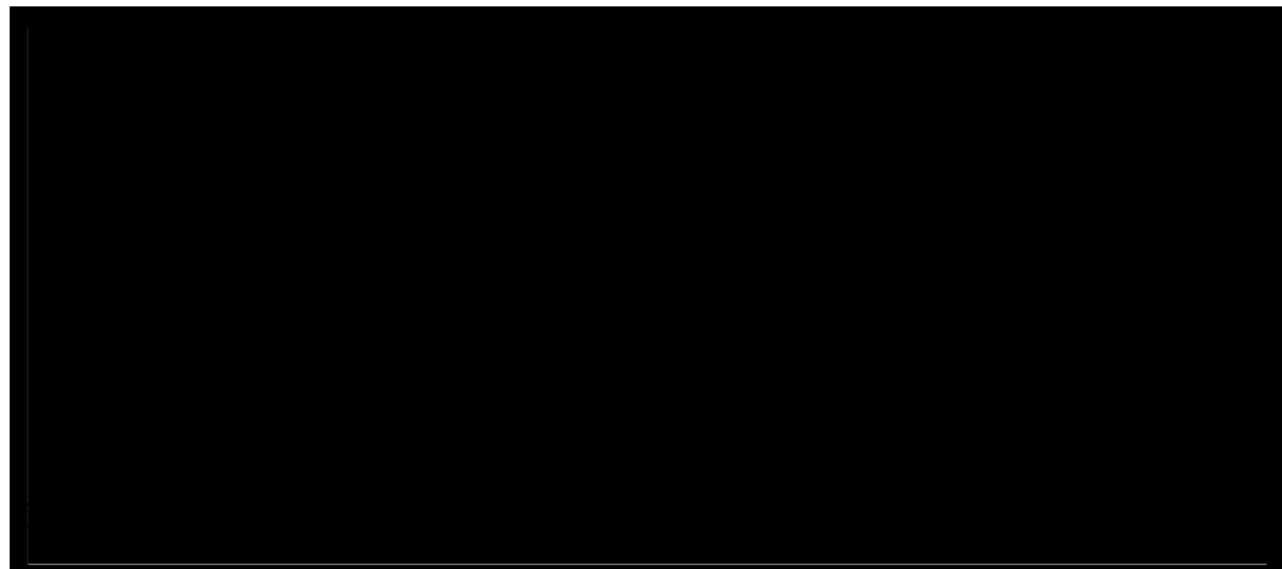
### **Lumen Connects You to the Cloud**

Unifying our teaming approach to providing cloud services is the Lumen network, which interconnects all solution elements. For example, Lumen's Cloud Connect solutions portfolio effectively places an agency's cloud resources *directly onto that agency's secure, private Layer 3 or Layer 2 network from Lumen (i.e., part of the same VRF or VFI)*. Secure, direct Layer 1 connectivity is an option as well. Therefore, compared to cloud access via the Internet, access is more expandable and flexible, higher performing, more reliable, and more secure. The pool is expanding, but major CSPs already part of Cloud Connect are [REDACTED]

[REDACTED] **Figure 1.4.5-2(a)** provides an overview of Lumen's expanding Cloud Connect solutions portfolio as well as highlights a

distinguishing benefit of Lumen's cloud connectivity - its ability to expand in response to surge conditions as they impact network access.

It is one matter to handle surges at Lumen/CSP interconnection points, but an entirely different one to handle them *at network access*. This is where the Dynamic Capacity feature of Lumen's Adaptive Network Control capability proves its merit by supporting surges in access bandwidth in step with surges in your cloud needs – and does so cost-effectively. These increases in bandwidth can be based either on utilization, a schedule, or on an ad hoc basis. Increases based on utilization are particularly useful in allaying concerns about meeting surges in cloud needs.



**Figure 1.4.5-2. Lumen Cloud Connect Solutions Portfolio.** *Cloud Connect offers multiple options for private, secure, high performance connectivity to an agency's cloud resources. For simplicity and focus on connectivity, no TIC is shown.*

Lumen has other solutions to connect an agency with its cloud resources as shown in **Figure 1.4.5-2(b)**. For example, many data centers are on-net with the Lumen network including [REDACTED]. In such cases, high performance, expandable and secure connectivity can be established between an agency's key locations and its cloud resources.

The Lumen approach to cloud services, brokering and managing teams tailored to meet specific requirements and unifying solutions with skilled management and a powerful network, results in low-risk, high-value cloud solutions under EIS.

**1.4.5.1 Infrastructure as a Service (IaaS)**  
**[L.29.2.1, C.2.5.1; C.4.4]**

Agencies have embraced cloud-based services on the basis of value and speed at which cloud service providers can incorporate advances in technology and address security vulnerabilities. Still a relatively new field, cloud services remain defined by rapid developments, time-to-market pressures, solution diversity, and overall complexity.

**Lumen Team IaaS**

- For IaaS, as a Cloud Broker Lumen can tailor solutions across a needs spectrum that can include provider choice, geography, small business procurement requirements, etc.
- Team members' considerable IaaS experience, including that of AWS, reduce IaaS transitional and operational risks in EIS.
- As needed, Lumen can provide TIC services for its Team members, potentially expanding agencies' supplier pool to foster competition.

In light of these, Lumen takes a teaming or brokerage approach to provide these services. For IaaS, Lumen team members include [REDACTED]

[REDACTED]

[REDACTED] **Figure 1.4.5.1-1** provides examples of Team Members' experience.

**Figure 1.4.5.1-1. Representative Lumen Team Member IaaS Experience**

LUMEN IAAS TEAM MEMBER	SAMPLE CUSTOMER AND IAAS EXPERIENCE
[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]

[REDACTED]

Under no circumstances will Lumen bid a solution to a Task Order (TO) that is not FedRAMP authorized. This paragraph underlies our references to FedRAMP compliance for all cloud services.

As an integrator, Lumen can team with the most appropriate supplier to address specific requirements for IaaS or other cloud service. Harnessing its transport network to interconnect providers' sites, Lumen can even offer an agency a unified IaaS solution using more than one of our Team partners.

Lumen's approach can offer a superb and dynamic fit to agency requirements, even in the face of rapid change. The flexibility afforded by this approach is extremely important to agencies across the Government.

Figure 1.4.5.1-2 highlights the features of the Lumen IaaS solution aligned with the evaluation criteria.

**Figure 1.4.5.1-2. Features of Lumen Team IaaS**

Evaluation Criteria	Features of Lumen Team IaaS
Understanding [M.2.1.1]	<ul style="list-style-type: none"> <li>The Lumen Team's understanding of IaaS in the GSA environment is supported by the experience of Team members and, for the AWS resellers, AWS' unique experience and understanding.</li> <li>Harnessing its transport network to interconnect providers' sites, Lumen can even offer an agency a unified IaaS solution using more than one of our Team partners.</li> </ul>
Quality of Service [M.2.1.2]	<ul style="list-style-type: none"> <li>Proven partners such as AWS have demonstrated their service quality and the Lumen Team IaaS satisfies all performance metrics outlined in SOW C.2.5.1.4.</li> <li>Lumen Team IaaS solutions are fully compliant with EIS requirements.</li> <li>Team members' architectures feature considerable redundancy and site diversity, and are designed for resilience and reliability. Lumen's powerful connectivity helps ensure these features, plus scalability.</li> <li>As an integrator and cloud service broker, Lumen teams with the most appropriate supplier(s) to address specific requirements for IaaS or other cloud service.</li> </ul>
Service Coverage [M.2.1.3]	<ul style="list-style-type: none"> <li>Through its partners, Lumen offers IaaS in [REDACTED]</li> <li>Lumen's Network connectivity between agency sites and Lumen's cloud/data center location(s) is supported by the Lumen network and network transport services specified in support of EIS.</li> </ul>
Security [M.2.1.4]	<ul style="list-style-type: none"> <li>All cloud traffic subject to security processing is processed by either one of Lumen's cloud service TICs (MTIPS) or, for CSPs that have them, the CSP's overlay TIC.</li> <li>Through Lumen Cloud Connect Solutions (Section 1.4.5), agencies on-net to Lumen can connect to their IaaS resources without traversing the Internet.</li> </ul>

---

#### **1.4.5.1.1 Service and Functional Description [L.29.2.1, M.2.1, C.2.5.1.1.1]**

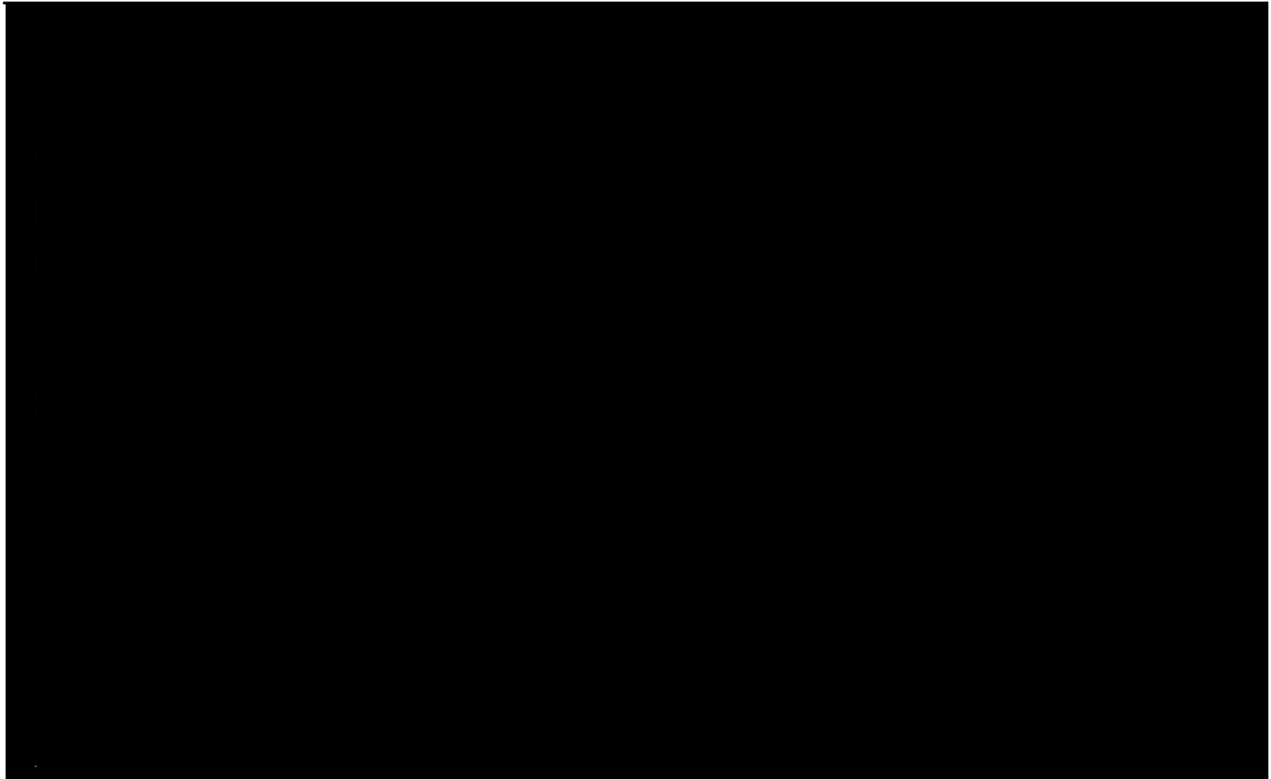
The Lumen Team's IaaS solution(s) enables agencies to avoid many of the costs of operating and maintaining a physical IT infrastructure of computing resources through virtualization and procurements on a service basis instead of a physical one.

Operationally, our IaaS solution satisfies the essential characteristics of cloud services defined by NIST. It offers: on demand self-service; broad access capabilities; independent pooling of resources that can be shared by multiple users; rapid scaling (up or down) of resources; and the ability to measure and pay for only those resources used. Our IaaS can be drawn from multiple providers, should geography or location come into play at the TO level. For example, to satisfy a diversity requirement, we can provide IaaS housed in at least 10 locations.

Different cloud service providers normally are not interconnected. However, under Lumen's approach as integrator and cloud service broker, it would be possible to provide diversity using different cloud providers using Lumen-provided high-speed connectivity between them, including via our Cloud Connect Solutions.

Our solution is FedRAMP-compliant and TIC overlay compliant. All cloud traffic subject to security processing is processed in either one of Lumen's full-service TICs or the CSP's overlay TIC(s). **Figure 1.4.5.1.1-1** depicts the high-level IaaS architecture employed by one of our Team members and suggests their technical approach.





**Figure 1.4.5.1.1-1. Lumen Team IaaS Architecture (Representative).** *All team members' architectural and operational approaches are very similar.*

There is a high degree of redundancy in all systems and between their data centers. This approach is representative of the architectural and technical approaches of the other team members. As suggested in the figure, the solution provides a flexible, standard, and virtualized infrastructure that can serve as a foundational building block for other cloud services like PaaS and SaaS.

The Lumen Team IaaS solution offers Private and Community Cloud IaaS, and Data Center Augmentation with Common IT Service Management (ITSM), often called Hybrid Cloud, as. All are detailed below as are the attributes and conformance of Lumen Team IaaS with all SOW requirements.

#### **1.4.5.1.2 Standards [C.2.5.1.1.2]**

The Lumen Team's IaaS solution(s) comply with all contractor-applicable standards outlined in SOW C.2.5.1.1.2. Most specifically, these pertain to NIST, ITIL, SNMP, FedRAMP (per comments above in Section 1.4.5.1) OMB, ISO, and FIPS. The

---

named DoD and NARA standards may be considered beyond the scope of IaaS, but the Lumen Team IaaS platforms support their implementation. Assuming FedRAMP authorizations proceed in track, Lumen Team members in total operate 10 data center locations with FedRAMP-certified enclaves - AWS by itself operates four of them.

#### **1.4.5.1.3 Connectivity to Cloud Data Center [C.2.5.1.1.3]**

Network connectivity between agency sites and Lumen's cloud/data center location(s) is supported by the Lumen network and network transport services specified in support of EIS. In these circumstances, an agency with on-net connectivity to Lumen could connect to its cloud IaaS without traversing the Internet. All Lumen Team member data centers are either directly on-net to Lumen or the data center's private transport network (e.g., AWS Direct Connect via Lumen's Cloud Connect Service) is on-net to Lumen. Lumen Cloud Connect service is discussed in Section 1.4.5 of this Volume.

Agencies with Ethernet-based access to the Lumen network enjoy the Dynamic Capacity feature of Adaptive Network Control whereby bandwidth can expand – and cost effectively so – according to demand and/or schedule. Dynamic Capacity and Adaptive Network Control are discussed in Ethernet Transport Service, Section 1.3.1.2 of this Technical Volume.

#### **1.4.5.1.4 Technical Capabilities [C.2.5.1.1.4]**

This section presents the technical capabilities for each of the subservice types defined as part of the overall IaaS requirements.

##### **1.4.5.1.4.1 Technical Capabilities for Private Cloud [C.2.5.1.1.4.1]**

Private (i.e., air-gapped) and the variant Community (i.e., virtual-gapped) cloud deployment models are similar. In the former, server hardware (e.g., blades) is dedicated to a single organization while in the community model this hardware is *shared* by organizations (agencies or sub-agencies in this context) that have similar security and performance goals. Because of the sharing and a greater ability to spread costs, the community model commonly offers economic advantages over the private one.

In practice in private cloud environments, some hardware elements of service delivery – such as storage systems – typically are still shared. The degree of any sharing or exclusivity is defined on a TO basis.

The Lumen Team provides IaaS in Private and Community cloud deployment models. Characteristics of virtualization, such as Virtual Machine (VM) migration, make it possible to migrate between these two cloud deployment models. Both models are compliant with the requirements defined in SOW C.2.5.1.1.4.1. **Figure 1.4.5.1.4.1-1** illustrates each SOW requirement and addresses the Lumen Team’s compliance with it.

**Figure 1.4.5.1.4.1-1. Technical Capabilities of Lumen Team Private Cloud per SOW Section C.2.5.1.1.4.1**

LUMEN COMPLIES	SOW C.2.5.1.1.4.1 REQUIREMENT	LUMEN TEAM'S COMPLIANT SOLUTION
✓	1. National Security Policy	<ul style="list-style-type: none"> <li>To the extent that cloud services are based and provided on a network external to that of the agency – which is the typical case – then access to the agency’s cloud based data is subject to OMB Memorandum M-15-01. As such, traffic has to be routed through an EINSTEIN Enclave and, in practice, processed by the TIC which in all likelihood is collocated with the Enclave. The same is true for traffic from External Networks (e.g., a home office) reaching the data within the cloud service. Accordingly, all such traffic either will be routed and processed through a Lumen TIC/Enclave, or through the TIC/Enclave of a CSP associated with the Lumen Team operating its own overlay TIC.</li> </ul>
✓	2. Cloud Data Center Security	<ul style="list-style-type: none"> <li>a) To the extent that computing resources are drawn upon in a second data center (i.e., for resource expansion), the connectivity – whether for expansion or contraction - between data centers is secured by encryption.</li> <li>b) Data moving between an agency site and the cloud data center is either carried over a trusted network (e.g., the Lumen private network) or should it come from an untrusted network such as the Internet, including for a public-facing website operating at the CSP, data is processed through a TIC. We note that some or all agency-cloud traffic may have underlying encryption applied by the agency.</li> <li>c) Additional compliance and certification requirements can be satisfied at the TO level.</li> </ul>
ü	3. Agency Cloud Service Security	<ul style="list-style-type: none"> <li>a) Security perimeter around data and VMs is maintained through methods including involving items such as virtual networking to/from the agency’s CSP resources, firewalls, VLAN separation within the VMs, and multi-tenancy security techniques performed by the hypervisor.</li> <li>b) Data-at-rest is encrypted per FIPS-197.</li> </ul>

LUMEN COMPLIES	SOW C.2.5.1.1.4.1 REQUIREMENT	LUMEN TEAM'S COMPLIANT SOLUTION
✓	4. Virtualized Elastic Computing	<ul style="list-style-type: none"> <li>Virtualized elastic computing offered by the Lumen Team is consistent with the Rapid Elasticity essential characteristic of the NIST cloud service description.</li> <li>a) Virtual Machines (VM): Lumen Team members support a wide range of VMs with an impressively wide range of Virtual CPU (vCPU), RAM and Disk storage options as well as a number of Operating Systems including Microsoft Windows, Unix, and Linux variants.</li> <li>b) Network Storage: Lumen Team members offer a range of Network Storage options in/for local and back-up needs (in Gigabyte (GB) blocks) in file and object configurations. Storage is offered in performance tiers, allowing agencies to balance performance needs with cost.</li> </ul>
✓	5. Server Hosting	<ul style="list-style-type: none"> <li>Server Hosting for a) Private-facing internal web hosting, and b) Public-facing external web hosting is a routine application of IaaS and is supported by the Lumen Team.</li> <li>In light of the potential for large traffic surges on agencies' public-facing websites, Lumen Team members offer high degrees of scalability. Lumen's role as one of the world's leading Internet carriers for traffic across the network and Dynamic Capacity on Cloud Connect assure that bandwidth can scale with high demand. We also note that public-facing Government websites are targets for DDoS attacks, against which Lumen anti-DDoS network tools can defend.</li> </ul>
✓	6**. Back-up and Restore Agency Data	<ul style="list-style-type: none"> <li>[** Numbering has been continued]</li> <li>Lumen Team members can manage the backup, restoration and archiving agency data in the cloud environment to/from Team members' storage infrastructure.</li> </ul>
✓	7. Self-Service On-Demand Capabilities	<ul style="list-style-type: none"> <li>On-demand IaaS self-service via a portal scripting language or API with role-based access that complies with OMB M-11-11 (Federal common identification standards) is supported. Control for IaaS is protected by a 2-factor authentication process consistent with FedRAMP requirements.</li> </ul>
✓	8. Usage Visibility	<ul style="list-style-type: none"> <li>Lumen Team-IaaS provides visibility into levels of measured/metered (usage-based) service.</li> </ul>
✓	9. Private IP Address Blocks	<ul style="list-style-type: none"> <li>VMs can use users' own private IP address-blocks.</li> </ul>
✓	10. VM Bulk Import/Export	<ul style="list-style-type: none"> <li>VMs can be imported and exported in bulk per ISO 17203 (Open Virtualization Format, OVF). This greatly expedites the transition process.</li> </ul>
✓	11. Access to Log Events	<ul style="list-style-type: none"> <li>Users have access to a variety of log events for at least 60 days.</li> </ul>
✓	12. Metadata Tagging (Optional)	<ul style="list-style-type: none"> <li><i>With the possible involvement of 3<sup>rd</sup> party tools, users can place metadata tags on provisioned resources.</i></li> </ul>
✓	13. Cost Control	<ul style="list-style-type: none"> <li>Lumen Team IaaS supports cost control measures such as resource quotas and time-to-live</li> </ul>

LUMEN COMPLIES	SOW C.2.5.1.1.4.1 REQUIREMENT	LUMEN TEAM'S COMPLIANT SOLUTION
	Measures	controls such as leases.
✓	14. 24/7 Customer Service	<ul style="list-style-type: none"> <li>• 24/7 customer service support via email, chat, and phone is provided; additional support is provided by the Lumen Team's account manager.</li> </ul>
✓	15. Cloud Data Ownership	<ul style="list-style-type: none"> <li>• Agencies retain ownership of their data in the cloud, and the Lumen Team solution includes data export and retrieval tools enabling the agency to retrieve data in its original or agreed upon common formats.</li> </ul>
✓	16. U.S. Jurisdiction	<ul style="list-style-type: none"> <li>• All cloud infrastructure and resources are located within the U.S. jurisdiction in potential support of the discovery phase of litigation. Physical access to our cloud facilities, technical capabilities, operations, records and documentation is provided to authorized Government personnel as needed.</li> </ul>
✓	17. DR/COOP	<ul style="list-style-type: none"> <li>• The Lumen Team provides Disaster Recovery (DR) and Continuity of Operations (COOP) per agency-specific requirements at the TO level..</li> </ul>

**1.4.5.1.4.2 Technical Capabilities for Data Center Augmentation with Common Information Technology Service Management [C.2.5.1.1.4.2]**

Data Center Augmentation with Common ITSM, often called hybrid cloud, can be an economical way to supplement (augment) the resources of an agency's existing in-house data center. In this approach, the VMs and other resources "in the cloud" largely appear as if they reside at the in-house data center. Hybrid clouds can provide a path for migration from an in-house approach to one heavily or fully based on cloud services.

Operating in a hybrid cloud environment is somewhat easier when the agency's cloud and that of the CSP are based upon the same hypervisor. An advantage of Lumen's broad and flexible approach is that not all of our IaaS solution partners rely on the same base hypervisor. Most rely on VMware, but AWS is fundamentally Xen-based. In this context we note that AWS developed a plugin, AWS Management Portal for vCenter (vCenter is the VMware user management system and console) that provides a management gateway between vCenter and AWS that is transparent to the user in terms of VMware look and feel.

Figure 1.4.5.1.4.2-1 presents the requirements defined in SOW C.2.5.1.1.4.2 and addresses the Lumen solution’s compliance with them.

**Figure 1.4.5.1.4.2-1. Compliant Technical Capabilities of Lumen Team Data Center Augmentation with ITSM (Hybrid Cloud) per SOW C.2.5.1.1.4.2**

LUMEN COMPLIES	SOW C.2.5.1.1.4.2 REQUIREMENT	LUMEN TEAM COMPLIANT SOLUTION
✓	1. Cross Platform Management	<ul style="list-style-type: none"> <li>The Lumen Team IaaS solution provides the ability to manage both cloud virtual-resources and the agency data center’s virtual resources using the same native “single pane of glass” management platform with the same monitoring and control capabilities (same menus). Therefore an agency data center enjoys the flexibility of being able to use and manage its cloud-based resources as if they are part of its internal virtualized data center.</li> </ul>
✓	2. Visual Indications	<ul style="list-style-type: none"> <li>The Lumen Team IaaS management platform provides a visual indication of which resources are in the cloud and which are in the agency’s data center.</li> </ul>
✓	3. Integration (Optional)	<ul style="list-style-type: none"> <li>Lumen and Team members have considerable experience with integrating SNMP-based systems. Therefore, in collaboration with the agency, the ability to integrate with the agency’s data center management platform, such as HP OpenView and IBM Tivoli, is – conceptually - readily achievable. It can be addressed at the TO level.</li> </ul>

**1.4.5.1.5 Features [C.2.5.1.2]**

Figure 1.4.5.1.5-1 summarizes the Lumen Team’s IaaS support for IaaS features per SOW C.2.5.1.2.

**Figure 1.4.5.1.5-1. Lumen Team Support for IaaS Features per SOW C.2.5.1.2**

LUMEN COMPLIES	SOW C.2.5.1.2 REQUIREMENT	LUMEN TEAM COMPLIANT SOLUTION
ü	1. “Bare Metal” Servers (Optional)	<ul style="list-style-type: none"> <li>The challenge of provisioning an unspecified number and type of “bare metal” physical servers is the two-hour window. In some cases servers can be rapidly provisioned using VLANs, but the open-ended nature of the feature has to be clarified at the TO level.</li> </ul>
✓	2. Data Management and Analytics	<ul style="list-style-type: none"> <li>The Lumen Team IaaS solution supports Data Management and Analytics capabilities directed at complementing and extending log management and analysis services and other data center management services, details of which are addressable at the TO level.</li> </ul>

**1.4.5.1.6 Interfaces [C.2.5.1.3]**

The Lumen Team will support the interfaces defined at the TO level.

**1.4.5.1.7 Performance Metrics [M.2.1, C.2.5.1.4, G.8]**

The Lumen Team meets and/or exceeds the Availability (IaaS Cloud Service) and Time to Restore (TTR) performance levels defined for Cloud Data Center in SOW C.2.5.1.4. – namely  $\geq 99.95\%$  Availability and  $TTR \leq 4$  hours without dispatch and  $\leq 8$  hours with dispatch. Scheduled maintenance windows are excluded from the availability calculation. The Lumen Team’s global cloud service design minimizes latency and packet loss among cloud service providers, private data centers and users, and provides highly efficient routing that helps agencies’ mission-critical IaaS services perform at optimal levels.

**1.4.5.2 Platform as a Service [L.29.2.1, C.2.5.2; C.4.4]**

As demand for new applications soars, developers in industry and Government alike have turned to readily available, complete software development platforms – Platform as a Service (PaaS) - to greatly reduce the complexity, cost and time from application conception to delivery while providing a level of security throughout the full platform stack. Accordingly, agencies need PaaS solutions that present a “sandbox” environment. That is, a solutions set that is comprehensive and complete, easy to reach and use, offers a superb level of operational performance, and is highly secure – while still affording value.

Lumen Team PaaS Solution
<ul style="list-style-type: none"><li>• FedRAMP PaaS via Microsoft Azure</li><li>• NOC and SOC Cloud Managed Services throughout the platform stack</li><li>• Cloud Managed Services contains a PaaS workflow enabling consistent support through the entire platform</li></ul>

Like most of Lumen’s cloud based offerings under EIS, our approach to providing PaaS is to broker and manage one or more focused and flexible partners to offer comprehensive PaaS solutions that can be well matched for any specific TO. [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]



The actual points of PaaS delivery, generally one or more data centers on-net to Lumen, are woven into the fabric of the Lumen’s high performance network and its operational support structure.

Figure 1.4.5.2-1 highlights the features of the Lumen Team PaaS solution aligned with the evaluation criteria.

**Figure 1.4.5.2-1. Feature of Lumen Team PaaS**

EVALUATION CRITERIA	FEATURES OF LUMEN TEAM PAAS
Understanding [2.1.1]	<ul style="list-style-type: none"> <li>Like most of Lumen’s cloud based offerings under EIS, our approach to providing PaaS is to manage one or more focused and flex ble partners to offer comprehensive PaaS solutions that can be well matched for any specific TO.</li> <li>[REDACTED]</li> </ul>
Quality of Service [2.1.2]	<ul style="list-style-type: none"> <li>Lumen Team PaaS satisfies all performance metrics outlined in SOW C.2.5.2.4.</li> <li>The PaaS solution platform features high degrees of redundancy for service resilience and reliability.</li> <li>Our PaaS has the ability for a Customer-specific (CPaaS) solution that can be approved as, and elevated to a secure, GSA Global PaaS (GPaaS) solution, enabling considerable efficiency through reuse – thereby fulfilling Government goals for cloud services and the FedRAMP process.</li> </ul>
Service Coverage [2.1.3]	<ul style="list-style-type: none"> <li>As a cloud-based service, Lumen Team PaaS is reachable from virtually anywhere. Note that all Internet traffic passes through a TIC as can on-net traffic.</li> <li>The actual points of PaaS delivery, generally one or more data centers on-net to Lumen, are woven into the fabric of the Lumen’s high performance network and its operational support structure.</li> </ul>
Security [2.1.4]	<ul style="list-style-type: none"> <li>All cloud traffic subject to security processing is processed by either one of Lumen’s cloud service TICs (MTIPS) or, for CSPs that have them, the CSP’s overlay TIC.</li> <li>Through Lumen Cloud Connect Solutions (Section 1.4.5), agencies on-net to Lumen can connect to their IaaS resources without traversing the Internet.</li> </ul>

**1.4.5.2.1 Service and Functional Description [L.29.2.1, M.2.1, C.2.5.2.1]**

Lumen Team PaaS is a secure, flexible and compliant offering that places a full set of tools at a developers’ disposal. Discussed below, a remarkable feature of our

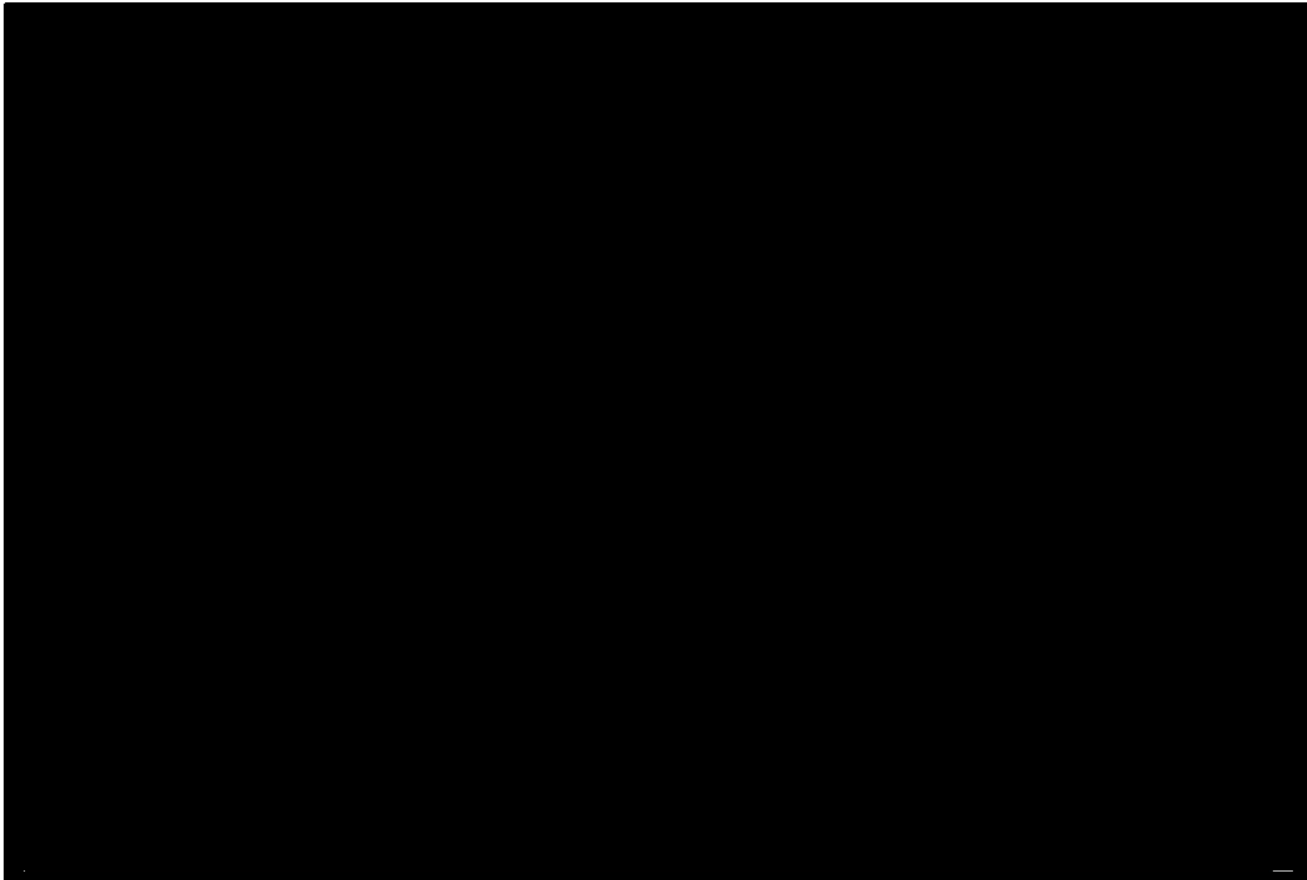


---

PaaS is the ability for a Customer-specific (CPaaS) solution that can be approved as, and elevated to a secure, GSA Global PaaS (GPaaS) solution, enabling considerable efficiency through reuse – thereby fulfilling Government goals for cloud services and the FedRAMP process. Architecture of our PaaS solution is shown in **Figure 1.4.5.2.1-1**.

Once a specific agency customer has been on-boarded to the PaaS portal via the Lumen GSA Customer Portal, the Ordering Contracting Officer (OCO) is sent, via secure email, credentials and directions on how to access the PaaS Customer Portal allowing him/her to review the catalog items noted in the figure. These catalog items could include the IaaS VMs and a series of GSA GPaaS solution offerings defined and built to be available for any GSA customer.

Each OCO representing his/her department or agency, can create a VM, build a platform within that VM, and then save the VM as a reusable Customer-specific Platform as a Service (CPaaS) solution that only his/her department or agency sees. This enables OCOs to define their own CPaaS solutions for their own requirements and mission. More broadly, an OCO can request that his/her CPaaS be a candidate for the GPaaS, where GSA can determine/verify if the CPaaS is FedRAMP-compliant and therefore available to all GSAs customers as a FedRAMP-approved GPaaS.



**Figure 1.4.5.2.1-1. Architectural Overview of Lumen’s PaaS Solution.** *The fully-compliant PaaS Solution operates on a FedRAMP-compliant cloud infrastructure.*

The attributes and conformance of Lumen PaaS with all SOW requirements are discussed in the following sections.

#### **1.4.5.2.1.2 Standards [C.2.5.2.1.2]**

The Lumen Team’s PaaS solutions comply with those contractor-applicable standards specified for IaaS and discussed in Section 1.4.5.1.2 of this Technical Volume; these pertain to NIST, ITIL, SNMP, FedRAMP, OMB, ISO, and FIPS. The named DoD and NARA standards may be considered beyond the scope of PaaS, but the Lumen Team PaaS platforms support their implementation.

#### **1.4.5.2.1.3 Connectivity [C.2.5.2.1.3]**

The Lumen Team’s PaaS solution is compliant with all connectivity requirements as discussed in Section 1.4.5.1.3 of this Technical Volume in support of EIS.

**1.4.5.2.1.4 Technical Capabilities [C.2.5.2.1.4]**

With particular reference to the PaaS architectural overview above, the Lumen Team’s PaaS solution draws upon commercially available platforms to offer the requisite technical capabilities. These are summarized in **Figure 1.4.5.2.1.4-1**. Any element not immediately available can be added which highlights the flexibility of our PaaS solution.

**Figure 1.4.5.2.1.4-1. Lumen Team Compliance with PaaS Technical Capabilities**

LUMEN COMPLIES	SOW C.2.5.2.1.4 REQUIREMENT	LUMEN TEAM COMPLIANT SOLUTION
✓	1. National Security Policy	<ul style="list-style-type: none"> <li>To the extent that cloud services are based and provided on a network external to that of the agency – which is the typical case – then access to the agency’s cloud based data is subject to OMB Memorandum M-15-01. As such, traffic has to be routed through an EINSTEIN Enclave and, in practice, processed by the TIC which in all likelihood is collocated with the Enclave. The same is true for traffic from External Networks (e.g., a home office) reaching the data within the cloud service. Accordingly, all such traffic either will be routed and processed through a Lumen TIC/Enclave, or though the TIC/Enclave of a CSP associated with the Lumen Team operating its own overlay TIC.</li> </ul>
✓	2. Developer Tools	<ul style="list-style-type: none"> <li>As noted in Figure 1.4.5.2.1.1-1, all developer tool types (SOW a – c) are available in the Lumen PaaS solution</li> </ul>
✓	3. Database Systems (DBMS/RDMS)	<ul style="list-style-type: none"> <li>Similarly as noted in Figure 1.4.5.2.1.1-1, DBMS/RDMS systems are available to manage large scale structured data sets</li> </ul>
✓	4. Big Data Solution Platform	<ul style="list-style-type: none"> <li>Numerous Big Data Solution Platform capabilities are available in the Lumen PaaS solution. Examples include capabilities for data management, advanced analytics and statistics, visualization and integration</li> </ul>
✓	5. Directories	<ul style="list-style-type: none"> <li>Foundation for directories includes LDAP/X.500</li> </ul>
✓	6. Testing Tools	<ul style="list-style-type: none"> <li>All Testing Tool types (SOW a – c) are available</li> </ul>

The Lumen Team recognizes that the agency retains exclusive ownership over all of its data in the cloud. The Lumen Team provides tools to allow the client agency to fully manage its PaaS-related data from the cloud in usable format as needed.

**1.4.5.2.1.5 Features [C.2.5.2.2]**

Not applicable.

**1.4.5.2.1.6 Interfaces [C.2.5.2.3]**

The Lumen Team supports the interfaces defined in the TO.

**1.4.5.2.1.7 Performance Metrics [M.2.1, C.2.5.2.4, G.8]**

The Lumen Team complies with PaaS KPIs defined in SOW C.2.5.1.4 and outlined in Section 1.4.5.1.7 of this Volume. In addition, the Lumen Team meets service level objectives for performance, privacy, security and support as specified in the TO.

**1.4.5.3 Software as a Service [L.29.2.1, C.2.5.3; C.4.4]**

Driven by its simplification of operations and value proposition, agencies are rapidly embracing SaaS. Similar to IaaS and PaaS, Lumen’s approach to SaaS is to broker managed partners who have deep, specific experience offering SaaS.

[REDACTED]

[REDACTED]

[REDACTED]

**Lumen Team SaaS Solution**

- A diverse SaaS team with notable transition and delivery experience.
- Lumen’s role as cloud service broker enables us to tailor a supplier and solution to a given situational requirement.
- Lumen’s transport and Cloud Connect solutions with Dynamic Capacity provide flexible, secure and high performance

Figure 1.4.5.3-1 highlights the features of the Lumen SaaS solution aligned with the evaluation criteria. As a cloud-based service, Lumen Team PaaS is reachable from virtually anywhere. Not that all Internet traffic passes through a TIC as can on-net traffic.

**Figure 1.4.5.3-1. Features of Lumen Team SaaS**

EVALUATION CRITERIA	FEATURES
Understanding [M.2.1.1]	<ul style="list-style-type: none"> <li>• Lumen’s cloud service brokering approach to SaaS is to manage partners who have deep, specific experience offering SaaS. [REDACTED]</li> <li>• [REDACTED]</li> <li>• [REDACTED]</li> <li>• [REDACTED]</li> </ul>
Quality of Service [M.2.1.2]	<ul style="list-style-type: none"> <li>• Lumen Team SaaS satisfies all performance metrics outlined in SOW C.2.5.3.4.</li> <li>• SaaS solutions, while FedRAMP-compliant in their own right, operate within FedRAMP-compliant infrastructures that offer the reliability and scalability expected of cloud-based services.</li> </ul>
Service Coverage [M.2.1.3]	<ul style="list-style-type: none"> <li>• As a cloud-based service, Lumen Team SaaS is reachable from virtually anywhere. Note that all Internet traffic passes through a TIC as can on-net traffic.</li> <li>• The actual points of SaaS delivery, generally one or more data centers on-net to Lumen, are woven into the fabric of the Lumen’s high performance network and its operational support structure.</li> </ul>
Security [M.2.1.4]	<ul style="list-style-type: none"> <li>• All cloud traffic subject to security processing is processed by either one of Lumen’s cloud service TICs (MTIPS) or, for CSPs that have them, the CSP’s overlay TIC.</li> </ul>

EVALUATION CRITERIA	FEATURES
	<ul style="list-style-type: none"> <li>• Through Lumen Cloud Connect Solutions (Section 1.4.5), agencies on-net to Lumen can connect to their IaaS resources without traversing the Internet.</li> <li>• The access control process ensures that the engineer requesting access to these IT systems has met the eligibility requirements.</li> <li>• Access to the Microsoft data center IT systems that store customer information is strictly controlled via role-based access control (RBAC) and lock box processes.</li> </ul>

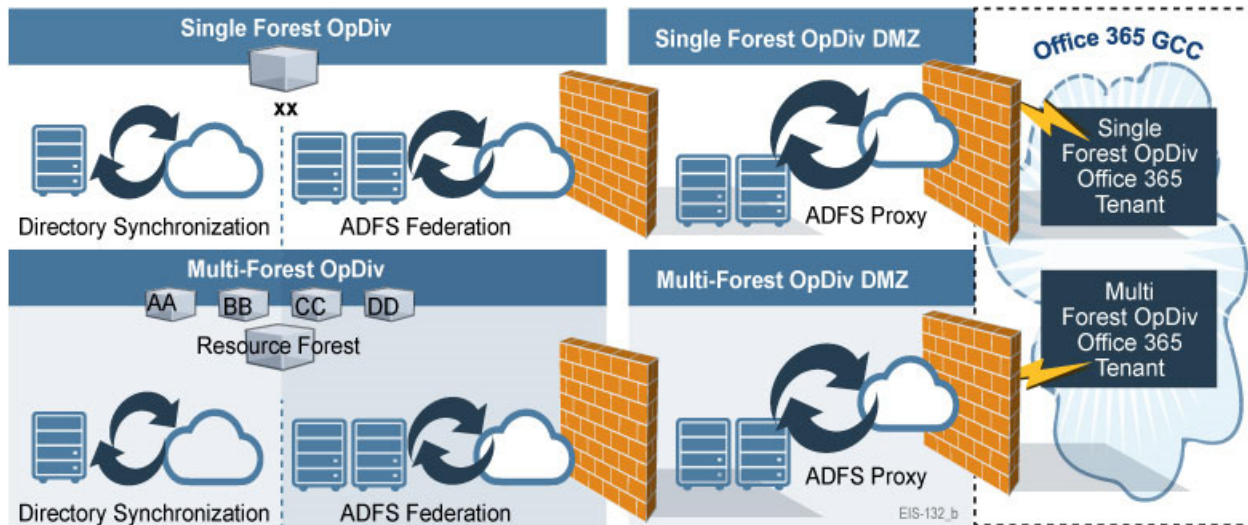
**1.4.5.3.1 Service and Functional Description [L.29.2.1, M.2.1, C.2.5.3.1.1]**

The Lumen Team’s SaaS solutions are compliant with all EIS requirements.

SaaS solutions, themselves FedRAMP-compliant, still operate within FedRAMP-compliant infrastructures. The architectural diagram of **Figure 1.4.5.3.1-1** is representative of the infrastructural base on which SaaS solutions are operated. We can examine elements of the architecture of the Microsoft Government Community Cloud (GCC) for Office 365 as representative of a SaaS deployment. Note that Office 365 Multi-Tenant & Supporting Services is FedRAMP compliant with the Departments of Commerce, and Health and Human Services as authorizing agencies.

Access to the Microsoft data center IT systems that store customer information is strictly controlled via Role-Based Access Control (RBAC) and lock box processes. The access control process ensures that the engineer requesting access to these IT systems meets the eligibility requirements. Office 365 GCC is designed to host multiple tenants in a highly secure way through data isolation. Data storage and processing for each tenant is segregated through the Active Directory (AD) structure and capabilities specifically developed to help build, manage, and secure multi-tenant environments. The AD architecture is shown in **Figure 1.4.5.3.1-1**. The AD access control features isolate customers using security boundaries (also known as silos). This safeguards customer data so that the data cannot be accessed or compromised by other tenants. These controls allow agencies to adhere to compliance requirements, give access to services and content to individuals within their organization, configure anti-malware/anti-spam controls, and encrypt data where a customer holds the keys. Data isolation is built into the software itself. The Microsoft Security Development Lifecycle (SDL) is a

comprehensive security assurance process that informs every stage of design, development and deployment of Microsoft software and services.



**Figure 1.4.5.3.1-1. Microsoft Active Directory Architecture.** AD provides highly secure multi-tenant environments, essential for any cloud service.

The attributes and conformance of Lumen Team SaaS with all SOW requirements are discussed below.

#### 1.4.5.3.2 Standards [C.2.5.3.1.2]

The Lumen Team's SaaS solutions comply with those contractor-applicable standards specified for IaaS and discussed in Section 1.4.5.1.2 of this Technical Volume. Those pertain to NIST, ITIL, SNMP, FedRAMP, OMB, ISO, and FIPS. The named DoD and NARA standards may be considered beyond the scope of SaaS, but the Lumen Team SaaS platforms support their implementation.

Of note regarding standards, Office 365 - a key desktop application platform - adheres to a number of industry best practices and operating standards including: SAS 70 / SSAE16 assessments, ISO 27001 (certified), HIPAA-Business Associate Agreement, FISMA and FedRAMP (JAB P ATO certified), the Gramm-Leach-Bliley Act, Payment Card Industry Data Security Standard (PCI-DSS) Level One and PCI-governed data, the Microsoft Data Processing Agreement, and EU Model Clauses and Safe Harbor.

---

**1.4.5.3.3 Connectivity [C.2.5.3.1.3]**

Connectivity for the Lumen Team's SaaS solutions is compliant with all requirements as discussed in Section 1.4.5.1.3 of this Technical Volume. As these call out the applicable EIS transport services, we again note Lumen Cloud Connect Solutions (Section 2.3.11 of this volume) with Dynamic Capacity and the flexible, high performance, and highly secure private connections they provide to cloud platforms. In the SaaS context, we note Cloud Connect's interconnection with Microsoft Express Route, which brings connectivity to Microsoft platforms for IaaS (Azure) and SaaS (including Office 365).

**1.4.5.3.4 Technical Capabilities [C.2.5.3.1.4]**

The Lumen Team for SaaS is experienced in delivering SaaS solutions and meets all of the technical capabilities defined in SOW C.2.5.3.1.4 and itemized below. To the extent that cloud services are based and provided on a network external to that of the agency – which is the typical case – then access to the agency's cloud based data is subject to OMB Memorandum M-15-01. As such, traffic has to be routed through an EINSTEIN Enclave and, in practice, processed by the TIC which in all likelihood is collocated with the Enclave. The same is true for traffic from External Networks (e.g., a home office) reaching the data within the cloud service. Accordingly, all such traffic either will be routed and processed through a Lumen TIC/Enclave, or through the TIC/Enclave of a CSP associated with the Lumen Team operating its own overlay TIC.

Members of the Lumen Team are able to provide SaaS tools for:

- Customer Relationship Management (CRM) - with integrated social media such as Twitter, Facebook, Pinterest, etc.
- Enterprise Resource Planning (ERP) for a variety of functional areas such as supply chain management, manufacturing, accounting, order processing, etc. Example platforms could include Oracle and SAP.
- Human Capital Management (HCM) used for talent management and areas such as payroll processing. Example platforms could include Oracle, SAP, and ADP.

- 
- Desktop Applications: Microsoft's Office 365 via the Microsoft GCC. We note that through the Cloud Premier for Office 365 Managed Support offering, the Lumen Team can provide agencies service delivery management, resolution services, and education to agencies so that Government administrators and all tiers of the help desk organization can support Office 365 end users.
  - Office Automation: including email and Microsoft Lync/Skype and SharePoint.
  - Security, such as endpoint protection, anti-virus, and anti-malware. Some security services may be provided under Lumen Managed Security Services (Section 1.4.8.4 of this Technical Volume).

The Lumen Team's SaaS solution draws upon commercially available platforms to offer the requisite technical capabilities. Any element not immediately available can be added which highlights the flexibility of our SaaS solution.

Specific solutions and other tools are formulated at the TO level.

The Lumen Team recognizes that the agency retains exclusive ownership over all of its data in the cloud. The Lumen Team provides tools to allow the client agency to fully manage its SaaS related data from the cloud in usable format as needed.

#### **1.4.5.3.5 Features [C.2.5.3.2]**

None are defined in the SOW.

#### **1.4.5.3.6 Interfaces [C.2.5.3.3]**

The Lumen Team supports interfaces defined at the TO level. Additionally, we provide the SaaS platform specific Application Programming Interface (API or Client software) to connect to the cloud SaaS platforms.

Note that Office 365 GCC delivers enterprise productivity tools across Windows Phone, iPhone, and Android phones or tablets with cross-device synchronization.

#### **1.4.5.3.7 Performance Metrics [M.2.1, C.2.5.3.4, G.8]**

The Lumen Team complies with the performance metrics:

- As outlined for IaaS, section 1.4.5.1.7 of this Technical Volume
- To provide the most current software release with all the patches applied or as specified at the TO level



**1.4.5.4 Content Delivery Network Service (CDNS) [L.29.2.1, C.2.5.4; C.4.4]**

Per analytics.usa.gov, for the 90-day period ending January 31, 2016, U.S. Government websites served some 1.5B visits. This staggering figure suggests agencies’ decided needs for global CDNS and its ability to address latency, reliability and scalability concerns – especially the latter in the face of flash crowd control.

**Lumen’s Leading CDNS**

- Broad feature set and global CDN coverage exceeds EIS requirements
- Dedicated pool of edge servers configured to cache and deliver secure, shared content using SSL or TLS and HTTPS
- 100% uptime SLA; service designed with no single points of failure
- A simplified, single source offering for delivery of all types of content

Lumen’s high-capacity, global network combined with our proven, sophisticated CDN platform make Lumen one of the world’s leading providers of CDNS. The Lumen CDNS is built on a scalable, high-performing, reliable and secure platform. It offers the expertise, technology, and applications required to easily meet the demands to reliably deliver content over the Internet, such as webpages and webpage assets, graphics and images, electronic documents, software libraries and patches, and live and pre-recorded audio and video media. Stemming from a 25-year pedigree of technology evolution, Lumen CDNS is prepared to meet the needs foreseen now for EIS, as well as those likely to arise.

**Figure 1.4.5.4-1** highlights the features of the Lumen CDNS solution aligned with the evaluation criteria.

**Figure 1.4.5.4-1. Features of Lumen CDNS**

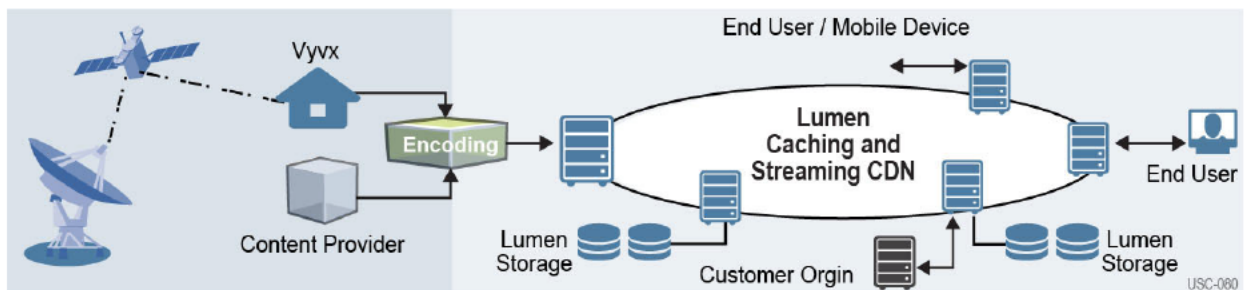
EVALUATION CRITERIA	FEATURES OF LUMEN CDNS
Understanding [M.2.1.1]	<ul style="list-style-type: none"> <li>• Lumen’s high-capacity, global network combined with our proven, sophisticated CDN platform <i>make Lumen one of the world’s leading providers of CDNS.</i></li> <li>• The Lumen CDNS is built on a scalable, high-performing, reliable and secure platform.</li> </ul>
Quality of Service [M.2.1.2]	<ul style="list-style-type: none"> <li>• Lumen CDNS satisfies all performance metrics outlined in SOW C.2.5.4.4.1.</li> <li>• The scope of Lumen’s CDN platform provides the reliability and scale agencies require for CDNS.</li> <li>• Lumen CDNS helps accelerate delivery webpages and webpage assets, transforming them on-the-fly to enable fast delivery and more efficient rendering across a broad spectrum of browsing platforms.</li> </ul>
Service Coverage	<ul style="list-style-type: none"> <li>• Lumen CDNS is delivered from some 15,000 servers on the worldwide Lumen network.</li> </ul>

EVALUATION CRITERIA	FEATURES OF LUMEN CDNS
{M.2.1.3}	
Security [M.2.1.4]	<ul style="list-style-type: none"> <li>• Our state-of-the-art Security Operations Center (SOC) monitors the complete threat landscape with a continuous cycle of protection.</li> <li>• Lumen and our subcontractors perform security operations in accordance with industry best practices and standards supporting Cyber, Personnel and Physical Security.</li> </ul>

**1.4.5.4.1 Service and Functional Description [L.29.2.1, M.2.1, C.2.5.4.1]**

Lumen CDNS helps accelerate delivery of webpages and webpage assets, transforming them on-the-fly to enable fast delivery and more efficient rendering across a broad spectrum of browsing platforms. By hosting cached versions of an agency’s website on local servers and automatically transforming HTML code for swift delivery to any device or browser, the Lumen CDNS enables outstanding performance while increasing website availability.

The purpose of Lumen’s CDN is to securely serve content to end-users while maintaining low levels of latency and high levels of performance, scalability, reliability, and availability. Built on our own network, Lumen’s CDN is a globally distributed system of over 15,000 servers with CDN nodes and supernodes. As such, it meets all GSA/agency CDNS coverage needs. (Supernode capabilities include concentrated clusters of CDN servers with delivery and ancillary capabilities.) A high-level view of the Lumen CDN architecture is shown in **Figure 1.4.5.4.1-1**. End users in the general public reach the CDN via the Internet. Internal agency users reach the CDN (e.g., for content updates or maintenance) via a secure, IP-based connection.

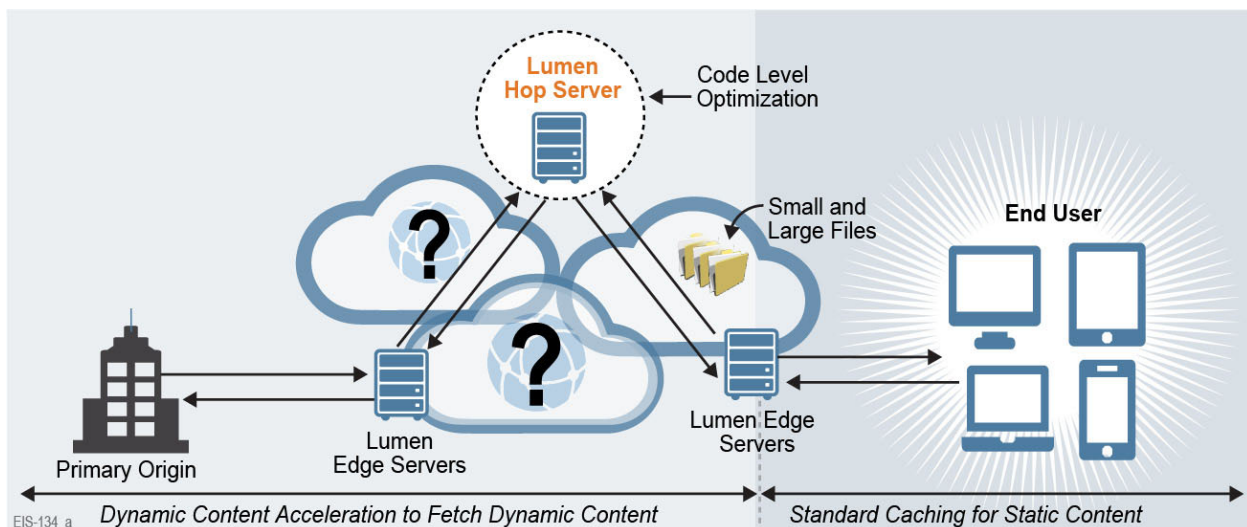


**Figure 1.4.5.4.1-1. Lumen's CDNS Architecture.** *The Lumen CDNS Architecture satisfies all EIS CDNS requirements.*

is a trusted provider of video acquisition, distribution, storage and delivery for many of the world's largest and most innovative broadcasting and media companies.

Lumen's approach to on-demand streaming is based on hosting/caching content at strategic locations so that requests made from particular locations are rapidly and efficiently served. This approach is represented in **Figure 1.4.5.4.1-2**. Our On-Demand Streaming platform enables content to be pulled into our CDN network from Lumen's own internal Origin Storage platform or from external storage sources. Lumen's CDN actively pulls the content into its content delivery platform from an origin storage source (such as an HTTP or HTTPS Web server) when content requests are made using the following methods:

- The end user requests an On-Demand streaming asset via a customer-specific hostname. End users are directed to the best performing edge server on the Lumen CDN for that particular user.
- The edgesever determines if it has the content: if so, it immediately streams the content; if not, it fetches the content from either the customer's web server or the Lumen Origin Storage repository and then populates the edge cache.
- The edgesever streams the content in the requested format. In addition, the Lumen CDN can be configured to encode content sent in raw form.



---

**Figure 1.4.5.4.1-2. Lumen’s Content Network Delivery and Optimization. Content**

*Requests made from particular locations are rapidly and efficiently served.*

Lumen achieves optimized real-time and on-demand streaming by dynamically calibrating video quality based on viewer bandwidth and device to increase reliability, reduce latency, and perform flash crowd control. The attributes and conformance of Lumen CDNS with all SOW requirements are discussed below.

**1.4.5.4.2 Standards [C.2.5.4.1.2]**

As a global leader in CDNS, Lumen complies with these CDNS-related standards: Hyper Text Transfer Protocol (HTTP), IETF – Request for Comments, and Transport Layer Security (TLS). Lumen continually monitors the development and revision of technical standards and best practices (including regulatory changes) related to CDN and incorporates new versions, amendments, and modifications to these standards and practices as they are finalized, tested, and approved.

**1.4.5.4.3 Connectivity [C.2.5.4.1.3]**

The public connects to and interoperates with the Lumen CDNS via the Internet/worldwide web. For example, a user typically would initiate a session with an agency by addressing its website, e.g., www.agencyxyz.gov. Transparent to the user, the CDN might deliver the website content from a CDN server geographically close to the user. All such user interactions occur via the Internet.

As noted above, Internal agency users reach the CDN (e.g., for content updates, maintenance or other administrative tasks) via a secure, IP-based connection.

**1.4.5.4.4 Technical Capabilities [C.2.5.4.1.4]**

This section presents the technical capabilities defined for CDN requirements. Those for Content Distribution are presented in **Figure 1.4.5.4.4-1** while those for Site Monitoring/ Server Performance Measurements are in **Figure 1.4.5.4.4-2**.

**Figure 1.4.5.4.4-1. Lumen’s Compliance with Requirements for Content Distribution**

LUMEN COMPLIES	SOW C.2.5.4.1.4-1 REQUIREMENT	LUMEN COMPLIANT SOLUTION
✓	a) Static Content Download Service	<ul style="list-style-type: none"> <li>Lumen CDNS provides the ability to download static content. Typically, this is done using HTTP or HTTPS protocols. Content is maintained on our CDNS servers located throughout the world to enable rapid delivery 24/7 and eliminate bottlenecks that could introduce latency.</li> </ul>
✓	b) Real-time Streaming (Webcasting)	<ul style="list-style-type: none"> <li>Lumen CDNS delivers streams in real-time; as necessary. Lumen provides signal encoding if it is sent in raw signal format by the content provider.</li> <li>Lumen's Live Streaming platform can support for RealNetworks Real Media, Microsoft's Windows Media, and Apple QuickTime. We note however, that these formats are rarely, if ever, used anymore in a CDN (Microsoft has "end-of-life'd" Windows Media). On a more current basis Lumen's Live Streaming platform provides support for the streaming delivery of any content format that can be delivered using the HTTP and HTTPS protocols, including Apple HTTP Live Streaming (HLS), Adobe HTTP Dynamic Streaming (HDS), and Microsoft Smooth.</li> </ul>
ü	c) On-demand Streaming	<ul style="list-style-type: none"> <li>Lumen hosts and delivers streams on demand or when requested by end-users. Lumen provides signal encoding if it is sent in raw signal format by the content provider.</li> <li>Lumen on-demand streaming content formats can include RealNetworks Real Media, Microsoft Windows Media, and Apple QuickTime. As noted above, these formats are rarely, if ever, used anymore in a CDN. As also noted, Lumen's on-demand streaming platform supports the streaming delivery of any content format that can be delivered using the HTTP and HTTPS protocols, including Apple HLS, Adobe HDS, and Microsoft Smooth.</li> </ul>

**Figure 1.4.5.4.4-2. Lumen Compliance with Requirements for Site Monitoring / Server Performance Measurements**

LUMEN COMPLIES	SOW C.2.5.4.1.4-2 REQUIREMENT	LUMEN COMPLIANT SOLUTION
✓	a) Continuous Monitoring Measurements	<ul style="list-style-type: none"> <li>The performance of the Lumen CDN is under continuous monitoring. Service features/parameters measured include: availability, latency, FTP load, CPU load, memory usage, TLS service load, HTTP port service load, and HTTP connections queue statistics.</li> </ul>
✓	b) Statistics via a Performance Dashboard	<ul style="list-style-type: none"> <li>Lumen's Media Portal Dashboard provides access to a broad set of functionality to view and manage service needs. In addition to CDN functions, other areas include ordering, ticketing, billing, and network performance reports. Access is available on a 24/7 basis and viewing permissions are customized based on user-specific requirements.</li> </ul>

**1.4.5.4.5 Features [C.2.5.4.2]**

SOW C.2.5.4.2 (CDNS) Features, outlines one mandatory feature, Failover Service; and one optional one, Redirection and Distribution Service (Global Load Balancing). Lumen CDNS supports both of them as summarized in **Figure 1.4.5.4.5-1**. In addition, Lumen CDNS supports a number of other features, discussed below and presented in **Figure 1.4.5.4.5-2**.

**Figure 1.4.5.4.5-1. Lumen Team Compliance with CDNS Technical Capabilities**

LUMEN COMPLIES	SOW C.2.5.4.2 REQUIREMENT	LUMEN COMPLIANT SOLUTION
✓	1. Failover Service	<ul style="list-style-type: none"> <li>Failover Service is a basic capability of a CDN, particularly a leading and feature-rich one like Lumen. In delivering this capability, Lumen monitors single-location web sites and redirects traffic to its CDNS in the event of failure. The failover and subsequent service via a CDNS is transparent to end-users.</li> </ul>
✓	2. (Optional) Redirection and Distribution Service (Global Load Balancing)	<ul style="list-style-type: none"> <li>Global Load Balancing is a basic capability for the large and global CDN that Lumen is. With Lumen CDNS Global Load Balancing, when users type in a website address (typically a Universal Resource Locator (URL)) they are ultimately directed to the closest, most available (i.e., not congested) Lumen CDNS cache server.</li> </ul>

The Lumen CDN is comprised of thousands of servers worldwide. If a single or set of servers goes offline or begins to experience poor performance (typically due to high traffic loads), the surrounding CDN servers assume or assist in serving the need(s). Therefore, the Lumen CDN is its own redundancy and failover system.

In addition, as one of the world’s leading CDNS providers, Lumen CDNS offers a broad additional set of features, some part of the basic CDNS offering, others as available options. By tapping into features as needed, agencies can tailor their

**Figure 1.4.5.4.5-2. Additional Lumen CDNS Features**

STANDARD FEATURES	OPTIONAL FEATURES
Flexible Capacity	Site Protect
Enhanced Availability	Origin Storage
Cache Optimization	Mobile Site Accelerator
HTTP Pipelining	Intelligent Traffic Manager
TCP Optimization	Secure Delivery
Route Availability	MidTier/Parent
Persistent Connections	Origin Shield
Dynamic Browser Caching	PCI Delivery
Dynamic Output Cache	Content Analytics
Resource Consolidation	Log Retrieval
Landing Page Optimization	Dynamic Cache Optimization
Predictive Browser Caching	Site Targeting
Payload Reduction	Token Authorization

CDNS to serve the range of needs from basic to highly sophisticated. The specific features needed for a given application can be determined at the TO level, but the important element to note is the breadth of Lumen's CDNS capabilities.

#### **1.4.5.4.6 Interfaces [C.2.5.4.3]**

For access via the Internet, Lumen CDNS offers Hyper Text Transfer Protocol (HTTP) as the User Network Interface (UNI).

For agency connectivity to the Lumen CDNS server (the CDNS service), agencies use the UNIs defined for VPNS in SOW C.2.1.1 and discussed in Section 1.3.3.1.6 of this Technical Volume.

#### **1.4.5.4.7 Performance Metrics [M.2.1, C.2.5.4.4.1, G.8]**

Lumen CDNS meets and/or exceeds the Availability (CDNS network), GOS (Time to refresh content) and Time to Restore (TTR) without and with dispatch defined in SOW C.2.5.4.4.1, including measurement techniques.

#### **1.4.6 Wireless Service [L.29.2.1, C.2.6]**

The Lumen Wireless Service (MWS) offering provides agencies with increased mobility, enhanced productivity, and the ability to collaborate where and when needed. For MWS, Lumen partners with

major cellular carriers for end-to-end wireless services. These carriers provide the ability to integrate mobile users, applications, and Machine-to-Machine (M2M) communications using, CDMA, 4G LTE, and in the near future 5G. Another capability we provide through our partner is a private cellular gateway service tied directly to our

##### **Lumen COMSATCOM Highlights**

- Highly experienced satellite team including RF Specialists, Teleport Design Engineers, and Field Service Engineers
- Teaming partner *By Light* brings 10 years COMSATCOM experience for customers including GSA, DoD, and industry
- Master Service Agreements in place with all major commercial space segment providers
- 24/7 live customer support and service monitoring

##### ***Lumen MWS***

- *Provides agencies with access to mobile voice, data, multimedia content, and the Internet*
- *Teaming Partners provides Nationwide Cellular Coverage with substantial experience delivering wireless solutions for the Government and industry*
- *Flexible service model that allows for quick customization and ensures agencies can leverage latest technology as needed*

VPNS core. This solution provides the government with a private connection by provisioning cellular devices to directly connect to a cellular carrier’s MPLS infrastructure and pass that traffic to Lumen at specific Network-to-Network Interconnections (NNIs). This allows agency end users direct access to agency enterprise services and applications from their cellular devices. **Table 1.4.6-1** highlights how the features of the Lumen MWS solution satisfy the EIS evaluation criteria.

**Table 1.4.6-1. MWS Feature Highlights**

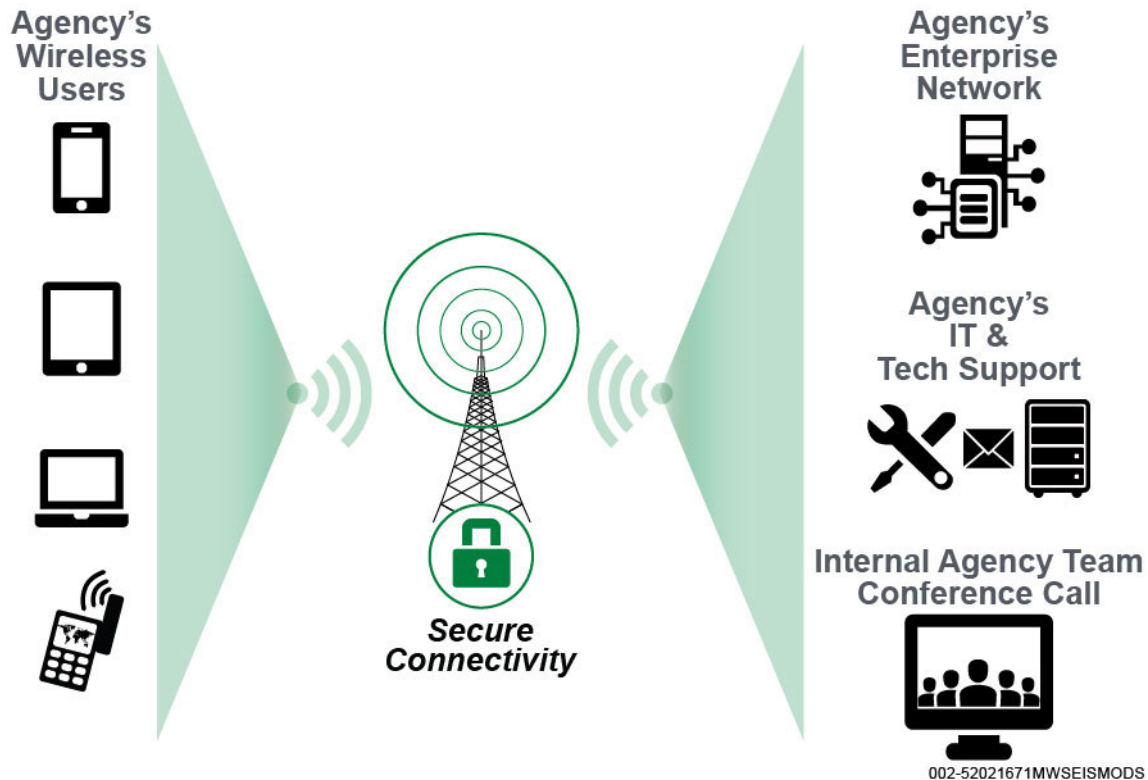
Evaluation Criteria	Features on Lumen MWS
Understanding [M.2.1.1]	<ul style="list-style-type: none"> <li>■ Delivers full capabilities for voice, data and connectivity to the Internet from mobile phones, fixed wireline networks, and satellite based networks</li> <li>■ Provides connectivity to Public Switched Telephone Network (PSTN) and worldwide dialing plan, commercial satellite-based services, the Internet, and agency mobile terminals including cellular phones, smartphones, wireless-enabled Notebook and Laptop PCs, and PDAs</li> <li>■ Furnishes mobile devices with built-in features meeting EIS cell phone and smart phone requirements</li> <li>■ Offers full range of plans to meet agency wireless requirements</li> <li>■ Complies with Wireless Enhanced 911 Rules</li> </ul>
Quality of Service [M.2.1.2]	<ul style="list-style-type: none"> <li>■ In-place relationships with telecommunications carriers with the most advanced network infrastructure ensures reliability, resiliency, and ability to seamlessly upgrade as new technology becomes available</li> </ul>
Service Coverage [M.2.1.3]	<ul style="list-style-type: none"> <li>■ Global wireless network via in-place relationships with major telecommunications carriers provides coverage in more than 400 U.S. cities including the top 100 CBSAs in addition to coverage for 225 countries worldwide.</li> </ul>
Security [M.2.1.4]	<ul style="list-style-type: none"> <li>■ Secure voice communications with FIPS-compliant encryption for cellular phones</li> <li>■ Built-in security features for smartphones including screen lock and password authentication</li> <li>■ Wireless Priority Services (WPS) allows authorized National Security and Emergency Preparedness personnel to gain access to next available wireless radio channel to initiate calls during an emergency.</li> </ul>

**1.4.6.1 Service and Functional Description [L.29.2.1, M.2.1, C.2.6.1]**

The Lumen MWS solution utilizes a National Cellular Carrier to provide a wireless network for the wireless transmission service between mobile devices as depicted in **Figure 1.4.6.1-1** and fulfill the mandatory service requirements for MWS identified in SOW C.2.6. Lumen’s service and bandwidth depends on the characteristics of the mobile device and wireless technology standard the network and service platform is based upon that may include 2G, 2.5G, 3G, 4G LTE, and in the future 5G. The Lumen MWS solution also offers Short Messaging Services. SMS is a feature of MWS that is highly used by mobile device users. It provides the capability of sending and receiving text messages. The text can be comprised of any alphanumeric characters and may be up to 160 characters in length. MMS is another MWS feature that provides



the ability to now send and receive multimedia content that includes images, streaming video, audio and graphics.



**Figure 1.4.6.1-1. Lumen MWS Offering.** Provides agencies mobile access to mission critical voice, video and data services when and where their mission requires.

The next several sections present a technical description of our offering, and demonstrate our capabilities in the following areas: Standards, Connectivity, Technical Capabilities, Features, Interfaces, and Performance Metrics. Lumen's MWS solution leverages the carriers' wireline backbone that transports both the wireless and wireline user traffic with global reach through their roaming arrangements, providing coverage in more than 400 U.S. cities including all of the top 100 CBSAs plus more than 225 countries worldwide.

#### **1.4.6.2 Standards [C.2.6.1.2]**

Lumen provides MWS in full compliance with the requirements of SOW C.2.6.1.2. Specifically, we will comply with the following standards:

- 
1. 2.5G [based on General Packet Radio Service (GPRS) or Code Division Multiple Access (CDMA-2000 – 1xRTT)]:
    - a) ETSI GSM-MAP
    - b) TIA IS-41
  2. 3G [based on CDMA] ITU-RTT IMT-2000:
    - a) European ETSI/GSM Wideband CDMA (WCDMA) (also known as Universal Mobile Telecommunications System (UMTS))
    - b) US CDMA Development Group (CDG) CDMA-2000 Evolution Data Optimized (EV-DO)
  1. 4G [based on 3GPP Long Term Evolution (LTE)]:
    - a) ETSI TR25.913
  2. Wireless Application Protocol (WAP):
    - a) WAP Forum (Wireless Application Protocol (WAP 1.1 and 2.0) via WAP Gateway)
    - b) IP Mobility Support, IETF RFC 2002
  3. 3G Security:
    - a) 3GPP TS 21.133
    - b) NIST FIPS Publication 140-2
  4. Short Messaging Service (SMS)
    - a) 3GPP TS 03.40
    - b) GSM 03.41
  5. Multimedia Messaging Service (MMS):
    - a) 3GPP TS 23.140
    - b) Open Mobile Alliance
  6. 5G Future (according to Next Generation Mobile Networks Alliance group) – draft standards are under study, but the service is expected to roll out by 2020:
    - a) Will efficiently support the Internet of Things, broadcast-like services, and lifeline communications in times of natural disaster, as well as novel applications such as mission critical control or traffic safety, requiring reduced latency and enhanced reliability.
    - b) May be based on new technologies such as mesh networking and/or beam-division multiple access and relays with group cooperation, whereby devices communicate with each other directly rather than relying on network operators' base stations.
  7. Lumen will comply with new versions, amendments and modifications made to the above-listed documents/standards including beyond 4G.

**1.4.6.3 Connectivity [C.2.6.1.3]**

As required by SOW C.2.6.1.3, the Lumen MWS connects to and interoperates with the PSTN, the worldwide dialing plan per ITU Recommendation E.164, the Internet, and agency mobile devices made up of smartphones, cell phones, wireless-enabled Notebooks, Laptop PCs and PDAs. Our MWS is also able to originate and terminate calls to users of commercial satellite-based services.

**1.4.6.4 Technical Capabilities [C.2.6.1.4]**

Lumen provides MWS including all required capabilities for voice, data and internet from mobile phones, fixed wireline networks, and satellite based networks. We furnish mobile devices with built-in features that meet EIS requirements for cellular phones and smart phones, offer the full range of plan options to meet agency wireless requirements, and comply with Wireless Enhanced 911 Rules. **Table 1.4.6.4-1** illustrates how the Lumen MWS complies with all SOW technical capabilities requirements.

**Table 1.4.6.4-1. Lumen’s MWS Technical Capabilities**

Lumen Compliance	SOW C.2.6.1.4 Requirement	The Lumen Compliant Solution
✓	1. Voice Call Origination and Termination	<ul style="list-style-type: none"> <li>■ The Lumen MWS has the ability to originate and receive voice calls from mobile phones, fixed wireline networks, and satellite-based networks.</li> </ul>
✓	2. Provisioning of Mobile Devices	<ul style="list-style-type: none"> <li>■ The Lumen MWS provides mobile devices (smartphones and cellular phones) as required, supporting capabilities that include:                             <ul style="list-style-type: none"> <li>▪ Cellular Phones, including built-in available features; wireless broadband devices (including mobile Wi-Fi hotspots and MiFi wireless routers); and secure voice communications with FIPS-compliant encryption (as available)</li> <li>▪ Smartphones, including built-in available features; e-mail; web browser; Personal Information Management (PIM)—including contact and calendar information and documents/notes; ability to sync with leading e-mail, contact/address, and calendar platforms; vibrate alert to e-mails and text messages; ring alert to e-mails and text messages; ability to transfer photos/pictures directly to computer; remote kill (as available); remote wipe (as available); ability to disable audio, video, and all recording functionality (as available); ability to transmit and receive data (including running an agency specific app) while conducting a voice session (as available).</li> </ul> </li> </ul>
ü	3. MWS Plans	<p>The Lumen MWS solution provides the following plans and plan aspects for GFP and user-owned devices;</p> <ul style="list-style-type: none"> <li>■ Voice Service Plans including voice calling and text messaging (SMS).</li> <li>■ Data Add-On Service Plans including data added to voice service plans. Data may include e-mail, Internet access, video, Multimedia Messaging Service (MMS), and other data.</li> <li>■ Data only Service Plans including e-mails, Internet access, video, MMS, and other data transport not combined with voice service plans.</li> <li>■ Optional machine-to-machine (M2M) - M2M and telemetry products providing</li> </ul>

Lumen Compliance	SOW C.2.6.1.4 Requirement	The Lumen Compliant Solution
		wireless connectivity to machines, vehicles, or assets. <ul style="list-style-type: none"> <li>■ Mobility applications for mobile device management in accordance with SOW C.2.8.6 Managed Mobility Service.</li> <li>■ Mobile Roaming Plans including both domestic and non-domestic plans covering voice calls, messaging, multimedia, and data.</li> <li>■ Pooling of domestic data (gigabytes) within the same billing account at a level specified by the ordering entity (e.g., an entire agency or multiple sub-bureaus within an agency).</li> <li>■ Voice add on to unlimited data plans do not apply as the SREs that support this capability must be a phone and not a data only device. This is not priced due to this issue. Tablets are an example of this.</li> </ul>
✓	4. Compliance with Wireless E911 Rules	<ul style="list-style-type: none"> <li>■ The Lumen MWS complies with Wireless Enhanced 911 (E911) Rules including Phases I and II as stipulated by the Federal Communications Commission.</li> </ul>

1.4.6.5 Features [C.2.6.2]

Table 1.4.6.5-1 presents the features of the Lumen MWS in compliance with requirements identified in SOW C.2.6.2.

Table 1.4.6.5-1. Features of Lumen’s MWS

Lumen Compliance	SOW C.2.6.1.4 Requirement	The Lumen Compliant Solution
✓	1. Wireless Priority Services (WPS)	<ul style="list-style-type: none"> <li>■ Allows authorized National Security and Emergency Preparedness (NS/EP) personnel to gain access to the next available wireless radio channel in order to initiate calls during an emergency when channels may be congested.</li> <li>■ Invokes WPS by dialing *272 prior to destination number on wireless terminals subscribed to WPS.</li> </ul>
✓	2. Directory Assistance with Call Completion	<ul style="list-style-type: none"> <li>■ Allows user to obtain at least two look-up phone numbers and connect to one of them.</li> </ul>
✓	3. Domestic to Non-Domestic Calling	<ul style="list-style-type: none"> <li>■ Allows user to make non-domestic calls.</li> </ul>
✓	4. International Mobile Roaming (Optional)	<ul style="list-style-type: none"> <li>■ Lumen provides this optional MWS feature allowing a user to roam internationally with wireless Internet connectivity and communications capability.</li> <li>■ The International Roaming plans are a monthly recurring charge. Additional usage rates per country will also apply. Roaming Countries must be defined by the Government.</li> </ul>
✓	5. Personal Hotspot	<ul style="list-style-type: none"> <li>■ Enables wireless device to be used as hotspot to connect another device to the Internet or private network.</li> </ul>
ū	6. Indoor Cellular System Installation	<ul style="list-style-type: none"> <li>■ Allows and/or improves indoor wireless operation using Femtocells and Microcells.</li> </ul>
✓	7. Push to Talk with Group Talk (Optional)	Lumen provides this optional MWS feature, which: <ul style="list-style-type: none"> <li>■ Enables users to connect directly with other users by pressing a button on their wireless terminals</li> <li>■ Indicates via an icon on the handset whether a user on their calling list is available</li> <li>■ Allows business colleagues or work teams to set up and manage group calling lists</li> <li>■ Supports groups of up to 10 participants</li> </ul>

Lumen Compliance	SOW C.2.6.1.4 Requirement	The Lumen Compliant Solution
		Allows users to create up to 50 group lists and store 100 individual contacts

**1.4.6.6 Interfaces [C.2.6.3, C.2.6.3.1]**

The Lumen MWS solution supports all of the interfaces for provisioning of MWS at the SDP specified in SOW C.2.6.3.1.

UNI Type	Interface Type and Standard	Payload Data Rate or Bandwidth	Protocol Type
1	Air Link: (Std: GSM and IS-136 TDMA)	Up to 116 Kbps	1. Transparent 2. IP v4 3. IP v6
2	Air Link: (Std: CDMA 1xRTT)	Up to 144 Kbps	1. Transparent 2. IP v4 3. IP v6
3	Air link: (Std: 3G WCDMA)	Up to 384 Kbps	1. Transparent 2. IP v4 3. IP v6
4	Air Link: (Std: CDMA EVDO)	Up to 500 Kbps	1. Transparent 2. IP v4 3. IP v6
5	Air Link: (Std: WCDMA-HSDPA) [Optiona ]	Up to 14.4 Mbps	1. Transparent 2. IP v4 3. IP v6
6	Air Link: (Std: 4G LTE)	Up to 100 Mbps (maximum 300 Mbps)	1. ITU 3GPP (TR25.913) 2. IP v4 3. IP v6

**1.4.6.7 Performance Metrics [M.2.1, C.2.6.4, G.8]**

The Lumen MWS solution meets all performance metrics specified in SOW C.2.6.4.1. We use tools to collect and monitor performance data.

Key Performance Indicator (KPI)	Service Level	Performance Standard (Threshold)	Acceptable Quality Level (AQL)	How Measured
Availability	Routine	99.5%	≥ 99.5%	See Notes 1 and 2
Time To Restore (TTR)	Without Dispatch	4 hours	≤ 4 hours	
	With Dispatch	8 hours	≤ 8 hours	

Notes:

- 1) MWS availability is calculated based on availability of access to the contractor's network from the contractor's cell site.



relevant COMSATCOM experience in both the Government/DoD and commercial sectors. Our teaming partner, [REDACTED] specializes in providing end-to end satellite solutions including design, integration, installation, operations, maintenance, and training.

The Lumen Team delivers integration and operation of global satellite solutions across multiple satellites, teleports, and backhaul terrestrial networks supported by on-site engineering and NOC services. The partnerships and agreements we have among multiple fleet owners such as Intelsat Government Corporation (IGC) and SES-Government Solutions (SES-GS) give us the flexibility to provide the most cost-effective design and technically advantageous CSCS solutions. We design, implement, and deliver all service enabling devices—including Earth Terminals (ET) and RF equipment—and provide satellite bandwidth, link budget analysis, transmission plans, and engineering services (e.g., integration, operations, and maintenance), and support systems. Our experienced field support personnel manage and oversee permitting, licensing, construction, installation, configuration, and management of earth station terminals in some of the most challenging locations around the globe. Additionally, Lumen’s CSCS is fully compliant with Section 508 requirements identified in SOW C.4.4. **Figure 1.4.8.1-1** highlights how the features of the Lumen CSCS solution satisfy the evaluation criteria.

**Figure 1.4.8.1-1.CSCS Feature Highlights**

EVALUATION CRITERIA	FEATURES OF LUMEN CSCS
Understanding [M.2.1.1]	<ul style="list-style-type: none"> <li>Satellite personnel with decades of relevant COMSATCOM supporting GSA, other Federal Government, State Government, and commercial sectors</li> <li>Current experience providing range of satellite solutions to customers with worldwide missions</li> </ul>
Quality of Service [M.2.1.2]	<ul style="list-style-type: none"> <li>Skilled technical experts monitor network to ensure compliant, scalable, reliable, resilient CSCS delivery</li> <li>[REDACTED]</li> </ul>
Service Coverage [M.2.1.3]	<ul style="list-style-type: none"> <li>Master Service Agreements in place with all major commercial space segment providers, providing global geographic coverage in any available COMSATCOM frequency band</li> </ul>
Security [M.2.1.4]	<ul style="list-style-type: none"> <li>CSCS solution complies with specified IA requirements, including CNSSP 12, DODI 8581.01, DODD 8581.1E and Minimum Security Controls</li> </ul>

EVALUATION CRITERIA	FEATURES OF LUMEN CSCS
	<ul style="list-style-type: none"> <li>Lumen and subcontracting partners perform security operations in accordance with industry best practices and standards in cyber, personnel and physical security</li> </ul>

**1.4.7.1 Service and Functional Description [L.29.2.1, M.2.1, C.2.7]**

The Lumen CSCS solution fulfills the mandatory service requirements for CSCS contained in SOW C.2.7. This section presents a technical description of our offering, demonstrating our capabilities in the following areas: Standards, Technical Capabilities, Features, Interfaces, and Performance Metrics. Lumen’s CSCS solution leverages our overall network architecture described in Section 1.1 to deliver the global reach of our satellite transmission capabilities as shown in **Figure 1.4.7.1-1**.

**1.4.7.2 Standards [C.2.7.1.2]**

The Lumen Team provides end-to-end EIS satellite RF transmission and air interface services in full compliance with the requirements of SOW C.2.7.1.2 and applicable TOs. These include Military Standard (MIL-STD)-188-164, MIL-STD-188-165, DODI 8581.01, North American Numbering Plan (NANP), ITU-TSS World Numbering Plan (Standard: ITU-TSS E-164), IETF RFCs for IPv4/v6, and proprietary air-link interface standards based on mobile satellite systems, such as the Inmarsat Broadband Global Area Network (BGAN) and the Iridium satellite constellation.



**Figure 1.4.7.1-1. EIS CSCS Resources.** *The Lumen Team satisfies all CSCS requirements.*

**1.4.7.3 Technical Capabilities [C.2.7.1.3]**

The Lumen Team provides CSCS bandwidth in compliance with SOW and TO requirements. At a minimum, CSCS provided is in full compliance with the performance



specifications of SOW C.2.7.3. The satellite bandwidth we deliver is non pre-emptible, unless otherwise specified in individual TOs.

Each Earth Terminal (ET) we provide is certified and approved for use by the satellite system operator of the system through which it is being used, with access to terrestrial backhaul connections across our Lumen owned, operated, and maintained MPLS backbone. This ensures maximum performance and immediate attention in the unlikely event a failure is experienced.

In our CSCS solution, we deliver CFSS Satellite Internet Service (SIS) providing internet access as well as global voice service. We also provide CMSS internet access, voice calling, SMS texting, facsimile, Machine to Machine (M2M), and streaming services. For CMSS, we provide dual-mode satellite/GSM and tri-mode satellite/CDMA/AMPS satellite phones/terminals and encrypted transmission.

#### **1.4.7.4 Features [C.2.7.2]**

The Lumen Team provides all of the following CFSS mandatory features:

**1. Capacity:** The Lumen Team provides scalable capacity in any available COMSATCOM frequency band. We currently have considerable Commercial Satellite Communications (COMSATCOM) bandwidth on lease across multiple satellites globally. We routinely provide surge capacity to meet both routine and emergency requirements.

**2. Coverage:** The Lumen Team is able to provide COMSATCOM coverage anywhere globally in any available COMSATCOM frequency band, as required by the SOW. Our access to global and regional constellation owners through in-place Master Service Agreements provides us the

#### **Strong History of COMSATCOM Performance**

Lumen teaming partner *By Light* has been awarded nine TOs on the GSA CS2-SB IDIQ

- Agencies supported include the Missile Defense agency, Defense Logistics agency (DLA), Asymmetric Warfare Group, Joint Communications Support Element, U.S. Army Corps of Engineers, U.S. Africa Command, and U.S. Northern Command
- Services provided include satellite transponder capacity, network monitoring, teleport services and commercial internet access services

capability to support coverage requirements in all available COMSATCOM frequency bands. Once the coverage requirements are specified our Team compares the available coverage between our global and regional constellation owners and provides the best value coverage and capacity determined on EIRP, G/T, and cost. [REDACTED]

[REDACTED]

[REDACTED]

**3. Network Monitoring (Net OPS):** The Lumen Team provides an integrated Net OPS capability that collects and delivers near real-time monitoring, fault/incident/outage reporting, and provide real-time information access to ensure effective and efficient operations, performance, and availability consistent with commercial best practices. The Lumen Team NOC is staffed with highly skilled and experienced technical experts possessing security clearances and having prior military and Government satellite experience. Our standard operating procedures define response actions to service degradation or system failures using standardized and well-documented troubleshooting and tiered on-call technical support escalation procedures. Our team manages the coordinated network monitoring activities for all of the elements of proposed solutions and delivers the specified Net OPS information in the frequency and format defined by the Ordering Contracting Officer (OCO).

**4. EMI/RFI Identification, Characterization, and Geo-location:** The Lumen Team provides Electro Magnetic Interference (EMI) / Radio Frequency Interference (RFI) identification, characterization, and geo-location. This capability is inherent in our proposed architecture as we use automated spectrum analyzers that monitor satellite RF power, noise, and waveform and alert NOC specialists to the presence of EMI/RFI. We endeavor to identify, and characterize sub-carrier EMI/RFI, and to geo-locate the source of EMI/RFI, reporting our findings. We also establish and use with the Ordering Activity a mutually agreed upon voice and media communications capability able to protect Controlled Unclassified Information (CUI) data.

**5. Interoperability (Net Ready):** The Lumen CSCS has the capability to access and interoperate with commercial and Government teleports/gateways, providing

service access to or among networks or enclaves. For EIS, all CSCS operates 24-hours daily, including weekends and holidays, and is monitored closely and operates under commercial standards and best practices. The teleport services provided contain all Inter-Facility Link (IFL), CAT-5/6, and fiber optic connections required for routing of the EIS network traffic.

**6. Information Assurance:** Our Team ensures that all provisioned services meet specified IA requirements, including CNSSP 12, DODI 8581.01, DODD 8581.1E and Minimum Security Controls. The Lumen solution also complies with FISMA as implemented by FIPS 200, meeting the requirements for a low-impact information system as described in NIST SP 800-53. Lumen provides a completed IA Compliance Matrix in accordance with the EIS contract and respective TO requirements. In providing CSCS, we continually monitor and verify IA compliance in accordance with the IA Compliance Matrix requirements for Mission Assurance Category (MAC) I, II, or II, as appropriate, throughout the life of each custom engineered end-to-end solution. We understand that the use of any satellite not compliant with DODI 8581.01 is contingent upon approval by the cognizant Authorizing Official accepting the associated risk.

#### **1.4.7.5 Interfaces**

Lumen provides radio frequency and other interfaces, as defined in individual TOs for CSCS.

#### **1.4.7.6 Performance Metrics [M.2.1, C.2.7.3, G.8]**

Lumen meets all of the CSCS performance metrics shown in the CSCS performance specifications table in SOW C.2.7.3. The Lumen GovNOC monitors all Lumen Enterprise services provided using our network.

#### **1.4.8 Managed Service (optional)**

##### **1.4.8.1 Web Conferencing Service [L.29.2.1, C.2.8.2; C.4.4]**

For EIS, Lumen provides comprehensive

#### **Experienced WCS Performance**

- Diverse WCS experience supporting industry and Government including multiple agencies through GSA WITS3
- Global reach provides scalable solutions driven by consistent network platforms for efficiency
- Secure, high-quality, carrier-grade connections via private IP backbone network
- Full-featured services enable better tracking, cost management, billing

WCS that enable rich, collaborative sharing of applications. Our WCS solution offers a working environment that enables shared, strategic decision-making, conference management, control of presentations, and recording of all participant meetings in a simple and user-friendly format.

**Figure 1.4.8.1-1** highlights how the features of the Lumen WCS solution satisfy the evaluation criteria.

**Figure 1.4.8.1-1. WCS Feature Highlights**

EVALUATION CRITERIA	FEATURES OF LUMEN OWS
Understanding [M.2.1.1]	<ul style="list-style-type: none"> <li>• Comprehensive WCS enables rich, collaborative sharing of applications</li> <li>• Working environment supports shared, strategic decision-making, conference management, control of presentations and recording of participant meetings in a simple and user-friendly format</li> </ul>
Quality of Service [M.2.1.2]	<ul style="list-style-type: none"> <li>• High quality web connections via private IP backbone networks</li> <li>• Flexible, scalable WCS using both the Lumen Web Meeting and Cisco WebEx platforms</li> <li>• Compatible with variety of commercial web browsers, ensuring compliant, reliable, accessible WCS</li> </ul>
Service Coverage [M.2.1.3]	<ul style="list-style-type: none"> <li>• WCS solution rides on globally distributed Lumen network, with integrated, strategically dispersed communications switches, switching centers, and dedicated network links to eliminate latency issues and service interruptions</li> </ul>
Security [M.2.1.4]	<ul style="list-style-type: none"> <li>• Multilayer security validated by rigorous independent audits, including SSAE-16</li> <li>• Lumen and subcontractor partners deliver security operations using industry best practices and standards in support of cyber, personnel, and physical security</li> </ul>

**1.4.8.1.1 Service and Functional Description [L.29.2.1, M.2.1, C.2.8.2]**

Lumen WCS fulfills the mandatory service requirements for WCS contained in SOW C.2.8.2 leveraging our overall network architecture described in Section 1.1. This section presents a technical description of our offering, demonstrating our capabilities in the following areas: Standards, Connectivity, Technical Capabilities, Features, Interfaces, and Performance Metrics.

Lumen WCS is part of a suite of services Lumen has developed, provided through Lumen resources and not outsourced. Our WCS brings a robust “Network of Networks” (NoN) approach to media delivery, an exemplary reputation for quality resulting in zero downtime, and a superior Web-based media management tool suite. Our WCS platform simplifies streaming tasks and minimizes delivery issues.

**1.4.8.1.2 Standards [C.2.8.2.1.2]**

Lumen’s WCS offering is compliant with the standards listed in SOW C.2.8.2.1.2. Members of our Team are active in a variety of industry forums and working groups, such as Internet Engineering Task Force (IETF), the North American Network Operators Group (NANOG) and the American Institute of Electrical Engineers (IEEE) and committed to implementing future standards as technologies are developed and standards are defined and become commercially available. Our WCS offering complies with the HTTP, HTTPS, Optional IETF RFC 3261 for Session Initiation Protocol (SIP), ITU-T T.120 series, TLS, and TCP/IP protocols. It also complies with the mandatory IETF RFC Initiation.

**1.4.8.1.3 Connectivity [C.2.8.2.1.3]**

Lumen’s robust WCS infrastructure is connected to and interoperates with the Internet subscribing Agencies’ IP networks. All WCS content is available through Universal Record Locators (URL) which users can access via the agency intranets or the Internet.

**1.4.8.1.4 Technical Capabilities [C.2.8.2.1.4]**

Lumen provides WCS using two service platforms: **Lumen’s Web Meeting** and **Cisco’s WebEx**. We provide scalable Web Meeting and WebEx solutions best matched to user requirements, on a case-by-case (TO) basis. Lumen WCS has built-in functionality providing the controls needed to manage web conference online, change account options, and record entire meetings, including any visuals for playback later.

**Figure 1.4.8.1.4-1** shows how the Lumen EIS WCS fully complies with all SOW technical capabilities requirements.

**Figure 1.4.8.1.4-1. WCS Technical Capabilities**

LUMEN COMPLIES	SOW C.2.8.2.1.4 REQUIREMENT	LUMEN COMPLIANT SOLUTION
✓	1. Capability for participant collaboration	<ul style="list-style-type: none"> <li>Allows real-time sharing of documents, and participants may exchange documents through file transfer and electronic whiteboard functions</li> </ul>

LUMEN COMPLIES	SOW C.2.8.2.1.4 REQUIREMENT	LUMEN COMPLIANT SOLUTION
✓	2. WCS capabilities	<ul style="list-style-type: none"> <li>Allows for user authentication by requiring a login and password for access</li> <li>Initial greeting screen can be customized to maintain agency look and feel</li> <li>On-line help available to presenters and end-users</li> <li>Supports both point-to-point and multi-point Web conferences</li> </ul>
✓	3. Interoperate with internet and IP network(s)	<ul style="list-style-type: none"> <li>Based on an Internet delivery model and fully capable of interoperating with an agency's Internet-connected networks and systems.</li> </ul>
✓	4. Compatible with commercial web browser software	<ul style="list-style-type: none"> <li>Compatible with most commercially available Internet Web browser software packages and successfully tested with Internet Explorer, Netscape, Firefox, Safari, and Opera for Microsoft Windows, Apple Macintosh, and Linux operating systems.</li> </ul>
✓	5. Capability for users to test and verify	<ul style="list-style-type: none"> <li>Delivers any plug-ins necessary to utilize the web conference users. Currently, this is supplied as a link or automatic download when the user attempts to enter the conference if the end-user does not already have it installed.</li> </ul>
✓	6. Support dynamic content	<ul style="list-style-type: none"> <li>Provides rich multimedia experience by allowing the sharing and display of dynamic content, including AVIs, flash animation, animated .gifs, and dynamic HTML pages.</li> </ul>
✓	7. Available on demand	<ul style="list-style-type: none"> <li>Available on demand through a scheduled reservation</li> <li>Presenters able to start a presentation without notice</li> <li>Meeting reservations may be scheduled for up to a year beyond the current date.</li> </ul>
✓	8. Provide a reservation system	<ul style="list-style-type: none"> <li>Authorized users can schedule, reserve, and cancel web conferences 1-year in advance</li> <li>Scheduling performed by time and day of the week, either as a single or recurring event</li> <li>Recurring events can be scheduled on a daily, weekly, monthly, or custom basis.</li> </ul>
✓	9. Provide email notification	<ul style="list-style-type: none"> <li>Meeting notifications and RSVP requests can be sent to invited participants</li> <li>Notifications sent via email and include information necessary to access Web conference</li> <li>Authorized users may add participants at any time, without advance notice, through a provided Web interface.</li> </ul>
ü	10. Capability to extend conference time	<ul style="list-style-type: none"> <li>Subscribing agency able extend the scheduled conference time as necessary.</li> </ul>
✓	11. Provide authentication and encryption	<ul style="list-style-type: none"> <li>WCS sessions are secured through SSL/TLS and AES encryption</li> <li>Meeting participants and agency administrators are authenticated by login and password to before being granted access.</li> </ul>
✓	12. Provide access through URL	<ul style="list-style-type: none"> <li>Web conferences are access ble via a URL address, with users prompted to enter a login and password to validate that they are authorized to participate.</li> </ul>
✓	13. Provide passwords	<ul style="list-style-type: none"> <li>Provides conference leaders and participants passwords necessary to use our services.</li> </ul>
✓	14. Support at least 1,000 participants	<ul style="list-style-type: none"> <li>Supports at least 1,000 simultaneous participants in a single Web conference.—the maximum number of concurrent conferences is not restricted.</li> </ul>
✓	15. Capability to traverse and interoperate with agency firewalls and layers	<ul style="list-style-type: none"> <li>Successfully operates through most firewalls and security layers using standard protocols.</li> <li>Lumen works with the agency to verify the agency firewall is compat ble with our service.</li> </ul>

LUMEN COMPLIES	SOW C.2.8.2.1.4 REQUIREMENT	LUMEN COMPLIANT SOLUTION
✓	16. Provide operator assistance	<ul style="list-style-type: none"> <li>Operator assistance is available via a toll-free number, providing immediate help to resolve technical problems or service issues</li> <li>Online Help is available to presenters and conference participants.</li> </ul>
✓	17. Provide annotation capability	<ul style="list-style-type: none"> <li>The presenter can provide annotation during a Web conference, using the presenter's mouse as a pointer.</li> </ul>
✓	18. Provide viewable participant list	<ul style="list-style-type: none"> <li>Through the Web interface, participants and presenters are able to view a list of attendees currently participating in a conference.</li> </ul>
✓	19. Support group web surfing	<ul style="list-style-type: none"> <li>Supports group web surfing, allowing multiple participants to see what the presenter is doing.</li> </ul>
✓	20. Support file transfer	<ul style="list-style-type: none"> <li>Participants have ability to transfer files while using the services provided by Lumen</li> <li>Once a file is uploaded, conference participants have the option to download it during the meeting or event, and files can be sent to all participants or selected participants, with participants having the option to accept or reject the file transfer.</li> </ul>
✓	21. Support multiple presenters for webcasts	<ul style="list-style-type: none"> <li>Supports multiple presenters within a meeting or event</li> <li>Presenters can be changed dynamically during the course of the meeting as necessary.</li> </ul>
✓	22. Support video webcasts	<ul style="list-style-type: none"> <li>Supports video webcasts up to 3,500 or more participants.</li> </ul>
✓	23. Provide polling, voting, and signaling capability	<ul style="list-style-type: none"> <li>Provides polling and voting capabilities. Polls can be established before a Web conference, and participants can signal the conference leader for questions.</li> </ul>
✓	24. Provide polling/voting feedback	<ul style="list-style-type: none"> <li>Provides polling and voting feedback. Presenters have the capability to instantly view polling and voting results.</li> </ul>
✓	25. Provide meeting lobby and access control (Optional)	<ul style="list-style-type: none"> <li>Satisfies optional meeting lobby requirement through which conference leaders can admit meeting participants</li> <li>Conference leaders can lock a conference through the Web interface, preventing additional users from joining and participating.</li> </ul>
ü	26. Provide capability to print and save conference presentations	<ul style="list-style-type: none"> <li>Conference leaders have capability to print or save to file the presentation used during the event, and can grant participants the same capabilities if desired.</li> </ul>
✓	27. Support text chat	<ul style="list-style-type: none"> <li>Supports text chat with chat sessions that can be made public, where the chat is visible to all conference participants, or kept private between select participants.</li> </ul>
✓	28. Provide survey capability	<ul style="list-style-type: none"> <li>Able to present a survey to all, or to a random percentage of participants—this can be used to gather feedback and/or capture customer satisfaction data.</li> </ul>

**1.4.8.1.5 Features [C.2.8.2.2]**

Lumen WCS provides the three mandatory features required: Streaming Audio, Streaming Video, and Web Based Presentation Replay. **Figure 1.4.8.1.5-1** shows how the Lumen EIS WCS fully complies with all SOW features requirements.

**Figure 1.4.8.1.5-1. WCS Service Features**

LUMEN COMPLIES	SOW C.2.8.2.2 REQUIREMENT	LUMEN COMPLIANT SOLUTION
✓	1. Streaming Audio	<ul style="list-style-type: none"> <li>If requested, we deliver one-way audio over the Internet during a WCS session. Audio streams are synchronized with the data portions of the Web conference. Audio can be streamed to our systems via UDP, TCP, or HTTP Streaming.</li> </ul>
✓	2. Streaming Video	<ul style="list-style-type: none"> <li>If requested, we deliver one-way video over the Internet during a WCS session. Video streams are synchronized with the data portions of the Web conference. Video can be streamed to the agency's systems via UDP, TCP, or HTTP Streaming.</li> </ul>
✓	3. Web Based Presentation Replay	<ul style="list-style-type: none"> <li>Web conferences and presentations can be recorded as a multimedia file with the capability to replay Web-based presentations to agency users. Recorded sessions can be archived for a minimum of 30 days after the initial conference. The conference replay can be maintained for a period of up to one (1) year in 30-day increments.</li> </ul>

**1.4.8.1.6 Interfaces [C.2.8.2.3]**

As stated in SOW C.2.8.2.3, there are no interface requirements for WCS, which is browser based.

**1.4.8.1.7 Performance Metrics [M.2.1, C.2.8.2.4, G.8]**

Lumen meets all of the WCS performance metrics shown in the Web Conferencing Service Performance Metrics table in SOW C.2.8.2.4.1. The Lumen GovNOC monitors all Lumen Enterprise services provided using our IP backbone.

**1.4.8.2 Unified Communications Service [L.29.2.1, C.2.8.3]**

[REDACTED]  
[REDACTED]  
[REDACTED] Our

**UCS Highlights**

- FedRAMP Ready status validates the service's high level of security
- Large catalog of collaboration applications, consistent across deployment models and devices, enhance user experience
- Management tools provide EIS customers full visibility and control while reducing total cost of ownership
- Flexible service model ensures EIS customers can leverage the latest technology and gain full user adoption by aligning resources to business needs

UCS maximizes user productivity in and out of the office, fully integrating voice, video, Instant Messaging & Presence (IM&P), Unified Messaging, mobility, desktop sharing, audio/video/web conferencing, and other custom deployments that we tailor to meet



customer requirements. Our UCS gives users a consistent experience across hard/soft phones, desktop, tablet and mobile operating systems.

The Lumen Team UCS solution leverages a secure hosted collaboration solution and a Cisco powered cloud service. This provides a compliant solution that satisfies all evaluation criteria. **Figure 1.4.8.2-1** highlights how the features of the Lumen UCS solution satisfy the evaluation criteria.

**Figure 1.4.8.2.-1. UCS Feature Highlights**

EVALUATION CRITERIA (M.2.1)	FEATURES OF LUMEN UCS
Understanding	<ul style="list-style-type: none"> <li>• Our UCS meets all service requirements through its reliable and secure architecture, availability over our large network, and tailorable user experience, able to be integrated in MS-Lync, Google Apps, and other customer-required applications</li> <li>• Lumen Hosted UCS maximizes user productivity in the office, on the road, or when accessed remotely</li> <li>• Our UCS encompasses fully integrating voice, video, instant messaging &amp; presence (IM&amp;P), mobility, desktop sharing, audio/video/web conferencing and other customer-demanded custom deployments</li> <li>• Our UCS gives users a consistent experience across hard/soft phones, desktop, tablet and mobile operating systems</li> </ul>
Quality of Service	<ul style="list-style-type: none"> <li>• Compliant—combines UC applications from hosted UC datacenters by connecting to Lumen IPVPN and SIP networks to quickly and cost-effectively deliver UC capabilities to EIS customers</li> <li>• Scalable—provides highly available bandwidth with dynamic connectivity regardless of VM UC instance movement—this is true for the network, call processing, and storage layers</li> <li>• Reliable—designed to provide uptime and availability similar to a local IP PBX</li> <li>• Resilient—robust systems and network infrastructure allows us to prevent, predict, minimize, and resolve system events and outages while providing a high-performing service with scalable capacity</li> </ul>
Service Coverage	<ul style="list-style-type: none"> <li>• Supports EIS customers worldwide because we leverage our expansive IP network, data center services, VPN, and SIP trunking capabilities</li> </ul>
Security	<div style="background-color: black; height: 15px; width: 100%; margin-bottom: 5px;"></div> <div style="background-color: black; height: 15px; width: 20%; margin-bottom: 5px;"></div> <ul style="list-style-type: none"> <li>• The Lumen Hosted UCS is architected to secure the ingress and egress points to the hosted infrastructure</li> <li>• Session Border Controllers (SBC) are included to protect and monitor the flows for all SIP connection points</li> <li>• Firewall/Router/IPS/IDS devices are used for all non-SIP traffic</li> <li>• UC Services accessed via the Internet from remote locations or mobile devices are protected by firewalls, DMZ, and higher level protection mechanisms in each data center</li> </ul>

**Proven UCS Solution.** Lumen currently provides the same Cisco-based UCS solution to the U.S. Department of Homeland Security (DHS) in the National Capital

---

Region under the WITS3 contract. Under WITS3, Lumen provides a combination of managed voice, audio and video conferencing, and Unified Communications services.

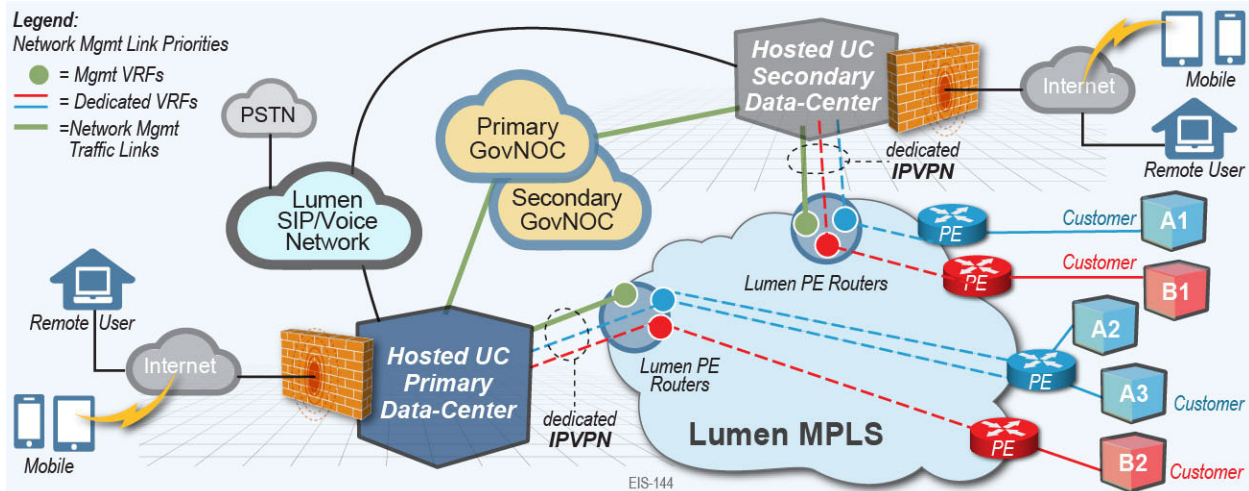
**Proven UCS Team Capability.** In addition to our highly reliable and feature-rich hosted solution, [REDACTED]

#### **1.4.8.2.1 Service and Functional Description [L.29.2.1, M.2.1, C.2.8.3]**

The Lumen UCS solution fulfills the mandatory service requirements for UCS contained in SOW C.2.8.3. We leverage our expansive IP network, data center services, VPN, and SIP trunking capabilities to deliver an integrated UCS solution. Our industry-leading IP-based integration capabilities and offerings to support UCS include the following:

- Global core IP Network infrastructure and expertise
- Managed IP connectivity solutions
- SIP trunking solutions to best suit customer needs
- API capabilities that imbed our communication and collaboration services into a customer's UCS environment
- Industry-leading customer satisfaction ratings

To implement our UCS solution for EIS customers, Lumen provides the necessary transport access paths between the Lumen MPLS/IPVPN network and the customer agency's sites, as well as between the Lumen IPVPN/SIP network and our hosted UC data centers. A high-level diagram of our UCS service architecture, showing reference points depicting separation of domains, is shown in **Figure 1.4.8.2.1-1**.



**Figure 1.4.8.2.1-1. Lumen's UCS Service Architecture.** *Our UCS solution provides connectivity regardless of VM UC instance movement.*

Individual customers can access Lumen UCS with dedicated Virtual Private Network Service (VPNS) access to Hosted UC data centers. Our GovNOCs monitor the status and analyze the performance of the service.

#### 1.4.8.2.2 Standards [C.2.8.3.1.2]

Lumen's EIS offering is compliant with the standards listed in SOW C.2.8.3.1.2.

#### 1.4.8.2.3 Connectivity [C.2.8.3.1.3]

The Lumen Team's UCS platform connects to and interoperates with PSTN (SIP trunk gateway) and agency communication subsystems. Lumen-hosted UC data centers host the UC infrastructure and connect to the Lumen MPLS/IPVPN network. They have alternate paths to Lumen SIP Core network for PSTN access. In case of a WAN failure at customer site, PSTN failover may be supported via Local Site Survivability Gateways and dedicated PRIs at the customer site. While the UC services are provided by the UCS infrastructure from the hosted UC data centers, the Lumen SIP network provides other PSTN services such as voice local services, long distance, toll-free, E911, and directory/operator assistance. This also facilitates agency communication subsystems such as e-mail, audio/video conferencing, IM, and others.

**1.4.8.2.4 Technical Capabilities [C.2.8.3.1.4]**

A summary description of our technical capabilities for UCS is provided in **Figure 1.4.8.2.4-1**.

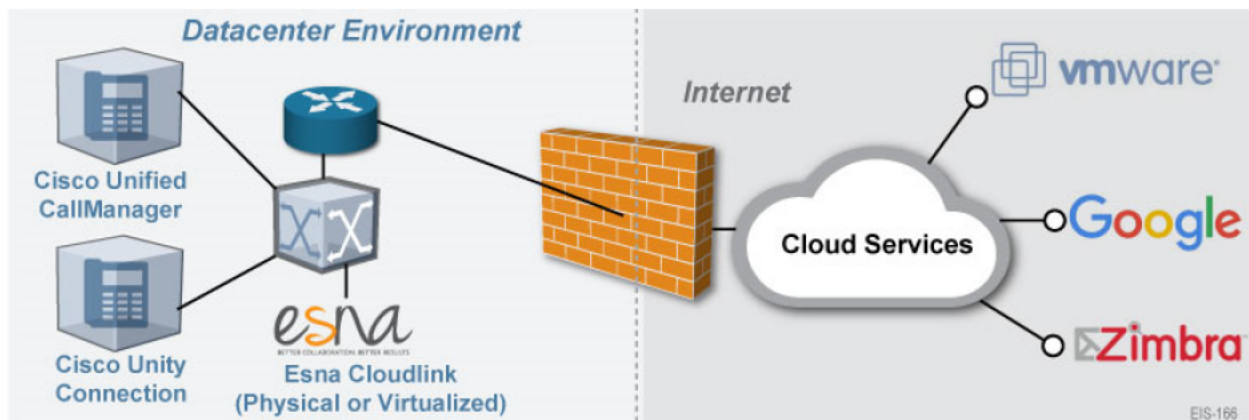
**Figure 1.4.8.2.4-1. Mandatory UCS Technical Capabilities**

LUMEN COMPLIES	SOW C.2.8.3.1.4 REQUIREMENT	LUMEN COMPLIANT SOLUTION
✓	1. Diversity of UC-enabled Devices	<ul style="list-style-type: none"> <li>Lumen engineers are responsive and knowledgeable with the challenges of providing UC across multiple platforms and devices, having provided UCS solutions for many Government and commercial customers. These include desktop phones, mobile devices, wireline and IP phones, soft clients, and video conferencing devices.</li> <li>We apply proven integration testing procedures to ensure consistent UC performance</li> </ul>
✓	2. Unified Messaging	<ul style="list-style-type: none"> <li>Lumen's UCS solution enables modular messaging, presence, instant messaging, text, and the capability to access and manage e-mail, voice mail, and fax messages via the same inbox or interface.</li> <li>The UC Messaging Directory logically represents a telephony hardware device and a telephony dial plan for the enterprise to support a specific UM feature and enables the integration of UM with existing telephony infrastructure.</li> </ul>
✓	3. Mobile Integration	<ul style="list-style-type: none"> <li>Cisco Unified Mobility provides users a single identify and the ability to redirect IP calls from Cisco Unified Communications Manager to different designated phones, such as cellular phones. Users can also transition active calls between their Cisco desktop and their mobile phones without interruption, including from Wi-Fi to cellular.</li> <li>Our solution also provides: simultaneous desktop ringing, desktop pickup, mobile call pickup, security and privacy for calls, mobile voice access, single enterprise voice mailbox, call filters, and caller identification. Users can initiate phone calls, retrieve voice mail and corporate directories, access instant messaging and participate in video conferencing.</li> </ul>
ü	4. Unified User Interface	<ul style="list-style-type: none"> <li>The Lumen Team's UCS solution provides a unified user interface through the Cisco Collaboration Edge Architecture. This allows Cisco Unified Communications Manager to manage endpoints outside the enterprise network. The expressway provides secure firewall traversal and lineside support for Unified Communications Manager registrations. Thus, users can access the applications anywhere and from any type of service</li> </ul>
✓	5. QoS Support	<ul style="list-style-type: none"> <li>The QoS is built into our whole solution from network infrastructure design, installation, and maintenance.</li> </ul>
✓	6. WAN Optimization (Optional)	<ul style="list-style-type: none"> <li>The Lumen applies key WAN Optimization strategies that enable our customers to establish and maintain an efficient and secure network</li> <li>Some optimization strategies include WAN de-duplication and compression, web catching, wide-area file services, and forward error correction</li> </ul>
✓	7. IPv4 and IPv6 Support	<ul style="list-style-type: none"> <li>Lumen's UCS offering fully supports IPv4 and IPv6 addresses, as well as migration arrangements to IPv6 for improved inter-network routing and substantial increase in the number of available, locally administered IP addresses</li> </ul>

LUMEN COMPLIES	SOW C.2.8.3.1.4 REQUIREMENT	LUMEN COMPLIANT SOLUTION
✓	8. Voice Quality	<ul style="list-style-type: none"> <li>Lumen's UCS supports G.711 &amp; G.729 codec. We use G.711 codec for excellent quality of voice. With a sample size of 64kbit/s, G.711 achieves a maximum MOS of 4.1</li> </ul>
✓	9. Security Practices and Safeguards	<ul style="list-style-type: none"> <li>The Lumen Team's hosted UCS solution has a FedRAMP Ready status</li> <li>We provide network and security operations support and monitoring, as required and comply with agency-specific security policies, regulations, and procedures.</li> </ul>

Further details on select technical capabilities of our UCS are provided below.

**Unified Messaging.** We deploy redundant voice messaging servers with Cisco Utility Connection for each customer, which provides centralized voice mail system and unified messaging. This supports access to voice mail, e-mail, and fax through the same inbox. We can integrate Unity Connection with Exchange server or Lotus Notes so voice messages can be received in the form of e-mail. Through the Esna Cloudlink platform, which we securely host, we offer new integrated services for corporate UC management solutions and Google Apps, shown in **Figure 1.4.8.2.4-2**.



**Figure 1.4.8.2.4-2. Esna Cloudlink Platform.** *Esna Cloudlink seamlessly integrates corporate UC applications with cloud-based programs, providing integrated unified messaging and communication services.*

Our UCS provides instant messaging through Cisco IM and Presence Service, shown in **Figure 1.4.8.2.4-3**.



EIS-154

**Figure 1.4.8.2.4-3. Cisco IM and Presence Service.** *The aggregated user information captured by the Cisco IM and Presence Service increases user productivity by helping colleagues to determine the most effective form of communication.*

Cisco IM and Presence Service incorporates the Jabber Extensible Communications Platform and supports SIP/SIMPLE and Extensible Messaging and Presence Protocol (XMPP) for collecting information regarding a user's availability status and communications capabilities. The user's availability status indicates whether the user is actively using a communications device such as a phone. The user's communications capabilities indicate the types of communications that user is capable of using, such as video conferencing, web collaboration, instant messaging, or audio.

**Quality of Service Support.** The Lumen Quality of Service (QoS) process is used to manage network resources and allow different types of traffic to contend inequitably for network resources. We deploy the Cisco UC Manager cluster across geographically distributed sites, connected by an IP WAN with QoS capabilities. Voice, video, and critical data applications may be granted priority or preferential services from network devices so that the quality of these strategic applications does not degrade to unacceptable levels. We use G.711 codec for excellent quality of voice. With a sample size of 64kbit/s, G.711 achieves a maximum MOS of 4.1.

---

**Security Practices and Safeguards.** The Lumen Team's hosted UCS solution, which has earned the status of FedRAMP Ready, implements a 3-layer security schema. The data center core provides a Layer 3 routing module for all traffic in and out of the data center. The aggregation layer serves as the Layer 3 and Layer 2 boundary for the data center infrastructure. The aggregation layer is the connection point for the primary data center firewalls. The data center access layer, serves as a connection point for the server-farm. The virtual-access layer refers to the virtual network that resides in the physical servers when configured for virtualization.

Four classes provide QoS for Voice, Video and Data. Some of these classes can be gradually split into more granular classes, as shown, and multiple DSCPs combine into a single queuing class. The Real-Time queue is for voice and video traffic in general, as they are time-sensitive applications. Signaling/control includes all the control signaling, meaning call signaling, and includes the management control traffic including vMotion traffic. Critical data includes any bulk data transfer, which may include databases. The last best effort class includes other data such as internet traffic.

#### **1.4.8.2.5 Features [C.2.8.3.2]**

Not applicable. No features are listed in the SOW for UCS.

#### **1.4.8.2.6 Interfaces [C.2.8.3.3]**

We support the seven device types listed in SOW C.2.8.3.3. We enable Cisco UC capabilities across different platforms, including desktop phones, smartphones, soft clients, and conferencing endpoints. Our solution can be integrated into MS-Lync, Google Apps, and others. Along with the full range of IP telephony features, users can remotely access voice mail/unified messaging. End-users can check voice mail through IP phones, softphones on their desktop, smartphones, or even through e-mail client. Instant message and presence help users to see the status of other users before initiating chat or an audio/video call. The Cisco Jabber application delivers business-quality voice and video to each desktop. Powered by the market-leading Cisco Unified Communications Manager, the Cisco Jabber application is a soft phone with wideband and high-fidelity audio, standards-based high-definition video (720p), and desk-phone

---

control features. These features mean that high quality and high availability voice and video telephony is available at all locations and to users' desk phones, soft clients, and mobile devices. The Cisco Jabber application makes voice communications simple, clear, and reliable.

#### **1.4.8.2.7 Performance Metrics [M.2.1, C.2.8.3.4, G.8]**

Lumen meets all of the UCS performance standards, thresholds, and quality levels shown in the UCS Performance Metrics table in SOW C.2.8.3.4.1 through the activities of Lumen's GovNOC. The GovNOC monitors all Lumen Enterprise services provided through our IP backbone. Our monitoring tools provide comprehensive visibility of numerous network elements and for accurately measuring AQLs for applicable KPIs.



**1.4.8.3 MANAGED TRUSTED INTERNET PROTOCOL SERVICE (C.2.8.4)**

Lumen was the first MTIPS provider to complete the TIC capability validation (TCV) and received an ATO from GSA on February 4<sup>th</sup>, 2010 for our two geographically diverse TIC Portals in Virginia and Illinois. We have consistently maintained our ATO along with an annual DHS US-CERT TCV/cybersecurity compliance validation (CCV) assessment score of 100% for all of the critical and mandatory MTIPS capabilities. Lumen is committed to maintaining our MTIPS ATO as the government’s security requirements evolve to address emerging cybersecurity threats. Lumen has provisioned MTIPS for more than forty (40) agencies, ranging in access speeds from 1.544 Mbps (T1) to 10Gbps (10GigE).

**1.4.8.3.1 Understanding (L.29.2.1-A; M.2.1-1)**

Lumen’s MTIPS is based upon a network architecture (see **Figure 1.4.8.3.1-1**) that is fully capable of meeting each of the DHS’ 74 TIC 2.2 requirements. Our solutions deliver high availability through a redundant architecture: TIC Portals [REDACTED] [REDACTED] SOCs [REDACTED] [REDACTED] NOCs [REDACTED] [REDACTED] portal-to-MPLS connections; portal-to-Internet dedicated edge (DE) connections; MPLS PE to private core (PCOR) connections; and access options with diversity for automatic failover.

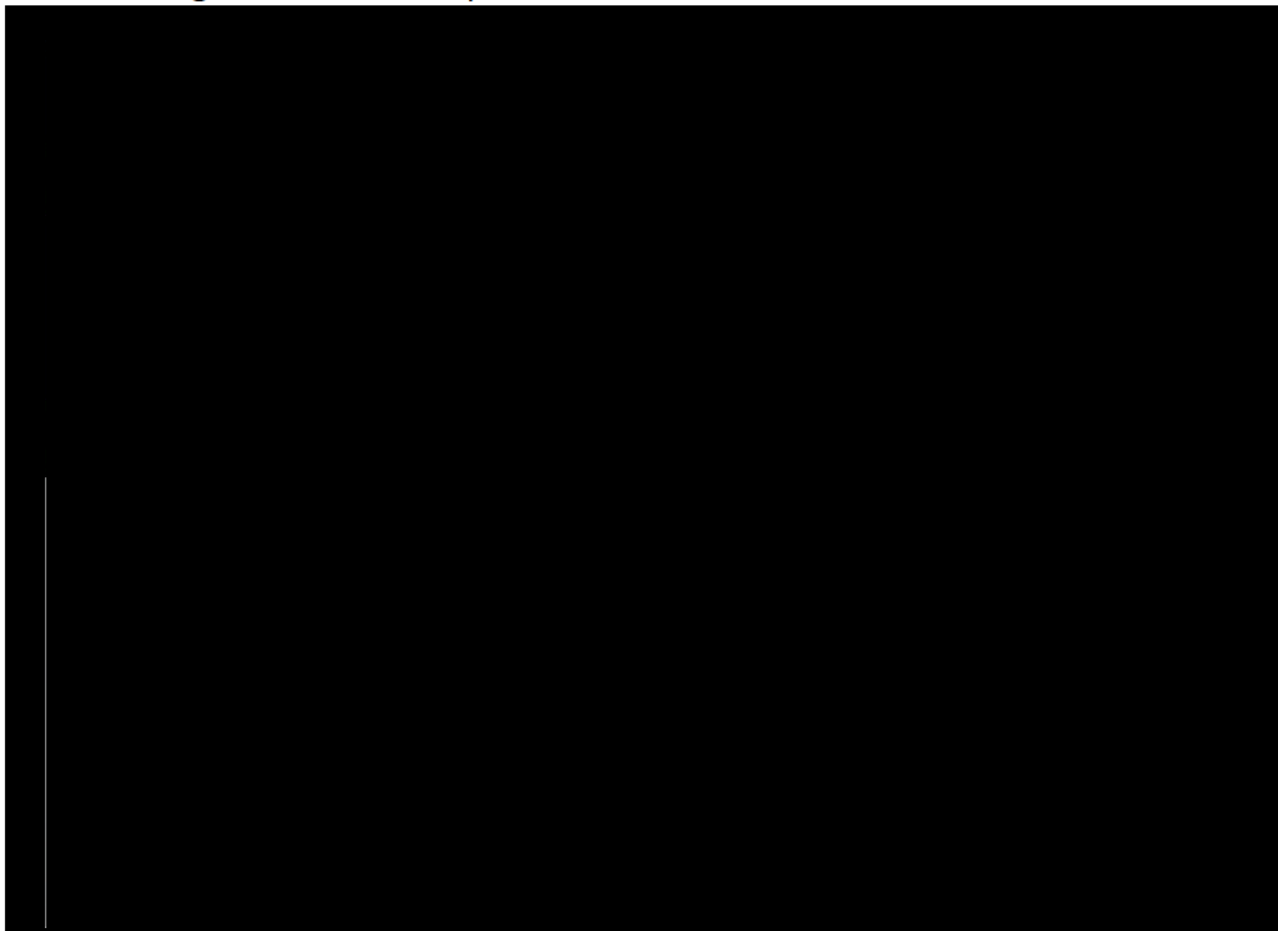
Lumen’s MTIPS provides agencies with numerous key features and benefits as highlighted in **Table 1.4.8.3.1-1**.

**Table 1.4.8.3.1-1. Lumen MTIPS Features and Benefits**

Lumen MTIPS Features	Lumen MTIPS Benefits
Bandwidth Scalability	An MTIPS infrastructure that has been engineered to be scalable as the government’s bandwidth needs increase to accommodate system and user demand.
High Reliability	99.999 percent POP-to-MTIPS network availability. Network transport links are implemented with a high degree of protection and redundancy along with sub 50 ms switchover.
Migration of Custom Signatures	Capability to easily migrate custom signatures during an agency’s implementation/transition.
Virtual Domain (VDOM)	VDOMs divide the MTIPS unified threat management (UTM) into two or more virtual instances that function independently. Each VDOM has its own logical interface, routing configuration, and security policies that allow component-specific rule sets that enable the components to manage their specific network segments. Our VDOM architecture scales to support multiple agencies without impact to the service.
Advanced Mail Filtering	Advanced mail filtering solution that uses an email scanning approach to provide security against email-based intrusion, phishing, spam, and other email-related malware threats.

Lumen MTIPS Features	Lumen MTIPS Benefits
Complete Cybersecurity Oversight	Partner (extranet) and remote access services will be scanned by the MTIPS UTM and DHS tools, and processed by EINSTEIN to provide subscribers with a complete cybersecurity oversight of all connections into the agency enterprise network.

Lumen’s MTIPS and web interfaces are engineered to provide high availability through the use of redundant network connections, assets, and operation centers. Subscribing agencies will be afforded a solution with capabilities offering the protection of the core security services of MTIPS to include managed firewall service (MFS), intrusion detection and prevention service (IDPS), antivirus management service (AVMS), email scanning and archiving, DNS logging, and full packet capture (FPC) functions. **Figure 1.4.8.3.1-1** depicts the Lumen MTIPS TIC 2.0 architecture.



**Figure 1.4.8.3.1-1. Lumen’s MTIPS TIC 2.0 Architecture.**

## Inspection and Filtering

Lumen’s firewall appliances are located within the four MTIPS TIC portals to provide stateful inspection, filtering, blocking, and alerting of all inbound and outbound agency IPv4/IPv6 traffic and protocols such as ICMP, TCP, and UDP protocols. This creates a defense-in-depth security framework and provides a layered inspection and filtering solution enabling individual packet inspection and admission based on an agency’s policy. Lumen’s MTIPS solution includes the following firewall and proxy service features:

- Full content inspection and application proxies
- Implicit deny, making an additional deny policy unnecessary. Traffic is denied unless a policy on the firewall device specifically allows for it
- Destination port(s) and ephemeral ports—only explicitly approved ports will be allowed while all other ports will be blocked by default
- The ability to filter on TCP, UDP, IP addresses, domain names, incoming interfaces, port numbers, and other IP header information
- HTTPS traffic proxies are filtered by the firewall, based on URL and/or direction from US-CERT (global response loop), regardless of the direction of traffic (inbound/outbound) unless an exception is granted
- All security devices use multiple security scanning and detection techniques. This solution goes far beyond stateful and deep packet inspection. It supports full content inspection, which allows security scanning and control to reach Layer 7

### Lumen Service Highlights—MTIPS

- ✦ MTIPS provider since 2010
- ✦ Existing MTIPS architecture is TIC 2.2 compliant
- ✦ Existing MTIPS service ranges from T1 to 10Gbps connections
- ✦ Four geographically diverse TIC Portals
- ✦ TIC Portal throughput scalable to 40 Gbps
- ✦ Route diversity or avoidance on the POP-to- SDP network segment to increase site and service survivability
- ✦ 24x7x365 NOC and SOC monitoring and management of EIS subscriber circuits, services, and service termination equipment

of the OSI stack. The firewall confirms requests that are made and will match open connections to valid packets prior to admittance through the network.

- The firewall capabilities provide both stateless and stateful packet filtering. Deep packet inspection technology (intrusion detection) is an inherent capability that has been implemented to inspect and analyze protocols from Layer 2 (Ethernet packet header) through Layer 7 (HTTP and HTTPS) application layer protocols. These capabilities exceed the existing MTIPS requirement.
- Security policies can be configured to allow blocking of URLs or IP.
- Documented MTIPS defense and filtration procedures for traffic passing through the MTIPS portals are based on DHS-approved security signatures and policies, including EINSTEIN interoperability.

### Intrusion Detection and Prevention Systems

The IDPS element of Lumen's MTIPS solution consists of hardware and software components that monitor and identify potential security threats on all inbound and outbound network traffic, including Internet and extranet traffic, and all internal and external DNS queries. The IDPS will connect to and interoperate with the agency's networking environment, including demilitarized zones (DMZs) and secure LANs. The Lumen current MTIPS UTM platform has the capability (through a virus database) to detect, remove, or block malicious traffic using intelligent security automation, scalability, and real time contextual awareness. Lumen's MTIPS is one of the most comprehensive threat prevention platforms in the industry, protecting against known threats such as:

- |                    |                             |                         |
|--------------------|-----------------------------|-------------------------|
| ■ Worms            | ■ Denial of service attacks | ■ Invalid headers       |
| ■ Trojans          | ■ Buffer overflows          | ■ Blended threats       |
| ■ Backdoor attacks | ■ P2P attacks               | ■ Rate-based threats    |
| ■ Spyware          | ■ Protocol anomalies        | ■ Zero-day threats      |
| ■ Port Scans       | ■ Application anomalies     | ■ TCP segmentations and |

- 
- VoIP attacks
  - Malformed traffic
  - IPv4/IPv6 attacks
- IP fragmentation

The Lumen MTIPS platform uses “flow-based” scanning to analyze traffic in real time, or proxy-based scanning that buffers and examines the file as a whole. Flow-based scanning reduces delay and maximizes bandwidth use in Internet traffic flows. To enhance the security posture, new virus signatures can be created and added to expand the IDPS capability to detect viruses known within the government’s security community. File size scanning is included in the protection scheme and can be configured for HTTP(S), Internet message access protocol (IMAP(S)), network news transfer protocol (NNTP), POP3(S), and simple mail transfer protocol (SMTP(S)) traffic according to an agency’s security policy. To protect an agency’s information, IDPS can block and drop the file if the file size exceeds the configured ranges.

## EINSTEIN

Lumen participates in, and our MTIPS complies with, all current connectivity and operations requirements of the NCPS, operationally known as EINSTEIN. Log data associated with EINSTEIN will be delivered through an IPSec tunnel to ensure compliance with remote access to MTIPS and EINSTEIN.

## Domain Name Service

Lumen will provide a managed external DNS infrastructure service that is responsive, robust, and secure both for agency personnel to reach the Internet and the general public to reach the agency’s public facing services to deliver the best security characteristics per the DHS TIC Reference Architecture. Lumen’s DNS service includes four elements: authoritative servers, recursive servers (caching), DNSSEC, and filtering that provides TIC reference architecture best practices and the security controls to meet NIST SP 800-81 revision 2, as authorized in our MTIPS System Security Plan (SSP) (as originally developed for Networx).

---

**Data Loss Prevention (DLP)**

Lumen will inspect all outbound Internet traffic to include web and email for data leakage based on factors such as pre-set size limits in accordance with agency TO requirements, and sensitive PII. Lumen's MTIPS will provide capabilities to detect PII including, but not limited to, social security numbers, driver's license numbers, or financial account numbers. Should a DLP rule violation occur, the violation will generate a log and an alert will be sent, in near real time, to the Lumen SOC and the agency's SOC or administrator. DLP rulesets have been developed based on patterns and regular expressions, keywords, or other government best practices. The subscribing agency will implement, by import or addition, custom DLP rulesets and subsequently document them in the MTIPS technical data requirements form (TDRF). Rules will be implemented according to the KPIs to ensure that DLP updates and custom DLP rules are applied in a timely manner. Subsequent rule changes will be accomplished using the ticketing system.

Lumen offers the integration with SIEM tools, including common event format, Syslog, Log Event Extender Format (LEEF). All decoding is done in memory, providing as close to real time detection as possible while offering active prevention capabilities for non-email traffic using TCP reset (RST) and quarantine or message drop capabilities for email traffic.

**Distributed Denial of Service Prevention**

Lumen will provide protection against DDoS attacks through the use of MTIPS DDoS, as well as work with external ISPs to minimize the risk of DDoS attacks against an agency.

Our MTIPS service provides managed filters for the type of traffic, bandwidth, and thresholds to mitigate the effects of a DDoS attack. Based on an agency's security policy and traffic types, traffic thresholds will be implemented to detect and mitigate DDoS attacks. Lumen will divert malicious traffic according to each agency's MTIPS

filtering methodology before attacks can impact service. Filters that can be implemented within the MTIPS solution include:

- Black hole filtering
- Port rate limiting
- Full blocking

Below is a list of what traffic types that can be allowed and/or blocked in accordance with the subscribing agency's security guidelines:

- |                   |                      |                    |
|-------------------|----------------------|--------------------|
| ■ TCP syn flood   | ■ User datagram      | ■ ICMP flood       |
| ■ TCP port scan   | protocol (UDP) flood | ■ ICMP sweep       |
| ■ TCP src session | ■ UDP scan           | ■ ICMP src session |
| ■ TCP dst session | ■ UDP src session    | ■ ICMP dst session |
|                   | ■ UDP dst session    |                    |

### Federal Video Relay Service

Lumen will support network connections for the Federal Video Relay Service (FedVRS) for the deaf, including devices implementing stateful packet filters.

### Email Filtering

Lumen's secure messaging platform is a modular hardware and software solution that seamlessly integrates into the MTIPS security platform. The solution provides a powerful and flexible analysis capability that can inspect all incoming and outgoing agency email traffic. To ensure the security of an agency's email transport, Lumen will configure the MTIPS portal to restrict email transmission to an agency's email infrastructure.

---

Lumen's MTIPS secure messaging platform performs the following automated functions:

- Email filtering for known virus patterns
- Detection and quarantine of all suspicious traffic patterns
- Content scanning (spyware and malware)
- File extension examination (Microsoft Excel, PDF, Microsoft Word)
- Quarantine of suspected malicious traffic
- Universal resource locator (URL) and sender validation authentication (anti-spoofing protection, Sender Policy Framework (SPF))

E-mail scanning highlights include:

- Scanning and detection of known email viruses. Newly discovered virus entities provided by the agency or other trusted government source like DHS, will be input into the email solution and implemented in the scanning function.
- Common virus detections such Trojan horses, worms, macro viruses, and other malicious files can be easily detected and emails subsequently quarantined.
- Maintenance of a local sender reputation list based on SPF and domain keys identified mail (DKIM).
- Behaviors and characteristics that may indicate the presence of email viruses will be baselined, thereby establishing an historical reference. When a pattern is detected, the email will be quarantined.
- Dictionary-based filtering in both inbound and outbound directions, including filtering by attachment file type and banned word filtering.



- Lumen uses a binary emulation that allows its antivirus engine to detect new malware and variants, regardless of whether a detection signature exists. This enables the engine to detect today's robust malware threats, even those that use sophisticated evasion techniques like polymorphism and encryption to avoid detection from other anti-malware products.
- Lumen's secure messaging platform has reliable and high performance features for detecting and blocking spam messages and malicious attachments. Once a malicious attachment is detected, it is immediately quarantined and stored in its original format and content for further review by an agency analyst. The platform's antivirus technology extends full content inspection capabilities to detect the most advanced email threats and provides for centralized management of all quarantined messages.

#### Success Story

*In 2010, Lumen was awarded three 1 Gbps MTIPS connections by the United States Patent and Trade Office (USPTO). The USPTO has experienced substantial increase in demand on Internet bandwidth, and recently worked with Lumen to upgrade their access to 10 Gbps with a 6-Gbps tiered MTIPS port. Should the USPTO require another upgrade to their available MTIPS bandwidth (up to 10 Gbps), they simply contact their Lumen customer service representative to initiate an upgrade order.*

### Inline Malware Detection Engine (IMDE)

Lumen will provide a powerful and comprehensive inline malware detection capability for inbound and outbound network, email, and web traffic that includes:

- Static analysis
- Dynamic analysis (dynamic execution/sandboxing—heuristics)
- Third party feed matches
- Manual file submission
- Advanced malware forensics (including all modified registry keys, PCAPs of virtualized malware detonation command and control (C2) beacons, etc.)

- 
- Vendor proprietary feed matches, including partial message-digest algorithm (MD5) matches
  - Rules/policies (recently compiled executable files, highly obfuscated scripts and executable files, etc.)

#### **1.4.8.3.1.1 Service Description (L.29.2.1-1; C.2.8.4.1) and Functional Definition (C.2.8.4.1.1)**

Lumen will comply with the requirements of RFP Sections C.2.8.4.1 and C.2.8.4.1.1 as described below.

Lumen's MTIPS enables agencies to physically and logically connect to the public Internet or other external connections, as required by the agency, in full compliance with OMB's TIC initiative (M-08-05), announced in November 2007 and subsequent modification to TIC 2.0, issued by DHS, in March 24, 2011. MTIPS facilitates the reduction of the number of Internet connections in government networks and a network-based approach at providing standard security services to all government users. Lumen's MTIPS has been engineered to permit simple integration with add-on security services like DDoS mitigation and E<sup>3</sup>A.

Lumen will continue to maintain our MTIPS ATO with GSA and participate in an annual DHS led CCV assessment of implementation of TIC capabilities and the NCPS program. Lumen's MTIPS puts the agency subscribers in a position to meet or exceed their annual CCV self-assessment and/or DHS on-site CCV conducted every three years. Lumen will continue to participate in the DHS compliance annual CCV assessment.

Lumen's MPLS/VPNS transport network will serve as a secure collection point for virtual or physical TIC connectivity by enabling the termination of MTIPS access connections to MPLS PE routers. Private virtual route forwarding (VRF) or closed user group (CUG) instances will be provisioned on the Lumen MPLS transport network to isolate an agency's internal network traffic from other agency's MTIPS or VPNS user traffic to include Internet and external networks originated or terminated traffic.

---

Lumen's MTIPS portals will function as an OMB-approved multi-service TICAP capable of hosting multiple agencies using VDOMs and Lumen's UTM platform that is capable of managing and correlating multiple independent traffic streams for each subscribing agency.

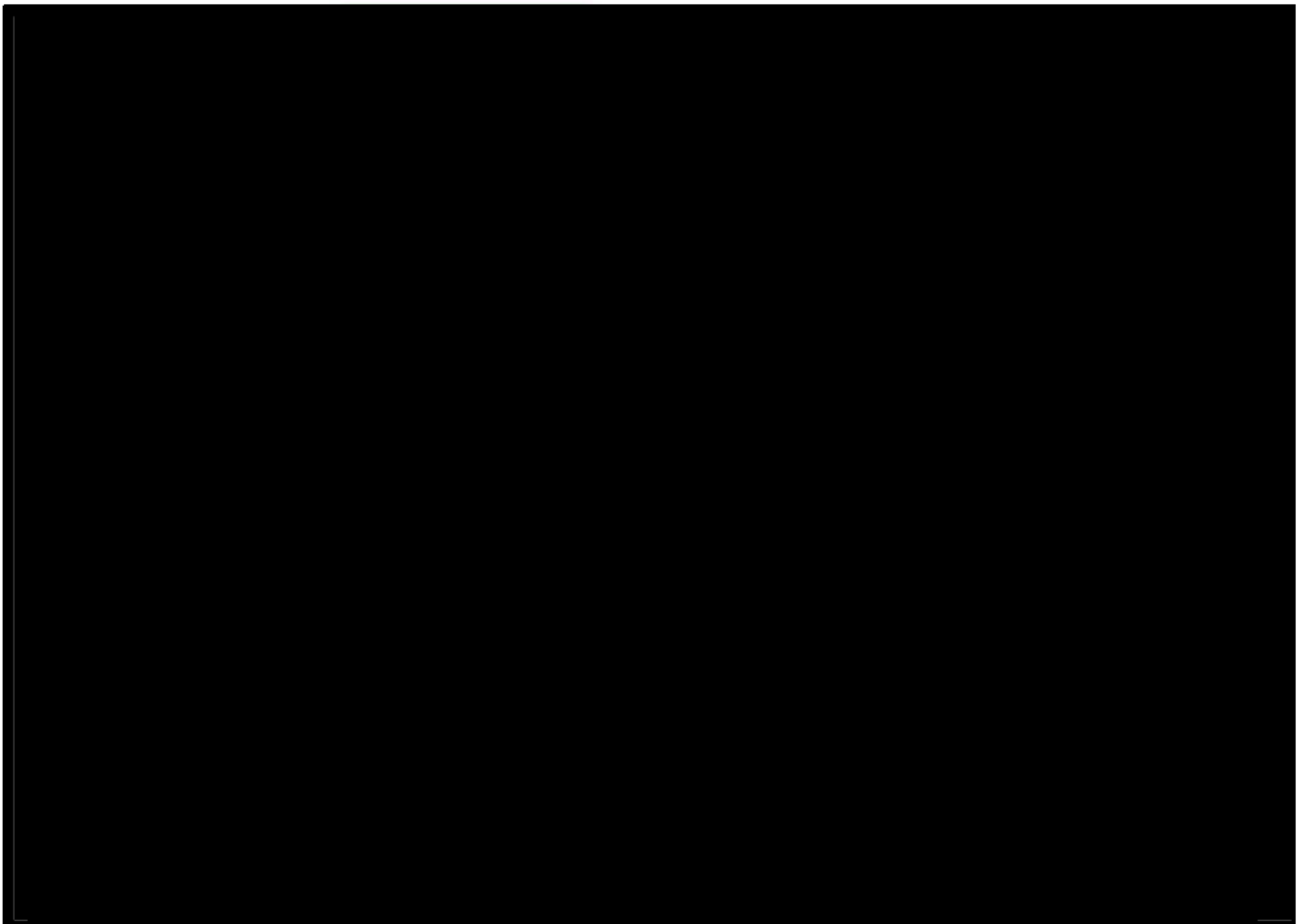
Lumen's MTIPS portals will not only provide the agency with physical and virtual security services, but also allow for specific controls and security policies as defined in the completed TDRF to be established on an individual case basis and in close coordination with the requesting agency, DHS, and GSA, when necessary.

Lumen has engineered and installed four geographically diverse domestic MTIPS TIC Portals in [REDACTED] that serve as secure Internet exchange points to subscribing departments/agencies.

Lumen provides staff at each MTIPS/TIC Portal location with local access to each MTIPS cage space. Lumen uses staff with remote access capability to remotely manage each MTIPS portal on a 24x7x365 basis.

Lumen will work with an agency to implement virtual TIC capabilities (as defined in agency TO), to agencies with resources hosted outside their physical boundaries.

The SOC systems providing management and monitoring of the MTIPS TIC Portals will be dedicated for the use of government entities and will be isolated from non-government/commercial systems. **Figure 1.4.8.3.1-2** shows Lumen's high-level overview of the SOC management process and systems.



**Figure 1.4.8.3.1-2. SOC Management Overview**

**1.4.8.3.1.2 Standards (L.29.2.1-2; C.2.8.4.1.2)**

Lumen will adhere to all standards included in RFP Section C.2.8.4.1.2.

As an established industry contributor to the government NIST standards committee, Lumen comments on and quickly adapts to emerging standards including current and future regulations, policies, requirements, standards, and guidelines for U.S. Government technology and cybersecurity standards. Lumen will submit an adoption plan to the contracting officer (CO) within 90 days of issuance of new TIC capabilities or policy changes.

**1.4.8.3.1.3 Connectivity (L.29.2.1-3; C.2.8.4.1.3)**

As shown in **Figure 1.4.8.3.1-1**, Lumen’s MTIPS will continue to connect and interoperate with:

1. The public Internet; we establish dedicated agency connections to the MTIPS portal
2. The EINSTEIN Enclaves; enclaves connect to the MTIPS portals in accordance with current DHS security guidelines
3. Global response loop to US-CERT with a cross-agency view; allows for coordination across TIC web interfaces. Our SOC has existing procedures for interfacing with US-CERT
4. Rapid response loop from DHS to agency communications for the dissemination of threats/events to/from the agency. Our SOC has existing procedures for interfacing with US-CERT
5. Other agency IP networks (external or internal connections); provisioned in accordance with MTIPS connectivity guidelines and agency requirements

**1.4.8.3.1.4 Technical Capabilities (L.29.2.1-4; C.2.8.4.1.4)**

Lumen’s compliance with the requirements of RFP Section C.2.8.4.1.4.1 is described in the tables below.

**1.4.8.3.1.4.1 TIC Portal Capabilities (C.2.8.4.1.4.1)**

RFP. Ref. Para#	Definition
C.2.8.4.1.4.1 (#1 a through e)	<p>TIC Portal access to external networks including the Internet –Lumen’s MTIPS/TIC Portal complies with the following requirements when establishing interconnection relationships.</p> <p>Lumen is a Tier 1 provider and is connected to multiple Tier-1 ISPs to allow traffic routing and aggregation to the MTIPS portal.</p> <p>Lumen will work with an agency to budget sufficient interconnection bandwidth to accommodate increasing agency demands. Each MTIPS portal is modular and scalable to accommodate the increased bandwidth demands by readily incorporating additional security and routing infrastructure with minimal service impact.</p> <p>Lumen’s MTIPS portals have been engineered to provide alternate and diverse routing using multiple redundant 10 Gbps connections to the MPLS transport network as well as multiple 10 Gbps connections to the Lumen Tier1 Internet backbone network. Lumen has engineered automatic failover between the geographically diverse TIC Portals to provide increased service survivability and resilience. The engineered</p>

**General Services Administration (GSA)**  
**Enterprise Infrastructure Solutions (EIS)**

Contract # GS00Q17NSD3006  
 Mod #: P00310  
 Submission #: CL01001.01a

RFP. Ref. Para#	Definition
	<p>solution allows Lumen MTIPS to survive various outage scenarios to include single or multiple Internet-to-TIC Portal connection outages, single or multiple MPLS-to-TIC Portal outages, complete TIC Portal outages and achieve MTIPS KPIs and SLAs.</p> <p>Lumen as a Tier-1 provider supports BGP, eBGP, BGP4, and other industry standard protocols for inter-ASN connectivity as specified by the IETF. This supports Lumen’s ability to establish connectivity to other ISPs or external networks and aggregate all traffic to the MTIPS portals.</p> <p>Lumen’s edge, core, and border routers are IPv4 and IPv6 enabled. Lumen provides IPv4 and IPv6 connectivity ranging from T1 to Nx10GigE port speeds on both the public Internet and private VPN services, using dedicated and dual-stack access methods, in accordance with OMB Memorandum M-05-22.</p>
C.2.8.4.1.4.1 (#2)	<p>Lumen will comply with RFP Section C.1.8.8 routing requirements routing all internet, extranet, and inter-agency traffic to an EINSTEIN Enclave. We will further ensure that any participating agency encrypted tunnels are applied and proxied to allow inspection. Our approach to applying and proxying encrypted tunnels is to use an in-line switch to break the tunnel so the traffic within the tunnel can be read.</p>
C.2.8.4.1.4.1 (#3)	<p>In order to empower agency security authorities/analysts to react and trigger appropriate control mechanisms the SOC hardware/software tools provide the ability for customized reports and supports the TIC Portal authorities/analysts by identifying security events of interest that may be negatively affecting the TIC Portal and subscribing agency environments, thus creating a rapid response loop. Lumen will ensure its SOC facilities are accredited in accordance with ICD 705 by DHS at the TS/SCI level as required, and are only accessible by DHS TS/SCI cleared personnel. The SOCs are staffed with at least two trained, qualified, and cleared staff (U.S. citizens) capable of managing the technical aspects of the network and related attacks and security functions on a 24x7x365 basis. Lumen will continue to comply with the DHS-published TIC 2.0 requirements.</p>
C.2.8.4.1.4.1 (#5).	<p>Lumen will comply with RFP Section C.1.8.8 routing requirements, routing all internet, extranet, and inter-agency traffic to an EINSTEIN Enclave. We will further ensure that any participating agency encrypted tunnels are applied and proxied to allow inspection and content filtering. Procedural documentation for our MTIPS products exists today and can be made available upon request.</p>
C.2.8.4.1.4.1 (#6)	<p>By design, Lumen’s adherence to proper BGP configuration ensures symmetric routing between the MTIPS portal and the Internet, as well as between the MTIPS portal and extranets.</p> <p>The BGP session configuration requirements for Lumen’s overall MTIPS service is divided into two complementary categories: shared and subscriber-specific. The shared category is the eBGP session established between the DE and the cybercenter infrastructure, and applies to all Internet destined/ sourced traffic, in and out of the TIC Portal. The subscriber-specific session is comprised of two sub-elements: the internal BGP session established between the DE router and the MTIPS firewall in the TIC web interface (applies to all MTIPS subscribers) and the eBGP session between the MTIPS firewall in the TIC Portal and the MTIPS SRE (applies to subscriber agencies running BGP). Proper BGP configuration is critical to achieving the desired operation including the design for symmetric routing through the TIC Portal. Symmetric routing is achieved within the BGP configuration using local preference weights. This allows for proper firewall state management. Lumen’s MTIPS design and BGP configurations force traffic to return to the originating MTIPS portal to prevent asymmetric routing.</p>
C.2.8.4.1.4.1 (#7)	<p>Lumen will support the GSA product requirements for MTIPS, including support for FedVRS for the deaf (<a href="http://www.gsa.gov/fedrelay">www.gsa.gov/fedrelay</a>) network connections including devices implementing stateful packet filters.</p>

RFP. Ref. Para#	Definition
C.2.8.4.1.4.1 (#8)	Lumen provides email forgery protection using MTIPS UTM within the MTIPS architecture that performs deep header inspection of incoming email. During this analysis, the sending domain is checked against the source IP address. If the IP address is not registered to the indicated domain, or if the sending IP address is not included as an authorized SMTP relay for the domain, the email is subject to the rules configured by the MTIPS subscribing agency (default rule is to discard). Scoring criteria for this capability will be aligned with the National Strategy for Trusted Identities in Cyberspace (NSTIC), and refers to SPAM score thresholding. Lumen follows the DKIM and SPF forgery protection standard. For email determined to be suspicious or undesirable, Lumen will take action according to the subscriber agency instruction/configuration.
C.2.8.4.1.4.1 (#9)	Lumen MTIPS can support the signing of outgoing email messages through its secure mail system by implementing DKIM to ensure outgoing emails have been digitally signed/encrypted at the domain level.
C.2.8.4.1.4.1 (#10)	The Lumen MTIPS solution is equipped with resolving/recursive name servers to properly filter DNS queries and perform validation of DNSSEC-signed domains for MTIPS subscribers in accordance with NIST SP 800-81.
C.2.8.4.1.4.1 (#11)	The Lumen data centers hosting the MTIPS enclaves are designed and equipped to provide uninterrupted operations in the event of a power outage for at least 24 hours. Details regarding uninterrupted power can be found in Section 3.4.1.1, collocated hosting.
C.2.8.4.1.4.1 (#12)	Lumen's MTIPS/TIC systems and components have been engineered to support both IPv4 and IPv6 protocols in accordance with OMB Memorandum M-05-22, and the "IPv6 Transition Guidance" issued by Federal Chief Information Officer (CIO) Council, Architecture and Infrastructure Committee.
C.2.8.4.1.4.1 (#13)	Lumen MTIPS UTM will support the DLP program. Lumen has been applying DLP to existing MTIPS customers since 2011. We were an early adopter of DLP characteristics that include searching for standard nomenclature such as 9-digit in sequence (e.g., SSN) and 16-digit in sequence (e.g., credit card number). DLP, as a subset of UTM, allows Lumen to customize alphanumeric arrays on a customer-by-customer basis.

**1.4.8.3.1.4.2 MTIPS Transport Collection and Distribution Capabilities**

**(C.2.8.4.1.4.2)**

Lumen's compliance with the requirements of RFP Section C.2.8.4.1.4.2 is defined in the tables below.

RFP Ref. #	Definition
C.2.8.4.1.4.2 (#1)	Lumen's MTIPS provides the following MTIPS transport collection and distribution capabilities: Lumen operates two TIC Portals: Sterling, Virginia; Chicago, Illinois; Burbank, CA; and Englewood, CO. Agency's Internet bound or sourced traffic will be processed by one of the TIC Portals.
C.2.8.4.1.4.2 (#2)	Lumen creates an agency trusted domain (DMZ) in one of two ways (encrypted DMZ (eDMZ) and inner firewall):  An eDMZ, a router-based security solution, ensures that an agency's traffic is protected and physically isolated when transported to the TIC Portal and the public Internet. In an eDMZ deployment, an IPsec/VPN tunnel is established between a FIPS 140-2 compliant router at the agency SDP and the firewall within the TIC Portal.

RFP Ref. #	Definition
	<p>An inner firewall is deployed by two options: 1) an IPSec/VPN tunnel between a FIPS 140-2 compliant firewall at the agency SDP and the firewall within the TIC Portals or 2) a pseudo-wire (layer 2) VPN tunnel between the agency termination point on CTL MPLS and the MTIPS gateway PE.</p> <p>Both DMZ approaches provide the necessary security from the agency SDP over the MTIPS access circuit and transport network to the TIC Portal, thus ensuring the agency traffic is not sniffable, and ports cannot be spoofed.</p>
C.2.8.4.1.4.2 (#3)	Lumen will comply with RFP Section C.1.8.8 and will route all external connection inter-agency traffic to a TIC Portal for inspection. Our approach is described in Section 1.1.1.5.2.

**1.4.8.3.1.5 Features (L.29.2.1-5; C.2.8.4.2)**

Lumen’s compliance with the requirements of RFP Section C.2.8.4.2 is defined in the tables below.

RFP. Ref. Para#	Definition
C.2.8.4.2 (#1)	Lumen will comply with RFP Section C.1.8.8 routing requirements routing all internet, extranet, and inter-agency traffic to an EINSTEIN Enclave. We will further ensure that any participating agency encrypted traffic is aggregated and proxied to allow inspection and permit the incoming and outgoing traffic to be monitored, scanned, and filtered for suspicious patterns or artifacts that may indicate malicious activity. Lumen will retain logs, including the source, destination, and size of the encrypted connections, for further analysis. Our approach is described in Section 1.4.2.
C.2.8.4.2 (#2)	<p>Lumen will support the ordering agency’s security policy to ensure compliance with security regulations. Based on Lumen’s broad experience in the delivery of MTIPS to agencies, we have developed an encompassing security service implementation practice that incorporates lessons learned. As a result, we have implemented the TDRF as part of the standard implementation process for all MTIPS customers. The TDRF includes standard security policies’ recommendations (e.g., SOC identified trends and intrusion behavior) and allows for negotiation of an agency’s operational model and specific security rules.</p> <p>Lumen supports adjustments to an agency’s security policy based on threats identified by the TIC Portal SOC that could impact any agency. Agency requested adjustments will be made and documented using the Lumen trouble ticketing process.</p>
C.2.8.4.2 (#3)	SOC personnel will use hardware/software tools to support full, real time, header and payload, raw packet capture of selected agency’s traffic flows, as necessary. SOC personnel will continue to support subsequent forensic traffic analysis of cyber incidents as required by the agency (administrative, legal, audit or other operational purposes). Lumen’s SOC personnel will work with an agency to identify the traffic of interest (relevant traffic to capture) and provide engineering to help design the appropriate capture solution and parameter settings.
C.2.8.4.2 (#4)	Lumen can provide support for custom reports as requested by an agency in a TO. Lumen will work with the agency to define the scope of information captured with the ad-hoc report.
C.2.8.4.2 (#5)	Lumen will work with the agency to determine the scope of customization or feature enhancements required beyond the existing capabilities of the standard portals and will develop a solution that accommodates the desired specifications as required by the TO. The NOC/SOC console access will be provided through a



**General Services Administration (GSA)**  
**Enterprise Infrastructure Solutions (EIS)**

Contract # GS00Q17NSD3006  
 Mod #: P00310  
 Submission #: CL01001.01a

RFP. Ref. Para#	Definition
	hyperlink to agency authorized users for the respective NOC/SOC console tools.
C.2.8.4.2 (#6)	Lumen will work with the agency to determine and negotiate the scope of custom security assessment and authorization (A&A) support required by the agency as required by the TO. Support may include the agency opting for security controls more stringent than the NIST high-impact baseline. Lumen will negotiate agency-unique requirements directly with the agency.
C.2.8.4.2 (#7 a through e)	<p>Lumen's external network connection will comply with the interconnection and routing requirements found in RFP Section C.1.8.8 and as described in Section 1.1.1.5.2. Lumen MTIPS enables agencies to connect to external IP networks (including EINSTEIN Enclaves) from their physical locations.</p> <p>All traffic exchanged by Lumen's MTIPS will be IP traffic only and compliant to TIC Portal's interconnecting requirements. We will further ensure that any participating agency encrypted tunnels are applied and proxied to allow inspection.</p> <p>Lumen will continue to support an agency's need for dedicated external connections to external partners with a documented mission requirement and approval (currently through the use of a memorandum of agreement (MOA). Agreements can include permanent VPN over external connections, including the Internet, and dedicated private line connections to other external networks.</p> <p>Lumen will support external dedicated VPN and private connections using the full range of the EIS provided transport services.</p> <p>Lumen will terminate the external network connections onto the public-facing firewalls within the TIC Portal architecture, at which point any encrypted traffic will be decrypted and routed through the EINSTEIN Enclave to allow traffic inspection.</p> <p>Lumen MTIPS architecture ensures incoming traffic from the external network will be routed through and inspected within the EINSTEIN Enclave and the MTIPS security stack before being routed to the agency internal network.</p> <p>Lumen will terminate the external network connections in accordance with RFP Section C1.8.8 in front of the full suite of MTIPS/TIC sensors/capabilities to allow traffic to/from external connections to be inspected.</p> <p>If the external network connections are established over the public networks including the Internet, Lumen will ensure the VPN connections will be encrypted, and FIPS 140-2 compliant.</p> <p>Lumen may use split tunneling for external connections terminated prior to routing through the EINSTEIN Enclave.</p> <p>Lumen will support an agency request to implement the MTIPS service with telecommunications service priority (TSP) on the external connections, including to the Internet, to provide for priority provisioning or restoration of telecommunication services.</p> <p>Lumen will adhere to SLAs for all EIS transport services.</p>
C.2.8.4.2 (#8)	Lumen will support encryption as required in RFP Section C.2.8.4.1.4.2.2 and described in Section 1.4.8.3.1.4.2.
C.2.8.4.2 (#9a through j)	Lumen MTIPS will provide remote access, including ad-hoc VPN, through external connections (including the Internet) to support telework applications for authorized users. As external partners are approved by an agency for implementation, Lumen will create and test the VPN connections and the appropriate configuration and security controls with the partner. In accordance with the requirements of OMB M-06-16, protection of sensitive agency information, the requisite baseline capabilities will be supported for telework/remote access at the MTIPS access point.

RFP. Ref. Para#	Definition
	<p>Lumen will terminate the external network connections onto the public-facing firewalls within the MTIPS portal architecture, at which point any encrypted traffic will be decrypted and routed through the EINSTEIN Enclave to allow traffic inspection. Lumen will terminate the external network connections in accordance with RFP Section C.1.8.8 to access the full suite of MTIPS/TIC sensors/capabilities and enable traffic to/from external connections to be inspected.</p> <p>Lumen will terminate the VPN connections at the public facing firewall within the MTIPS portal to allow traffic to/from remote access users to internal networks to be inspected by the MTIPS portal's security stack and EINSTEIN Enclave prior to reaching the public Internet.</p> <p>Lumen will terminate the VPN connections at the public facing firewall within the MTIPS portal to allow traffic to/from remote access users to internal networks to be inspected by the portal's security stack and EINSTEIN Enclave.</p> <p>Lumen will require that all VPN connections terminate on NIST FIPS 140-2 compliant devices.</p> <p>Lumen MTIPS and MPLS PE devices are configured to prevent split tunneling.</p> <p>Multi-factor authentication is required by our accredited MTIPS solution. Agency users can use RSA SecurID, common access card (CAC)/personal identity verification (PIV) cards, and other forms of multi-factor authentication.</p> <p>Lumen deploys VPN concentrators and virtual-desktop/application gateways using hardened devices which are maintained within a separate network security boundary.</p> <p>Lumen will allow telework/remote clients to use GFP by tunneling through the gateway rather than terminating traffic at the MTIPS portal. The VPN connection may use access at the IP network-level and access through dedicated remote client VPN.</p> <p>If telework/remote clients use non-GFP (e.g., a user's home PC), the VPN connection will be configured so that the connection traverses a specific virtual domain at the MTIPS portal.</p> <p>Implementation Requirements: Lumen will comply with the following requirements:</p> <ul style="list-style-type: none"> <li>i. Lumen existing MTIPS remote access solution supports TLS and IPSec VPNs to connect to the MTIPS portals. Lumen will provide the end client device if required by the agency</li> <li>ii. Lumen's existing remote access solution is FIPS 140-2 compliant.</li> <li>iii. Lumen supports multi-factor authentication services</li> <li>iv. Lumen has built separate DMZs for remote access at the TIC Portal to secure the VPN concentrators, application gateways, and virtualized infrastructure.</li> </ul> <p>At the TO level, Lumen will develop customized remote access solutions for agency-specific teleworking requirements.</p>
<p>C.2.8.4.2                      (#10 a through e)</p>	<p>Extranet Connections: Lumen's TIC Portal supports dedicated extranet connections to internal partners with a documented mission requirement and approval. This includes, permanent VPN over external connections, including the Internet, and dedicated connections to other internal networks provided by communication services offered through this contract. Lumen supports the following baseline capabilities for extranet dedicated VPN and private line connections at the TIC Portal.</p> <p>Lumen will terminate the extranet connection (e.g., IPSec tunnel) on the public-facing firewall within the TIC Portal before routing through the EINSTEIN Enclave and the full suite of TIC sensors/capabilities so that all outbound traffic to/from the extranet connections to external connections, including the Internet, is inspected within the EINSTEIN Enclave.</p>

RFP. Ref. Para#	Definition
	<p>Lumen will terminate the extranet connection on a public-facing firewall within the TIC Portal that is in front of the MTIPS-managed security controls including allowing traffic to/from extranet connections to internal networks, including other extranet connections, to be inspected.</p> <p>Lumen will ensure the extranet VPN connections over shared public networks, including the Internet will be NIST FIPS 140-2 compliant.</p> <p>Lumen will not permit split tunneling in an extranet connection scenario.</p> <p>Implementation Requirements:</p> <ul style="list-style-type: none"> <li>i. Lumen will implement the extranet connections using a FIPS 140-2 compliant solution by establishing IPsec VPN tunnels from the fixed remote location (e.g., business partners, remote agency's sites, other agencies' sites) to a public facing firewall within the MTIPS solution.</li> <li>ii. Lumen will work with the agency to determine the necessary multi-factor authentication services required that may include the support of passwords, cryptographic tokens, or PIV cards/readers.</li> </ul> <p>Lumen will support custom remote access implementations for extranet connectivity in order to meet agency-specific requirements. Lumen will work with the agency to determine the full scope of the extranet customization and design components.</p>
C.2.8.4.2 (#11)	<p>At the TO level, if requested by the agency, Lumen will document and maintain a current inventory of all MTIPS information systems and components, including relevant ownership information, and maintain complete maps, and other related inventories, of agency networks connected to the MTIPS access point. These maps will include physical maps with rack and slot numbers, wiring diagrams, and logical topologies. Lumen will facilitate and validate, using network mapping devices, government validation of the map and inventories. Static translation tables and appropriate POCs will be provided to the US-CERT on a quarterly basis.</p>

**1.4.8.3.1.6 Interfaces (L.29.2.1-6; C.2.8.4.3)**

Lumen’s MTIPS will comply with the UNI requirements at the SDP to connect to MTIPS transport POP using the SONET and Ethernet access requirements found in Section C.2.9.1.4 of the RFP, and as described in Access Arrangements, Section 1.2.1.5 of this response.

**1.4.8.3.2 Quality of Service (L.29.2.1-B; M.2.1-2)**

Lumen was the first MTIPS provider to complete the TCV and to receive an ATO from GSA in 2010. Lumen has consistently maintained a 100% score during the annual DHS US-CERT TCV assessment for all of the critical and mandatory capabilities. MTIPS is a premiere core security service, and Lumen is dedicated and committed to maintaining MTIPS compliance and our ATO as security requirements evolve to address the ever-changing threat vectors focused upon the government.

As an established and experienced MTIPS provider, scalability of our solution is demonstrated by the growth of its service to include more than forty government departments and agencies that have recognized Lumen as the MTIPS provider offering the best engineered network and security solutions. Lumen service has increased to provide over 18 Gbps of MTIPS bandwidth for these government customers.

As discussed in Section 1.4.8.3.1, our MTIPS solution delivers high availability resulting from an architecture that includes redundant TIC Portals, SOCs, NOCs, portal-to-MPLS connections, portal-to-Internet DE connections, MPLS PE-to-PCOR connections, and critical access options with diversity for automatic failover. Our network design has resulted in 99.999 percent POP-to-MTIPS network availability.

Lumen achieves its success in MTIPS RFP awards by engineering cost-effective solutions that comply with the department/agency security, operations, performance, management, and budgetary service requirements. Lumen's MTIPS is in full compliance with the security requirements set forth by DHS, validated through our scoring 100% on the TCV and maintaining our MTIPS ATO.

**1.4.8.3.2.1 Performance Metrics (L.29.2.1-7; C.2.8.4.4)**

Lumen's MTIPS will meet all performance metric requirements.

**1.4.8.3.2.1.1 PMs for TIC Portal (C.2.8.4.4.1)**

KPI	Approach
Availability	Lumen actively monitors all components within the TIC Portal. In the event a component fails, an alarm is generated and a ticket is opened. SOC and NOC engineers will confirm availability of the secondary TIC Portal while working to eliminate the alarm and restore service to the failed portal. In the event both portals are out of service, Lumen will measure the period of unavailability as the total time where neither portal is available for agency use. Lumen MTIPS will maintain a average availability of $\geq 99.5$ percent.
Grade of Service (Failover Time)	Lumen configures two IPSec tunnels; one each from the agency SDP to each TIC Portal. Lumen uses eBGP within each tunnel with a 30 second hold timer. All service will failover to the secondary portal in the event of primary portal failure. Alarms will be generated at the time of a failover. Failover time is measured by reviewing log files of the SRE to confirm route propagation took place within one minute.
Grade of Service (Monitoring and Correlation)	At all SDP's, Lumen will place a security SRE (SEC SRE) log collector where all events and logs are collected and subsequently forwarded back to the SOC locations [REDACTED] [REDACTED] [REDACTED]

KPI	Approach
	<p>██████████</p> <p>All systems in use for event detection are synchronized using the Stratum 1 or 2 NTP sources. The monthly AQL report shows the interval between the SEC SRE event timestamp and the timestamp of the ██████████ correlated event, meeting the requirements of EIS for both routine and critical service event detection.</p>
Grade of Service (Configuration/ Rule Change)	<p>All configuration rule changes (including requested virus protection updates from the agency) are tracked in Lumen's ticketing system from the time of an agency's request (ticket opened) until the time the request is completed (ticket closed). Lumen will comply with the EIS SLAs (&lt;5 hours for normal priority change and &lt; 2 hours for urgent) and provide reports showing the average time for ticket closure meets the AQL. In many instances, when agencies will initiate a request for a configuration change to be performed at a specific time (e.g., during non-business hours), Lumen will follow the requirements of the agency's request and exclude that ticket from its report. Lumen will obtain agency consent prior to implementation of any Lumen initiated changes.</p>
Event Notification (Firewall Security Event Notification)	<p>If an alarm is triggered ██████████ a SOC analyst is notified. If the alarm is determined to be an event, a ticket is initiated within the Lumen ticketing system, triggering an email event notification to the agency within the SLA timeframes. Event times for notifications will correspond with the event category threshold of low (next business day or within 24 hours), medium (within four hours), and high (within 30 minutes). As in the MPS process, the event notification email will be automatically triggered by the Lumen ticketing system.</p>
Event Notification (Intrusion Detection/ Prevention Security Event Notification)	<p>Lumen's incident response event notification process follows the same methodology as MPS event notification. Event times for notifications will correspond with the event category threshold of low (within 24 hours) and high (within 10 minutes). As in the MPS process, the event notification email will be automatically triggered by the Lumen ticketing system.</p>
Grade of Service (Virus Protection Updates and Bug Fixes)	<p>Anti Virus Updates – Lumen will track SRE vendor antivirus updates and maintain a comparison database of antivirus release date and time and update implementation date and time on the MTIPS SRE. Adherence to indicated SLAs statistics will be provided monthly.</p> <p>Bug fixes – Lumen is notified of by MTIPS SRE vendor that a bug fix has been released. The implementation of a bug fix typically requires a reboot of the SRE, which will cause a disruption of service to the affected agency(ies). Currently, disruptions to service cannot take place without ten days notification, unless the bug fix is deemed critical or is considered an emergency. Once notification has been made that a potentially service affecting bug fix is to be applied, Lumen will coordinate with agency representatives to establish an implementation schedule with the understanding that if the agency requests a longer timeframe than the stated SLA, Lumen will not be held responsible.</p>

**1.4.8.3.2.1.2 PMs for MTIPS Transport Collection and Distribution (C.2.8.4.4.2)**

Lumen's MTIPS will comply with the performance levels and AQL of KPIs for MTIPS as required in RFP Section C.2.8.4.4.2.

KPI	Approach
Availability (Port) Latency (CONUS)	<p>Methodology for management and reporting for all transport service KPIs is consistent with the approach described in Section 1.2.8.</p>

GOS (Data Delivery Rate)	
Time to Restore	
Event Notification (Security Incident Reporting)	<p>We will follow the methods and procedures established by US CERT and in place today to report detected security events to US CERT within 30 minutes.</p> <p>At the time of a security incident, an incident ticket is entered into Lumen's trouble ticketing system. An incident will trigger notification to DHS US-CERT congruent with NIST SP 800-61 Rev 2) based on workflow in near real time. Calculation of the AQL is time reported minus time detected.</p>

**1.4.8.3.3 MTIPS Service Coverage (L.29.2.1-C; M.2.1-3)**

Lumen operates [REDACTED]

[REDACTED]

[REDACTED] Lumen MNS will be available at all locations where the underlying Lumen EIS services are provided.

Lumen's service coverage has been defined in accordance with the requirements of RFP Section J.1 for domestic (CONUS and OCONUS) as well as non-domestic locations. Lumen is proposing service coverage that significantly exceeds the minimum requirement of 25 CBSAs out of the top 100 CBSAs. A detailed description of the geographic coverage for all Lumen services for EIS is provided in Technical Volume, Section 1.3.

**1.4.8.3.4 MTIPS Service Security (L.29.2.1-D; M.2.1-4a; C.2.8.4.5)**

Lumen uses proven information security mechanisms, controls, and measurements based on accepted policies and federal IT security requirements to create a security infrastructure further that is enhanced by our A&A processes. Lumen's comprehensive security approach includes categorizing all Lumen-provided components in the Federal Information Security Management Act (FISMA) scope per the FIPS 199 security categorization and based on NIST SP 800-53 at a minimum. The Lumen approach for assessing federal systems ensures that we meet all three security objectives for confidentiality, integrity, and availability across the solution. Lumen ensures that its solutions meet the required controls for operational, management, and technical functions based on federal policy and procedures, NIST-based security requirements guidance, and industry best practices.

---

Lumen periodically conducts self-evaluation and compliance reviews to ensure the security requirements defined in the System Security Plan (RFP Section F.2.1, Contract Data Requirements List (CDRL) 5) are met at a high impact level, and support the government security and authorization efforts. Lumen works to support the government's efforts to verify that its security and authorization standards are being met.

The following information is extracted from the 2015 Lumen Capability Validation Report, and indicates a scoring analysis based on the TIC capability security families and functions. The 74 critical and recommended capabilities are organized into three types of security families, designated by the first two letters in the Formal ID: TIC services, TIC management, and TIC operations. Within each security family, the capabilities are further organized by security function, the second set of letters in the formal ID. This analysis by family and function is provided as an aide in understanding the different technical aspects in which an MSTICAP/MTIPS provider is assessed and a means of easily identifying how Lumen is performing in each broad grouping. The TIC services family is a grouping of capabilities performed by the TIC access point in order to secure agency networks. This includes functions such as packet and content filtering, packet inspection, and remote access. The TIC management family is a grouping of capabilities performed on the TIC access point in order to secure TIC systems and components. This includes functions such as user authentication on a TIC component, securing communications with customers, TIC configuration, data storage, event logging, and physical control of TIC devices and systems. The TIC operations family is a grouping of capabilities performed by the MSTICAP/MTIPS provider in order to ensure TIC access points are properly operated and maintained. This family includes functions such as general management, monitoring and audit, reporting, and incident response. **Table 1.4.8.3.4-1** provides a scoring analysis based on the TIC capability security families and functions of Lumen's MTIPS functionality.

**Table 1.4.8.3.4-1. Lumen's 2015 MTIPS Security Families  
 and Functions Scoring Analysis**

TIC Services Implementation				
Formal ID (count)	Function	Description	Met	Not Met
CF (13)	Content Filtering	Blocking traffic based on packet content	13	0
INS (2)	Inspection	Detecting intrusions	2	0
PF (7)	Packet Filtering	Blocking traffic based on data flow	7	0
RA (3)	Remote Access	Providing virtual private networks	3	0
TS (25)		TIC Services Score:	25	0
TIC Management Implementation				
Formal ID (count)	Function	Description	Met	Not Met
AU (1)	Authentication	Complying with FIPS 199 specifications for high-impact systems. Requires two factor authentication for access to TIC devices	1	0
COM (3)	Communication	Secure communications with customers, TS/SCI staff readily available at all times	3	0
DS (5)	Data Storage	Restoring from backup, capturing logs, separation of agencies' data, data loss prevention process	5	0
LOG (4)	Logging	Timestamps, log retention policy, session traceability	4	0
PC (6)	Physical Control	Backup power, SCIF, dedicated spaces, geographic diversity	6	0
TC (7)	Configuration	Route diversity, principle of least functionality, IPv6, devolution of authority, 24x7x365 staffing	7	0
TS (25)		TIC Services Score:	26	0
TIC Operations Implementation				
Formal ID (count)	Function	Description	Met	Not Met
MG (11)	Management	Multi-service TICAPs accommodate customized security and communications policies	11	0
MON (5)	Monitoring	Event correlation, security reviews, vulnerability scanning, operational exercises, government auditing	5	0
REP (4)	Reporting	Customer service and operational metrics, incident reports	4	0
RES (3)	Response	Reporting to US-CERT and following US-CERT guidelines, having agreements in place with ISPs for handling DDoS attacks	3	0
TS (25)		TIC Services Score:	23	0

#### **1.4.8.3.4.1 General Security Compliance Requirements (C.2.8.4.5.1)**

As an accredited MTIPS provider since 2010, with the latest accreditation being 28 October 2013, Lumen will continue to with FISMA associated guidance and directives to include FIPS, NIST SP 800 series guidelines (available at: <http://csrc.nist.gov/>), GSA IT security directives, policies and guides, and other appropriate government-wide laws



---

and regulations for protection and security of government IT in order to obtain reaccreditation in 2016. Compliance references will include the acts, directives, circulars, memoranda, standards, publications, guides, revisions, and policies as listed in RFP Section C.2.8.4.5.1 (including the GSA policies, directives, and guides).

#### **1.4.8.3.4.2 Security Compliance Requirements (C.2.8.4.5.2)**

Lumen's MTIPS SSP was approved on 28 October 2013 and describes in detail how Lumen complies with each and every security requirement. Lumen will comply with the security compliance requirements as detailed in Section C.2.8.4.5.2 of the EIS RFP. An RMFP, submitted with the proposal, describes our approach to MTIPS security compliance and in accordance with NIST SP 800-37. (Reference: NIST SP 800-37 Rev 1, and NIST SP 800-53 Rev 4: SA-3, RA-3). Our SSP describes in detail how Lumen complies with each and every security requirement.

#### **1.4.8.3.4.3 Security Assessment and Authorization (A&A) (C.2.8.4.5.3)**

Lumen will comply and continue to support the security assessment and authorization requirements as delineated in Sections C.2.8.4.5.3 and C.1.8.7.3 of the EIS RFP. Lumen was the first contractor to achieve ATO under the Network contract in 2013, was subsequently reaccredited in 2013, and is in the process of obtaining a new accreditation as required in the NIST in 2016.

#### **1.4.8.3.4.4 System Security Plan (C.2.8.4.5.4)**

Lumen's security team is fully integrated into the Lumen PMO. We have an MTIPS PM, Information Systems Security Manager (ISSM), and Information Systems Security Officer (ISSO) in place to ensure full compliance of system security requirements. Security reviews and audits are held at least annually and reviews with operational teams are conducted as part of standard operational procedures.

Lumen's SSP has been accepted by GSA since 2010 and by DHS since its first audit in 2010. As of February, 2019, our MTIPS SSP complies with NIST SP 800-53 Revision 4 and is delivered to GSA at least annually with system updates.

---

Lumen will continue to comply with all security A&A requirements as mandated by federal laws, directives and policies, including making available any documentation, physical access, and logical access needed to support this requirement. The level of effort for the security A&A is based on the System's NIST FIPS Publication 199 categorization. At a minimum, Lumen will create, maintain and update the following security A&A documentation:

1. Lumen structures the SSP in accordance with the latest revision of NIST SP 800-18 and other relevant NIST and GSA guidelines. Our SSP includes appendices that include required policies and procedures across 18 control families mandated per FIPS 200. Our MTIPS SSP is maintained and updates are regularly delivered at least once per year, along with the monthly Plan of Action and Milestones (POA&M) reports as appropriate.
2. As required by the GSA, the Lumen SSP will include the Security Assessment Boundary and Scope Document (BSD) as identified in NIST SP 800-37 to specify the actual security assessment boundary (also referred to in this proposal as the "A&A boundary") and components within the information system. The initial boundary, and subsequent changes to it, will be a cooperative effort between the federal government and Lumen Information System Owners, Chief Information Security Officers, the GSA Authorizing Official, and Information Systems Security Manager/Officer. Our initial EIS BSD, which is based on our currently approved Networkx BSD, will be completed and submitted within 15 days of the NTP.
3. Lumen will develop and maintain Interconnection Security Agreements (ISAs) in accordance with NIST SP 800-47, as we have done under Networkx, to be included in the initial security A&A package and with annual updates.
4. Under Networkx, Lumen has an approved GSA NIST SP 800-53 Rev 3 Control Tailoring Workbook as identified in GSA IT Security Procedural Guide 06-30, "Managing Enterprise Risk." It will be updated to Rev 4, as required for EIS, and will be provided with the initial security A&A package, with annual updates (as we are providing under Networkx).

- 
5. Under Networx, Lumen has an approved GSA NIST SP 800-53 Rev 3 Control Summary Table for a High Impact Baseline as identified in GSA IT Security Procedural Guide 06-30, "Managing Enterprise Risk." It will be updated to Rev 4 as required and will be provided with the initial security A&A package, with annual updates (as we are providing under Networx).
  6. Lumen will develop and maintain Rules of Behavior (RoB), based on our RoB approved under Networx, for information system users as identified in GSA IT Security Procedural Guide 06-30, "Managing Enterprise Risk" and GSA Order CIO 2104.1, "GSA IT General Rules of Behavior." We will provide an RoB with the initial security A&A package, with annual updates (as we are providing under Networx).
  7. Lumen will develop and maintain a System Inventory that includes hardware, software, and related information as identified in GSA IT Security Procedural Guide 06-30, "Managing Enterprise Risk." We will provide a previously accredited System Inventory, updated as needed for EIS, with the initial security A&A package, with annual updates (as we are providing under Networx).
  8. Lumen will develop and maintain a contingency plan (CP) including disaster recovery plan and business impact assessment (BIA) following NIST SP 800-34. We will provide the CP (based on a previously approved one) with the initial security A&A package, with annual updates (as we are providing under Networx).
  9. Lumen will develop and maintain a Contingency Plan Test Plan (CPTP), based on a previously approved and tested one, completed in agreement with GSA IT Security Procedural Guide 06-29, "Contingency Planning." We will provide the CPTP with the initial security A&A package, with annual updates (as we are providing under Networx).
  10. Lumen will test the CP and document the results in a Contingency Plan Test Report (CPTR), in agreement with GSA IT Security Procedural Guide 06-29, "Contingency Planning." We will provide a CPTR with the initial security A&A package, with annual updates (as we are providing under Networx).

- 
11. As has been done under Networx, Lumen will perform a Privacy Impact Assessment (PIA) as identified in GSA IT Security Procedural Guide 06-30, "Managing Enterprise Risk." We will provide the PIA with the initial security A&A package with annual updates (as we are providing under Networx).
  12. Lumen will develop and maintain a Configuration Management Plan (CMP), based on a previously approved CMP, and will provide it with the initial security A&A package, with annual updates (as we are providing under Networx).
  13. Lumen will develop and maintain a System(s) Baseline Configuration Standard Document, based on a prior approved document. We will provide a well-defined, documented, and up-to-date baseline specification to which the information system is built. We will provide the System Baseline Configuration, updated as needed for EIS, as a part of the CMP with the initial security A&A package and will provide annual updates (as we are providing under Networx).
  14. Lumen will develop and maintain System Configuration Settings standards, based on an already approved version. We will establish and document mandatory configuration settings for information technology products employed within the security assessment boundary that reflect the most restrictive mode consistent with operational requirements. As we have done under Networx, Lumen will configure the systems in accordance with GSA technical guides, NIST Special Publications, Center for Internet Security (CIS) guidelines (Level 1), or industry best practice guidelines in hardening systems, as deemed appropriate by the Authorizing Official. System configuration settings will be included as part of the CMP and will be updated and/or reviewed at least on an annual basis (as we are providing under Networx).
  15. Lumen will develop and maintain a security Incident Response Plan (IRP), based on a previously approved one. We will provide the IRP with the initial security A&A package, with annual updates (as we are providing under Networx).

- 
16. Lumen will test the IRP and document the results in an Incident Response Test Report (IRTR). We will provide an IRTR with the initial security A&A package, with annual updates (as we are providing under Networx).
  17. Lumen will develop and maintain a Supply Chain Risk Management (SCRM) Plan to reduce supply chain risks to performance and security throughout our services' lifecycle. We will provide the SCRM Plan with our proposal and with annual updates to the security A&A package.
  18. Lumen will operate continuous monitoring of security controls of the system and its operational environment, as we are providing under Networx, to ensure that the security controls continue to be effective over time and as changes occur in the system and environment. We have developed and will maintain a Continuous Monitoring Program (Continuous Monitoring Plan) to document how continuous monitoring is accomplished. Through continuous monitoring, security controls and supporting deliverables will be updated and submitted to GSA per the GSA-defined schedules. We will provide a Continuous Monitoring Plan, based on a previously approved one, with the initial security A&A package and with annual updates (as we are providing under Networx).
  19. Lumen will develop and maintain a Plan of Action and Milestones, based on a previously approved one, completed in agreement with GSA IT Security Procedural Guide 06-30, "Plan of Action and Milestones (POA&M)." All subsystems will be scanned as authenticated users with elevated privileges from internal management networks, in addition to scans sourced from the public internet where appropriate. We will reflect and show mitigation of vulnerability scan results in the POA&M, and submit scan results together with each quarterly POA&M submission. Scans will include all computing and networking components that fall within the security assessment and authorization boundary. Appropriate vulnerability scan reports will be submitted with the initial security A&A package. An annual information system User Certification/Authorization

---

Review will be annotated in each POA&M. We will provide the POA&M with the initial security A&A package and at least quarterly thereafter.

20. Lumen is required to maintain MTIPS accreditation and will engage, as it has done under Networkx, an independent security firm to complete an internal and external penetration test and provide an Independent Penetration Test Report documenting the results of vulnerability analysis and exploitability of identified vulnerabilities with security assessment package and on an annual basis in accordance with GSA CIO-IT Security Guide 11-51. GSA will provide for the scheduling and performance of these penetration tests. All penetration test exercises will be coordinated through the GSA Office of the Chief Information Security Officer (OCISO) Security Engineering (ISE) division.
21. Lumen will conduct code analysis reviews in accordance with GSA CIO Security Procedural Guide 12-66 using Fortify or an equivalent tool to examine source code for common flaws. We will provide document results in a Code Review Report prior to placing our system into production, when there are changes to code, and on an annual basis.
22. Lumen will allow GSA employees (or GSA designated third-party contractors) to conduct security A&A activities, as it has done since 2010 with the initial MTIPS A&A exercise, to include control reviews in accordance with NIST SP 800-53/NIST SP 800-53A and GSA IT Security Procedural Guide 06-30, "Managing Enterprise Risk." We know that review activities will include but not be limited to operating system vulnerability scanning, web application scanning, and database scanning of all systems and software within the authorization boundary. We know that all subsystems will be scanned as authenticated users with elevated privileges from internal management networks, in addition to scans sourced from the public internet where appropriate.
23. Lumen will resolve or mitigate all identified gaps as documented in the Security/Risk Assessment Report (SAR), as we have been providing under Networkx. We will track gaps for mitigation in the POA&M document in

---

accordance with GSA IT Security Procedural Guide 06-30, "Managing Enterprise Risk." As detailed in our Networx ATO dated 28 October 2013, we understand that the AO may require gap remediation before issuing an ATO.

24. Lumen will resolve or mitigate all security risks found during security A&A and continuous monitoring activities, as we have been providing under Networx. All critical and high-risk vulnerabilities will be mitigated within 30 days, and all moderate risk vulnerabilities will be mitigated within 90 days from the date vulnerabilities are formally identified. We understand that the government will determine the risk rating of vulnerabilities. Updates on the status of all critical and high vulnerabilities that have not been closed within 30 days will be provided on a monthly basis.
25. Lumen will deliver the results of the annual FISMA assessment conducted per GSA CIO IT Security Procedural Guide 04-26, "FISMA Implementation," as we have been providing under Networx. Each fiscal year the annual assessment will be completed in accordance with instructions provided by GSA.
26. As has been done under Networx, Lumen will follow the three year security reauthorization process, and will accommodate an ongoing security authorization process for EIS if/when our system is accepted by the GSA AO into the GSA Continuous Monitoring Program. As required by EIS, we will provide the following deliverables to the GSA Contracting Officer's Representative (COR)/ISSO/ISSM on a monthly basis in accordance with GSA COI Security Procedural Guide 12-66:
  - a) Reports on SCAP Common Configuration Enumerations (NIST SP 800-53 Rev 4: CM-6)
  - b) Reports on SCAP Common Platform Enumeration (NIST SP 800-53 Rev 4: CM-8)
  - c) Reports on SCAP Common Vulnerabilities and Exposures (NIST SP 800-53 Rev 4: CM-8)

---

27. As we have done under Networkx, Lumen will develop and keep current all policy and procedures documents, as outlined in the specified NIST Special Publications as well as appropriate GSA IT Security Procedural Guides. The following documents will be verified and reviewed during the initial EIS security assessment and update review capability will be provided to the GSA COR/ISSO/ISSM biennially:

- a) Access Control Policy and Procedures (NIST SP 800-53 Rev 4: AC-1)
- b) Security Awareness and Training Policy and Procedures (NIST SP 800-53 R4: AT-1)
- c) Audit and Accountability Policy and Procedures (NIST SP 800-53 Rev 4: AU-1)
- d) Security Assessment and Authorization Policies and Procedures (NIST SP 800-53 Rev 4: CA-1)
- e) Configuration and Management Policy and Procedures (NIST SP 800-53 Rev 4: CM-1)
- f) Contingency Planning Policy and Procedures (NIST SP 800-53 Rev 4: CP-1)
- g) Identification and Authentication Policy and Procedures (NIST SP 800-53 Rev 4: IA-1)
- h) Incident Response Policy and Procedures (NIST SP 800-53 Rev 4: IR-1)
- i) System Maintenance Policy and Procedures (NIST SP 800-53 Rev 4: MA-1)
- j) Media Protection Policy and Procedures (NIST SP 800-53 Rev 4: MP-1)
- k) Physical and Environmental Policy and Procedures (NIST SP 800-53 Rev 4: PE-1)
- l) Security Planning Policy and Procedures (NIST SP 800-53 Rev 4: PL-1)
- m) Personnel Security Policy and Procedures (NIST SP 800-53 Rev 4: PS-1)
- n) Risk Assessment Policy and Procedures (NISTSP 800-53 Rev 4: RA-1)
- o) Systems and Services Acquisition Policy and Procedures (NIST SP 800-53 Rev 4: SA-1)



- 
- p) System and Communication Protection Policy and Procedures (NIST SP 800-53 Rev 4: SC-1)
  - q) System and Information Integrity Policy and Procedures (NIST SP 800-53 Rev 4: SI-1)

Lumen complies with system security plan requirements as mandated by federal laws, directives and policies, including making available any documentation, physical access, and logical access needed to support the requirement as detailed in Sections C.2.8.4.5.4 and C.1.8.7.4 of the EIS RFP.

Lumen's Network SSP has been accredited by GSA since 2010 and has passed all DHS reviews since the first audit in 2010. As requested by GSA, we are currently updating our MTIPS SSP to reflect NIST SP 800-53 Revision 4 and will deliver this to GSA in the 2nd quarter FY 2016. We have exceeded contract requirements with quarterly SSP updates.

Our SSP includes:

- Security Assessment BSD
- ISA, MOA, MOU
- 800-53 Control Tailoring Worksheet (CTW)
- 800-53 Baseline Control Summary
- Rules of Behavior
- PIA
- BIA
- System Hardware and Software Inventory
- Security IRP
- Security Incident Response Test Plan
- Security Incident Response Test Report
- Contingency Plan (AKA Business Continuity Plan/DR Plan)
- CPTP

- 
- CPTR
  - CMP
  - Audit Monitoring Program
  - Continuous Monitoring Program (for security)
    - Access Monitoring
    - Configuration Monitoring
    - Vulnerability Monitoring (Scanning)
    - Third-Party Penetration Test Report
    - Automated reporting to customer (as requested)
  - Security Incident Response Plan
  - Security Incident Response Plan Test Plan
  - Security Incident Response Plan Test Report
  - e-Authentication documents:
    - e-Authentication Executive Summary
    - e-Authentication Detail Report
    - e-Authentication Risk and Requirements Assessment Tool (database file)
  - User Access Authorization & Management Process
  - Personnel Security Procedures
  - Suitability Report (employee background investigation report)
  - Security Test and Evaluation (ST&E) Plan
  - Security Test and Evaluation (ST&E) Report

GSA requires artifacts to demonstrate compliance with SP 800-53 controls in “Annual FISMA Assessments” in years that do not include ATO audits. POA&M reports are provided to GSA on a monthly basis. We currently run security vulnerability scans weekly as part of our continuous monitoring program, to discover and rapidly resolve any weaknesses that occur.

---

#### **1.4.8.3.4.5 Additional Security Requirements (C.2.8.4.5.5)**

All deliverables identified in this section will continue to be labeled as CUI and Lumen Confidential. Per company and government policy all external transmission/dissemination of Lumen data to or from a GSA computer must be encrypted in accordance with FIPS PUB 140-2, “*Security requirements for Cryptographic Modules.*”

In accordance with the FAR (see Section I, 52.224-1, “*Privacy Act Notification*” and FAR 52.224-2, “*Privacy Act.*”), Lumen has worked with GSA to create MTIPS non-disclosure agreements that other third parties must sign when acting as the federal government’s agent.

Lumen will continue to support the government in any requested manual or automated audits, scans, reviews, or other inspections of Lumen’s MTIPS environment. Lumen agrees not to publish or disclose in any manner, without the CO’s written consent, the details of any safeguards either designed or developed by Lumen under this contract or otherwise provided by the government (except for disclosure to a consumer agency for purposes of security A&A verification).

Lumen will continue to support the government or its agents to carry out a program of inspection to safeguard against threats and hazards to the confidentiality, integrity and availability of any non-public government data collected and stored by Lumen. This includes providing the government logical and physical access to the Lumen’s MTIPS facilities, installations, technical capabilities, operations, documentation, records, and databases within 72 hours of the request. Automated audits can include, but are not limited to, the following methods:

- Authenticated and unauthenticated operating system/network vulnerability scans
- Authenticated and unauthenticated web application vulnerability scans
- Authenticated and unauthenticated database application vulnerability scans
- Internal and external penetration testing

---

Automated scans of the MTIPS environment can be performed by government personnel, or agents acting on behalf of the government, using government operated equipment, and government specified tools. If Lumen chooses to run its own automated scans and/or penetration tests of the MTIPS environment, results from these scans and/or penetration tests may, at the government's discretion, be accepted in lieu of government performed vulnerability scans and/or penetration tests. This can only be done if the scanning tools and their configurations have been approved by the government in advance. The results of Lumen-conducted scans and/or penetration tests will be provided, in full, to the government.

#### **1.4.8.3.4.6 Personnel Background Investigation Requirements** **(C.2.8.4.5.5.1)**

As detailed in the approved MTIPS SSP, Lumen follows the following process to satisfy the Homeland Security Presidential Directive (HSPD)-12 requirements for background investigations for contractors working on government/government-contracted systems, such as MTIPS, the following criteria has been established:

There are two levels of clearance proposed: Level 1 and Level 5. Level 1 is the National Agency Check with Inquiries (NACI) for low risk positions, and Level 5 is the Minimum Background Investigation (MBI) for moderate risk positions.

The following criteria pertain to government sensitive information inside the security assessment boundary.

Staff members who have read-only access and cannot alter the government sensitive information are candidates for the Level 1 (NACI). This is considered a low risk position and may include most PMO and Operations staff unless they fall into the Level 5 category.

Individuals who have physical access to the system equipment inside the "System Boundary," or who have privileged user access with ability to alter the data at rest or in transport, as well as individuals who have read and write access to government sensitive information are candidates for Level 5 (MBI). This is considered a moderate

---

risk position and would include most System Analysts, System Engineers, Database Managers, and System Administrators, etc.

### ***Low Risk Suitability Determinations***

Applicants must possess at least an interim suitability determination approval prior to being granted access to provide “low risk/Level 1” support to MTIPS systems. Investigation requests are coordinated between the hiring manager and the Corporate Special Security Officer (CSSO).

### ***Moderate Risk Background Investigation***

Applicants must possess at least an interim MBI approval prior to being granted access to provide “moderate risk/Level 5” support to MTIPS systems or have access within the MTIPS boundary. Investigation requests are coordinated between the hiring manager and the CSSO. MBI investigation dates must be less than five years old. Investigation dates are tracked by the CSSO in a Security Information Management System as well as in an Excel spreadsheet. When applicable, reinvestigations will be coordinated between the CSSO and the cleared personnel.

### ***Single Scope Background Investigation (SSBI)***

Applicants must possess a current SSBI, which is less than five years old or, new applicants must be willing to undergo an SSBI prior to be given access to MTIPS program classified material. SSBIs are conducted by investigators contracted by the DSS who verify records and conduct personal interviews concerning one’s personal background. SSBIs that are two years old will undergo a reinvestigation to ensure that they are properly updated. When applicable, reinvestigations will be coordinated between the CSSO and the cleared personnel. Investigation dates are tracked by the CSSO in a Security Information Management System as well as in an Excel spreadsheet.

There is no distinction between a person who performs a task on a daily basis from the person who is assigned a backup role, and would only perform the duties in a particular circumstance.

---

Individuals supporting the MTIPS contract must meet the eligibility requirements as described in government policies and directives related to the level of risk and support associated with the type of work an individual is assigned to perform.

The hiring and screening process begins with the hiring manager or designee preparing a detailed job description or personnel requisition that includes such information as job title; essential and related job functions and responsibilities; required education, experience, skills, knowledge, and physical abilities; and other qualifications needed to perform the job. Candidates are screened for applicable skills training and security clearance requirements. Education and former employment are verified, and all new employees must pass a drug screen. The hiring manager will request the CSSO or designee to complete a security screening for personnel who are being considered for a position involving duties that fall into one of the risk categories stated above. The CSSO will interview potential nominees and advise them of the nature and the extent of the required security processing. The CSSO will require a "Program Access Request" (PAR) form be completed for all personnel requiring a clearance/SCI access in order to perform their job.

Individuals being considered for a position of trust must meet the eligibility requirements as described in applicable government policies and directives related to the level of risk and support associated with the type of work the individual will be assigned to in support of the contract.

It is the security policy of Lumen to only submit those personnel who pass an initial security screening and will make a valid contribution to the contracts herein. The applicant must have excellent character and discretion, and not be subject to influence through exploitable personal conduct. In arriving at a decision consistent with the eligibility criteria, the adjudicator must give scrutiny to the following matters:

- Loyalty to the United States
- Close relatives and associates who are not citizens of the United States
- Cohabitation arrangements

- 
- Undesirable character traits
  - Excessive absenteeism or tardiness
  - Recurring security violations
  - Financial irresponsibility
  - Alcohol abuse
  - Illegal drugs and drug abuse
  - Emotional, mental, and personality disorders
  - Record of law violations and criminal conduct
  - Security violations
  - Involvement with subversive activities or organizations.

Once the investigation process is completed, only those persons who have completed the investigation and have been approved by DHS/GSA will be allowed to work on the MTIPS system.

To assist the GSA and DHS in the validation process, the Lumen MTIPS Program Manager will ensure a detailed program specific justification is required and documented for nominating all new personnel to the contract.

The CSSO will provide personnel security reports semi-annually to the Program Manager and the managers/supervisors of personnel assigned to support MTIPS. The reports will be reviewed to ensure personnel listed are still supporting MTIPS and the level of investigation held complies with contract requirements for the risk level assigned to the position.

*1.4.8.4 Managed Security Services [L.29.2.1, C.2.8.5]Lumen provides a comprehensive MSS offering to include managed prevention, vulnerability scanning and incident response services. These MSS solutions include core protections such as managed firewall, antivirus, intrusion detection and prevention. Our network based MSS solution delivers a fully integrated, carrier-grade, GSA accredited platform that meet all EIS network security requirements. Additional benefits of our MSS for the agency include security event and incident management, vulnerability management services, patch management, custom signature, policy*

*application, and role based identity and access management.*

#### 1.4.8.4.1 Understanding (L.29.2.1-A; M.2.1-1)

Agency security experts are engaged in an ongoing fight to protect information assets from cybercriminals. Hacktivists and nation states attempt to steal or destroy critical agency information and infrastructure. As agency networks expand, so do the cyber battle space and threat landscape. Defending against threats and securing Lumen's network and information assets is critical to agencies' success.

##### *Lumen's MSS Highlights and Endpoint Protections*

- ✦ **Traffic Volume:** Our managed security solution handles more than 20 Gbps of agency traffic
- ✦ **Trusted Choice:** More than 40 U.S. departments and agencies currently provisioned using network based security solution
- ✦ **Scalable:** Flexible platform that meets changing technology and security needs while integrating with existing agency protections

Lumen protects a global network that connects 60+ Lumen data centers and numerous global agency networks. We see the emerging threat vectors multiply with new attack methods and strategies on a daily basis. Lumen is a critical infrastructure provider, a world-class leader in information assurance (IA), and a leading MSS provider. We know firsthand how to detect and defeat attacks against our infrastructure and customer networks because we understand the signs of a cyber attack and how best to protect agencies from subsequent compromises and breaches.

Our managed services SOC professionals use automated security monitoring and analysis tools to identify vulnerabilities and uncover preliminary indicators of compromise to network traffic and security logs. We proactively assist each agency with MSS related requirements to remain ahead of would-be attackers.

With Lumen's experience in advanced security monitoring and analysis service, we can reinforce an agency's defenses with threat intelligence and provide expert suggestions to mitigate risks to the network. We bring together dedicated security experts, state-of-the-art technology and analytics tools, and efficient, real time attack-detection processes. We regularly improve and strengthen our security services and



---

thwart potential attacks by gathering and applying threat intelligence that helps us to identify, understand, and respond to threats as early as possible. Lumen's MSS monitoring and analytics solutions include:

- Network threat monitoring
- Automated collection and analysis of agency traffic flows from our IP backbone network to discover early indicators of compromise and suspicious communications
- Our SOC monitors and manages the security devices that control agency network traffic with log monitoring and analysis, incident investigation, and handling
- Advanced next generation monitoring tools and applied analytics

#### ***1.4.8.4.1.1 Service Description (L.29.2.1-1; C.2.8.5.1) and Functional Definition (C.2.8.7.1.1)***

Lumen's MSS solution includes our proven managed firewall, anti-virus/malware, intrusion detection/prevention, vulnerability scanning, and incident response service (INRS). These services provide endpoint protection for network applications including email, web, and networking assets. Our security management experts will lead joint event management efforts between the agency and Lumen to proactively protect the agency's infrastructure and information against cyber criminals and corrupt organizations.

Lumen provides a comprehensive MSS portfolio that uses both network- and premise-based solutions to secure agency boundaries. These fully managed services form the core capabilities to protect agency endpoints from known malware threats. Lumen will deploy MPS, INRS, and vulnerability scanning service (VSS) as part of our MSS offering for endpoint and network based security.

Each managed security service component provides an agency with linked defenses against cyber attacks. Lumen's SIEM system will monitor the network elements and provide alerting, notification, and event management. At all SDPs, Lumen will place a

---

SEC SRE where all events and logs are collected and subsequently forwarded to the SIEM. The SIEM will correlate the event to its extensive database that contains indicators and triggers of nefarious activity within the network. If there is a correlation, the SIEM will initiate an alarm to both the SOC employee and the investigation and tracking console.

Lumen's SOC team of cyber analysts is extensively trained in their ability to investigate SIEM identified events and analyze data streams for malware signatures, attack vectors, and indicators of compromise. Our SOC analysis tools go beyond the standard toolsets that telecommunications companies, or ISPs that use legacy SIEMs, commonly deploy to monitor and manage security events. We collect and store network and device outputs to catalog signature patterns, traffic anomalies, and other attack stream indicators to update the heuristics within the SIEM, allowing for future detection of malware code and security anomalies within the agency's network.

Our MSS solution leverages best of breed technologies to deliver an effective security to agencies. Compliance with security standards is the foundation for creating a secure boundary and for performing ongoing risk assessments and threat analyses.

Lumen's MSS solution is:

- A fully integrated protection service that defends against internal and external endpoint attacks
- Interoperable with agency infrastructure elements
- Able to provide security at the endpoint or in the cloud
- Scalable to meet the expanding and evolving threat environment
- Capable of rapid deployment of mitigation tactics, techniques, and procedures
- Continuously monitored to detect and prevent attacks against the agency infrastructure
- Compliant with industry and federal standards and guidelines for securing agency information

---

Lumen's MSS provides protection of endpoints, email, web, and networks, through authentication, anti-virus, anti-malware/spyware, intrusion detection, and security event management. A breach can significantly affect national security and be costly in both dollars and reputation. Lumen's MSS is a cost-effective and efficient service that provides protection of endpoints, email, web, and networks. To mitigate cyber-related threats, we protect agency information assets while providing best-in-class risk authentication, anti-virus, anti-malware/spyware, intrusion detection, and security event management.

#### **1.4.8.4.1.2 Standards (L.29.2.1-2; C.2.8.5.1.2)**

Compliance with the appropriate standards and guidelines is critical for effective managed security services. We incorporate standards-based controls into each EIS security service we provide. This standards based approach provides the agencies with verifiable control sets and documentable artifacts for compliance purposes. As evidenced by our MTIPS and IPSS offerings, our compliance with NIST standards supports confidentiality, integrity, and availability of agency data across the enterprise.

Lumen will ensure that as we provide MSS to the Federal Government, we will comply with applicable federal IT security directives, standards, policies, and reporting requirements found in RFP Section C.2.8.5.1.2. Lumen will comply with applicable FISMA and applicable FIPS, NIST SP 800 series guidelines, agency-specific security directives, policies, guides, and other appropriate government-wide laws and regulations that are established to protect and secure government systems and data.

We will follow US-CERT reporting requirements in current and amended guidelines. Lumen will continuously evaluate and apply emerging standards and modifications or amendments to existing standards and guidelines.

#### **1.4.8.4.1.3 Connectivity (L.29.2.1-3; C.2.8.5.1.3)**

Lumen's MSS is designed and implemented with federal security requirements embedded into its solution. This approach allows our MSS to connect and interoperate with existing agency network environments including WAN/LAN, extranets, and DMZs.

Lumen’s MSS will support connectivity to extranets and agency Internet access points, as required by agency-specific transport and access requirements. MSS can be offered with all Lumen proposed network transport solutions. The underlying network architecture supports direct connectivity for MSS integration (consistent with our managed service integration) as described in Section 1.1, Network Architecture.

**1.4.8.4.1.4 Technical Capabilities (L.29.2.1-4; C.2.8.5.1.4)**

**1.4.8.4.1.4.1 Managed Prevention Service (MPS) (C.2.8.5.1.4.1)**

RFP. Ref. Para. #	Response
C.2.8.5.1.4.1 (#1)	Lumen will provide design and implementation services to the agency. The TDRF and technical interchange meeting (TIM) processes are used by Lumen and agency security personnel to discuss and document matters such as system recommendations, a baseline assessment, rules, signature sets, configurations, and escalation procedures with data provided by the agency.
C.2.8.5.1.4.1 (#2)	At the TO level, Lumen will provide all software and hardware components, including log servers to meet the service requirements and final agency design.
C.2.8.5.1.4.1 (#3)	Lumen will implement a hardware or software load balancing capability and provide redundancy as necessary to meet KPI and agency requirements. For example, Lumen’s current critical service’s solution for a single circuit incorporates redundant infrastructure to ensure immediate failover in the event of loss of service in either route. Each solution will meet the agency KPI and SLA requirements as stated in the TO.
C.2.8.5.1.4.1 (#4)	Lumen will provide on-site installation support including testing of equipment, testing of software, and loading of any agency-relevant data, as required by the TO. On-site installation and testing will be conducted based on the agency approved TDRF and in accordance with the service turn-up schedule.
C.2.8.5.1.4.1 (#5)	As part of our MSS offering, Lumen will maintain the latest configuration information for restoration purposes, reporting, and forensics analysis. Configuration and agency policy will be stored securely in Lumen SOC databases. Authorized agency personnel will have access to this information for further analysis. Configuration information will be automatically captured every twelve hours and transmitted to the SOCs for archival.
C.2.8.5.1.4.1 (#6)	Lumen will maintain the managed service capabilities, performing the necessary hardware/software upgrades, regular content updates, and necessary replacements to ensure performance requirements are maintained. The SOC will work with each agency to integrate our activities into its maintenance windows for software updates, patch management, or any other network activity that impacts work to be performed within the service.
C.2.8.5.1.4.1 (#7)	Lumen will ensure that MPS systems and components that reside within the security assessment boundary comply with NIST SP 800-53 identification and authentication controls for high impact systems (FIPS 199). Administrative access devices requires multi-factor authentication (OMB M-11-11). Lumen will apply NIST SP 800-53 access controls as appropriate for administrative access to the MPS systems or components which reside within the security assessment boundary.
C.2.8.5.1.4.1 (#8)	Lumen will use agency-requested means of communication to notify the agency about the patches and bug fixes as soon as they become available.

**General Services Administration (GSA)**  
**Enterprise Infrastructure Solutions (EIS)**

Contract # GS00Q17NSD3006  
 Mod #: P00310  
 Submission #: CL01001.01a

RFP. Ref. Para. #	Response
C.2.8.5.1.4.1 (#9)	As part of our MSS offering, Lumen will deploy the latest patches and bug fixes following testing and agency approval in accordance with our change management procedures.
C.2.8.5.1.4.1 (#10)	Lumen follows a configuration management process to perform and document configurations and configuration changes, ensuring that agency requested security, access, and information-flow policies are enforced. No changes to organizational security technologies will be made unless the proposed change has gone through agency change control management procedures and authorized personnel have submitted a ticket. After a change has been implemented Lumen and the agency will test it for proper application and the agency then approves the ticket closure.
C.2.8.5.1.4.1 (#11)	Lumen's SOC tool set [REDACTED] and SOC security personnel monitor the health and status of MPS hardware/software components on a 24x7x365 basis for indications of compromise such as intrusions, anomalies, malicious activities, and network misuse.
C.2.8.5.1.4.1 (#12)	The SOC actively monitors all services to ensure performance is in compliance with the established SLAs. The SOC/NOC systems and SOC personnel jointly perform these monitoring activities. Based on performance findings, Lumen will make recommendations for hardware/ software component upgrades and/or additions as the network expands or contracts to optimize the agency network.
C.2.8.5.1.4.1 (#13)	Prior to service implementation, a documented TDRF will be completed. This agency approved document provides the connectivity, permissions, and functionality of the service. Subsequent changes must be initiated through the ticketing system and approved by the agency in accordance with the change management procedures.
C.2.8.5.1.4.1 (#14)	Where the TO requires, Lumen will conduct validation activities to ensure integrity of the service configurations. For example, validation scans can be scheduled, performed and documented to verify enforcement of agency policy. Additionally, Lumen works with the vendors to ensure no OS-level vulnerabilities exist within the service.
C.2.8.5.1.4.1 (#15)	Lumen's SOC will notify the agency, using their directed process, of failures in MPS elements.
C.2.8.5.1.4.1 (#16)	Lumen currently receives and processes as appropriate SBU cyber indicators from the agency or DHS and will maintain that capability under EIS.
C.2.8.5.1.4.1 (#17)	Service statistics, event logs and messages are sent through the SEC SRE at the SDP to the agency-specified collection server. For suspected attack information, Lumen will include all details within the system which is secure and available to the agency's SOC.
C.2.8.5.1.4.1 (#18)	Lumen will ensure that event messages associated with DHS-provided indicators are sent by secure means to DHS. Examples of secure means of communication include IPSec tunnels or dedicated private lines sourcing from Lumen's systems and terminating at DHS- specified locations.
C.2.8.5.1.4.1 (#19)	Lumen uses industry best practices to establish coordinated universal time (UTC) as the standard timing for all systems and devices, independent of time zone or location. This enables correlation of events to be recognized at the exact time that they occur. Lumen's log capture and event correlation systems will ensure event messages have the necessary context based on time/date of occurrence; related indicators, policies, and anomalies; source and destination addresses, ports, and protocols; operating system, processes, and application; and detection source and location.
C.2.8.5.1.4.1 (#20)	Lumen uses security SREs to provide SDP-level customer agency data for the agency. The security SRE will only contain a single agency's data and therefore cannot divulge any other agency's data.
C.2.8.5.1.4.1 (#21)	Lumen provides secure web access to information and service status to the agency. Authorized agency

RFP. Ref. Para. #	Response
	<p>users will use secure web access to view logs and service information including the following:</p> <ul style="list-style-type: none"> <li>a. Active Sessions</li> <li>b. Port and Protocol Activity</li> <li>c. Authentication Statistics</li> <li>d. Connections/Attempts counts and results (accepted/rejected) by port</li> <li>e. Events, rule violations, and attacks detected including name, description, level, impact date, time, vulnerabilities and targeted weakness, and remedies.</li> <li>f. Source and Destination IP Addresses, domains (fully-qualified domain name) and URLs; as well as statistics</li> <li>g. Affected endpoints</li> <li>h. Managed Prevention Service Statistics and Utilization</li> <li>i. Outages</li> <li>j. Configuration Modifications.</li> <li>k. Change Requests and Event Tickets.</li> </ul>

**1.4.8.4.1.4.2 Vulnerability Scanning Service (VSS) (C.2.8.5.1.4.2)**

RFP. Ref. #	Response
C.2.8.5.1.4.2	<p>Lumen will support the agency to establish, implement, and maintain a VSS. Lumen’s VSS solutions will be created at the TO level using best practices and tools to meet each agency’s LAN/WAN scanning requirements.</p> <p>Lumen is providing a fully functional VSS including all tools, processes and personnel to perform each aspect of VSS. In our experience, some agencies will wish to use some subset of the full complement of VSS, and our approach is to accommodate this (e.g., agencies schedule and run scans independently of Lumen) as negotiated in each TO to meet individual agency’s need.</p> <p>Lumen’s geographically disbursed, redundant SOCs manage VSS to provide the service on a 24x7x365 basis.</p> <p>As part of our fully managed offering, Lumen will provide:</p> <ul style="list-style-type: none"> <li>• External scanning to include port scans, web application scans, and network device security testing.</li> <li>• Internal scanning which consists of scanning for system flaws, ports/protocols/services, and application fingerprinting.</li> </ul> <p>Lumen supports agencies through our VSS by using an SDP based application that allows authorized agency users to scan the internal LAN. Lumen will perform VSS external scanning from the WAN to seek system flaws, open ports and protocols, and other elements within the agency that are visible from the Internet.</p> <p>VSS is established according to the agency specific LAN/WAN scanning requirements for periodic probing. The periodic scans include operating systems and application software, for potential openings, security holes, and improper configuration.</p>
C.2.8.5.1.4.2 (#1-48)	Using a combination of Lumen’s internal and external VSS, we will continue to scan agency systems for vulnerabilities in the areas included in RFP Section C.2.8.5.1.4.2, 1 through 48.
C.2.8.5.1.4.2 (#1)	The VSS maintains a database of vulnerabilities and their associated countermeasures, fixes, patches, and workarounds. Mitigation strategies and recommendations are automatically provided to the agency using its

RFP. Ref. #	Response
	preferred method of contact. We actively track known vulnerabilities as well as recommended remediation plans for any vulnerabilities.
C.2.8.5.1.4.2 (#2)	Lumen will notify the agency as directed and in accordance with its requirements for preferred method.
C.2.8.5.1.4.2 (#3).	Lumen will provide secure web access to authorized agency personnel to vulnerability report systems information including vulnerability information, scan summaries, device/host reports, and trend analyses.
C.2.8.5.1.4.2 (#4)	Lumen will review and document all vulnerability findings upon completing a vulnerability scan of the agency environment as required. Lumen will provide the agency with the completed scan report and will discuss the details of that report with agency personnel
C.2.8.5.1.4.2 (#5)	Using the secure web interface, Lumen’s team will work with the agency to schedule, conduct, and repeat vulnerability scans at any time for any specified duration using various scanning methodologies. The flexibility of scheduling various scan types at specific times minimizes the likelihood of interruptions in normal business activities. Additionally, authorized agency users may schedule scans through the same secure web interface without Lumen’s assistance.
C.2.8.5.1.4.2 (#6)	Lumen will provide non-destructive, non-intrusive scanning. Non-destructive scanning will be performed across agency environments in accordance with the agency scanning schedule and IP range. Lumen’s VSS is adjustable and can be configured with a “light to medium touch” scan. This capability will minimize potential impact to agency systems or disrupt agency operations during the scanning process. Lumen’s VSS is fully adjustable and is designed to safeguard against the provocation of a potential denial of service attack. Authorized users (Lumen or agency) can configure scans so that it does not provoke a denial of service condition on the agency system being probed. Vulnerability scanning provides users the ability to test its systems for vulnerabilities and resilience to any potential attacks. Lumen’s VSS can be adjusted to simulate a brute force attack to either penetrate or disable a device should the agency request more invasive testing. Lumen suggests more invasive tests be conducted during maintenance windows.
C.2.8.5.1.4.2 (#7)	Lumen’s VSS engineers have extensive experience using the VSS system with a vast database that contains results of previous scans from similar systems. This allows the engineers to use analytics to ascertain the vulnerability of the agency system currently in place, and whether a particular scan would be potentially destructive or intrusive to the agency’s systems.
C.2.8.5.1.4.2 (#8)	Lumen’s VSS is instantly, continually, and globally updated as all scanning systems leverage common core database of vulnerabilities. All scanning systems perform outbound-only data flows for vulnerability analysis and reporting; VSS systems do not need to have information pushed to the individual scanners (regardless of location of the scanner) because information is pulled on a regular basis. The centralized database of vulnerability reporting and analysis ensures the results of the scans contain up-to-date knowledge of all known vulnerabilities.
C.2.8.5.1.4.2 (#9)	Lumen’s VSS infrastructure is adjustable and fully configurable to support networks of varying size and complexity. The VSS scanning infrastructure is hierarchical and is fully scalable to support the environment required by individual agencies.

**1.4.8.4.1.4.3 Incident Response Service (INRS) (C.2.8.5.1.4.3)**

RFP. Ref. #	Response
C.2.8.5.1.4.3( #1 )	In collaboration with the agency, Lumen security subject matter experts (SMEs) will review the agency security infrastructure and develop appropriate strategic plans to provide an optimized compliant INRS. From

**General Services Administration (GSA)**  
**Enterprise Infrastructure Solutions (EIS)**

Contract # GS00Q17NSD3006  
 Mod #: P00310  
 Submission #: CL01001.01a

RFP. Ref. #	Response
	agency TO specifics, Lumen will use appropriately skilled INRS specialists and develop an INRS process with the agency to: <ul style="list-style-type: none"> <li>• Identify internal resources</li> <li>• Assign duties to team members</li> <li>• Describe incident response policies</li> <li>• Define severity levels</li> <li>• List escalation chains (within Lumen and the agency)</li> <li>• Specify emergency/recovery procedures</li> </ul>
C.2.8.5.1.4.3 (#2)	Lumen will provide effective incident response support on a 24x7x365 basis from the SOC. INRS uses available logs and packet analysis techniques to identify known attack signatures and potential “zero-day” attacks.
C.2.8.5.1.4.3 (#3)	Lumen uses ██████████ to monitor available logs and packet information for the diagnosis of alerts and violations. SOC personnel are alerted in near real time of activity that is suspicious or violates an agency’s security policy. The SIEM is configured in a “hot-hot” availability configuration to ensure agency data is continuously being monitored.
C.2.8.5.1.4.3 (#4)	Lumen’s SOC will monitor agency traffic 24x7x365 for any activity that is suspicious, utilizing available logs and packet analysis. The SOC verifies the validity of the threat by utilizing security relevant information from various sources to ensure the incident is not a false positive alert. In the event that a category 1 or 2 event (categories defined by US-CERT where category 1 and 2 are an emergency) is detected, the SOC will follow agreed upon procedures and immediately notify the agency. The notification process can include the execution of an agency specific call list, as well as other agency defined notification procedures. For all other categories, the SOC will provide the agency pertinent information through Lumen’s secure web access.
C.2.8.5.1.4.3 (#5)	The Lumen SOC will immediately make available to the affected agency all vulnerability (i.e., as detected by signatures or known vulnerabilities) and severe alert information.  Provided severe alert information will include, at a minimum, the following information: description, target, origin, potential incident impacts, remedies, prevention measures. Suggested methods of delivery include, but are not limited to: <ul style="list-style-type: none"> <li>a. Secure file transfer                             <ul style="list-style-type: none"> <li>i. SSH encrypted file copy (SCP)</li> <li>ii. Encrypted email attachment to un-encrypted email</li> </ul> </li> <li>b. Secure email transmission</li> </ul>
C.2.8.5.1.4.3 (#6).	During the on-boarding process, Lumen will provide our standard procedure for handling of potential security incidents using this as the blueprint to develop and maintain an agency specific standard operating procedure (SOP). This will include appropriate responses to potential cyber-security incidents and events. The SOC can, if provided, use the agency’s own IRP to respond to cyber incidents. Lumen will coordinate the response with the agency to specific events in accordance with these procedures.
C.2.8.5.1.4.3 (#7)	The SOC has “preprogrammed” responses (countermeasures) to cybersecurity events to contain the incident, limit its spread, and protect internal agency systems. These countermeasures will be activated in parallel with an initial event investigation and notification procedures. Counter measures are finalized with each agency in accordance with TO requirements.



**General Services Administration (GSA)**  
**Enterprise Infrastructure Solutions (EIS)**

Contract # GS00Q17NSD3006  
 Mod #: P00310  
 Submission #: CL01001.01a

RFP. Ref. #	Response
C.2.8.5.1.4.3 (#8)	<p>Lumen will provide recommendations for the elimination of identified vulnerabilities, as well as procedures to guard against future attacks on agency assets.</p> <p>As described in our response to VSS requirements, Lumen has mature relationships, collaborating with multiple security vendors (as well as DoD and DHS) to identify and eliminate present and future agency vulnerabilities and develop mitigation strategies.</p>
C.2.8.5.1.4.3 (#9)	<p>Lumen will use our ticketing system, through a secure web interface with access provided to authorized agency users, to provide incident analysis findings and recommendations.</p>
C.2.8.5.1.4.3 (#10)	<p>The Lumen SOC (as well as any on site personnel) will assist the agency with the containment of a cyber security incident or event using existing SREs or through the use of GFP. The SOC takes containment actions that include:</p> <ul style="list-style-type: none"> <li>a. Blocking traffic to or from specified hosts or network IP addresses</li> <li>b. Blocking specified TCP or UDP ports from entering or exiting an agency network</li> <li>c. Capturing traffic between specific hosts or networks that are owned and managed by the agency</li> </ul> <p>At the conclusion of the cybersecurity incident or event, Lumen will assist the agency in restoring the affected systems to their original state. We will assist the agency with the search for further indicators of compromise by comparing the systems traffic to known command and control channels or malware sites, prior to restoration to the normal operational state.</p>
C.2.8.5.1.4.3 (#11)	<p>The Lumen SOC will assist the agency in testing to verify that the identified vulnerabilities have been corrected and that restored systems are functioning correctly. The SOC will monitor traffic from affected systems for continued indicators of compromise, including traffic to known command and control channels or malware sites. The SOC can review agency provided information, such as system configuration information, agency specific cyber security tool configurations, or other log information, to verify that the vulnerabilities have been corrected.</p>
C.2.8.5.1.4.3 (#12)	<p>Lumen personnel provide dedicated support for the MSS offering and will provide dedicated support until the problem is resolved. Lumen will initiate a teleconference bridge between the affected agency, the SOC, associated security device vendors, and any on-site Lumen personnel for the duration of the cyber security incident or event.</p>
C.2.8.5.1.4.3 (#13)	<p>Lumen personnel will provide post-incident investigative and forensics services including the following post-incident tasks:</p> <ul style="list-style-type: none"> <li>• Isolate and contain impacted area—On-site personnel will disconnect affected systems from the network, and physically secure the systems from tampering. Once contained, we can begin a remediation phase to cure the affected systems and put in place safeguards to help prevent against future incidents.</li> <li>• Capture and collect evidentiary data—Lumen’s digital forensics team of information security consultants will quickly move to capture and analyze data stored in the agency’s network to find indicators of compromise. We will interview and advise onsite staff on the proper handling of potentially compromised disks and devices. Our incident response and forensics team uses advanced tools for monitoring, forensics and analysis to contain the breach.</li> <li>• Categorize the (malicious or illegal) event—US-CERT provides a framework for categorization of malicious events and serves as the foundation for Lumen’s categorization process. Lumen will use US-CERT’s incident categorization and apply appropriate designations based on the incident.</li> <li>• Perform reconstruction analysis—Lumen’s post mortem process will include post-incident investigative and forensic services on the affected systems. Security and event logs from the affected system that</li> </ul>

RFP. Ref. #	Response
	<p>have been collected by additional security tools, such as an end-point-protection application, will be reviewed, as well as traffic logs from perimeter security devices to perform the reconstruction analysis.</p> <p>Lumen recommends that prior to any isolation activity, an agency and Lumen perform an analysis of the live system (e.g., to avoid malware defense mechanisms and loss of memory resident information).</p>
C.2.8.5.1.4.3 (#13)	<p>Lumen SOC personnel will handle and preserve the data collected according to sound scientific, evidence rules, and chain of custody requirements.</p> <p>For example, raw log files that are gathered from impacted systems and network devices will be stored in accordance with practices established by US-CERT.</p> <p>Lumen understands the information collected may serve as evidence in administrative actions and legal proceedings.</p>
C.2.8.5.1.4.3 (#13)	<p>Lumen personnel will assist the agency, as required, in tracing the source of the attack to the extent possible and provide this information to agency personnel.</p>
C.2.8.5.1.4.3 (#14)	<p>Lumen personnel will be available to provide support over the telephone to the agency as required.</p>
C.2.8.5.1.4.3 (#15)	<p>As necessary, Lumen will provide cybersecurity personnel to specified agency locations in order to assist the agency's cybersecurity personnel with resolution of cyber security incidents or events.</p>
C.2.8.5.1.4.3 (#16)	<p>Lumen will provide security awareness training to agency personnel as required by TO.</p>

**1.4.8.4.1.5 Features (L.29.2.1-5; C.2.8.5.2)**

RFP. Ref. Para. #	Response
C.2.8.5.2 (#1a)	<p>Lumen's SOC personnel will provide, operate, and manage the MSS firewall services. Lumen uses a combination of local syslog capture, firewall ACLs, and correlation systems [REDACTED] analyze packet headers and enforce policy based on protocol type, source address, destination address, source port, and/or destination port.</p>
C.2.8.5.2 (#1a)	<p>SOC personnel will ensure that the SOC's firewall solutions apply stateful protocol analysis to compare traffic to generally accepted definitions of benign protocol activity and identify deviations. The stateful firewall protocol analysis and event correlation system incorporates continuous signature updates as the accepted definitions become available. When the correlation system detects deviant protocol activity, an alarm is sent to the SOC technician for investigation and analysis.</p>
C.2.8.5.2 (#1a)	<p>Lumen configures the firewall with appropriate NAT between public and private IP addresses to disguise internal agency IP addresses, as well as port address translation (PAT) for specified ingress and egress traffic for specific inbound and outbound traffic from the SDP.</p> <p>Lumen's SOC will configure firewalls to enforce agency-specified security policies (policies specified through the TDRF onboarding process and maintained through trouble ticketing) and will block all packets and terminate sessions for any traffic that violates those policies. The firewall service will implement a "default deny" policy that will block any traffic not specifically allowed by policy.</p>
C.2.8.5.2 (#1b)	<p>Lumen's MSS provides our MPS capability regardless of location. Lumen will provide personal firewalls or personal firewall appliances in order to secure remote personal computers or small remote networks, as required by the agency. Personal firewalls, like enterprise firewalls, are part of the MSS, our SOC supports personal firewalls, which, like enterprise firewalls, are SREs.</p>
C.2.8.5.2 (#1c)	<p>Lumen will deploy an in-line intrusion prevention SRE with deep-packet capabilities at the agency SDP. The</p>

**General Services Administration (GSA)**  
**Enterprise Infrastructure Solutions (EIS)**

Contract # GS00Q17NSD3006  
 Mod #: P00310  
 Submission #: CL01001.01a

RFP. Ref. Para. #	Response
	<p>SRE enables Lumen’s event collection and correlation system to monitor agency network traffic (HTTP/S, FTP, etc.), analyze network application protocol activity and content to identify and mitigate suspicious activity, and block or disrupt activity based on signatures and behavior. Lumen can monitor encrypted agency web traffic with agreement from and in cooperation with the agency. Lumen requires agency encryption certificates to facilitate this functionality. Lumen’s log collection system pushes feeds sourced from the SRE to the [REDACTED] system which maintains signatures and correlated events that will trigger an alarm when suspicious traffic or behavior occurs at the SDP.</p>
C.2.8.5.2 (#1d)	<p>Lumen will provide host-based intrusion prevention capabilities, including application firewall, endpoint recording, threat detection, whitelisting, banning, and remediation in order to protect agency endpoints</p>
C.2.8.5.2 (#1e)	<p>Lumen will provide an SRE to act as the intermediary between endpoints. The SRE will allow URL- and domain-based filtering as well as obfuscation of internal IP addresses and supports URL blocking. Lumen establishes the baseline configuration for web-proxy requirements according to the agency’s organizational web usage policies as part of the onboarding process. Changes to the deployed web-proxy configuration can be easily accommodated through ticketing system requests.</p>
C.2.8.5.2 (#1f)	<p>Lumen’s MPS SRE will provide filtering of inbound web sessions to web servers at the HTTP/HTTPS/SOAP/extensible markup language (XML)-remote procedure call (RPC)/Web Service application layers from, but not limited to, cross site scripting (XSS), SQL injection flaws, session tampering, buffer overflows and malicious web crawlers. Lumen will ensure all SREs provided to the agency SDP in support of inbound web filtering meet all inbound web filtering requirements specified by the agency.</p>
C.2.8.5.2 (#1g)	<p>Lumen’s MPS SREs will provide an intermediary between endpoints allowing for application layer control/data protocols (e.g., FTP, SIP, instant messaging (IM)) to be proxied. These are standard firewall capabilities provided as part of the service.</p>
C.2.8.5.2 (#1h)	<p>Lumen will provide a SRE-resident capability to perform network behavior analysis. We will develop ‘normal’ agency behavior profiles with the ability to examine network traffic for threat identification including recognition of unusual traffic flows. Such log information will include, but not be limited to, source, destination and encrypted connection size to facilitate additional analysis.</p> <p>For example, DDoS analysis capabilities and process steps include:</p> <ul style="list-style-type: none"> <li>• Learning period – sample flow data such as TCP, UDP, Port 25, Port 80, packet size, etc. is polled over a two-week period, the data used to set baselines and thresholds</li> <li>• Baselines – continually updated and are used to identify normal versus abnormal network behavior</li> <li>• Threat monitoring tuning – incident identification and alert notification of your traffic profile to help ensure your business’s monitoring needs are met</li> <li>• Deployment – traffic is redirected for scrubbing with customer permission</li> </ul>
C.2.8.5.2 (#1i)	<p>Lumen will deploy SREs to provide network traffic content analysis and sandboxing. Our sandboxing technologies receive files, email attachments, web downloads, ftp session files, from multiple sources in real time and uses in-depth binary and execution engine analysis to protect agencies against known and “zero-day” threats.</p>
C.2.8.5.2 (#1j)	<p>Lumen’s SDP SRE-based email protection solution will provide capabilities for inbound and outbound email forgery protection (domain-level sender forgery analysis equivalent to DKIM or Sender Policy Framework standards, digital signing procedures for outgoing email messages to ensure that they have been digitally signed at the domain level), as well as domain and header-based filtering, phishing and spam filtering, block</p>

**General Services Administration (GSA)**  
**Enterprise Infrastructure Solutions (EIS)**

Contract # GS00Q17NSD3006  
 Mod #: P00310  
 Submission #: CL01001.01a

RFP. Ref. Para. #	Response
	<p>attachments violating policy (e.g., size, file type), sanitize malicious content and quarantine messages, as well as measures that can conceal, limit, or change information about the agency's networks or domains, reducing visibility to outsiders. The email security solution integrates seamlessly with other deployed security technologies to provide a comprehensive security solution.</p>
C.2.8.5.2 (#1k)	<p>Lumen will deploy SREs to provide e-mail content analysis and sandboxing. Our sandboxing technologies receive files, and email attachments from multiple sources in real time and uses in-depth binary and execution engine analysis to protect agencies against known and "zero-day" threats.</p>
C.2.8.5.2 (#1l)	<p>Lumen's MSS supports the integration of the email-based threat mitigation service with the agency's own authentication service, as specified by the agency. Lumen uses technologies that can integrate with an organizational authentication services (as well as all specified examples) to allow fine grained policy enforcement. Additional user authentication integration technologies include incorporation of web access policies, email policies, and file transfer policies.</p>
C.2.8.5.2 (#1m)	<p>Lumen's MSS supports DNSSEC capabilities (described in NIST SP800-81-2) to ensure data integrity and source authentication.</p>
C.2.8.5.2 (#1n)	<p>To provide DNS sinkholing, Lumen receives lists of malicious DNS source intelligence from various organizations and agencies that are applied to an identified malicious domain database. DNS queries are applied against the database and queries to malicious domains are sinkholed by providing the address for the sinkhole server. DNS sinkholing will require changes to the DNS infrastructure of the agency.</p>
C.2.8.5.2 (#1o)	<p>Lumen's DLP feature is a function of the UTM within the SRE. DLP will discover and identify sensitive data and manage, monitor, and protect it from being deleted, destroyed or divulged. Lumen's default DLP configuration is incorporated in the TDRF and specifics are identified as part of the onboarding process. DLP can be configured to search for an array of sequences and adjusted to search for agency-specified SBU data criteria. DLP searches for specific alphanumeric sequences (nine digits imply social security numbers, 16 digits imply credit cards) and detects quantified inbound and outbound traffic. DLP prevents specified file types (or even file names) from passing through the SRE, and the SRE can either eliminate or quarantine the potential sensitive data leak based on agency requirements. Lumen will be required to have access to files and directories where data is stored for discovery. To protect data from deletion or destruction, Lumen requires agency authorization to set permissions on agency files and directories. Agency-specific requirements will be addressed at the TO level.</p>
C.2.8.5.2 (#1p)	<p>Lumen's MSS SRE supports 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. The creation and isolation of DMZs is an inherent feature of all MPS SREs.</p>
C.2.8.5.2 (#1q)	<p>Lumen's MSS SRE will support connections to extranets which can facilitate inter-agency interactions or enable the agency to interface with trusted stakeholders. Lumen enables extranets by configuration of a secure tunnel (e.g., IPsec) to allow for direct point-to-point access between two endpoints.</p>
C.2.8.5.2 (#1r)	<p>Lumen's MSS SRE supports firewall-to-firewall VPNs which establishes secure tunnels between agency firewalls, and between firewalls and Lumen's SOC. Lumen treats firewall-to-firewall VPNs in the same manner we treat extranets by establishing end-to-end IPsec tunnels between the firewall endpoints.</p>
C.2.8.5.2 (#1s)	<p>Lumen's MSS solution provides remote agency users with secure access to the network, using VPN encryption technology. Secure remote user VPN access will be accomplished using IPsec or TLS encryption</p>

RFP. Ref. Para. #	Response
	technologies, interconnecting the agency user's endpoint with the remote termination device.
C.2.8.5.2 (#1t)	Lumen currently (and will continue to) interacts with DHS to obtain indicators, establish US-CERT event feeds, and provide EINSTEIN network flow and detection capabilities for agency-specified traffic.
C.2.8.5.2 (#1u)	Lumen's MSS system tools gather and temporarily store security related data. On-site deployed technology will be sized to accommodate at least 24 hours of agency-specific MPS-generated data. Retained data will be securely available to the agency.
C.2.8.5.2 (#1v)	Lumen deploys long term storage capabilities for agency or organizational-specific data collectors. This capability will be sized to accommodate at least one year of organizational data. MPS-generated data will be selectively filtered, stored, and retained data will be securely available to the agency.
C.2.8.5.2 (#1w)	Lumen works with agencies to develop, implement, and enforce agency-specific policy. Security related features are activated at the request of the agency. All security policies are periodically reviewed with the agency to ensure validity and applicability. Agencies have the ability to make policy changes as deemed necessary.
C.2.8.5.2 (2a)	Lumen's VSS API has XML based output, has been integrated with industry leading tools such as Splunk, Archer, ArcSight, and QRadar, and supports multiple formats for information delivery. Our VSS can be integrated with nearly any SIEM system or big-data analytics environment to assist agency security personnel with tasks such as scanning IP addresses, assessing host vulnerabilities, creating user accounts, and exporting vulnerability data.  Lumen's team will work with the agency to provide agency users the ability integrate our VSS API in to their existing infrastructure as part of the initial agency onboarding process.
C.2.8.5.2 (3a)	For our INRS, Lumen uses various statistical techniques, such as malware code clustering based on known exploits. SOC personnel will incorporate big data analytics to perform quantitative analysis and statistical techniques including modeling, machine learning algorithms, and data mining to analyze relevant observations for threat discovery, assessment, situational awareness, and prediction.  Lumen analysts establish performance and event baselines to document high/low thresholds and establish a threat baseline for anomaly detection and predictive threat vector models. This process enables Lumen to analyze event data and extrapolate anomalies that occur in the network, trace their origin and if statistically relevant to perform cluster testing to identify similarities in the threat vector, malware or attack profile.  Lumen will include in our analysis the statistical significance of the findings, and in any case where we are unable to yield a confidence interval, we will so caveat our analysis.

**1.4.8.4.1.6 Interfaces (L.29.2.1-6; C.2.8.5.3)**

The Lumen provided MSS is service independent and will support the VPNS, ETS, and IPS services. Lumen's MSS could be provided for any other network service being proposed under this contract.

**1.4.8.4.2 Quality of Service (L.29.2.1-B; M.2.1-2)**

Lumen's MSS is a fully compliant, network-based, service offering that provides protection for an agency's network and end points. Lumen's MSS supports connectivity

to extranets and the Internet as well as endpoint protection within the agency networking environment including Intranet elements, DMZs, and secure LANs.

Lumen’s incident and event logging data collection systems and our signature-based database correlation system, combined with incident related data for use by our security experts are scalable to meet agencies’ evolving MSS requirements. We routinely adjust the sizing of physical assets that support MSS to meet agency demands. We adjust our security team staffing to meet an agency’s need.

Lumen’s resilient solution consists of managed protection services, vulnerability scanning services, and incident response services supported by geographically redundant SOCs, available 24x7x365, as well as redundant event correlation and collection systems integrated with Lumen’s network. This level of redundancy combined with the reliability of our systems and network enable Lumen to meet all MSS AQLs.

**1.4.8.4.2.1 Performance Metrics (L.29.2.1-7; C.2.8.5.4, C.2.8.5.4.1)**

KPI	Approach
Availability	Lumen’s MSS will meet the 99.5-percent AQL. MSS unavailability, based on a confirmed alarm or trouble report from an agency user, will be measured from the time a ticket is opened with the Lumen NOC and concludes when the alarm is resolved and/or the trouble is rectified to the agency’s satisfaction. The total quantity of unavailability time for all events in the reporting period will be subtracted from the total amount of time in the monthly reporting period to calculate the monthly availability of MSS.
Event Notification (MPS)	If an alarm is triggered [REDACTED] a SOC analyst is notified. If the alarm is determined to be an event, a ticket is initiated within the Lumen ticketing system, triggering an email event notification to the agency within the SLA timeframes (≤ 10 minutes).
Event Notification (INRS)	Lumen incident response event notification process follows the same methodology as MPS event notification. Event times for notifications will correspond with the event category threshold of low (next business day or within 24 hours), medium (within four hours), and high (within 1 hour). As in the MPS process, the event notification email will be automatically triggered by the Lumen ticketing system.
Grade of Service (Configuration Change, Virus Protection Updates)	<i>MPS:</i> All configuration rule changes (including requested virus protection updates from the agency) are tracked in Lumen’s ticketing system from an agency’s request (ticket opened) until the request is completed (ticket closed). Lumen will comply with the EIS SLAs (≤5 hours (MPS) and 24 hours for VSS for normal priority change and ≤ 2 hours for urgent) and provide reports showing the average time for ticket closure meets the AQL. When agencies initiate a request for a configuration change to be performed at a specific time (e.g., during non-business hours), Lumen will follow the requirements of the agency’s request and exclude that ticket from its report. Lumen will obtain agency consent prior to implementation of any Lumen initiated change.
Incident Response	Lumen’s telephone incident response time interval will be measured from the time Lumen accepts the call

Time (Telephone)	from the agency user (time of call identified during the creation of the ticket) to the time in which the SOC responds to the incident, following the response procedures (procedures as identified at the TO level) for investigation and action. Lumen will meet the following telephone incident response time AQLs: <ul style="list-style-type: none"> <li>• Within 1 hour of the notification for a low category incident</li> <li>• Within 15 minutes of the notification for a high category incident</li> </ul>
Incident Response Time (On-Site)	The Lumen response team is geographically dispersed and able to arrive onsite within the required timeframes. Lumen’s on-site incident response value represents the elapsed time between the agency’s notification (identified by the time the ticket is open) to Lumen and our arrival to the affected site for implementation of response and investigative procedures. These procedures, will be defined at the TO level. Lumen will meet the following on-site incident response time AQLs: <ul style="list-style-type: none"> <li>• Within 36 hours of the notification for a low category incident</li> <li>• Within 24 hours of the notification for a high category incident</li> </ul>
Time to Restore (TTR)	For all managed devices, Lumen will meet both AQLs for TTR, with monitoring of these metrics consistent with the approach described in Section 1.2.1.2.

**1.4.8.4.3 Service Coverage (L.29.2.1-C; M.2.1-3)**

MSS will be available to all locations where the underlying Lumen EIS services are provided.

Lumen’s service coverage has been defined in accordance with the requirements of RFP Section J.1 for domestic (CONUS and OCONUS) as well as non-domestic locations. Lumen is proposing service coverage that significantly exceeds the minimum requirement of 25 CBSAs out of the top 100 CBSAs. A detailed description of the geographic coverage for all Lumen services for EIS is provided in Technical Volume, Section 1.2.1.3.

**1.4.8.4.4 Service Security (L.29.2.1-D; M.2.1-4a)**

Lumen’s MSS offering is a service that is specifically designed to enhance the agency’s security posture and provide protection of endpoints, email, web, and networks, including capabilities such as authentication, antivirus, anti-malware/spyware, intrusion detection, and security event management. This offering will comply with the MSS-specific security requirements set forth in RFP Section C.2.8.5.

**1.4.8.5 Managed Mobility Service [L.29.2.1, C.2.8.6, C.4.4]**

The Lumen Team Managed Mobility Service (MMS) solution helps agencies operate in a “Bring Your Own Device” (BYOD) environment through secure network services, software and hardware management for mobile devices. For MMS, Lumen partners with Manage Mobility, a leading provider of custom managed mobility solutions designed to deliver optimal balance between security, total costs and functionality for Government and industry customers. Manage Mobility brings 10 years of experience in mobile logistics and advisory services and utilizes in-place relationships with mobile technology providers to deliver the full-range of MMS capabilities required.

**Managed Mobility Service**

- Enables participants to securely access agency networks and applications using agency-owned and personal mobile handheld devices
- More than 10 years of experience through teaming partner *Manage Mobility* delivering managed mobility solutions to Government and industry for anytime, anywhere secure access to computing systems

Figure 1.4.8.5-1 highlights how the features of the Lumen MMS solution satisfy the evaluation criteria.

**Figure 1.4.8.5-1. MMS Feature Highlights**

EVALUATION CRITERIA	FEATURES OF LUMEN MMS
Understanding [M.2.1.1]	<ul style="list-style-type: none"> <li>• Delivers full capabilities for mobile device management (MDM), mobile application management (MAM), mobile content management (MCM), mobile security, and deployment support.</li> <li>• Provides connectivity to 3G/4G Cellular Service (based on standards for CDMA, GSM, and LTE), Smartphones and Tablets (based on smartphone Oss) and Wi-Fi.</li> </ul>
Quality of Service [M.2.1.2]	<ul style="list-style-type: none"> <li>• [REDACTED] demonstrates quality through 10 years of experience delivering reliable MMS solutions for Government and industry, successfully scaling secure deployment and management of mobile devices, applications, and enterprise data to meet customer requirements.</li> </ul>
Service Coverage [M.2.1.3]	<ul style="list-style-type: none"> <li>• Global mobile network via in-place relationships with major telecommunications carriers provides coverage in more than 400 U.S. cities including the top 100 CBSAs plus 225 countries worldwide.</li> </ul>
Security [M.2.1.4]	<ul style="list-style-type: none"> <li>• Provides secure access to agency networks and applications per agency’s IT security policy.</li> <li>• Delivers full range of application and mobile security including mutual authentication, application installation control, password authentication policy enforcement, and data encryption.</li> <li>• Complies with all required security standards including FISMA, NIST SP 800-53 Moderate, FIPS 140-2, and specific standards identified in the TO.</li> </ul>



---

#### **1.4.8.5.1 Service and Functional Description [L.29.2.1, M.2.1, C.2.8.6]**

The Lumen MMS solution fulfills the mandatory service requirements for MMS identified in SOW C.2.8.6. This section presents a technical description of our offering, demonstrating our capabilities in the following areas: Standards, Connectivity, Technical Capabilities, Features, Interfaces, and Performance Metrics. Lumen's MMS solution leverages our overall network architecture described in Section 1.1 and a global wireless network through in-place relationships with major telecommunications carriers providing coverage in more than 400 U.S. cities including all of the top 100 CBSAs plus more than 225 countries worldwide.

#### **1.4.8.5.2 Standards [C.2.8.6.1.2]**

The Lumen Team provides MMS in compliance with the standards listed in SOW C.2.8.6.1.2 including FISMA Moderate Impact level or higher, NIST SP 800-53 Moderate, FIPS 140-2, IPv4 and IPv6, and specific standards identified in applicable TOs.

#### **1.4.8.5.3 Connectivity [C.2.8.6.1.3]**

The Lumen Team's MMS interoperates with the following:

- 3G/4G Cellular Service, based on standards for CDMA, GSM, and LTE
- Smartphones and Tablets, based on smartphone OSs
- Wi-Fi

#### **1.4.8.5.4 Technical Capabilities [C.2.8.6.1.4]**

The Lumen Team technical capabilities in (1) mobile device management (MDM), (2) mobile application management (MAM), (3) mobile content management (MCM), (4) mobile security and (5) deployment support are described in the subsections that follow.

##### **1.4.8.5.4.1 MDM Capabilities [C.2.8.6.1.4.1]**

The Lumen Team, [REDACTED] brings 10 years of experience and full capabilities supporting device management and other mobile management functions including operations, policy, security, configuration, mobile network performance, application support (application performance, version

control, distribution, etc.), mobile data management (on device), and mobile network monitoring.

**Figure 1.4.8.5.4.1-1** shows how the Lumen EIS MMS MDM complies with all SOW technical capabilities requirements.

**Figure 1.4.8.5.4.1-1. Lumen Team MMS MDM Capabilities**

LUMEN COMPLIES	SOW C.2.8.6.1.4.1 REQUIREMENT	LUMEN COMPLIANT SOLUTION
✓	1. MDM Capabilities	<ul style="list-style-type: none"> <li>The Lumen Team MDM includes all capabilities specified in SOW C.2.8.6.1.4.1.1.</li> <li>Our MDM applies easy-to-use processes to assign and view policies and applications.</li> <li>The Lumen Team Software Development Kit (SDK) allows agencies to build applications on a secure platform.</li> <li>We monitor the MDM system via industry standard tools that also provide quick fix options to common issues to keep users up and running.</li> </ul>
✓	2. Device Enrollment	<ul style="list-style-type: none"> <li>The Lumen Team MDM device enrollment capabilities include all capabilities specified in SOW C.2.8.6.1.4.1.2.</li> <li>Agencies can log into the Lumen Team MWS console and manage all devices from the same screen.</li> <li>The Lumen MDM sends a user or group an activation enrollment message (e-mail or SMS). When adding users in bulk all users receive enrollment e-mail with unique enrollment pins.</li> </ul>
✓	3. Device Profiles	<ul style="list-style-type: none"> <li>The Lumen MDM device profile solution includes all capabilities specified in SOW C.2.8.6.1.4.1.3, enabling creation, copying, and editing of device profiles per user and group.</li> <li>The Lumen MDM solution supports automatic updates based on Profile Geofences.</li> <li>The Lume 3 MDM can push a profile to any individual device, automatically remove profiles from devices whose state changes from qualifying to not-qualifying, support multiple profiles being applied to a single device, delete profiles, and set profile descriptions.</li> </ul>
✓	4. Device Feature Management	<ul style="list-style-type: none"> <li>Our MDM solution provides all device feature management capabilities specified in SOW C.2.8.6.1.4.1.4 to manage multiple OS devices, password enforcement, and application installation.</li> <li>Our MDM solution manages the enabling and disabling of cameras and control radios/communications.</li> </ul>
✓	5. Data Management	<ul style="list-style-type: none"> <li>In compliance with SOW C.2.8.6.1.4.1.5, the Lumen MDM solution provides the capabilities to read, write, transmit, and receive data on mobile devices/backend systems/ repositories, providing required file management and personal information management.</li> </ul>
ü	6. NIST SP 800-126 Security Content Automation Protocol	<ul style="list-style-type: none"> <li>Our MDM solution provides NIST SP 800-126 Security Content Automation Protocol (SCAP) support as required.</li> </ul>
✓	7. Device Inventory	<ul style="list-style-type: none"> <li>The Lumen Team MDM provisions, controls and tracks devices connected to</li> </ul>

LUMEN COMPLIES	SOW C.2.8.6.1.4.1 REQUIREMENT	LUMEN COMPLIANT SOLUTION
	Management and Reports	corporate/agency applications and data, and relates this data to user information, in accordance with applicable TOs. <ul style="list-style-type: none"> <li>• Our MDM solution provides access to manage Device Inventory Reports including all data associated with device, OS and applications.</li> </ul>
✓	8. System Performance Reports	<ul style="list-style-type: none"> <li>• The Lumen MDM delivers ability to collect, monitor and send alerts for key performance data to provide insight into reliability of the solution and device usage and performance in accordance with applicable TOs.</li> </ul>
✓	9. MDM Security/ Compliance Reports	<ul style="list-style-type: none"> <li>• The Lumen MDM provides security/compliance reports that include all data relevant to monitoring and support of system's vulnerabilities and defenses, including attempts at fraud in accordance with the applicable TOs. We also run security status reports as requested.</li> </ul>
✓	10. TO Level Capabilities (Optional)	<ul style="list-style-type: none"> <li>• Our MDM solution delivers all optional capabilities that may be required at the TO level as defined in C.2.8.6.1.4.1.10.</li> </ul>

**1.4.8.5.4.2 MAM Capabilities [C.2.8.6.1.4.2]**

The Lumen Team provides the full range of MAM capabilities required for EIS. **Figure 1.4.8.5.4.2-1** shows how the Lumen MMS MAM complies with all SOW technical capabilities requirements.

**Figure 1.4.8.5.4.2-1. Lumen Team MMS MAM Capabilities**

LUMEN COMPLIES	SOW C.2.8.6.1.4.2 REQUIREMENT	LUMEN COMPLIANT SOLUTION
✓	1. Application Deployment	<ul style="list-style-type: none"> <li>• Our MAM AppCentral application manager meets all SOW C.2.8.6.1.4.2 requirements. Our solution allows users to deploy and manage applications as required. The flexibility of AppCentral includes the ability to deploy applications in controlled stages or to limited users as may be desired.</li> </ul>
✓	2. Mobile Application Store	<ul style="list-style-type: none"> <li>• Our MAM solution provides the Mobile Application Store (MAS) capabilities specified in SOW C.2.8.6.1.4.2.2. This capability is integrated into the MDM portal and allows application provisioning by group policy and mandatory application deployment.</li> </ul>
✓	3. Application Security	<ul style="list-style-type: none"> <li>• The Lumen Team MDM capabilities provide application security that fully satisfies the requirements of SOW C.2.8.6.1.4.2.3.</li> <li>• Application security solution includes mutual authentication, application installation control, blacklisting/whitelisting and ability to detect and enforce device environment conditions.</li> <li>• Our MAM solution supports requiring digital signatures for application installation.</li> </ul>
ü	4. TO Level Capabilities	<ul style="list-style-type: none"> <li>• Our MAM solution delivers the Third-party Application Mutual Authentication and MAM</li> </ul>

LUMEN COMPLIES	SOW C.2.8.6.1.4.2 REQUIREMENT	LUMEN COMPLIANT SOLUTION
	(Optional)	Software Integration Services optional capabilities that may be required at the TO level as defined in SOW C.2.8.6.1.4.2.4.

**1.4.8.5.4.3 MCM Capabilities [C.2.8.6.1.4.3]**

The Lumen Team provides the full range of MCM capabilities required for EIS, enabling secure mobile access to content anytime, anywhere, and on any device. The Lumen Team provides access to centrally stored content via Microsoft SharePoint and SMB network drives. In addition, Google Access allows access to internal web site and Office web apps.

**1.4.8.5.4.4 Mobile Security Capabilities [C.2.8.6.1.4.4]**

The Lumen Team delivers the full range of mobile security capabilities required for EIS. **Figure 1.4.8.5.4.4-1** shows how the Lumen MMS mobile security complies with all mandatory and optional technical capabilities requirements specified in SOW C.2.8.6.1.4.4.

**Figure 1.4.8.5.4.4-1. Lumen Team MMS Mobile Security Capabilities**

LUMEN COMPLIES	SOW C.2.8.6.1.4.4 REQUIREMENT	LUMEN COMPLIANT SOLUTION
✓	1. Device Enrollment and Null Policy	• Enrolls a device before applying any policy (null policy).
✓	2. Whitelists/Blacklists and OC Versions	• Creates Whitelists/Blacklists for device enrollment including OS versions and device models.
✓	3. Enrollment of Untrusted Devices	• Allows enrollment of untrusted devices and anonymous / unknown users outside the enterprise as individuals or to groups under the MDM.
✓	4. Use of Existing MDM User Attributes	• Uses an existing MDM user attribute repository for enrollment to new MDM system.
✓	5. Actions based on Compliance Rules	• Takes action based on compliance rules, in support of MDM's ability with active and passive tools to detect, report, and alert on a compromised device.
ü	6. Conditions for Device Blocking or Erasure	• Blocks the device or erases managed data on a device under conditions identified in SOW C.2.8.6.1.4.4 (a-f), using compliance rules to set a device to either lock, prevent access to enterprise data, or destroy enterprise data when these conditions are present.
✓	7. Password Policy	• Provides password policy enforcement including: minimum complexity (length,

**General Services Administration (GSA)**  
**Enterprise Infrastructure Solutions (EIS)**

Contract # GS00Q17NSD3006  
 Mod #: P00310  
 Submission #: CL01001.01a

LUMEN COMPLIES	SOW C.2.8.6.1.4.4 REQUIREMENT	LUMEN COMPLIANT SOLUTION
	Enforcement	composition, common words); password lifetime limit; password re-use limits; password inactivity timeout (grace period) for device and MDM application; password failure reports beyond threshold to MDM; maximum password attempts before lock or wipe.
✓	8.Password Marking	<ul style="list-style-type: none"> <li>Masks passwords when they appear in the Management GUI.</li> </ul>
✓	9. Determination of Administrative User Activity	<ul style="list-style-type: none"> <li>Provides reports indicating which administrative user made a configuration change in the MDM administrative environment.</li> </ul>
✓	10. Determination of User Activity	<ul style="list-style-type: none"> <li>Determines which device user made a configuration change in the MDM console (self-service logging).</li> </ul>
✓	11. Installation and Configuration of Soft Authentication Certificates	<ul style="list-style-type: none"> <li>Provides installation and configuration (update, revocation checking, revocation) of individual and group soft authentication certificates for purposes to include e-mail (S/MIME) signing and encryption; Wi-Fi Configuration; and VPN Configuration.</li> </ul>
✓	12. Send/Receive Encrypted Messages	<ul style="list-style-type: none"> <li>Sends/receives (encrypt and sign, decrypt and verify) messages that use PKI or S/MIME encryption, where e-mail functionality is delivered by the service/system.</li> </ul>
✓	13. Restrictions on Personal Data	<ul style="list-style-type: none"> <li>Restricts downloading attachments, copying of data to/from removable media, or otherwise creates separate spaces or virtual containers for agency data and applications from personal data.</li> </ul>
✓	14. (Optional) GPS Location Views	<ul style="list-style-type: none"> <li>Our MMS solution provides the optional capability to view the current GPS location of a device or logical grouping of devices on a map.</li> </ul>
✓	15. FIPS 140-2 Encryption Support	<ul style="list-style-type: none"> <li>Encrypts data in transit between the MDM and the device in accordance with FIPS 140-2.</li> <li>Data is encrypted at both the data level and packet level.</li> </ul>
✓	16. Mobile Device Data at Rest Security	<ul style="list-style-type: none"> <li>Separates the data at rest on a mobile device in different containers for agency data and personal data while protecting agency data from access by uncontrolled applications to limit interaction between agency data and personal data, with agency data encrypted if underlying platform does not encrypt all data on the device.</li> </ul>
✓	17. User Authentication	<ul style="list-style-type: none"> <li>Trusted authentication frameworks supports PIN or password authentication for the managed applications, and optionally multifactor authentication with any two of the following three authentication types: (1) Shared Secret - something the user knows such as a PIN or password; (2) Token - something a user possesses such as a cryptographic key (e.g., RSA token-soft or hard, a challenge/response token, a PIV or CAC, or a key generator device); (3) Biometric.</li> </ul>
✓	18. User Compliance	<ul style="list-style-type: none"> <li>The Lumen solution provides user compliance capabilities required by SOW C.2.8.6.1.4.4.18.</li> </ul>
✓	19. Alerting	<ul style="list-style-type: none"> <li>The Lumen MMS provides alerting that notifies agency operations staff about agency devices in compliance with SOW C.2.8.6.1.4.4.19.</li> </ul>
ü	20. Audit Reports	<ul style="list-style-type: none"> <li>The Lumen MMS solution provides audit reports with data needed to monitor, reconcile, and audit system processing and reconciliation activities. Audit reports are exportable, run as requested by the agency, and may include: administrator activity; user access times</li> </ul>

LUMEN COMPLIES	SOW C.2.8.6.1.4.4 REQUIREMENT	LUMEN COMPLIANT SOLUTION
		and enrollments; device numbers, type, OS version; console logins and functions; policy changes and versions; and policy violations.
✓	21. Personally Identifying Information (PII) Safeguarding	<ul style="list-style-type: none"> <li>Our MMS solution safeguards PII, including directory data stored in the information system, in accordance with NIST SP 800-122.</li> </ul>

**1.4.8.5.4.5 Deployment Support Capabilities [C.2.8.6.1.4.5]**

The Lumen Team MMS solution satisfies all of the requirements specified in SOW C.2.8.6.1.4.5. **Figure 1.4.8.5.4.5-1** shows how the Lumen MMS Deployment Support solution complies with all SOW technical capabilities requirements.

**Figure 1.4.8.5.4.5-1. Lumen Team MMS Deployment Support Capabilities**

LUMEN COMPLIE	SOW C.2.8.6.1.4.5 REQUIREMENT	LUMEN COMPLIANT SOLUTION
✓	1. Deployment	<ul style="list-style-type: none"> <li>Supports MMS for installing, configuring, and certifying initial deployment of MDM, MAM and Container solutions and supports integrations or customizations as specified in the TO.</li> <li>Assists the agency in achieving accreditation and authorization objectives by producing supporting documentation and/or modifications to the solution to reach compliance.</li> </ul>
✓	2. Enterprise Systems Integration	<ul style="list-style-type: none"> <li>Assists in deploying and integrating MMS into agency-wide environment including systems such as enterprise e-mail, directories, and trouble-ticketing.</li> </ul>
✓	3. Training	<ul style="list-style-type: none"> <li>Provides MDM/MAM training material content and pre-packaged online training and associated materials in accordance with TO requirements.</li> </ul>
✓	4. Help Desk	<ul style="list-style-type: none"> <li>Provides a Help Desk for MDM/MAM that supports online requests and resolutions via e-mail and telephone.</li> </ul>

**1.4.8.5.5 Features [C.2.8.6.2]**

As stated in SOW C.2.8.6.2, there are no feature requirements for MMS.

**1.4.8.5.6 Interfaces [C.2.8.6.3]**

The Lumen MMS solution supports the UNIs for all Smartphones and Tablets operating under 3G/4G Cellular Service as required in SOW C.2.8.6.3.

**1.4.8.5.7 Performance Metrics [M.2.1, C.2.8.6.4]**

Lumen meets all MMS performance metrics for Event Notification (EN), Grade of Service (Configuration Change), Telephone Incident Response Time, and Dispatch Incident Response Time, as specified in SOW C.2.8.6.4.1. We use our mobile device performance tools to collect and monitor performance data.

**1.4.8.6 Audio Conferencing Service [L.29.2.1, C.2.8.7, C.4.4]**

Clear and reliable audio conferencing enables efficient and cost-effective agency communication and collaboration. Lumen’s Audio Conferencing Service (ACS) allows agency participants to engage in multi-point audio conference calls through landline voice and cellular voice services using an audio connection

**Lumen ACS Highlights**

- Single dial-in number and access code for instant conferencing 24/7
- Intelligent, dynamic routing architecture ensures high reliability and availability
- Flexible, reliable ACS helps Agencies maximize time, resources, and global communications

from the conference participants to the ACS conference-bridge. Our ACS user experience also ensures accessibility in compliance with 508(c) requirements. **Figure 1.4.8.6-1** highlights how the features of the Lumen ACS solution satisfy the evaluation criteria.

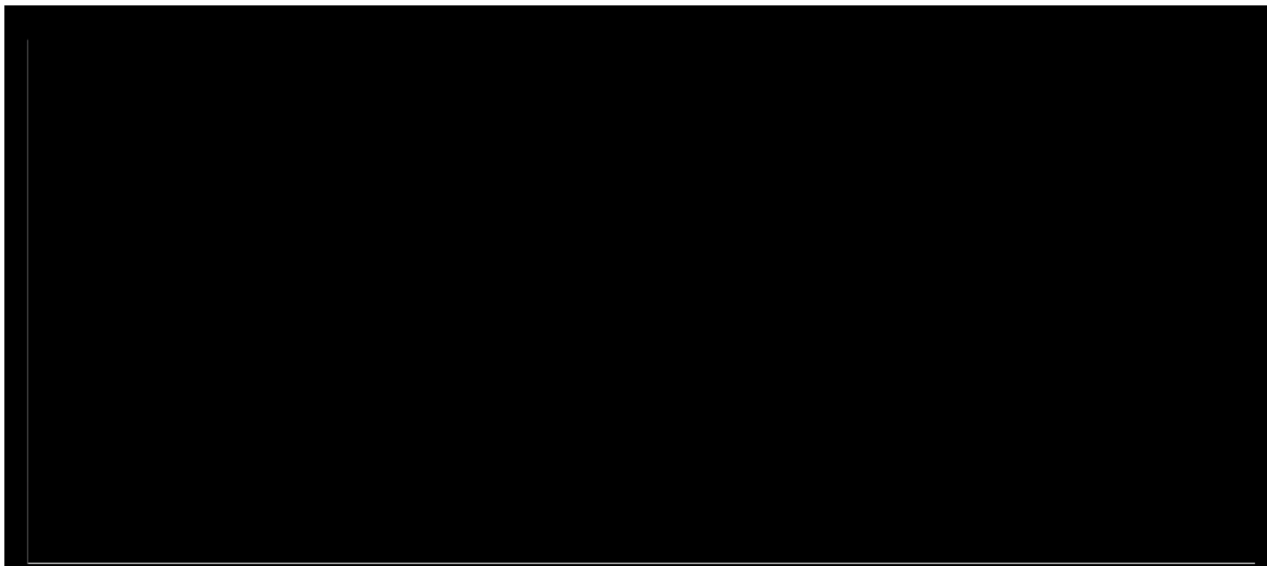
**Figure 1.4.8.6-1 ACS Feature Highlights**

EVALUATION CRITERIA	FEATURES OF LUMEN ACS
Understanding [M.2.1.1]	<ul style="list-style-type: none"> <li>• Allows agency participants to engage in multi-point audio conference calls through landline voice and cellular voice services using an audio connection from the conference participants to the ACS conference-bridge.</li> <li>• Offers both traditional ACS and strategic integrations with leading unified communications and collaboration (UC&amp;C) applications such as Microsoft® Lync® and Cisco® WebEx®.</li> </ul>
Quality of Service [M.2.1.2]	<ul style="list-style-type: none"> <li>• Compliant—features dynamic call routing that is tightly integrated with our network and supports high quality connections and voice quality</li> <li>• Scalable—core infrastructure is built for business continuity and delivering superior audio quality</li> <li>• Reliable and Resilient—intra-platform, hardware, and network redundancies, with real-time conference state awareness for automatic disaster recovery, all to ensure high-availability</li> </ul>
Service Coverage [M.2.1.3]	<ul style="list-style-type: none"> <li>• PSTN dial-in options for ubiquitous access to customers, vendors and employees in 118 countries utilizing a robust toll and toll free phone number set for on-demand access.</li> </ul>
Security [M.2.1.4]	<ul style="list-style-type: none"> <li>• Security features such as lock conference, waiting room, and conference-specific passcodes help Agencies maintain chairperson control and conference security.</li> </ul>

#### **1.4.8.6.1 Service and Functional Description [L.29.2.1, M.2.1, C.2.8.7]**

The Lumen ACS solution fulfills the mandatory and optional service requirements for ACS contained in SOW C.2.8.7. This section presents a technical description of our offering, demonstrating our capabilities in the following areas: Standards, Connectivity, Technical Capabilities, Features, Interfaces, and Performance Metrics.

The Lumen Team offers both traditional ACS and strategic integrations with leading unified communications and collaboration (UC&C) applications such as Microsoft® Lync® and Cisco® WebEx®. Flexible options include up to 300-line subscriptions, multiple language prompts and recording capabilities, single dial-in number and access code for instant conferencing, and global conference numbers allowing worldwide participation. Lumen's high-quality ACS is enabled by a dynamic call routing architecture that is tightly integrated with the Lumen network, shown in **Figure 1.4.8.6.1-1**.



**Figure 1.4.8.6.1-1. ACS Architecture.** *Designed for Reliability and Flexibility.*

#### **1.4.8.6.2 Standards [C.2.8.7.1.2]**

The Lumen Team's ACS complies with the standards identified in SOW C.2.8.7.1.2 and complies with new versions, amendments, and modifications to these



standards. Our ACS architecture comprises modular technologies, many with updatable firmware, to ensure we can remain compliant with new standards.

**1.4.8.6.3 Connectivity [C.2.8.7.1.3]**

The Lumen ACS connects to and interoperates with: Customer-specified locations; PSTN; Internet; and Lumen’s network and all other contractors’ networks for circuit-switched services and VoIP.

**1.4.8.6.4 Technical Capabilities [C.2.8.7.1.4]**

As described in **Figure 1.4.8.6.4-1**, the Lumen Team ACS complies with all required technical capabilities identified in SOW C.2.8.7.1.4.

**Figure 1.4.8.6.4-1. Lumen Compliance with ACS Technical Capabilities Requirements**

LUMEN COMPLIES	SOW C.2.8.7.1.4 REQUIREMENT	LUMEN COMPLIES COMPLIANT SOLUTION
✓	1. Multipoint Bridging Capability	<ul style="list-style-type: none"> <li>Secure, end-to-end communication network and redundant audio conferencing architecture features bridging capability that supports selective (i.e., conferee subset) two-way or one-way conversations between conferencing ports. During multi-point conferences, the addition of a party to or deletion of a party from the conference is indicated by tone or verbal announcement.</li> </ul>
✓	2. Conference Set-up Capability	<ul style="list-style-type: none"> <li>User-friendly solution supports user-controlled conference where authorized users and users with a calling-card can establish a conference call by dialing a designated number to access the service. The Lumen AWS solution supports the Meet-Me Conference and Preset Conference automated modes of user-initiated conferencing capabilities as described in the SOW.</li> <li>Supports Attendant (Operator) Assisted Conference set-up so that conferees are able to recall an operator during a conference for immediate attention.</li> </ul>
✓	3. Audio Conference Reservation System (ACRS)	<ul style="list-style-type: none"> <li>Exceeds requirements by offering on-demand audio conferencing to connect with anyone, anytime, anywhere while at the same time supporting reservation system allowing authorized Government users to schedule audio conferences using ACRS.</li> <li>ACRS offered includes all capabilities specified in the SOW, including: single point of contact; scheduling as single or recurring events and emergency scheduling if bridging capacity is available; ability to request reservations up to one year in advance, store and retrieve predefined conferences; create printed reports with reservation confirmation and cancellation notices.</li> </ul>
✓	4. Automatic Port Expansion	<ul style="list-style-type: none"> <li>Provides automatic expansion without operator assistance to support additional users in conferences in progress as long as facilities are available. Dynamic routing architecture includes intra-platform hardware and network redundancies for automatic disaster avoidance and recovery. This architecture, combined with our fully redundant network, helps protect the reliability of agency connections.</li> </ul>

LUMEN COMPLIES	SOW C.2.8.7.1.4 REQUIREMENT	LUMEN COMPLIES COMPLIANT SOLUTION
✓	5. Conferee Tones	• Supports enable or disable function for conferee tone when a participant enters or exit a conference.
✓	6. Participant Count	• Supports a count of participants.
ü	7. Roll Call	• Operators can conduct roll call of participants identifying participants on the conference.
✓	8. Attendant Assistance	• Available at any time during an audio conference.

**1.4.8.6.5 Features [C.2.8.7.2]**

The Lumen ACS is feature rich and complies with ACS feature requirements detailed in SOW C.2.8.7.2 and summarized in **Figure 1.4.8.6.5-1**.

**Figure 1.4.8.6.5-1. Lumen Team ACS Complies with Required Features**

LUMEN COMPLIES	SOW C.2.8.7.2 REQUIREMENT	LUMEN COMPLIES
✓	1. Audio Recording of Call	• Supports recording of conference call into a storage media for later replay.
✓	2. Spanish Language Translation	• Provides language translation to English from Spanish for transcription of pre-recorded audio conference.
✓	3. Language Translation (Optional)	• Provides optional language translation to English from other languages for transcription of pre-recorded audio conference. We add specific languages based on customer requirements.
✓	4. Moderator-Led Q&A	• Provides conference moderator-led questions and answers only.
✓	5. Participant List Report	• Provides a report showing all participants in a conference.
✓	6. Password Protected Session	• Screens password(s) for joining a conference to authorized participants only.
✓	7. Download and Replay a Pre-Recorded Audio Conference	• Supports, under password protection, the replay of pre-recorded audio conference at a later time and allows remote control of the recording with keypad access to functions like pause, rewind, and fast-forward.
✓	8. Transcription of Audio Call	• Provides transcription of pre-recorded audio calls.
✓	9. Temporary Blocking	• Supports temporary blocking of audio conference participants so that a sub-set of participants/users can be removed from the conference.
✓	10. Secured Audio Conference (Optional)	• Supports optional voice conferencing capability for sensitive voice conferences with end-user encryption to support discussions of a CUI nature between multiple locations with protection from unauthorized interception. When the Government furnishes premise-

LUMEN COMPLIES	SOW C.2.8.7.2 REQUIREMENT	LUMEN COMPLIES
		residing, commercially available encryption units, Lumen synchronizes the encryption key of similar encryption unit(s) of the audio conference bridge before each conference.
ü	11. Operator Dial-Out	<ul style="list-style-type: none"> <li>Using the attendant interface, the attendant can place an outbound call to a new participant and add the party to a conference in progress.</li> </ul>
✓	12. Host Dial-Out	<ul style="list-style-type: none"> <li>Using the touchtone and Web interfaces, the host can place an outbound call to a new participant.</li> </ul>
✓	13. Executive Conference	<ul style="list-style-type: none"> <li>For Executive teleconferences, Lumen's ACS provides an interface for a professional moderator to assist with control of conference attendant functions.</li> </ul>
✓	14. International Global Meet	<ul style="list-style-type: none"> <li>Lumen's ACS provides a non-North American toll number assigned to a specific country and bridge in-country local access.</li> </ul>
✓	15. Host Controls	<ul style="list-style-type: none"> <li>Lumen's ACS allows the conference host to control conference attendant functions by touchtone and the Web.</li> </ul>

**1.4.8.6.6 Interfaces [C.2.8.7.3]**

The Lumen ACS solution supports audio connection to the conference-bridge from services such as voice service (CSVS and IPVS) and cellular voice service.

**1.4.8.6.7 Performance Metrics [M.2.1, C.2.8.7.4, G.8]**

Lumen complies with all performance levels and AQL of KPIs for ACS specified in SOW C.28.9.4. Lumen uses monitoring tools that allow for comprehensive visibility of numerous network elements and the ability to accurately measure AQLs for the applicable KPIs.

**1.4.8.7 Video Teleconferencing Service [L.29.2.1, C.2.8.8, C.4.4]**

The Lumen Team offers Video Teleconferencing Service (VTS) that allow agencies to connect geographically dispersed people around the world at a moment's notice. Lumen's VTS is an application-layer service using underlying network service(s) to carry video traffic

**Lumen VTS Highlights**

- Interoperable with traditional VTS
- Simple onboarding: no downloads or plug-ins required
- Global fiber optic network with more than 10M fiber route miles

and is available for domestic and non-domestic users. Our intelligent network enables the highest quality video and audio for video teleconferencing participants. Our VTS user experience also ensures accessibility in compliance with 508(c) requirements.

**1.4.8.7.1 Service and Functional Description [L.29.2.1, M.2.1, C.2.8.8]**

The Lumen VTS solution fulfills the mandatory service requirements for VTS contained in SOW C.2.8.8. This section presents a technical description of our offering, demonstrating our capabilities in the following areas: Standards, Connectivity, Technical Capabilities, Features, Interfaces, and Performance Metrics. **Figure 1.4.8.7.1-1** summarizes our VTS solution for EIS.

**Figure 1.4.8.7.1-1. Features of Lumen’s VTS Solution**

EVALUATION CRITERIA	FEATURES OF LUMEN VTS
Understanding [M.2.1.1]	<ul style="list-style-type: none"> <li>• Allows agencies to connect geographically dispersed people around the world at a moment’s notice</li> <li>• Fully interoperable in a heterogeneous environment of networks and equipment operating in a diverse range of speeds</li> </ul>
Quality of Service [M.2.1.2]	<ul style="list-style-type: none"> <li>• Compliant—user experience also ensures accessibility in compliance with 508(c) requirements</li> <li>• Scalable—simple onboarding: no downloads or plug-ins required</li> <li>• Reliable—global fiber optic network with more than 10M fiber route miles</li> <li>• Resilient—intelligent network enables the highest quality video and audio for video teleconferencing participants</li> </ul>
Service Coverage [M.2.1.3]	<ul style="list-style-type: none"> <li>• Global network provides the reach, efficiency, flexibility, and quality to deliver VTS that helps agencies increase productivity while maximizing resources</li> <li>• Global fiber optic network with more than 10M fiber route miles ensures maximum reliability and availability</li> </ul>
Security [M.2.1.4]	<ul style="list-style-type: none"> <li>• Reservation System and Multi-Point VTS provide password protected participation</li> <li>• Traverses and successfully interoperates with agency firewalls and security layers</li> <li>• Lumen verifies with the agency that their firewall is compatible with this service</li> </ul>

In addition to traditional VTS, our service and solutions fully support all standards-based IP VTS products and services. Our Smart WAN service matches our Multipoint Control Unit (MCU) bridges around the world to customer needs, providing the best quality of service possible. Lumen’s high-quality VTS is enabled by our global network to deliver video and other applications through a single VPN port and local loop (see **Figure 1.4.8.7.2-1**).



**Figure 1.4.8.7.2-1. VTS Architecture.** *Reliable and flexible global solution.*

#### **1.4.8.7.2 Standards [C.2.8.8.1.2]**

The Lumen Team's VTS complies with the standards identified in SOW C.2.8.8.1.2. In addition, Lumen complies with new versions, amendments, and modifications to the documents and standards listed above. We remain cognizant of standards through Lumen leadership and expert staff participation in relevant standards bodies.

#### **1.4.8.7.3 Connectivity [C.2.8.8.1.3]**

Lumen's VTS connects to and interoperates with IP Networks and PSTN.

#### **1.4.8.7.4 Technical Capabilities [C.2.8.8.1.4]**

Lumen VTS is fully compliant with all required technical capabilities outlined in SOW C.2.8.8.1.4, summarized in **Figure 1.4.8.7.4-1**.

**Figure 1.4.8.7.4-1. Lumen Compliance with VTS Technical Capabilities**

LUMEN COMPLIES	C.2.8.8.1.4 REQUIREMENT	LUMEN SOLUTION COMPLIANCE
✓	1. General, Capability	<ul style="list-style-type: none"> <li>Allows participants at different locations to simulate in-person meetings and conduct interactive dialogue using point-to-point and point-to-multi-point video teleconference arrangements.</li> </ul>
✓	2. General, Communications	<ul style="list-style-type: none"> <li>Supports two-way video, one-way video with interactive voice and/or instant sharing of various types of documents/data files among participants as adjunct to video teleconferencing session.</li> </ul>
✓	3. Document Sharing	<ul style="list-style-type: none"> <li>Supports document sharing (data conferencing) which enables conference participants to interactively view, edit, and share or transfer data files and documents.</li> </ul>
✓	4. Audio Conferencing Add-on	<ul style="list-style-type: none"> <li>Supports non-video conference participants in VTS call.</li> </ul>
✓	5. Teleconferencing Bridging	<ul style="list-style-type: none"> <li>Includes Internet Protocol (IP) packet switched bridging services for multiple IP VTS devices.</li> </ul>
✓	6. Operating Modes	<ul style="list-style-type: none"> <li>The Lumen VTS solution supports Dial Out, Meet Me (Dial In), and Mixed Dial operating modes.</li> </ul>
✓	7. Operator Assistance	<ul style="list-style-type: none"> <li>Provides capability for VTS users to request operator assistance to resolve technical issues.</li> </ul>
✓	8. Synchronization	<ul style="list-style-type: none"> <li>Maintains synchronization between the audio and video signals within <math>\pm 2</math> video frames to the extent possible with the video frame rate employed in the video teleconference.</li> </ul>
✓	9. Reservation-less point-to-point VTS	<ul style="list-style-type: none"> <li>Allows users to establish point-to-point VTS on demand without reservation. Point-to-point VTS includes full-duplex video, audio, and ancillary data transmission between participating locations.</li> </ul>
✓	10. Multipoint Arrangements	<ul style="list-style-type: none"> <li>Provides VTS multi-point arrangements in conjunction with VTS reservation system that can simultaneously provide VTS to users of a different Enterprise contractor's network and users of public or other private networks. During multi-point conference, the addition of a party to, or deletion of a party from the conference is indicated by tone or verbal or visual announcement.</li> </ul>
✓	11. Reservation System	<ul style="list-style-type: none"> <li>VTS provides access to secure central reservation system to permit authorized VTS users to schedule multi-point video teleconferences.</li> <li>VTS reservation system provides: (a) the ability to schedule and cancel multi-point or point-to-point VTS conferences, (b) the ability to add participants or join a conference; (c) the ability for the VTS users to schedule a "meet-me" reservation based video teleconference, and many more features</li> </ul>
ü	12. Video Format Conversion	<ul style="list-style-type: none"> <li>When providing codec functionality, Lumen provides video format conversion capability that permits operation between: a) codecs operating in the NTSC video format and codecs operating in the Phase Alternation by Line (PAL) video format; b) codecs operating in NTSC video format and codecs operating in Système Electronique Couleur Avec Memoire (SECAM) video format.</li> </ul>

LUMEN COMPLIES	C.2.8.8.1.4 REQUIREMENT	LUMEN SOLUTION COMPLIANCE
✓	13. Firewalls and Security Layers	<ul style="list-style-type: none"> <li>Lumen VTS traverses and successfully interoperates with agency firewalls and security layers.</li> <li>Lumen verifies with the agency that the agency firewall is compatible with this service.</li> </ul>
✓	14. Reports	<ul style="list-style-type: none"> <li>Lumen's monitoring tools allow us to provide VTS reports in accordance with the TO.</li> </ul>

**1.4.8.7.5 Features [C.2.8.8.2]**

The Lumen VTS is feature rich and complies with VTS feature requirements detailed in SOW C.2.8.10.2, summarized in **Figure 1.4.7.8.5-1**.

**Figure 1.4.7.8.5-1. Lumen Team VTS Complies with Required Features**

LUMEN COMPLIES	SECTION C.2.8.10.2	LUMEN VTS SOLUTION CAPABILITIES
✓	1. Attended Service	<ul style="list-style-type: none"> <li>Provides call monitoring, roll call, and coordination for a VTS conference.</li> </ul>
✓	2. Verification	<ul style="list-style-type: none"> <li>Provides pre-testing, registration, and verification that agency-owned equipment operates correctly with the contractor's VTS.</li> </ul>
✓	3. Coding Conversion (Transcoding)	<ul style="list-style-type: none"> <li>Provides transcoding that is compliant with FTR 1080 formats.</li> <li>Provides (optional) a coding conversion capability that permits operation between CODECs, all of which use the National Television Standards Committee (NTSC) video format, but none of which support the FTR 1080 standard and none of which use the same encoding/decoding algorithm(s), supporting at a minimum the following compression algorithms as needed by the agency: SG3/SG4, CTX, and CTX+.</li> <li>Provides a coding conversion capability (optional) that permits operation between CODECs, all of which use the NTSC video format, in which one or more of the CODECs support the FTR 1080 and in which one or more of the CODECs do not support the FTR 1080, supporting at a minimum the following compression algorithms as needed by the agency: SG3/SG4, CTX, and CTX+.</li> </ul>
ü	4. Rate Adaption (Optional)	<ul style="list-style-type: none"> <li>Provides optional data rate adaptation capability to ensure that all VTS locations participating in a video teleconference can interconnect with each other at dissimilar data rates.</li> </ul>
✓	5. Security – CUI (Optional)	<ul style="list-style-type: none"> <li>Provides optional transparent and secure VTS communications paths to support CUI video communications per the security capabilities described in the FTR1080 recommendation.</li> </ul>
✓	6. Security – Classified	<ul style="list-style-type: none"> <li>Provides optional transparent and secure VTS communications paths and supports video</li> </ul>

LUMEN COMPLIES	SECTION C.2.8.10.2	LUMEN VTS SOLUTION CAPABILITIES
	(Optional)	information that is categorized as classified (National Security agency type 1 encryption) video communications, per the security capabilities described in the FTR1080 recommendation.

**1.4.8.7.6 Interfaces [C.2.8.8.3]**

The Lumen VTS solution supports the UNIs at the SDP defined in SOW C.2.8.8.3.1. If the agency provides the CODEC and the inverse multiplexer and Lumen provides only reservation, coding conversion, and/or format conversion, then the UNIs supported by Lumen include: a) ITU-TSS V.35, b) EIA RS-449, c) EIA RS-530, d) RJ-x (e.g., RJ-45), and e) Data Interface(s) supporting any combination of i. EIA RS-232, ii. EIA RS-449, iii. ITU-TSS V.35, iv. EIA RS-530.

**1.4.8.7.7 Performance Metrics [M.2.1, C.2.8.8.4, G.8]**

Lumen meets all of the VTS performance metrics shown in the Video Teleconferencing Service Performance Metrics table in SOW C.2.8.8.4.1. The Lumen GovNOC monitors all Lumen Enterprise services provided through our IP backbone. Lumen uses monitoring tools that allow for comprehensive visibility of numerous network elements, and the ability to accurately measure AQLs for the applicable KPIs.

**1.4.8.8 DHS Intrusion Prevention Security**

**Service [L.29.2.1, C.2.8.9; C.4.4]**

Lumen works with DHS to develop and support an EINSTEIN based Intrusion Prevention Security Service in support of the EIS contract. Lumen provides a comprehensive service aggregation methodology that integrates EINSTEIN enclaves into authorized agency traffic

routes. We are proposing ICD 705 certified facilities co-located in Lumen facilities where we are deploying our MTIPS solution (Lumen is currently in the process of adding MTIPS to our Networx Enterprise contract). Lumen has previously deployed fiber assets

**Lumen Team DIPPS Solution**

- Lumen has a history of working with DHS NPPD. We capitalize on this history, incorporating lessons learned, and continuing to develop our working relationship.
- Our EIS solution includes ICD 705 certified facilities collocated with Lumen facilities where we are deploying MTIPS.



to or near the data centers utilized by US-CERT in preparation for EINSTEIN based service requirements. When fully implemented, these assets provide dedicated, secure and reliable communications between Lumen and US-CERT in support of the DHS IPSS (DIPSS) program.

The content and figures contained within this section are at a conceptual level. Specific and detailed Lumen DIPSS design information has not been included in order to avoid inadvertent disclosure of information that may be subsequently identified as classified. Lumen welcomes the opportunity to discuss our design in detail with DHS prior to consideration of a TO award.

**Figure 1.4.8.8-1** highlights the features of the Lumen DIPSS solution, which are aligned with the evaluation criteria.

**Figure 1.4.8.8-1. Compliant Lumen DIPSS**

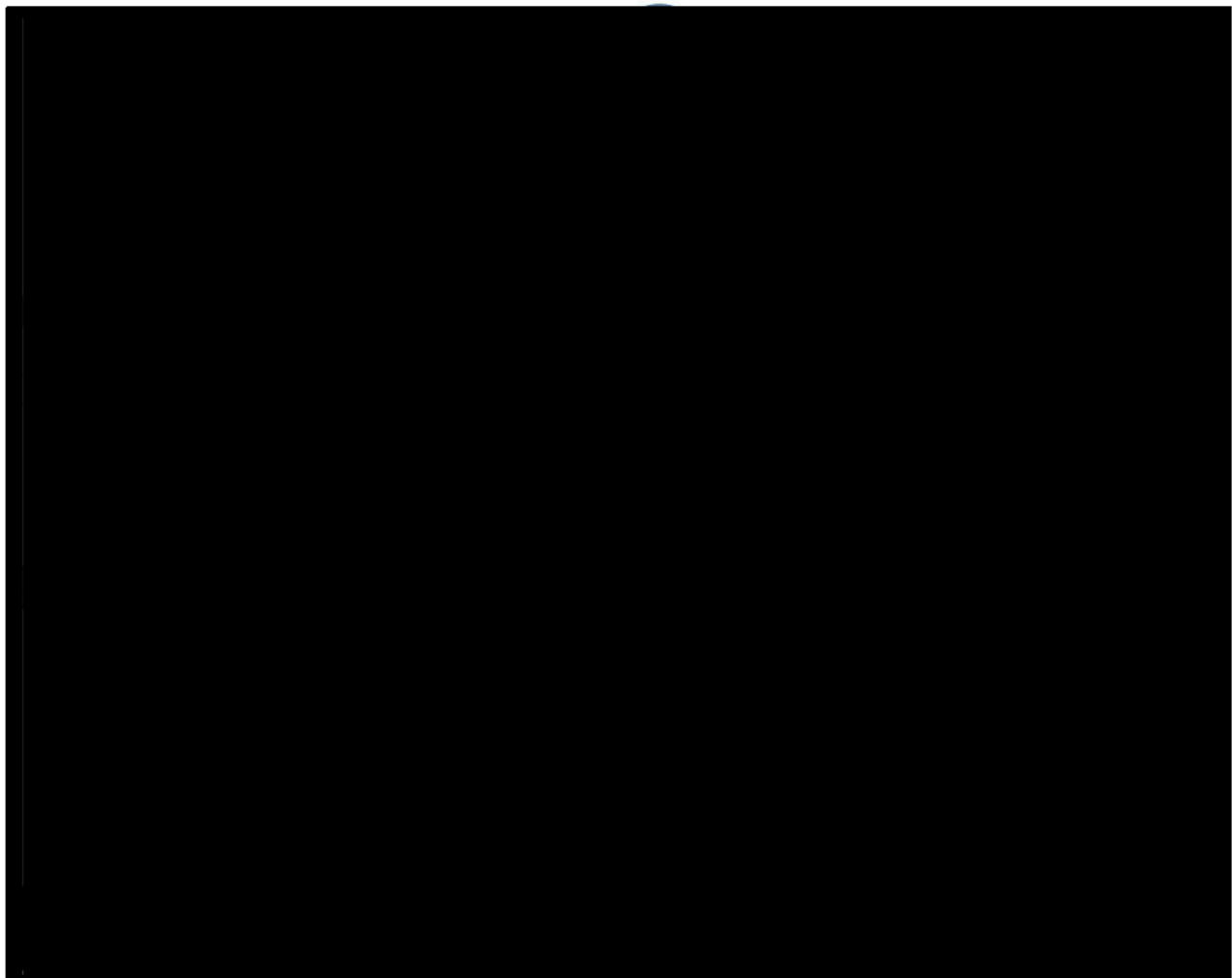
EVALUATION CRITERIA	FEATURES OF LUMEN DIPSS
Understanding [M.2.1.1]	<ul style="list-style-type: none"> <li>Lumen has a history of working with DHS NPPD. We capitalize on this history, incorporate lessons learned and continue to develop our working relationship.</li> <li>We bring additional subject matter experts and consultants with past experience in supporting DHS IPSS and other DHS programs as necessary to provide an expedient, compliant and robust service implementation.</li> </ul>
Quality of Services [M.2.1.2]	<ul style="list-style-type: none"> <li>Our conceptual DHS IPSS implementation is strategically located to minimize additional latencies of the aggregation service.</li> <li>We employ performance measurement equipment at the ingress and egress to the DHS IPSS environment to ensure traffic is not intentionally corrupted and is compliant with service level agreements. Related performance reports are available to DHS and the participating agencies.</li> </ul>
Service Coverage [M.2.1.3]	<ul style="list-style-type: none"> <li>The aggregation service supporting the DHS IPSS deployment provides the same service coverage as the Lumen EIS VPNS, ETS and optionally Optical Wavelength, SONET &amp; Private Line services. The aggregation service provides an Ethernet handoff to the DHS IPSS environment.</li> </ul>
Security [M.2.1.4]	<ul style="list-style-type: none"> <li>Lumen provides 2 ICD 705 facilities to support the DHS IPSS program to support GFP and GFI to the TS/SCI level. Security Operations, Smart Hands and Program Management support are provided by cleared personnel.</li> <li>The DHS IPSS program provides connections to the US-CERT data centers as specified in TOs.</li> </ul>

**1.4.8.8.1 Service and Functional Description [L.29.2.1, M.2.1, C.2.8.9]**

Lumen delivers a functionally compliant service supporting the following high level DHS IPSS components:

- 
- **Indicator Management.** Lumen develops indicator management systems and processes that meet DHS specifications.
  - **Detection.** Lumen provides threat detection services based upon DHS provided indicators and DHS approved signature or other mitigation actions.
  - Lumen provides cyber threat response and protection functions and measures based upon specifications provided by DHS.
  - **Alerting and Reporting.** Lumen develops alerting and reporting methods and procedures per DHS and subscribing agency requirements.
  - **Protection/Mitigation.** Per DHS instruction, Lumen will take action to protect the Participating Agency (PA) and mitigate the cyber threat.

A high level conceptual diagram of the Lumen DIPSS architecture is provided in **Figure 1.4.8.8.1-2**. An explanation of the Item reference numbers shown in Figure 1.4.8.8.1-2 is provided in Figure 1.4.8.8.1-3.



**Figure 1.4.8.8.1-2. Lumen Conceptual DIPSS Architecture.** *Our DIPSS architecture provides functionality and facilities that are compliant with EIS requirements.*

**Figure 1.4.8.8.1-3. Lumen Conceptual DIPSS Architecture Elements Description**

FIGURE ITEM NUMBER	DESCRIPTION
1.	The Lumen aggregation service utilizes the Lumen Enterprise Network(s) to support EIS customers. Traffic requiring EINSTEIN3 - Accelerated (E3A) inspection is routed to the Aggregation Service Boundary Environment.
2.	The Aggregation Service Boundary Environment provides a demarcation point for the PA traffic entering the E3A enclave. It contains the following appliances/devices:

**General Services Administration (GSA)**  
**Enterprise Infrastructure Solutions (EIS)**

Contract # GS00Q17NSD3006  
 Mod #: P00310  
 Submission #: CL01001.01a

	<ul style="list-style-type: none"> <li>• <b>2a:</b> Aggregation Service Boundary Router - This device provides a termination point for PA VPNS, ETHS, OWS, PLS, and SONETS. These services are converted to PA specific Ethernet VLANs in preparation for ingress to the E3A enclave.</li> <li>• <b>2b.:</b> IPSec VPN Appliance - PA IPSec tunnels are terminated and delivered to the E3A enclave as unencrypted IP traffic. The IPSec VPN appliance may be integrated into the Aggregation Service Boundary Router.</li> <li>• <b>2c:</b> SSL Appliance - SSL traffic terminates within the Aggregation Service Boundary and is delivered to the E3A enclave as unencrypted IP traffic.</li> <li>• <b>2d:</b> Unified Threat Management (UTM) Appliance - This device provides multiple functions in support of the aggregation service:             <ol style="list-style-type: none"> <li>I. Firewall protection - Access Control Lists are implemented to allow only authorized PA traffic into the E3A enclave.</li> <li>II. Netflow records are generated to provide performance and metadata information.</li> <li>III. Intrusion Detection System/Intrusion Prevention System, which provides additional inspection for unauthorized traffic.</li> <li>IV. Ethernet handoff(s) to the E3A enclave.</li> </ol> </li> </ul>
<p>3.</p>	<p>E3A enclave - Housed in an ICD 703 SCIF supporting classified and unclassified reach-back capability to DHS and US CERT. The classified and unclassified environments within the SCIF are appropriately separated. The E3A enclave contains Lumen provided Commercial-Off-the-Shelf (COTS) products purposed to support the EINSTEIN initiative. Elements and capabilities include:</p> <ul style="list-style-type: none"> <li>• Classified environment - A repository for classified GFI and GFP communications equipment.</li> <li>• Service Verification Environment (SVE) - A validation environment for indicator to signature correspondence, threat identification, and mitigation functions.</li> <li>• Email Threat Protection - A purpose specific appliance that provides email scanning for email destined for the .gov domain for malicious attachments, Uniform Resource Locaters (URL), and other forms of malware. Depending upon requirements from DHS, the infected email may be quarantined or redirected from the target email address to another location for further inspection by DHS. Only emails determined to be malicious, e.g. those matching a given signature, may be quarantined and further reviewed.</li> <li>• Domain Name Server (DNS) Threat Protection (DNS Sinkholing) - The DNS Sinkhole server prevents malware infected on .gov networks from communicating with known or suspected malicious Internet domains.</li> <li>• Future Threat Protection capabilities - Lumen will develop and support additional DHS E3A cyber protection initiatives, e.g. Web Content Filtering, as required.</li> <li>• Optical Tap - Lumen will install an optical tap that provides the ability to direct IP traffic to a specific cyber protection component, including GFP.</li> <li>• Layer 2/3 Gigabit Ethernet Switch - Provides an inspection point to check for unauthorized traffic. A positive event will generate an alert to the E3A Security Operations environment and DHS.</li> <li>• Unified Threat Management (UTM) Appliance - Similar in function to item 2.d, only this appliance faces the public Internet.</li> <li>• Security Operations Environment - A collection of security management tools to support E3A operations. User access for all devices and systems within the E3A enclave is controlled via 2 factor authentication.</li> <li>• Connection to US CERT - Classified and unclassified connections to US CERT data center as required by RFP Section C.2.8.9.1.3. It is assumed that classified connections are required for timely information flow of classified GFI.</li> </ul>
<p>4.</p>	<p>DHS IPSS Internet Boundary - This environment provides a demarcation point for the Internet traffic destined for</p>

	<p>the PA networks.</p> <ul style="list-style-type: none"> <li>• <b>4a:</b> Internet Access Router/Firewall - Provides the boundary firewall and routing functions for Internet traffic destined to the PA (via the E3A enclave).</li> <li>• <b>4b:</b> IPSec VPN Appliance - PA IPSec tunnels transiting the Internet to the PA are terminated and delivered to the E3A enclave as unencrypted IP traffic.</li> <li>• <b>4c:</b> SSL Appliance - SSL traffic terminates within the Internet Boundary and delivered to the E3A enclave as unencrypted IP traffic.</li> </ul>
5.	Lumen Internet Backbone - Public Internet, AS3356.
6.	DHS IPSS Bypass - Redundant connections between the Aggregation Service Boundary and the Lumen public Internet (DIA) routers. These connections are disabled under normal operations. In the event of a failure within the E3A enclave, DHS will instruct Lumen E3A Security Operations personnel to enable the bypass interfaces and invoke the necessary routing to bypass the E3A enclave. For security control purposes, this is a manual process.

**1.4.8.8.2 Standards [C.2.8.9.1.2]**

Lumen’s DIPSS offering is compliant with the standards and guidance listed in SOW C.2.8.2.1.2.

**1.4.8.8.3 Connectivity [C.2.8.9.1.3]**

As described in further detail in Section 1.4.13 of this Volume, Lumen has designed an External Traffic Routing solution, also referred to as an Aggregation Service, that meets the requirements of the SOW C.1.1.8 (item 3), L.29.2.3 and M.2.1 (item 4) c). Our approach provides clear termination boundaries to present participating agency traffic to the EINSTEIN enclaves, considerations for Lumen MTIPS and agency specific TICAP services, bypass controls, encrypted VPN tunnel termination and re-establishment where applicable, failsafe mechanisms, performance measurement and reporting and unauthorized traffic detection and notification. IPv4 and IPv6 traffic is supported. As mentioned in the introduction above, and per requirements stated in RFP Section C.2.8.9.1.3, Lumen has previously extended our fiber network to one of the existing US-CERT data centers and have fiber assets in proximity of the second US-CERT data center. We are prepared to build to the second data center upon receipt of authorization to enter the property. Providing Lumen fiber to the second data center provides an additional layer of service reliability, since we would own and control the fiber assets to the data center, as opposed to contracting to a third party provider.

**1.4.8.8.4 Technical Capabilities [C.2.8.9.1.4]**

Lumen provides the mandatory DIPSS capabilities specified in SOW C.2.8.9.1.4.

Figure 1.4.8.8.4-1 shows how the Lumen EIS DIPSS fully complies with all SOW technical capabilities requirements.

**Figure 1.4.8.8.4-1. DIPSS Technical Capabilities**

LUMEN COMPLIES	SOW C.2.8.9.1.4 REQUIREMENT	LUMEN COMPLIANT SOLUTION
✓	1.	<ul style="list-style-type: none"> <li>Lumen works with DHS to develop a process or integrate existing DHS methods and procedures for cyber threat indicator and protection information exchange. Examples of information exchange could include STIX/TAXII methods and procedures or e-mail exchange provided over secure FIPS 140-2 communications. Courier based information delivery could also be utilized as a baseline of information exchange.</li> </ul>
✓	2.	<ul style="list-style-type: none"> <li>Lumen provides a Service Verification Environment (SVE) to develop indicator to signature translation and rule sets. The SVE has the complete functionality of the production DHS IPSS environment, plus additional traffic simulation equipment necessary to validate the functionality of indicator based threat detection and response methods defined by DHS. Production deployment and activation of new or modified indicators do not occur until SVE functionality is compliant with the DHS threat detection/protection objectives.</li> </ul>
✓	3.	<ul style="list-style-type: none"> <li>The Lumen DHS IPSS environment has the capability to gather additional cyber threat information via full packet capture, storage and playback. A sandbox environment is provided to allow DHS to further investigate, manipulate and respond to a given cyber threat. The DHS IPSS Security Operations team, upon direction from DHS initiates actions to stop cyber attacks or otherwise respond to cyber incidents.</li> </ul>
✓	4.	<ul style="list-style-type: none"> <li>The Lumen DHS IPSS facility is housed in an ICD-705 compliant facility. Lumen DHS IPSS support personnel obtain DHS suitability and cleared to the TS/SCI level. We develop methods and procedures to receive, accept, utilize and secure GFI up to the TS/SCI level. Information is compartmentalized, isolated and utilized in accordance with DHS-approved security guidelines.</li> </ul>
✓	5.	<ul style="list-style-type: none"> <li>Lumen develops automated means e.g., STIX, TAXII, CyBOX, to receive and utilize DHS provided GFI within the IPSS environment in a near real-time manner.</li> </ul>
✓	6.	<ul style="list-style-type: none"> <li>Lumen utilizes information sharing mechanisms with DHS to identify and potentially implement commercially available cyber threat information, signatures and mitigations that are available for deployment within the IPSS environment. Commercially based signatures and mitigations are not implemented in the Lumen DHS IPSS environment unless authorized by DHS.</li> </ul>
ü	7.	<ul style="list-style-type: none"> <li>Indicators and actions will only be applicable to Participating Agencies (PA). Lumen Aggregation Service limits ingress traffic to the Lumen DHS IPSS environment to PA only. Aggregation Service is implemented upon direction from DHS and the PA. Corresponding EIS IPSS orders are necessary to implement PA IPSS support. PA traffic is further identified by IP address blocks utilized by the agency. Aggregation service border routers block/drop all IP address traffic by</li> </ul>

LUMEN COMPLIES	SOW C.2.8.9.1.4 REQUIREMENT	LUMEN COMPLIANT SOLUTION
		default and allow PA IP addresses by specific Access Control List (ACL) rules.
✓	8.	<ul style="list-style-type: none"> <li>Traffic for PA are identified by specific 802.1Q VLAN tag. Lumen shares VLAN tagging information with DHS and the PA. This traffic identification and control method allows the ability to apply indicators and mitigations to a specific agency and more broadly to groups or all PA.</li> </ul>
✓	9.	<ul style="list-style-type: none"> <li>GFI remains contained within the Lumen DHS IPSS environment and not distributed, shared or used outside of the IPSS environment unless specifically authorized by DHS. Only authorized Lumen personnel have access to the IPSS SCIF. Any action related to binary GFI stored within the IPSS environment triggers an event, logged within the IPSS management systems. Event management of this nature is further defined by DHS.</li> </ul>
✓	10.	<ul style="list-style-type: none"> <li>Lumen delivers Internet based traffic from any PA that subscribes to Lumen IPS under EIS to the Lumen DHS IPSS environment for inspection and protection. This includes PA that subscribe to Lumen MTIPS or PA that operate as a TICAP. This traffic contained within a PA specific 802.1Q VLAN.</li> </ul>
✓	11.	<ul style="list-style-type: none"> <li>The Lumen DHS IPSS environment includes IDS/IPS, NetFlow collection and analysis, deep packet inspection, full packet capture, event logging and SEIM capabilities necessary to support the detection of malicious network traffic and provide additional contextual information associated with alerts to aid in post-incident analysis.</li> </ul>
✓	12.	<ul style="list-style-type: none"> <li>The Lumen DHS IPSS IDS/IPS platform is the latest next generation Unified Threat Management device. It supports signature-based and heuristic-based detection. The flexible architecture of the IDS/IPS provides the capability to upgrade and integrate future threat detection technologies without requiring equipment replacement. Any future technology based service or feature enhancements is validated in the SVE prior to production implementation.</li> </ul>
✓	13.	<ul style="list-style-type: none"> <li>When Lumen provides encryption as a component within a service, Lumen decrypts the traffic prior to the handoff point to the EINSTEIN enclave. Flows that are encrypted by external sources can be inspected for malicious activity using heuristic analysis of NetFlow data or statistical traffic analysis via a packet capture of a given traffic flow. Only the packet header information is captured and analyzed in this case. Another means of malicious activity detection may be possible using DHS authorized deep packet inspection of traffic flows to detect attacks in encrypted VPNs. Lumen implements additional encrypted traffic inspection methods upon further guidance from DHS.</li> </ul>
✓	14.	<ul style="list-style-type: none"> <li>The Lumen DHS IPSS environment provides enhanced detect/protect capabilities. When instructed by DHS, Lumen initiates procedures to:                             <ol style="list-style-type: none"> <li>Collect additional detailed information after malicious activity has been detected. Methods include deep packet inspection, full packet capture, and SEIM based event analysis.</li> <li>Prevent or block detected threats from reaching the threat target. Traffic can be blocked, dropped, quarantined or redirected.</li> <li>The Lumen DHS IPSS environment has the ability to remove or replace content of a session flow in order to defeat or alter the attack's operational capabilities.</li> <li>The Lumen solution provides 'sandbox' capabilities to enable DHS to simulate the threat's target and observe threat procedures, develop and apply mitigation scenarios and observe</li> </ol> </li> </ul>

LUMEN COMPLIES	SOW C.2.8.9.1.4 REQUIREMENT	LUMEN COMPLIANT SOLUTION
		<p>threat mutations in response to mitigation scenarios.</p> <p>e. The Service Verification Environment is utilized to baseline indicator performance and develop improvements in detection accuracy. Detection results including false positive/false negative events is also be monitored and evaluated in the production. Improvements and enhancements in indicator/mitigation performance is developed and re-baselined prior to deployment in the production environment. The Service Verification Environment is utilized to develop improvements in detection accuracy.</p>
ü	15.	<ul style="list-style-type: none"> <li>• A safe server environment is provided in the Lumen DHS IPSS environment. The safe server is utilized to re-direct and store threat traffic for additional evaluation and analysis.</li> </ul>
✓	16.	<ul style="list-style-type: none"> <li>• Capture and data storage actions may be specifically directed to a given network traffic flow. Capture and storage may be triggered by a specific indicator or condition within an indicator.</li> </ul>
✓	17.	<ul style="list-style-type: none"> <li>• Under normal circumstances the Lumen DHS IPSS environment collects meta-data in the form of NetFlow records or packet capture of header information only. No payload information is inspected, captured or stored unless explicitly directed by DHS. Attempts to invoke deep packet inspection or full packet capture generates an alert which automatically notifies Lumen security operations, DHS and US-CERT.</li> </ul>
✓	18.	<ul style="list-style-type: none"> <li>• A dedicated Lumen security operations team manages the DHS IPSS environment. This team follows directions provided by US-CERT in the application of DHS-directed prevention services.</li> </ul>
✓	19.	<ul style="list-style-type: none"> <li>• The Lumen traffic aggregation solution described in section 1.4.13 of this volume is used to deliver participating agency traffic to the Lumen DHS IPSS environment. The design and functionality of this is reviewed and approved by DHS prior to Authority to Operate (ATO) certification is granted. The traffic aggregation solution is designed to deliver only designated, Federal System network traffic. System failsafe, service violation and alert mechanisms have been integrated into the traffic aggregation design.</li> </ul>
✓	20.	<ul style="list-style-type: none"> <li>• The Lumen DHS IPSS architecture is based upon an in-line traffic flow for inspection and response purposes. The Lumen DHS IPSS design provides a 'man in the middle' architecture that allows for inspection and mitigation as the traffic flows from the PA WAN to the Internet and from the Internet to the PA WAN. The PA WAN shall be designed so that no Internet traffic can leak from other sources/locations within the WAN environment.               <ul style="list-style-type: none"> <li>a. All traffic sourced from the Internet and destined to PA users or hosts shall be monitored/inspected and protected via threat mitigation actions by systems and functions within the Lumen DHS IPSS environment.</li> <li>b. All PA traffic destined to be delivered through the Internet is monitored/inspected and protected via threat mitigation actions by systems and functions within the Lumen DHS IPSS environment.</li> </ul> </li> </ul>
ü	21.	<ul style="list-style-type: none"> <li>• Lumen adheres to the initial DHS IPSS functional requirements and schedules as defined in the DHS IPSS TO. Lumen supports the evolution of the DHS IPSS capabilities and develop and apply future functions based upon a technology roadmap at cyber-relevant speed in order to maintain counter threat capabilities.</li> </ul>



LUMEN COMPLIES	SOW C.2.8.9.1.4 REQUIREMENT	LUMEN COMPLIANT SOLUTION
✓	22.	<ul style="list-style-type: none"> <li>Quarantined malware diverted to the Lumen DHS IPSS safe server, packet capture or other storage environments is available to DHS US-CERT malware lab or other DHS entity and the affected Participating agency. Delivery methods are to be defined by DHS and the PA.</li> </ul>
✓	23.	<ul style="list-style-type: none"> <li>Lumen demonstrates the functionality of threat indicator detection, signature and/or all countermeasures within the SVE to ensure desired functionality.</li> </ul>
✓	24.	<ul style="list-style-type: none"> <li>Event and syslog generated alerts may be delivered to DHS and PA in raw form as they occur within the Lumen DHS IPSS environment. Additionally SEIM based post analysis information is available to DHS and PA. The depth of alerts, any filtering and delivery options are developed jointly.</li> </ul>
✓	25.	<ul style="list-style-type: none"> <li>NetFlow analysis, packet capture analysis and results of other traffic pattern discovery methods are made available to DHS and PA. Raw information will also be available. Any information deemed to be classified is managed accordingly.</li> </ul>
✓	26.	<ul style="list-style-type: none"> <li>The Lumen DHS IPSS program provides a robust reporting capability availability to DHS, US-CERT and Participating agencies. A catalog of standard reports is available and customer and event specific reports may be requested. Reports are provided via a secure portal that incorporates two factor authentication for access control.</li> </ul>
✓	27.	<ul style="list-style-type: none"> <li>Participating agency traffic information is compartmentalized in relation to threat activity, alerts and reporting. Access to PA is limited authorized PA staff and/or contractors. Access to the Lumen DIPSS portal is strictly controlled and audited. Retention of PA threat information is dictated by DHS and the PA security office.</li> </ul>
✓	28.	<ul style="list-style-type: none"> <li>Development of threat identification, mitigation and reporting procedures are initially developed in the Lumen DHS IPSS Service Verification Environment. The SVE are located in Northern Virginia and are accessible to the Government to participate and/or observe activities within the SVE or the production environment.</li> </ul>
✓	29.	<ul style="list-style-type: none"> <li>The Lumen DHS IPSS environment incorporates an unauthorized access detection capability at the ingress point of the aggregation service traffic to the Lumen DHS IPSS enclave. Traffic flows are inspected to confirm address validity against an authorized 'white list' of PA addresses. Any violation of the authorized address listing generates a syslog event and automated alarm notification to DHS. DHS is provided access to violation information including any threat management processes applied to the unauthorized traffic.</li> </ul>
ü	30.	<ul style="list-style-type: none"> <li>Lumen will provide an ICD 705 Sensitive Compartmented Information Facility (SCIF) and personnel with TOP SECRET/SCI clearances. Facility size, number of personnel and other details will be based on DHS Task Orders.</li> </ul>

**1.4.8.8.5 Features [C.2.8.9.2]**

Lumen DIPSS provides the three mandatory features required in SOW C.2.8.9.2. **Figure 1.4.8.1.5-1** shows how the Lumen EIS DIPSS fully complies with all SOW

features requirements.

**Figure 1.4.8.1.5-1. DIPSS Service Features.**

LUMEN COMPLIES	SOW C.2.8.9.2 REQUIREMENT	LUMEN COMPLIANT SOLUTION
✓	1. Classified Email Threat Detection and Countermeasures	<ul style="list-style-type: none"> <li>Lumen provides capabilities that apply sensitive and classified (up to TS/SCI) indicators and countermeasures offered by DOD/DHS to e-mail messages and with real-time secure exchange with DHS for global awareness.</li> </ul>
✓	2. Classified DNS Threat Detection and Countermeasures	<ul style="list-style-type: none"> <li>Lumen provides capabilities that apply sensitive and classified (up to TS/SCI) indicators and countermeasures offered by DOD/DHS to DNS queries and responses and with real-time secure exchange with DHS for global awareness.</li> </ul>
✓	3. Additional Countermeasures	<ul style="list-style-type: none"> <li>Detailed architectural concepts, Concepts of Operations, Staffing Plan, and Service Management plan is available to DHS subsequent to Technical Exchange Meetings (TEM) and additional program information exchange between Lumen and DHS.</li> </ul>

**1.4.8.8.6 Interfaces [C.2.8.9.3]**

The Lumen DIPSS supports the UNI at the SDP to connect to the DHS IPSS through Ethernet access as defined in SOW C.2.1.2. Lumen delivers traffic from the PA WAN and IPS Aggregation Service elements via an Ethernet handoff.

**1.4.8.8.7 Performance Metrics [M.2.1, C.2.8.9.4, G.8]**

Lumen adheres to performance metrics of the DHS IPSS as defined in the TO.

**1.4.8.9 Software Defined Wide Area Network Service (SDWANS) [C.2.8.10]**

As agencies modernize and optimize their network infrastructure, many are considering a Software Defined WAN (SD-WAN) service. The benefits include cost-effectiveness, improved network management, increased routing flexibility, security, and network redundancy/availability/resiliency.

The Software Defined Wide Area Network



016-57476515NAVYJAG

Service (SDWANs) will support a wide range of connectivity requirements that enable government users to access cloud services, the Internet, government-wide intranets, and extranets, via EIS transport services and commercial broadband Internet. SDWANs will use the TCP/IP protocol suite to interconnect GFP/SRE with other government networks and the public Internet Service Provider (ISP) networks.

Lumen is well versed in working closely with agencies in modernization efforts and in the deployment and implementation of renovated networks, based on a modern SD-WAN environment. Lumen is committed to GSA and Federal agencies, in their journey towards SD-WAN and we look forward to a strong collaboration in making significant steps forward into next generation networking. Lumen's SD-WAN solution supports connectivity that will enable government users with the ability to efficiently access cloud services, the Internet, government-wide intranets and extranets; leveraging EIS transport services and commercial broadband Internet, as underlay networks. SD-WAN supports the use of the TCP/IP suite and supports interconnects with other government networks and the public ISP networks.

Lumen has a broad range of commercial customers for which we have successfully deployed SD-WAN solutions since 2016, across a range of next generation platforms. Lumen is well versed in the complexities and nuances in designing and deploying SD-WAN overlay networks. We bring a strong operational track record in terms of modernization approaches, designs, migration plans and Managed Network Services (MNS) expertise for SD-WAN rollouts.

In 2019, the respected market research firm Frost & Sullivan awarded Lumen (as CenturyLink) its Innovation Excellence Award, in recognition of our success in combining our broad network footprint and expertise in managed network services to deliver exceptional SD-WAN services to our North



---

American customers, noting that “This recognition is strictly reserved for companies that are market leaders and are reinventing themselves through R&D investments and innovation. Achieving Innovation Excellence is never an easy task, but it is one made even more difficult considering today’s intense competitive environment, customer volatility, economic uncertainty, and rapid technology evolution. Within this context, CenturyLink’s receipt of this Award signifies an even greater accomplishment.”

Virtualized Services and SD-WAN will be the building blocks of the Federal agency modernized WAN. These technologies help abstract the network layer from the services layer and incorporate high degrees of efficiency and innovation in the form of network optimization, automation, orchestration, application-based routing, and resiliency across virtually every level of the agency and end-user experience. SD-WAN can leverage low-cost, high-capacity access as a means to replace expensive, inflexible and static traditional technologies. An SD-WAN managed service creates a solution that will position agencies to leverage the next generation of enterprise networking by separating the data plane from the control plane and virtualizing many of the network functions that used to require dedicated, specialized hardware, thereby reducing hardware sprawl at remote office and branch locations. This overlay will help agencies realize cost containment benefits, support centralized orchestration, improve visibility and management and create an agile architecture across all agency locations. In addition, increased reliability, enhanced flexibility along with optimized performance will be achieved. The ability to fine tune agency’s network to meet the needs of specific workloads and applications is one of the key benefits inherent with SD-WAN. Policy-based routing and oversight will ensure optimal performance for Federal market’s unique workloads and applications.

#### **1.4.8.9.1 Service Description [C.2.8.10.1]**

The SD-WAN Service will create a transport agnostic overlay network to monitor, manage, and optimize the use of the underlying physical transport networks (underlays) for routing of session-based IP-packets by de-coupling the transport service from its

applications and software control function in a separate control plane. The underlying transport can be any IP based service, including IPS, VPNS, ETS and BIS.

The Lumen SD-WAN creates a transport-agnostic overlay network to monitor, manage, and optimize the use of the underlying physical transport networks (underlays) for routing of session-based IP packets by decoupling the transport service from its applications and software control function in a separate control plane. This separation of the control plane from the data plane, allows for efficient control, policy oversight and optimized performance of data traffic flow between and across agency locations. The underlying transport capabilities include IPS, VPNS, ETS, and BIS. The transport-agnostic flexibility of the SD-WAN overlay along with the ability to support multiple underlay transport networks, creates a highly flexible and responsive approach to next generation networking.

**Table 1.4.8.9-1 Benefits of SD-WAN Use Cases**

USE CASE	KEY BENEFIT TO FEDERAL AGENCIES
Secure Automated WAN	Secure connectivity between offices, and public/private cloud over a transport independent network
Application Performance Optimization	Improves the application experience for users at remote offices
Secure Direct Internet Access	Locally offloads Internet traffic at the remote office, subject to security posture
Multicloud Connectivity	Connects remote offices with cloud (SaaS and IaaS) applications over an optimal path and through either remote offices or regional colocation/exchange points where security services can be applied.
Network Segmentation	VPN Support across agency user types/functional departments
uCPE & Service Chaining	Reduction of hardware sprawl, platform and device consolidation, optimize operational support, centralized management of network functions

**1.4.8.9.1.1 Functional Description [C.2.8.10.1.1]**

The Lumen SDWANS solution fulfills the functional requirements defined in Section C.2.8.10.1.1.

- ***A secure IP-based virtual overlay network over physical IP networks (underlays) using Internet Protocol Security (IPSec) tunnels, compliant with the FIPS 140-2 standard for approved cryptographic modules.***

The SD-WAN architecture from Lumen is a secure IP-based virtual overlay network. SD-WAN routers that are part of a Lumen SD-WAN solution use IPSec with encryption keys to encrypt and decrypt data. IPSec is the primary

---

method of site-to-site tunnel encryption. Lumen's solution ensures that a secure IP-based overlay network is deployed over physical IP network underlays; and is compliant with FIPS 140-2. IPSec tunnels ensure that the data that is exchanged between site locations is encrypted and secure.

- ***Transport-independence of underlay network types, including IPS, VPNS, ETS and BIS.***

Lumen's SD-WAN solution is transport agnostic and transport independent and can support single or multiple underlay network connections that include: IPS, VPNS, ETS and BIS. One of the key benefits of SD-WAN is the ability to leverage various types of underlay transport types, to ensure that traffic has the most appropriate path available to optimize performance and associated metrics. By enabling application-based routing, Lumen can help Federal agencies realize optimal performance and optimal path selection.

- ***Quality-of-Service (QoS) assurance of each FIPS 140-2 compliant encrypted connection is to be measured in real-time on key parameters (latency, packet loss, and jitter) to ensure that the performance level specified is being achieved.***

Real-time measurements of path performance across the IPSec tunnels for metrics such as QoS and other real-time parameters such as latency, packet loss and jitter are supported. These key parameters are made available to Federal agency customers as well as the Lumen NOC, to ensure that performance is tailored and closely aligns with the applications and workloads being supported. Performance metric visibility helps give operations and engineering staff the intelligence and data that is needed to determine if there is a requirement to alter traffic policies by site type.

- ***Policy-based packet forwarding of different types of packet flows for QoS, security, and/or business policy for the best-matching transport underlay (physical network).***

---

Application and policy-based packet forwarding and routing supports various types of traffic flows, from high priority, latency sensitive applications that require stringent metrics, to lower priority workloads with more flexible metrics. The Lumen solution is based on an SD-WAN overlay, running over multiple underlay transport networks, thereby ensuring that specific traffic is routed over the best performing path; in order to optimize performance based on specific application requirements. QoS, security and business policies are closely evaluated and serve as the basis for policy and template creation within the orchestration and control layers of Lumen's SD-WAN solution.

- ***High availability through multiple underlays for transport diversity for increased overall availability and resiliency, including dynamic traffic routing to avoid network congestion and outage.***

Lumen's SD-WAN solution helps to ensure high availability through the use of multiple underlay connections, which enable transport diversity and optimal path selection. Real time, latency sensitive traffic can route over VPNS links for example, while lower priority traffic can utilize IPS and / or commercial broadband Internet connections. Lumen can develop policies to aid path conditioning by helping to identify the best route that an agency's traffic should take in order to optimize performance. SD-WAN ensures a high level of availability and dynamic traffic routing to avoid network congestion and outages. Improved resiliency and reliability across sites will be realized through the deployment multiple underlays. It is common to see in SD-WAN deployments remote offices or branches with a Single or Dual commercial broadband circuit(s), a VPNS and broadband circuit or perhaps dual VPNS circuits. The flexibility to mix and match transport agnostic underlay networks is a significant benefit of SD-WAN.

- ***Zero touch provisioning of CPE (e.g. customer edge router) when powered up and connected by automatically retrieving its configuration and security policies without manual intervention.***

---

Zero touch provisioning (ZTP) of the SD-WAN CPE router is a key feature benefit of the proposed Lumen solution. Automated device provisioning occurs when the SD-WAN CPE router is powered up at the initial install. The SD-WAN CPE router connects to the SD-WAN server following an authentication process and receives its configuration detail from the centralized orchestration and control components. Following this authentication and initial provisioning and configuration process, the SD-WAN CPE router can begin to learn routes, templates, and policies associated with that particular site and join the overlay network. ZTP will enable Federal agencies to efficiently and expeditiously deploy SD-WAN across the network topology. A key provisioning component of our SD-WAN solution is the central controller. The SD-WAN controller supports automatic retrieval of configuration and security policies. Near-real-time changes to application-based routing, security directives, template alterations, and policy-based changes that can easily be communicated to the SD-WAN CPE router automatically.

- ***Centralized management, including the ability to establish policies and monitor performance.***

All management of the SD-WAN overlay is carried out by centrally managed orchestration engines and controllers. For each Federal agency, Lumen creates custom templates containing critical site data, including policies and performance specifications, which are housed in centralized orchestrators. In addition, the ability to monitor performance levels and adjust traffic policies as needed, across the overlay network will be supported by the centralized management and control plane. Experienced Lumen network engineers will assist Federal agencies in the development and deployment of custom templates, policies and monitoring efforts to ensure ease of adoption and use of SD-WAN technology. A centralized dashboard provides a detailed view of application performance, access and well as transport metrics.



**1.4.8.9.2 Standards [C.2.8.10.1.2]**

Lumen’s SDWANS offering shall comply with the standards listed in Section C.2.8.10.1.2 as solutions become commercially available. **Figure 1.4.8.9.2-1** shows how the Lumen EIS SDWANS complies with standards requirements.

**Table 1.4.8.9.2-1 SDWANS Standards Compliance**

REQUIREMENT	LUMEN COMPLIANT SOLUTION
1. Metro Ethernet Forum on SD-WAN	Lumen will support this standard.
2. MEF CE 2.0 for Carrier Ethernet	Lumen will support this standard.
3. MEF 3.0 – Framework for dynamic Carrier Ethernet, SD-WAN, Optical Transport, IP, Security-as-a-Service, and other virtualized services	Lumen complies and has achieved MEF 3.0 Ethernet Certification. This certification has only been given to very few select carriers currently offering Ethernet services, and is a key differentiator for Lumen. We continue to drive investment around Ethernet, Optical Services, Virtual Services, and “as-a-Service” type offerings.
4. Internet Engineering Task Force (IETF) Request for Comments (RFC) for Internet Protocol Version 6 (IPv6)	Lumen will support this standard.
5. Institute of Electrical Engineers (IEEE):	a. 802.1Q; b. 802.1P; and c. (Optional) 802.3AD - Planned
6. Network Function Virtualization (NFV): European Telecommunications Standards Institute (ETSI) Industry Specific Group (ISG) NFV Releases	Lumen will support this based on agency specific requirements.
7. All new versions, amendments, and modifications to the above documents and standards	Lumen will support all new versions, amendments, and modifications.

**1.4.8.9.3 Connectivity [C.2.8.10.1.3]**

Lumen’s SD-WAN solution is transport agnostic and transport independent and can support single or multiple underlay network connections that include: IPS, VPNS, ETS and BIS. One of the key benefits of SD-WAN is the ability to leverage various types of underlay transport types, to ensure that traffic has the most appropriate path available to optimize performance and associated metrics. By enabling application-based routing, Lumen can help Federal agencies realize optimal performance and optimal path selection.

Lumen’s SD-WAN offering can provide support and connectivity to Government’s

Cloud Service Providers SDP. SD-WAN custom policies per site, can be developed to direct traffic and workload to CSPs as is required by each agency.

**1.4.8.9.4 Technical Capabilities [C.2.8.10.1.4]**

Lumen provides the mandatory SDWANS capabilities specified in EIS Section C.2.8.10.1.4. **Figure 1.4.8.9.4-1** shows how the Lumen EIS SDWANS fully complies with all technical capabilities requirements.

**Figure 1.4.8.9.4-1. SDWANS Technical Capabilities**

LUMEN COMPLIES	SOW C.2.8.10.1.4 REQUIREMENT	LUMEN COMPLIANT SOLUTION
✓	1. The contractor shall provide optional commercial broadband Internet service required for the SDWANS at Agency sites, when specified in the Agency TO, at available data rates.	<ul style="list-style-type: none"> <li>Lumen’s SD-WAN offering can leverage low-cost, high-capacity alternative access methods as well as various underlay transport methods to “right-size” the network to ensure optimization and controlled WAN spend is achieved. One of the key strategies in moving towards SD-WAN is leveraging hybrid access methods based on broadband. As Federal agencies look towards a more modern architecture and consider innovative approaches towards networking, multiple access methodologies can be incorporated to improve the reliability at the remote offices while achieving WAN cost improvements. Commercial broadband access that may include Internet access, Ethernet, 4G/5G Wireless, Digital Subscriber Line (DSL), Cable, and Fiber to the Premises (FTTP) can be combined with Lumen’s Managed SD-WAN solution to play a key role in delivering scalable bandwidth at agency locations, while controlling WAN costs. While hybrid access methods are not a required element for SD-WAN, we have seen agencies benefit from moving in that direction. Lumen has the experience and ability to leverage proven access technology to supply agencies with the best possible, carrier-agnostic and high-bandwidth solutions available. Lumen recommends that agencies consider including commercial broadband Internet as part of a migration plan to SD-WAN.</li> <li>Lumen has established carrier relations with Tier 1 and Tier 2 broadband and wireless providers, and we have partnered with over 30 broadband vendors, including Local Exchange Carriers (LECs), Regional Bell Operating Companies (RBOCs), Multiple Service Operators (MSOs), and aggregators to provide the Federal market with a comprehensive footprint of coverage. Lumen provides support for the procurement, installation and management of facilities owned by third-party broadband providers.</li> </ul>
ü	2. Tunnel virtual connection over the underlay networks	<ul style="list-style-type: none"> <li>The SD-WAN architecture proposed by Lumen ensures a Secure IP-based virtual overlay network. The proposed SD-WAN routers use IPSec with encryption keys to encrypt and decrypt data. IPSec is the primary method of site-to-site tunnel encryption IPSec tunnels are built site-to-site using one or more underlay networks. IPSec tunnels ensure that the data that is exchanged between site locations is encrypted and secure. The IPSec virtual tunnels maintain end-to-end encryption of traffic between agency site locations and traffic moving through access circuits will be encrypted. Lumen’s SD-WAN solution is transport and carrier agnostic in terms of underlay connections which may include: BIS and IPS, ETS, VPNS and Layer 1-type transport such as PLS.</li> </ul>

LUMEN COMPLIES	SOW C.2.8.10.1.4 REQUIREMENT	LUMEN COMPLIANT SOLUTION
✓	3. Policy-Based Packet Forwarding	<ul style="list-style-type: none"> <li>Lumen's SD-WAN solution supports agencies desire to define policies in order to make appropriate and customized application-aware routing decisions. Application based routing takes into account, not only the overlay network, but the underlay networks as well, to ensure both real time traffic and less stringent traffic is being treated appropriately and best matches specific workload performance metrics. The Lumen solution is based on an SD-WAN overlay that can run over multiple transport agnostic underlays, thereby ensuring that specific traffic is routed over the best performing path, in order to optimize performance based on application requirements. QoS, security and business policies are closely inspected and serve as the basis for policy and template creation within the orchestration and control layers of solution. Application-aware policies can be created in a customized fashion and tailored to specific applications or application groupings. Lumen's SD-WAN QoS process starts at the edge of the network with the examination of packets. Each WAN edge router can be configured to provision QoS. The localized data policy can control the flow of data traffic into and out of the SD-WAN appliance interface and enable QoS feature support for traffic such as VoIP. In addition, policies can be activated in the outbound or inbound direction. The centralized data policy provides the ability to manage traffic along the path. This combination of localized and centralized management along with policy creation and oversight is the basis for QoS delivery across an IPSec SD-WAN overlay. A centralized controller can determine path selection, based on the specific criteria and metrics within the stated traffic policy. Application and performance-based routing is an inherent characteristic of Lumen's SD-WAN solution offering and remains one of the cornerstones of optimized traffic performance. Lumen will work closely with Federal agencies in QoS governance to protect real-time application optimization.</li> <li>Lumen will work with each agency, to create policies as part of SD-WAN orchestration and control that ensure bandwidth intensive applications take for example an Internet path, while latency sensitive applications such as VoIP sessions and other type traffic that require stringent jitter or packet loss metrics are able to utilize MPLS connections.</li> <li>Lumen's SD-WAN solution will ensure that QoS is monitored closely and that latency sensitive applications take priority over those less critical across the overlay and underlay networks.</li> <li>Lumen's SD-WAN solution supports traffic segmentation and traffic isolation. This feature provides logical separation of user/department/organizational data from "other" agency network traffic at a given physical location. This segmentation feature can be supported within the encrypted IPSec tunnels. The IPSec tunnels ensure secure data exchange for site-to-site communication. Guest access, Wi-Fi, access, component specific Intranet and network management VLANs can be supported as part of the proposed solution. Traffic entering the router can be assigned a VPN, which isolates user traffic from other user traffic that belongs to a different functional group. Each VPN has its own routing forwarding table thereby supporting routing table isolation. VPN-to-VPN transmission of traffic cannot occur unless explicitly configured to do so.</li> <li>Lumen will define CIR and associate bandwidth for each application flow and will ensure that connections are sized appropriately to meet application requirements.</li> </ul>

LUMEN COMPLIES	SOW C.2.8.10.1.4 REQUIREMENT	LUMEN COMPLIANT SOLUTION
ü	4. Zero-Touch Provisioning of Site Equipment	<ul style="list-style-type: none"> <li>• Lumen's SD-WAN solution supports a uCPE appliance or virtualized edge router that is capable of automatically retrieving and installing specific configuration and policies via remote provisioning. Manual intervention is not required for deployment, turn-up and provisioning of new devices across an agency SD-WAN environment. SREs that are configured to run as uCPE devices will support NFV capabilities for various network functions to include routing and network security functions if required by a specific agency. If for any reason the proposed SD-WAN platform is not capable of supporting an agency desired Virtual Network Function (VNF) as in the context of service chaining, Lumen would provide a specialized SRE appliance as needed.</li> <li>• Lumen's SD-WAN solution typically can support specific security functions within a uCPE device via service chaining of MSS functions or catalog-based CLINs. Each SD-WAN platform provides support for a variety of third-party security vendor services and can be examined closely and selected based on each agency's security requirement.</li> </ul>
ü	5. Management and Control	<ul style="list-style-type: none"> <li>• A key component of the Lumen SD-WAN solution is the centralized controller. Through the SD-WAN Console, and with appropriate credentials, an agency can view or manage customizable site policies and deep traffic visibility and statistics collections in addition to the following features: <ul style="list-style-type: none"> <li>• Single Pane of Glass</li> <li>• Role-based operational access</li> <li>• Multitenant support for sub-agencies/sub-organizations/network segmentation</li> <li>• Bandwidth allocation per application flow</li> <li>• Zero Touch Provisioning (ZTP)</li> <li>• Centralized provisioning, troubleshooting, and monitoring</li> <li>• Distribution and implementation of data and control plane policies</li> <li>• Provisioning and configuration of vendor neutral virtual network functions.</li> </ul> </li> <li>• The Lumen SD-WAN service comes with a centralized dashboard that facilitates automatic configuration, management, and monitoring of the SD-WAN overlay network. The Lumen StratGov TAC personnel and agency administrators (if desired) will have the ability to log into the dashboard to centrally manage all aspects of the network life cycle from initial deployment, ongoing monitoring, and troubleshooting to change control and software upgrades. Lumen can support a fully managed SD-WAN overlay or a co-Managed SD-WAN overlay solution. Our approach is to offer as much flexibility to the Federal market. Centralized controllers establish connections to across an agency network. They also exchange routing, security, and policy information. The centralized policy engine provides policy constructs to manipulate routing information, access control, segmentation, extranets, and service chaining.</li> </ul>

**1.4.8.9.5 Features [C.2.8.10.2]**

Lumen shall provide the features defined in EIS Section C.2.8.10.2 based on agency specific requirements.

**1.4.8.9.6 Interfaces [C.2.8.10.3]**

The Lumen SDWANS supports the UNIs at the SDP to connect uCPE (e.g. virtualized edge router) to multiple underlays (e.g. BIS, IPS, VPNS and ETS services) with access arrangements to their respective POPs as defined in SOW C.2.8.10.3.

**1.4.8.9.7 Performance Metrics [C.2.8.10.4, G.8]**

Lumen will adhere to the performance metrics of the SDWANS overlay as defined in the Agency TO. SDWANS underlays performance metrics (including Time to Restore) will be managed via the underlay transport service.

**1.4.9 Access Arrangements [L.29.2.1, C.2.9]**

For EIS, Lumen provides dedicated end-to-end Access Arrangements (AA) at all required transmission rates, supporting high-quality voice, data, video, and multi-media requirements. Lumen AA are delivered using transmission services (e.g., Private Line, Ethernet) described in detail in their respective sections of our technical proposal. Our dedicated AAs ensure Agencies have reliable bandwidth to Lumen’s global network. LumenAAs include design, ordering, installation coordination, pre-service testing, trouble sectionalization, and restoration coordination. **Figure 1.4.9-1** highlights how the features of our AA solution satisfy the evaluation criteria.

**Lumen Access Arrangements Highlights**

- High flexibility with multiple connection options tailored to customer sites
- Proven service with 630+ dedicated access arrangements successfully supporting agencies on Network and WITS3
- Interoperable with many communication platforms, topologies, and bandwidth

**Figure 1.4.9-1. Features of Lumen’s Access Arrangements Solution**

EVALUATION CRITERIA	FEATURES OF LUMEN AA
Understanding [M.2.1.1]	<ul style="list-style-type: none"> <li>• AAs vary depending on the agency site location and requirements</li> <li>• Lumen offers flexible and dedicated access arrangements that allow Government agencies to interconnect to our backbone network</li> </ul>
Quality of Service [M.2.1.2]	<ul style="list-style-type: none"> <li>• Compliant—our TO Leads are responsible for AA requirements compliance, including compliance with site survey and special construction approval procedures</li> <li>• Scalable—our AAs include wireline, broadband, and satellite to accommodate all EIS customers’ infrastructures</li> <li>• Reliable—solution architecture maximizes flexibility and reliability</li> <li>• Resilient—solution architecture is resilient to a variety of stresses and extreme events through its</li> </ul>

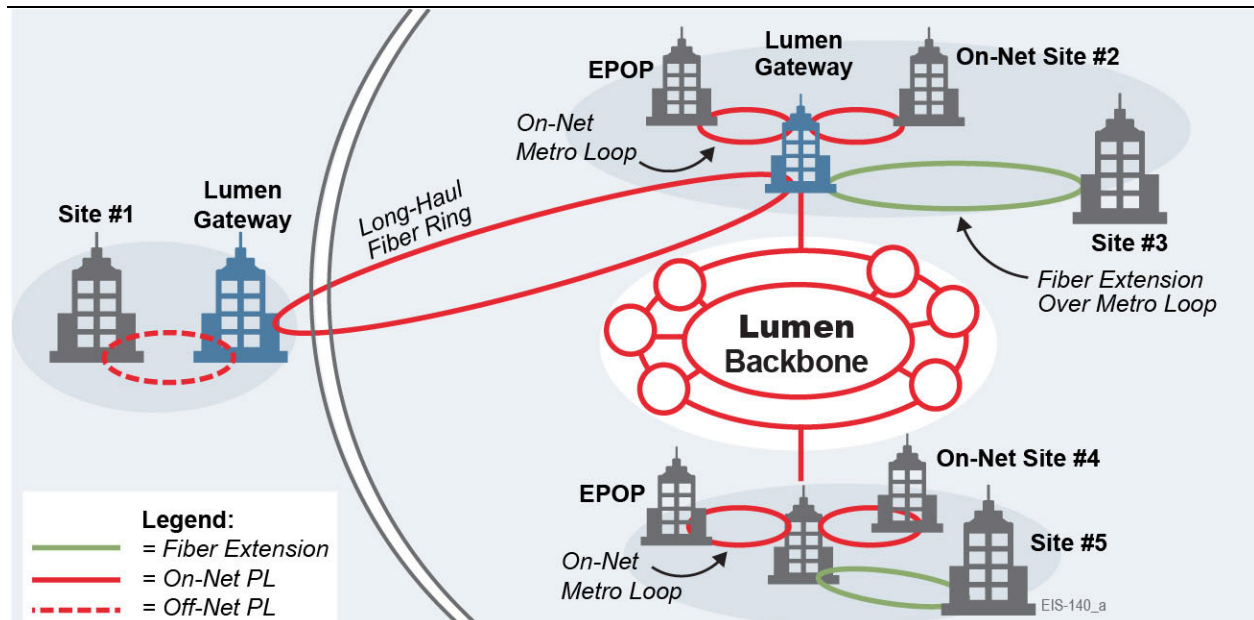
EVALUATION CRITERIA	FEATURES OF LUMEN AA
	use of complementary technologies and access diversity techniques
Service Coverage [M.2.1.3]	<ul style="list-style-type: none"> <li>• Able to provide AAs to our backbone for all geographical locations required by EIS</li> </ul>
Security [M.2.1.4]	<ul style="list-style-type: none"> <li>• Implements appropriate security measures that adhere to current industry standards, such as access authentication and data encryption, to ensure security from the customer's site to our backbone</li> </ul>

**1.4.9.1 Service and Functional Description [L.29.2.1, M.2.1, C.2.9, J.1]**

The Lumen Access Arrangements solution fulfills the requirements for AA contained in SOW C.2.9. This section presents a technical description of our offering, demonstrating our capabilities in the following areas: Standards, Connectivity, Technical Capabilities, Access Diversity and Avoidance, Interfaces, and Performance Metrics. Lumen offers flexible and dedicated access arrangements that allow Government agencies to interconnect to our backbone network and include wireline, broadband, and satellite. The Lumen AA approach is shown in **Figure 1.4.9.1-1**.

**Physically Disparate, Diverse, and Redundant Paths.** As depicted, our AA solution provides physically disparate, diverse, and redundant paths between the SDP and contractor POPs as required. This ensures the reliability and resilience of our services that satisfy diverse agency needs to access the Lumen network.

**Special Construction.** To provide access between agency sites and the Lumen network, we investigate constructing new fiber routes, purchasing third-party dark fiber, and leasing off-net Private Line Service (PLS) from another service provider as required. Third-party fiber requires industry-standard KPIs/AQLs from the supplier to support industry best practices. Leased PLS terminates services on Lumen-owned ADMs. If we identify the need for special construction, Lumen performs the site surveys and documents and reports them in compliance with the SOW and J.10.



**Figure 1.4.9.1-1. Lumen Access Arrangements.** *Our AAs maximize flexibility with numerous connection options tailored to customer site.*

#### 1.4.9.2 Standards [C.2.9.1.2]

Lumen's AA offering is fully compliant with the standards identified in SOW C.2.9.1.2.

#### 1.4.9.3 Connectivity [C.2.9.1.3]

Lumen's AA services provide connection and interoperability with agency-specified locations and equipment (including Service Delivery Points (SDP) such as PBX, Centrex, Multiplexer, Router, Video codec, and Group 4 FAX) and with Lumen network POPs.

#### 1.4.9.4 Technical Capabilities [C.2.9.1.4]

Lumen is able to provide all 15 mandatory AAs, as well as the six optional AAs, as specified in SOW C.2.9.1.4. Our AA capabilities include integrated access of different services via IP packets for converged IP services, and over the same access circuits for both Circuit Switched Voice and Data. Lumen AAs are transparent to any protocol used by the GFP and transparent to all bit sequences transmitted by the GFP. AAs provided by Lumen are described in **Figure 1.4.9.4-1**.

**Figure 1.4.9.4-1. Access Arrangement Technical Capabilities**

LUMEN COMPLIES	SOW C.2.9.1.4 REQUIREMENT	LUMEN SOLUTION COMPLIANCE
✓	1. T1	<ul style="list-style-type: none"> <li>Supports line rate of 1.544 Mbps for channelized or unchannelized T1 AA</li> </ul>
✓	2. ISDN PRI	<ul style="list-style-type: none"> <li>Supports 23 separate DS0 clear channels of 56/64 kbps over an interface of ISDN PRI (23B+D) with a line rate of 1.544 Mbps</li> </ul>
✓	3. ISDN BRI	<ul style="list-style-type: none"> <li>Supports 2 separate DS0 clear channels of 56/64 kbps over an interface of ISDN BRI (2B+D) with a line rate of 144 Kbps</li> </ul>
✓	4. T3	<ul style="list-style-type: none"> <li>Supports line rate of 44.736 Mbps to provide channelized or unchannelized T3 access arrangement. Provides PRI Ports so customers can PRI channels on channelized T3 (DS3) access line</li> </ul>
✓	5. E1	<ul style="list-style-type: none"> <li>Supports a line rate of 2.048 Mbps for channelized or unchannelized E1</li> </ul>
✓	6. E3	<ul style="list-style-type: none"> <li>Supports a line rate of 34.368 Mbps for channelized or unchannelized E3 For higher-capacity circuits, our network control features can be configured with a size approaching up to 2% of the aggregate link bandwidth</li> </ul>
✓	7. – 11. SONETS OC-3, -12, -48, -192, and (Optional) -768	<p>Lumen SONETS use standard industry Add and Drop Multiplexer (ADM) and Wavelength Division Multiplexing (WDM) and dense (WDM) equipment with appropriate interfaces from OC-3 to OC-768. SONETS are available throughout Lumen’s global network, including coverage of 57 metro areas in the U.S. Using ring architecture, our network is route-diverse and all routes protection capacity is non-pre-emptible. Lumen supports the following:</p> <ul style="list-style-type: none"> <li><u>SONET OC-3</u>. Supports line rate of 155.520 Mbps for channelized or concatenated access</li> <li><u>SONET OC-12</u>. Supports line rate of 622.080 Mbps for channelized or concatenated access</li> <li><u>SONET OC-48</u>. Supports a line rate of 2.488 Gbps for channelized or concatenated service</li> <li><u>SONET OC-192</u>. Supports a line rate of 10 Gbps for channelized or concatenated service</li> <li><u>SONET 768 (Optional)</u>. Supports a line rate of 40 Gbps for channelized or concatenated service</li> </ul>
ü	12. Analog Line (Optional)	<ul style="list-style-type: none"> <li>Supports 2 wire 4 kHz analog lines and trunks without access integration for voice service</li> </ul>
✓	13. DS0	<ul style="list-style-type: none"> <li>Supports information payload data rates of 56 kbps and 64 kbps</li> </ul>
✓	14. Subrate DS0 (Optional)	<ul style="list-style-type: none"> <li>Supports optional Subrate DS0 at information payload data rates of 4.8, 9.6, and 19.2 kbps</li> </ul>
✓	15. Optical Wavelength	<ul style="list-style-type: none"> <li>Supports bi-directional wavelengths (WDM) connections to an optical network for the following speeds: 1 Gbps; 2.5 Gbps; 10 Gbps; and 40 Gbps (Optional)</li> </ul>
✓	16. Dark Fiber (Optional)	<ul style="list-style-type: none"> <li>The Lumen AA solution support all of the dark fiber requirements of C.2.9.1.4.16. For on-net fiber, we provide Agencies with dark fiber handoffs in our collocation facilities or in another metro-area on-net building. Off-net agency buildings use a combination of new construction and third-party dark fiber to find optimum solution</li> <li>The Lumen AA solution supports all dark fiber requirements of SOW C.2.9.1.4.</li> </ul>
✓	17. Digital Subscriber Line	<ul style="list-style-type: none"> <li>The Lumen AA support all of the mandatory and optional Digital Subscriber Line (DSL) requirements of SOW C.2.9.1.4.17.</li> </ul>



LUMEN COMPLIES	SOW C.2.9.1.4 REQUIREMENT	LUMEN SOLUTION COMPLIANCE
✓	18. Ethernet	<ul style="list-style-type: none"> <li>Lumen provides Ethernet AA for both dedicated and shared access over a Metro Ethernet service from SDP to SDP, as required by SOW C.2.9.1.4.18</li> <li>For Ethernet AA connections, we maintain appropriate committed bandwidth or CIR (Committed Information Rate), as supported by MEF ENNI standard for each of the access connections</li> </ul>
✓	19. High-Speed Cable (Optional)	<ul style="list-style-type: none"> <li>Supports high-speed cable AAs including data rates of 256 Kbps to 150 Mbps as specified in SOW C.2.9.1.4.19.</li> </ul>
✓	20. Fiber-to-the-Premises (Optional)	<ul style="list-style-type: none"> <li>Supports Fiber-to-the-Premises (FTTP) AA as specified in SOW C.2.9.1.4.20.</li> </ul>
✓	21. Wireless	<ul style="list-style-type: none"> <li>Supports wireless AA as specified in SOW C.2.9.1.4.21.</li> </ul>

**AA Transport Categories.** Lumen offers SONETS as a wireline AA. Our SONETS use industry-standard ADMs and Wavelength Division Multiplexing (WDM) equipment with the appropriate interfaces and transmission rates (e.g., OC-3, OC-12, etc.). For long-distance connection, Lumen provides a dedicated long-haul ADM network employing four-fiber Bi-directional Line-Switched Ring (BLSR) self-healing rings in the continental U.S. Our metro ADM connects to the Lumen facility using 1+1 protection, Unidirectional Path Switched Ring (UPSR) protection, or two-fiber BLSR protection, as appropriate for the use-demand of the applicable Government site.

Lumen offers Dark Fiber Service (DFS) as a wireline AA. We provide an on-net agency dark fiber handoffs in our collocation facilities or in another metro-area, on-net building. If an agency building is off-net, then we choose appropriate combinations of new construction and third-party dark fiber.

Lumen offers Optical Wavelength Service (OWS) over Wave Division Multiplexing (WDM) as a wireline AA. The Lumen OWS over WDM is a bi-directional, point-to-point offering that provides Agencies the capability to interconnect their offices with fully dedicated wavelength-based channels at speeds of 2.5 Gbps and 10 Gbps. As part of our Broadband Access Service, Lumen offers satellite access arrangements (SatAA) that meet SOW requirements and standards for transmission performance and GFP interfaces, including ANSI, Telcordia, ITU, USB, and IEEE.

---

For an alternative form of network access, Lumen provides Agencies with Ethernet MAN access in most major cities in the continental U.S., linking many agency locations to Lumen's core services using a Layer 2-switched Ethernet port-based service. This AA facilitates access to EIS core services and reduces access costs.

#### **1.4.9.5 Access Diversity and Avoidance [C.2.9.2]**

Lumen provides the mandatory AA features specified in SOW C.2.9.2. We understand the need for Access Route or Path Diversity and Avoidance as part of our AA solution, to minimize risks that could affect service quality or result in service loss. Lumen's optical network design and architecture is completely homogenous, ensuring consistent delivery of high-quality services, supporting fully diverse paths everywhere with no spurs or collapsed paths. Many cities within our metro network also feature building diversity. We will provide at least two physically separated routes for access diversity in accordance with the options specified by the SOW. This includes the capability for automatic switching of transmission on a case by case basis.

**Control Measures.** In coordination with the OCO, we maintain graphical representations of our current and proposed access circuit routes as part of our internal control measures for both Access Route or Path Diversity and Avoidance. Lumen incorporates the customer agency's requirements for a specific geographic location or route to avoid between an SDP and its associated connecting network point.

#### **1.4.9.6 Interfaces [C.2.9.3]**

Lumen provides all 26 mandatory UNIs at AA SDPs, as specified in SOW C.2.9.3.

#### **1.4.9.7 Performance Metrics [M.2.1, C.2.9.1, C.2.9.1.4, G.3.5.3]**

Lumen provides AAs in compliance with the performance requirements of the individual transport categories specified in SOW C.2.9.1.4. Dedicated AAs support overall quality of services provided through the EIS contract by providing reliable bandwidth to Lumen's global network across the range of speeds and reliability options needed.

**1.4.10 Service Related Equipment [L.29.2.1, C.2.10, M.2.1, Section D]**

The Lumen Team furnishes all Service Related Equipment (SRE), hardware and materials not otherwise provided by the Government as needed to complete TOs in accordance with requirements. The Lumen Team provides in a timely fashion all networking and security equipment such as, but not limited to: Switches, Routers, PBXs, Telephones, Servers, Security Appliances, Firewalls, Conferencing-Related Equipment, and other equipment necessary to provide the requested service.

**Service Related Equipment Highlights**

- Delivers high quality, timely warranty services that agencies expect
- Ensures that SRE problems are resolved quickly and accurately
- Provides high responsiveness to SRE requirements through communication with EIS customers throughout TO

The Lumen Team provides per TO requirements all designated hardware and materials that are incidental to the installation, operation and maintenance of EIS procured services. All equipment provided to the Government under the EIS contract is new and not used or refurbished. **Figure 1.4.10-1** highlights how the features of our SRE solution satisfy the evaluation criteria.

**Figure 1.4.10-1. Features of Lumen’s SRE Solution**

EVALUATION CRITERIA	FEATURES OF LUMEN SRE
Understanding [M.2.1.1]	<ul style="list-style-type: none"> <li>• The Lumen Team furnishes all Service Related Equipment (SRE), hardware and materials not otherwise provided by the Government as needed to complete TOs in accordance with requirements</li> <li>• Lumen furnishes the required Service Related Equipment and honor the required one-year warranty</li> </ul>
Quality of Service [M.2.1.2]	<ul style="list-style-type: none"> <li>• Compliant—Lumen uses only new and genuine equipment sourced through authorized retailers or the OEMs directly</li> <li>• Scalable—Lumen logistics capabilities can cost effectively meet increasing EIS customer demand</li> <li>• Reliable—Specific models and manufactures of equipment are tested and certified by Lumen labs before they are authorized for use in Lumen’s solutions</li> <li>• Resilient— Lumen enforces OEM warranties on equipment in order to honor the EIS requirement for a one-year warranty on all SRE</li> </ul>
Service Coverage [M.2.1.3]	<ul style="list-style-type: none"> <li>• Lumen is able to furnish SRE in all geographic areas required by EIS TOs</li> </ul>
Security [M.2.1.4]	<ul style="list-style-type: none"> <li>• Lumen’s lab tests and certifications on equipment include adherence to applicable security standards</li> <li>• Lumen’s SCRUM Plan ensures that equipment is stored and handled in a secure manner from the source, to a Lumen warehouse or staging point, and upon deployment into the field for installation and use</li> </ul>

**1.4.10.1 Warranty Service [C.2.10.1]**

Lumen's goal as a provider of network and telecommunication services is to provide industry leading warranties. The Lumen Team provides, at no additional cost to the Government, a minimum one (1)-year system warranty (or the warranty provided by the OEM , whichever is longer) for all hardware and software purchased under the EIS contract, including all equipment supplied, installed, and integrated by our Team. During transition we identify which assets require warranty renewal or high-priority replacement. The equipment warranty provides repair and distribution of updated software to all users who purchased the software under the EIS contract. The Lumen Team maintains an asset inventory of all service related equipment, provides warranty information associated with each product and service, and delivers to the GSA CO or OCO when requested.

We repair or replace malfunctioning equipment covered by warranty within five (5) business days (or sooner), or as specified in the TO. Upon award, we provide to the Government an employee point of contact for the warranty during the Normal Business Day (7AM – 7PM Local Time) or for a longer period if so specified in the TO. All warranties begin at the time the final system acceptance form is signed.

**1.4.10.1.1 Preservation, Packaging and Packing [D.1]**

Unless otherwise specified, all items are preserved, packaged, and packed in accordance with normal commercial practices defined in the applicable commodity specification instructions. Our packaging and packing complies with requirements of the Uniform Freight Classification and the National Motor Freight Classification (applicable at time of shipment), and each shipping container or each item in a shipment is of uniform size and content, except for residual quantities. When special or unusual packing is specified in a TO but not specifically provided for by the contract, such packing details are independently agreed upon between ordering agency and Lumen.

#### **1.4.10.1.2 Packing List [D.2]**

Lumen produces a packing list or other suitable shipping documents to accompany each shipment that include:

- Name and address of the consignor
- Name and complete address of the consignee
- Government order or requisition number
- Government bill of lading number covering the shipment (if any)
- Description of the material shipped, including item number, quantity, number of containers, package number (if any), and weight of each package

#### **1.4.10.1.3 Initial Packing, Marking, and Storage of Equipment [D.3]**

All initial packing, marking and storage incidental to shipping of equipment to be provided under this contract is made at Lumen's expense. Packing, supervision marking and storage costs are not billed to the Government. Supervision of packing and unpacking of initially acquired equipment is supplied by Lumen.

#### **1.4.10.1.4 Equipment Removal [D.4]**

All leased equipment, accessories, and devices located on Government property are dismantled and removed from Government premises by the Lumen Team, at our expense, within 90 calendar days after the service termination date. All dismantling and removal of equipment is performed by our Team during normal Government business hours at the equipment's' location. We provide advance notice to the Local Government Contact to ensure that such dismantling and removal occurs with minimal disruption.

#### **1.4.11 Service Related Labor [L.29.2.1, C.2.11, J.5]**

The Lumen Team understands that the EIS services defined in SOW C.2.1 through C.2.10, and in C.2.12 include all Service Related Labor (SRL) required to implement the various program services. As a partner of the GSA for the last 10 years, we are very experienced in providing a wide

range of highly qualified candidates for service positions. Specific Agencies may also

##### **Service Related Labor Highlights**

- 10 years of experience delivering a wide range of highly qualified candidates for service positions to GSA
- Hundreds of qualified Lumen Team staff to fully support all positions

include labor on TOs to support services for EIS. We understand that labor for construction, alteration, and repair is only in scope as deemed necessary to offer a complete telecommunications solution for a given TO, and we coordinate with the OCO to authorize and scope such labor. **Figure 1.4.11-1** highlights how the features of our SRL solution satisfy the evaluation criteria.

**Figure 1.4.11-1. Features of Lumen’s SRL Solution**

EVALUATION CRITERIA	FEATURES OF LUMEN SRL
Understanding [M.2.1.1]	<ul style="list-style-type: none"> <li>Provides cost effective service labor as required to complete TOs</li> <li>Labor for construction, alteration, and repair is considered to be in scope if it is necessary to offer a complete solution for a TO</li> </ul>
Quality of Service [M.2.1.2]	<ul style="list-style-type: none"> <li>Compliant—Lumen identifies, scopes, staffs, and performs Service Related Labor in a timely manner through our TO management approach and EIS staffing approach</li> <li>████████████████████ with more than 2,000 IT professionals, bolsters our ability to source qualified personnel for TOs</li> <li>Reliable—Subject to Lumen quality processes, including timely completion of services</li> <li>Resilient—Honors required warranty on SLR</li> </ul>
Service Coverage [M.2.1.3]	<ul style="list-style-type: none"> <li>Lumen is able to provide Service Related Labor associated with TOs in all required geographical locations</li> </ul>
Security [M.2.1.4]	<ul style="list-style-type: none"> <li>The Lumen Team staffs EIS TOs with only vetted and appropriately cleared personnel. We identify and manage TO-specific virtual and physical security access in the performance of Service Related Labor</li> </ul>

Lumen recognizes that the following labor categories are included in this contract as summarized in **Figure 1.4.11-2**, and Lumen provides as needed the following Service Related Labor Positions as needed for TO support.

**Figure 1.4.11-2. Service Related Positions and SOC Code with Occupational Group**

SERVICE RELATED POSITION FOR EIS [J.5]	SOC CODE WITH OCCUPATIONAL GROUP
Business Continuity Planner	SOC Code 131199.04; Occupational Group "Professional and related"
Computer Network Architect	SOC Code 151143.00; Occupational Group "Professional and related"
Computer Network Support Specialist	SOC Code 151152.00; Occupational Group "Professional and related"
Computer Systems Analyst	SOC Code 151121.00; Occupational Group "Professional and related"
Computer Systems Engineers/Architect	SOC Code 151199.02; Occupational Group "Professional and related"
Customer Service Representatives	SOC Code 434051.00; Occupational Group "Service Occupations"
Database Administrator	SOC Code 151141.00; Occupational Group "Professional and related"
Database Architect	SOC Code 151199.06; Occupational Group "Professional and related"

SERVICE RELATED POSITION FOR EIS [J.5]	SOC CODE WITH OCCUPATIONAL GROUP
Business Continuity Planner	SOC Code 131199.04; Occupational Group "Professional and related"
Electrical Drafter – Computer Aided Design (CAD) Operator	SOC Code 17-302.02; Occupational Group "Professional and related"
Information Security Analyst	SOC Code 151122.00; Occupational Group "Professional and related"
Information Technology Project Manager	SOC Code 151199.09; Occupational Group "Management, business, and financial"
Network and Computer Systems Administrator	SOC Code 151142.00; Occupational Group "Professional and related"
Software Developer – Applications	SOC Code 151132.00; Occupational Group "Professional and related"
Software Developer – Systems Software	SOC Code 151133.00; Occupational Group "Professional and related"
Software Quality Assurance Engineer/Tester	SOC Code 151199.01; Occupational Group "Professional and related"
Sustainability Specialist	SOC Code 131199.05; Occupational Group "Professional and related"
Telecommunications Engineering Specialist	SOC Code 151143.01; Occupational Group "Professional and related"
Telecommunications Equipment Installer/Repairer	SOC Code 492022.00; Occupational Group "Service Occupations"
Telecommunications Line Installer/Repairer	SOC Code 499052.00; Occupational Group "Service Occupations"
Web Administrators	SOC Code 151199.03; Occupational Group "Professional and related"
Web Developers	SOC Code 151134.00; Occupational Group "Professional and related"

**1.4.12 Cable and Wiring [L.29.2.1, C.2.12]**

Lumen applies extensive cable and wiring experience supporting Government and commercial customers worldwide to meet EIS Cable and Wiring (C&W) requirements. **Figure 1.4.12-1** highlights how our (C&W) solution satisfies evaluation criteria.

**Figure 1.4.12-1. Features of Lumen’s Cable and Wiring Solution**

EVALUATION CRITERIA	FEATURES OF LUMEN CABLE AND WIRING
Understanding [M.2.1.1]	<ul style="list-style-type: none"> <li>Lumen tasks qualified personnel to perform cabling and wiring services as required by TOs</li> <li>Honors the one-year warranty on the installation of cabling and, by managing applicable OEM warranties, enforces the one-year warranty on the equipment</li> </ul>
Quality of Service [M.2.1.2]	<ul style="list-style-type: none"> <li>Compliant—we are experienced in analyzing TOs requirements to determine the correct cabling and wiring solution that also adheres to appropriate standards and codes. We scope necessary cabling and wiring work and coordinates with the Ordering Contracting Officer (OCO)</li> <li>Scalable—methods follow standards that easily scale from simple configurations to complex architectures</li> <li>Reliable—Lumen lab-tests and certifies types, models, and brands of cables and wires before authorizing their use in our solutions</li> <li>Resilient—we analyze the environmental conditions and stresses that affect cabling and wiring for the need to enhance their resiliency, such as shielding.</li> </ul>
Service Coverage	<ul style="list-style-type: none"> <li>Lumen provides provide cabling and wiring services in conjunction with TOs in all required</li> </ul>

EVALUATION CRITERIA	FEATURES OF LUMEN CABLE AND WIRING
[M.2.1.3]	geographical locations
Security [M.2.1.4]	<ul style="list-style-type: none"> <li>Lumen develops the appropriate cabling and wiring solution to support the security requirements of the TO</li> <li>Physical security considerations include preventing unauthorized access to the cabling itself, such as through the use of locked access panels and closets</li> </ul>

Through our SRE approach (Section 1.4.10), demarcation point in the service order. Depending on requirements, Lumen cabling typically includes fiber optic cabling. As summarized in **Figure 1.4.12-2**, Lumen complies with all requirements as stated in SOW C.2.12.

**Cable and Wiring Highlights**

- Lumen brings extensive cabling and wiring experience supporting our global network
- Lumen uses Lessons Learned from other Government and Commercial Customers to help meet or exceed all of the EIS requirements

**Figure 1.4.12-2. Cable and Wiring Compliance with SOW Requirements**

LUMEN COMPLIES	SOW C.2.12 REQUIREMENT	LUMEN COMPLIANT SOLUTION
✓	Installation services and labor	<ul style="list-style-type: none"> <li>Leverage experienced team, capitalizing on lessons learned, to provide wiring and equipment installation services and labor meeting requirements</li> <li>All equipment and material provided is new and conforms to applicable standards</li> </ul>
✓	Cabling, ducting, grounding, lightning protection systems	<ul style="list-style-type: none"> <li>Comply with TO requirements and appropriate standards, and follow industry best practices, in providing cabling, wiring, trenching, ducting, grounding, and lightning protection systems</li> </ul>
✓	Site preparation	<ul style="list-style-type: none"> <li>Site preparation complies with applicable codes and conforms to accepted industry construction and installation practices</li> <li>Coordinate preparation work with appropriate Government facility and organizational personnel</li> </ul>
✓	Government review	<ul style="list-style-type: none"> <li>Ensure planned work and code compliance information is available for OCO review and approval prior to the start of work</li> <li>Submit detailed schedule for all work to Government review</li> </ul>
✓	Tools and test equipment	<ul style="list-style-type: none"> <li>As specified in the applicable TO, all tools and test equipment needed to perform site preparation are provided by the Lumen Team</li> <li>Lumen team maintains ownership of tools and test equipment, unless otherwise specified by the TO</li> </ul>
✓	Temporary utilities	<ul style="list-style-type: none"> <li>The Lumen Team provides temporary utilities that are not available in the work area, coordinating with the Government any utility disconnection</li> </ul>
✓	Building additions and/or changes	<ul style="list-style-type: none"> <li>Provide building additions and/or alterations to the existing structure and space if required to provide C&amp;W installation in compliance with TO requirements</li> </ul>



LUMEN COMPLIES	SOW C.2.12 REQUIREMENT	LUMEN COMPLIANT SOLUTION
		<ul style="list-style-type: none"> <li>If modifications are required, licensed architect and engineering professionals provide design documents complying with applicable codes and building standards</li> </ul>
✓	HVAC and Electrical construction	<ul style="list-style-type: none"> <li>HVAC and electrical construction is provided as necessary to support new or upgraded installations needed to support provision of C&amp;W in compliance with TO requirements</li> </ul>
✓	Power systems	<ul style="list-style-type: none"> <li>Lumen modifies or expands power systems as required to provide environmental controls supporting C&amp;W installation</li> <li>All work to meet applicable NEMA requirements</li> </ul>
✓	Warranty period	<ul style="list-style-type: none"> <li>All work includes a minimum one (1) year warranty on material and labor, per our warranty support process described in section 1.4.10.1</li> </ul>

**1.4.13 External Traffic Routing [L.29.2.3, M.2.1 (item 4) c), C.1.8.8 (item 3)]**

Lumen has designed an External Traffic Routing solution that meets the requirements of the SOW C.1.8.8 (item 3), L.29.2.3, and M.2.1 (item 4) c). Our approach provides clear termination boundaries to present participating agency traffic to the EINSTEIN enclaves, considerations for Lumen MTIPS and agency-specific TICAP services, bypass controls, encrypted VPN tunnel termination and re-

**Lumen External Traffic Routing Highlights**

- Our External Traffic Routing solution meets all of the requirements of the RFP.
- Lumen aggregates and presents authorized traffic to the EINSTEIN enclaves per memorandum of agreement between DHS, Lumen and the participating agencies.

Lumen has a history of working with DHS NPPD. We capitalize on this history, incorporating lessons learned, and continuing to develop our working

establishment where applicable, failsafe mechanisms, performance measurement and reporting, and unauthorized traffic detection and notification. Conceptually, the aggregation services create a ‘man-in-the-middle’ environment, where the EINSTEIN enclave is inserted into the authorized Participating Agency (PA) service-specific traffic flows. Non-participating agency traffic is not allowed into the EINSTEIN enclave unless it is flowing to/from an authorized agency IP address.

The impact on hop count and latency depends upon the enclave’s location relative to the agency site and the service provisioned. Given the proposed locations of the aggregation points, e.g., the proposed ICD 705 sites, the the net impact is that Lumen will satisfy all latency SLAs.

---

The MNS Traffic Aggregation Service is the conceptual foundation for the External Traffic Routing Service. Lumen is proposing to locate and support National Cyber Protection System (NCPS) enclaves known operationally as EINSTEIN in [REDACTED]. [REDACTED] The proposed sites serve as gateways to longhaul transport fiber routes and support local metro networks.

The proposed sites will provide aggregation points for authorized PA external traffic. The site locations provide a balanced proximity to the majority of department/agency traffic and support major Internet access capabilities. The locations also provide interconnection support for alternate carriers, e.g., [REDACTED]. [REDACTED]

PA external traffic will be routed and delivered to the EINSTEIN enclaves via discrete in-line, and department/agency identifiable ingress and egress points. Service offerings include VPNS, Ethernet Transport, Private Line Service, Internet Protocol Service, Cloud Services (IaaS, PaaS, SaaS), MNS Traffic Aggregation Service, MTIPS. The External Traffic Routing solution will have the ability to convert and deliver traffic to the EINSTEIN enclave as Ethernet VLANs or natively within the service definition. Conversion would be performed at the Traffic Aggregation Service boundary to the EINSTEIN enclave.

1. PA external traffic utilizing VPNS is delivered per PA VRF (VRF naming convention and assignment scheme to be developed with DHS upon Task Order). The PA will be required to work with DHS and Lumen to identify IP addresses to be routed to the EINSTEIN enclave. The interface to the EINSTEIN enclave will be per DHS requirements. Options range from 1Gb to 100Gb.
2. PA external traffic utilizing ETS is delivered per PA VLAN ID. VLAN ID mapping scheme is to be developed with DHS upon Task Order. The PA will be required to work with DHS and Lumen to identify IP addresses that will be carried within the ETS environment. The ETS interface to the EINSTEIN enclave will be per DHS requirements. Options range from 1Gb to 100Gb.

- 
3. PAs utilizing Private Line Service to reach external sources will need to identify specific PLS circuits to be incorporated into the External Routing scheme, upper layer protocols utilized, IP addressing (if applicable), and encryption methods (if applicable). Interfaces to the EINSTEIN enclave may range from T1 to OC-192 or 1Gb to 100Gb OWS. PLS circuits will require physical routing that will incorporate the EINSTEIN enclave as an intermediate node in the circuit path.
  4. External Routing support for Internet Protocol Service will be provided through purpose built interfaces to Lumen AS3356. A boundary router will provide traffic routing from the public Internet to the PA authorized IP addresses. The boundary router will map PA specific traffic to VPNS VRFs or ETS VLANs in accordance with the transport services required by the PA. EINSTEIN Enclave interfaces may be 1Gb to 100Gb Ethernet.
  5. Cloud Services (IaaS, PaaS, SaaS). Lumen connects to Cloud Service Providers (CSPs) via Ethernet, MPLS VPNS or OWS. Lumen will incorporate the External Routing capability to integrate PA traffic flowing to and from CSPs through an EINSTEIN enclave per transport service subscribed as cloud access.
  6. Lumen is proposing a Managed Trusted IP Service under EIS. This service will utilize the Aggregation Service for PA to public Internet traffic flows. The MTIPS equipment will be optimally located in the same facility as the the DHS EINSTEIN enclaves. The DHS EINSTEIN enclaves will be incorporated in-line with the PA MTIPS traffic. PAs that are TICAPs and utilize Lumen for Internet access will be supported via the methods developed for the Internet Protocol Service described in Item #4 above. Ingress from the PA will be VPNS (VRF).
  7. Traffic aggregation and external routing in support of the DHS Intrusion Prevention Security Service is the same as MTIPS. The DHS EINSTEIN enclaves will be incorporated as an additional in-line inspection. The DHS

IPSS will optimally be hosted in the same facility as the DHS EINSTEIN enclaves.

Diversity is incorporated in the design on a per customer and per service basis. Each Participating Agency (PA) will be provisioned with a primary route to the closest EINSTEIN enclave and a diverse route to the alternative EINSTEIN enclave. The proposed distribution of EINSTEIN enclaves will allow the primary path to meet the latency SLA objectives for the respective transport service, as applicable.

**Figure 1.4.13-2** highlights how the features of our External Traffic Routing solution satisfy the evaluation criteria.

**Figure 1.4.13-2. Features of Lumen’s External Traffic Routing Solution**

EVALUATION CRITERIA	FEATURES OF LUMEN EXTERNAL TRAFFIC ROUTING
Understanding [M.2.1.1]	<ul style="list-style-type: none"> <li>With our 10-year incumbency supporting GSA, Lumen has a comprehensive understanding of EIS traffic routing requirements</li> <li>Lumen has a history of working with DHS NPPD concerning traffic security, and applies this in our external traffic routing solution.</li> </ul>
Quality of Service [M.2.1.2]	<ul style="list-style-type: none"> <li>The Lumen GovNOCs and GovSOCs provide 24/7 proactive real-time monitoring and performance management to help ensure that all traffic routing performance requirements are consistently met.</li> <li>The Lumen Team’s extensive past performance experience with similar scope contracts results in the development of mature reporting services required for EIS External Traffic Routing</li> </ul>
Service Coverage [M.2.1.3]	<ul style="list-style-type: none"> <li>Our network architecture provides global service coverage that significantly exceeds the minimum CBSA requirements specified in SOW C.1.3</li> <li>Our EIS network provides secure and compliant External Traffic Routing wherever it is required.</li> </ul>
Security [M.2.1.4]	<ul style="list-style-type: none"> <li>The Lumen External Traffic Routing solution fully meets the requirements of the SOW C.1.8.8 (item 3), L.29.2.3 and M.2.1 (item 4) c).</li> <li>Our approach provides clear termination boundaries to present participating agency traffic to the EINSTEIN enclaves.</li> </ul>

**1.4.13.1 Identifying Participating Agency Traffic [L.29.2.3, M.2.1 (item 4) c)i., C.1.8.8 (item 1)]**

The aggregation point of PA traffic will reside outside of the EINSTEIN security boundary. IPv4 and IPv6 capabilities are fully deployed and are inherently supported.

---

Non-participating IP traffic would be blocked from enclave access through the use of firewalls at the ingress/egress edge of the enclave, denying all traffic that does not contain either a PA source or destination address in the IP header. An IDS function will also be incorporated at the ingress to the EINSTEIN to detect the inadvertent routing of non-PA traffic. The IDS/IPS will contain a 'white list' of authorized PA addresses and generate a syslog event to notify Lumen GovSOC and DHS operations of the non-PA event and consequently block the traffic if directed by DHS policy.

PLS and other layer 1 service will be identified per circuit provisioning order. The circuit orders will have an obfuscated customer name associated with the order. The obfuscation information translations will be provided to DHS as sensitive information, potentially categorized as CUI by GSA.

#### **1.4.13.2 Traffic Control Mechanisms [L.29.2.3, M.2.1 (item 4) c)iv. and v., C.1.8.8]**

Departments/agencies participating in the NCPS program will have a corresponding indicator in their service order. This will ensure that the service ordered will incorporate the aggregation service as a component of the order. Routing for IP based services will be limited to ensure that traffic requiring EINSTEIN processes have no routing means other than the through the EINSTEIN enclave. Layer 1 services such as PLS are physically routed to the aggregation locations routed through the EINSTEIN enclave as an intermediate hop. At each aggregation point, a fail-safe bypass will be configured and manually activated/restored in the event of a failure of an EINSTEIN enclave. Failsafe activities will generate events that will be sent to Lumen and DHS/US CERT information management systems.

#### **1.4.13.3 Encryption Tunnel Proxy [L.29.2.3, M.2.1 (item 4) c), C.1.8.8]**

SSL and IPSec tunnels will terminate at the Aggregation Service ingress boundary. Unencrypted traffic will be sent to the EINSTEIN enclaves for inspection and action. Clean traffic will be sent from the EINSTEIN enclave to the Aggregation Service egress boundary where it will SSL and IPSec tunnels will be re-established. This functional representation is provided in **Figure 1.4.8.8.1-2**.

---

**1.4.13.4 Smart Hands Support [L.29.2.3, M.2.1 (item 4) c)vii, C.1.8.8]**

Lumen will provide TS/SCI-cleared personnel to support 'smart hands' functions of DHS supplied equipment. Staffing and response KPIs/SLAs will be per DHS requirements.

**1.14.13.5 Performance Measurement [L.29.2.3, M.2.1 (item 4) c)viii, C.1.8.8]**

Lumen will provide performance measurement capabilities at the ingress and egress points of the EINSTEIN enclave. KPI metadata for each department/agency traffic flow will be captured, correlated and measured against service specific latency SLAs. Flows are timestamped at the ingress and egress points of the EINSTEIN enclave. This provides a means to isolate the EINSTEIN enclave processing from the overall latency measurement. Other KPIs and SLAs will continue to be supported as applicable to the provisioned transport service.

---

## **2.0 RISK MANAGEMENT FRAMEWORK PLAN [L.29.3A), C.1.8.7]**

### **2.1 Risk Management Framework (RMF) Approach [L.29.3.a), C.1.8.7]**

Lumen is committed to maintaining the security, confidentiality, integrity, and availability of its networks and services, and of customer data transported therein. Lumen operates an integrated security architecture managed by several dedicated security groups. They are responsible to identify and correct vulnerabilities that affect the commercial and internal networks, associated products and services, and related support systems. Lumen believes that the early detection and analysis of security threats that could impact the network is critical to consistently assess the security level being provided.

The EIS Service RMF supports the following goals:

- Integration of information security requirements into the service architecture and corresponding Systems Development Life Cycle (SDLC)
- Implementation of Continuous Monitoring (CM) to support ongoing security authorization decisions
- Implementation of appropriate risk mitigation strategies

For guidance, the Lumen EIS Service RMF Plan draws upon the following documentation:

- Federal Information Security Management Act (FISMA) of 2002; (44 U.S.C. Section 301. Information security).
- Federal Information Security Modernization Act of 2014; (to amend Chapter 35 of 44 U.S.C.).
- FIPS PUB 199, "Standards for Security Categorization of Federal Information and Information Systems." Dated February 2004.
- FIPS PUB 200, "Minimum Security Requirements for Federal Information and Information Systems." Dated March 2006.
- NIST SP 800-18 Revision 1, "Guide for Developing Security Plans for Federal Information Systems." Dated February 2006.

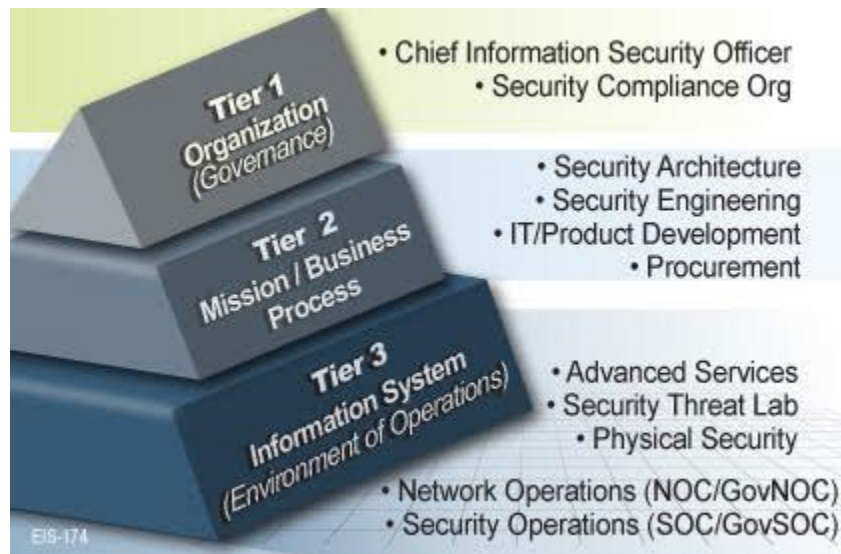
- 
- NIST SP 800-30 Revision 1, “Guide for Conducting Risk Assessments.” Dated September 2012.
  - NIST SP 800-34 Revision 1, “Contingency Planning Guide for Information Technology Systems.” Dated May 2010.
  - NIST SP 800-37 Revision 1, “Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Lifecycle Approach.” Dated February 2010.
  - NIST SP 800-40 Revision 3, “Guide to Enterprise Patch Management Technologies.” Dated July 2013.
  - NIST SP 800-47, “Security Guide for Interconnecting Information Technology Systems.” Dated August 2002.
  - NIST Special Publication 800-53 Revision 4, “Security and Privacy Controls for Federal Information Systems and Organizations.” Dated April 2013.
  - NIST Special Publication 800-53A, Revision 4, “Assessing Security and Privacy Controls in Federal Information Systems and Organizations, Building Effective Assessment Plans.” Dated December 2014.
  - NIST SP 800-60 Revision 1, “Guide for Mapping Types of Information and Information Systems to Security Categories.” Dated August 2008.
  - NIST SP 800-60 Revision 1, “Guide for Mapping Types of Information and Information Systems to Security Categories.” Dated August 2008.
  - NIST SP 800-160 “Systems Security Engineering.” Draft dated May 2014.
  - NIST SP 800-161 “Supply Chain Risk Management Practices for Federal Information Systems and Organizations.” Dated April 2015.
  - NIST SP 800-171, “Protecting Controlled Unclassified Information in the Nonfederal Information Systems and Organizations.” Dated June 2015.
  - DODI 8510.01 “Risk Management Framework (RMF) for DOD Information Technology (IT).” Dated 12 March 2014.

Led by the Chief Information Security Officer (CISO), the Lumen Security Compliance organization is responsible for the design, maintenance, and enforcement



of the security framework and other security initiatives within Lumen. As illustrated in **Figure 2.1-1**, this organization supports the governance of Tier 1 functions described in NIST SP 800-37.

From an EIS services perspective, NIST SP 800-37 Tier 2 risk management functions are overseen by the Security Architecture and the Security Engineering organizations. Security Architecture provides a focus for research and development in identifying, investigating, and testing newly discovered security trends, capabilities, and technologies. This group is also responsible for the overall security architecture used to protect the Lumen systems and infrastructure. The focus of Security Engineering is the development and/or purchase of technology that ensures the security and integrity of Lumen's assets and infrastructure as well as the testing and integration of this technology into the logical and physical environment. Additionally, the Lumen Information Technology and Product Development organizations are responsible for information systems associated with a given service and the respective SDLC management of internally developed systems. The Lumen procurement organization is also integrated into this layer to ensure that risk management constructs are incorporated into the procurement/supply chain.



**Figure 2.1-1. Lumen Risk Management Approach per NIST SP 800-37 Tiers.**

As suggested in **Figure 2.1-1**, within the EIS services risk management construct, there are multiple Lumen organizations supporting relative NIST SP 800-37 Tier 3 support functions. The Network Operations and Security Operations groups provide 24/7 monitoring and incident management to all operational aspects including security threats. The Network and Security Advanced Services organizations provide Tier 3 support for the Enterprise Managed Security Services, Facilities, and Lawful process to ensure the availability and reliability of network and security applications and services within defined SLAs. These organizations also ensure adherence to all processes in the documentation and implementation of systems. Additionally, Lumen maintains a Security Threat Lab (Lab) to provide an evaluation and assessment function to the Security Engineering department. The Lab is used to regularly review commercial security products and to perform assessments on the network, systems, applications, and functions, and to test functional aspects of code used within the infrastructure. Protection of service infrastructure extends to the physical security of the service environment. Lumen's Physical Security organization develops, designs, deploys and maintains access control and video surveillance systems at Lumen locations worldwide.

In support of informed risk determination, Lumen has developed and implemented a risk assessment process that includes a systematic approach for identifying threats, vulnerabilities, likelihood of exploitation, and potential impact. Lumen implements security technology and process controls to measure compliance with risk management practices. The risk determination model is based upon ensuring that security is covered at the following layers:

- Transport
- Network
- System
- Applications
- Data
- Users

In addition, the model provides for compliance coverage in the following areas:

- Authentication
- Accounting
- Confidentiality
- Availability
- Integrity
- Trust Domains  
(Security Boundaries)

---

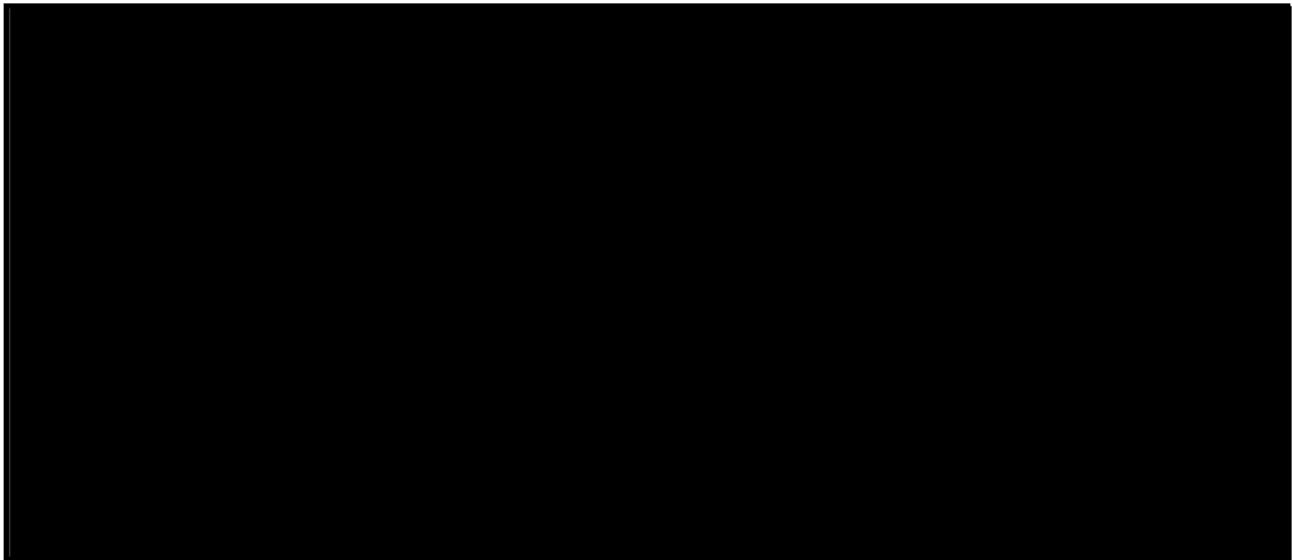
## **2.2 Systems Development Life Cycle [L.29.3.a), C.1.8.7]**

Security requirements for internally developed systems are included during the planning, development, and implementation stages. Lumen employs an “Envision, Engineer, Operate, and Respond” risk management lifecycle to ensure processes and systems are fully optimized. From a services perspective, each product/service maintains a systems registry that includes functional description documentation, security documentation, engineering and operations guides, maintenance procedures, service release documentation, and a product/service roadmap. Lumen utilizes a LifeCycle Management Database as a repository for service Change Management and lifecycle tracking purposes. Customer-facing or general public service SDLC information such as change management events is posted on a public-facing web server or distributed by email to Lumen customers. Proprietary SDLC service information is posted on a secure, access-controlled web server for internal purposes. Only persons with a ‘need to know’ relative to their job functions have access to this system.

## **2.3 Information System Boundaries [L.29.3.a), C.1.8.7]**

Lumen has developed methods and procedures to protect Government information within a system security boundary that is separate from the information systems that control EIS services. There are three security boundaries in support of EIS: the BSS security boundary, a FISMA Moderate (MOD) environment; the MTIPS security boundary; a FISMA HIGH environment; and the EIS services security boundary, a FISMA MOD environment.

The methods, procedures, and controls implemented within the BSS security boundary protect Government information within the BSS operating environment. All EIS-related Government information is contained within the BSS security boundary. Government information passed to systems outside of the BSS security boundary is obfuscated. A conceptual representation of the agency-specific and obfuscated information separation is provided in **Figure 2.3-1**.



**Figure 2.3-1. Conceptual Agency Data Protection Schema.** *This methodology limits the number of confidentiality and integrity based security controls applicable to the EIS services security boundary.*

#### **2.4 Security Control Allocation [L.29.3.a), C.1.8.7]**

The services-based RMF primarily focuses on the protection within the D/A information transport element of the EIS services. Services-based information system controls are generally not applicable to protection of Government information as this information is obfuscated through methods and procedures contained within the BSS security boundary. Common Controls will be utilized within the systems where possible and applicable.

#### **2.5 The Risk Management Framework Process [L.29.3.a), C.1.8.7]**

Lumen utilized NIST SP 800-37 and internal best practices in the development of this EIS Services RMF Plan document. As a living document, it will be updated throughout the EIS services SDLC. From NIST SP 800-37, the six RMF process steps<sup>1</sup> are represented in **Figure 2.5-1**.

---

<sup>1</sup> NIST SP 800-37, Figure 2-2 Risk Management Framework



**Figure 2.5-1. Risk Management Framework Process Steps (NIST SP 800-37).**

### **2.5.1 Step 1: Categorize Information System [L.29.3.a), C.1.8.7]**

#### **2.5.1.1 RMF Step 1 – Task 1-1, Security Categorization [L.29.3.a), C.1.8.7]**

GSA has categorized all EIS services to be FISMA Moderate.<sup>2</sup> EIS services will utilize the existing Lumen Enterprise service environment wherever possible.

#### **2.5.1.2 RMF Step 1 - Task 1-2, Information System Description [L.29.3.a), C.1.8.7]**

Lumen is proposing the following services for EIS. Service descriptions are provided in detail in this Lumen EIS Technical Volume. Network service boundaries are the SDPs of the respective network service. (Technical Volume reference sections are provided in parentheses adjacent to service bullet item below):

- Data Service – Virtual Private Network Service (1.3.1.1)
- Data Service – Ethernet Transport Service (1.3.1.2)

<sup>2</sup> RFP #QTA0015THA3003, Amendment 4, Revisions, Questions, Answers and Clarifications to the EIS RFP, Question # 840, Section C, Section #1.8.7.3

- 
- Data Service – Optical Wavelength Service (1.4.1.1)
  - Data Service – Private Line Service (1.4.1.2)
  - Data Service – Synchronous Optical Network Service (1.4.1.3)
  - Data Service – Dark Fiber Services (1.4.1.4)
  - Data Service – Internet Protocol Service (1.4.1.5)
  - Voice Service – Internet Protocol Voice Service (1.3.2.1)
  - Voice Service – Circuit Switched Voice Service (1.4.2.1)
  - Voice Service – Toll Free Service (1.4.2.2)
  - Voice Service – Circuit Switched Data Service (1.4.2.3)
  - Contact Center Services (1.4.3)
  - Colocated Hosting Service (1.4.4)
  - Cloud Service – Infrastructure as a Service (1.4.5.1)
  - Cloud Service – Platform as a Service (1.4.5.2)
  - Cloud Service – Software as a Service (1.4.5.3)
  - Content Delivery Network (1.4.5.4)
  - Commercial Satellite Communications Service (1.4.7)
  - Managed Service – Managed Network Service (1.3.3.1)
  - Managed Service – Web Conferencing Service (1.4.8.1)
  - Managed Service – Unified Communication Service (1.4.8.2)
  - Managed Service – Managed Trusted Internet Protocol Service (1.4.8.3)<sup>3</sup>
  - Managed Service – Managed Security Service (1.4.8.4)
  - Managed Service – Managed Mobility Service (1.4.8.5)
  - Audio Teleconferencing Service (1.4.8.6)
  - Video Teleconferencing Service (1.4.8.7)
  - DHS Intrusion Protection Security Service (1.4.8.8)<sup>4</sup>

---

<sup>3</sup> Managed Trusted Internet Protocol Service functions is a FISMA HIGH environment. Therefore, the service is excluded from this RMF Plan.

- 
- Access Arrangements (1.4.9)
  - Service Related Equipment (1.4.10)
  - Service Related Labor (1.4.11)
  - Cable and Wiring (1.4.12)
  - External Traffic Routing (1.4.13)

### **2.5.2 RMF Step 2: Select Security Controls [L.29.3.a), C.1.8.7]**

In NIST SP 800-53, Security and Privacy Controls for Federal Information Systems and Organizations, NIST presents the set of baseline controls for FISMA Low, Moderate and High (LOW, MOD, HIGH) impact level systems. As a reference, in Section 2.6 we provide a summary of the baseline controls from NIST SP 800-53 for the FISMA MOD impact level.

Baseline control sets represent the starting point for security control tailoring (adding, subtracting and/or modifying controls) as needed by the responsible security organization. Given the diversity of EIS services being offered by Lumen, we anticipate that security control selection is tailored by EIS Service (RMF Task 2-2, Security Control Selection).

As part of the security control selection process, we identify (as RMF Task 2-1, Common Control Identification) and utilize common controls to the greatest extent where applicable. The information systems supporting the Enterprise services utilized for EIS will only contain obfuscated Government information. These systems will have a limited applicable control set as confidentiality and integrity requirements are diminished by the incorporation of the obfuscation methods. Enterprise system availability controls will incorporate common controls utilized for the EIS BSS environment.

Government information is not provided to our EIS service partners. They provide service to Lumen with Lumen as the customer of record or under specific arrangements where Government information is obfuscated. Therefore, partner IT systems are

---

<sup>4</sup> DHS Intrusion Protection Security Service functions as a FISMA HIGH environment. Therefore, the service is excluded from this RMF Plan.

considered to be outside the services security boundary. While not directly under the risk management framework, in practice partner network components are considered in relation to integrity and availability. Partner compliance is evident through SLA validation of the overall service.

We consider the protection of the network transport as an important component of a service. The security controls of a given network service will focus primarily on methods protecting the integrity and availability of Government traffic. These methods are typically inherent to the network service design and capabilities necessary to meet SLAs of the specific EIS services. The FIPS 200 Security Control Catalog families are provided in **Figure 2.5.2-1**. Appendix G of NIST SP 800-53 defines a security family for Program Management and Appendix J defines several Privacy Control families. The Program Management and Privacy Control families are impact baseline independent. All are presented in Section 2.6.

**Figure 2.5.2-1. FIPS 200 Security Control Families**

IDENTIFIER	FAMILY	CLASS
AC	Access Control	Technical
AT	Awareness and Training	Operational
AU	Audit and Accountability	Technical
CA	Security Assessment and Authorization	Management
CM	Configuration Management	Operational
CP	Contingency Planning	Operational
IA	Identification and Authentication	Technical
IR	Incident Response	Operational
MA	Maintenance	Operational
MP	Media Protection	Operational
PE	Physical and Environmental Protection	Operational
PL	Planning	Management
PS	Personnel Security	Operational
RA	Risk Assessment	Management
SA	System and Service Acquisition	Management
SC	System and Communication Protection	Technical
SI	System and Information Integrity	Operational
PM	Program Management (NIST SP 800-53)	Management



Lumen identifies assets requiring protection and will correlate methods and procedures against NIST SP 800-53 security controls. These methods and procedures form the common controls for EIS Services. Protecting Lumen assets supports the FISMA moderate protection relating to the confidentiality, integrity and availability of Government information that is transported by Lumen EIS services. **Figure 2.5.2-2** provides a matrix of threat management aspects of the EIS services, e.g., threats, countermeasures and related NIST SP 800-53 technical and operational control families under consideration.

**Figure 2.5.2-2. Management of Threats against Physical Assets of Lumen**

ASSET PROTECTED	THREATS	COUNTERMEASURES	CONTROL FAMILIES TO BE EVALUATED
Lumen Technical Facility	<ul style="list-style-type: none"> <li>Unauthorized access &amp; malicious attacks</li> <li>Natural &amp; other disasters, fire &amp; accidents</li> </ul>	<ul style="list-style-type: none"> <li>Access controls, locks &amp; alarms</li> <li>Self-contained industrial strength power &amp; HVAC extinguishing systems, alarms and continuous monitoring</li> </ul>	<ul style="list-style-type: none"> <li>AC, CA, CP, IR, PE, IA, PS</li> </ul>
Network Systems	<ul style="list-style-type: none"> <li>Unauthorized access</li> <li>Natural &amp; other disasters</li> <li>Fire &amp; accidents</li> <li>Malicious Attacks</li> </ul>	<ul style="list-style-type: none"> <li>Access controls, intrusion detection and scans</li> <li>Fail-over systems</li> <li>Systems security, continuous monitoring, recovery</li> </ul>	<ul style="list-style-type: none"> <li>AC, AU, CA, IA, MP, PE, PS, RA, SA, SC, SI</li> </ul>
Fiber-Optic Cables	<ul style="list-style-type: none"> <li>Accidental breakage</li> <li>Unauthorized access to signals</li> </ul>	<ul style="list-style-type: none"> <li>Shielding and burial</li> <li>Technical difficulty and rapid detection of taps</li> <li>SONET rings and nets</li> </ul>	<ul style="list-style-type: none"> <li>AC-1, CP, IA, IR, PE, RA</li> </ul>
Lumen switching equipment Telcom carrier's equipment Colocation customers' equipment	<ul style="list-style-type: none"> <li>Unauthorized access</li> <li>Natural &amp; other disasters</li> <li>Fire &amp; accidents</li> <li>Malicious Attacks</li> </ul>	<ul style="list-style-type: none"> <li>Continuous monitoring, rerouting and back-up systems</li> <li>Physical security and network monitoring</li> <li>Access control and response to alarms</li> <li>Note: Telcom carrier's equipment is housed in separate, secured spaces</li> </ul>	<ul style="list-style-type: none"> <li>AC, AU, CA, IA, MP, PE, PS, RA, SA</li> </ul>
Authorized Personnel	<ul style="list-style-type: none"> <li>Awareness &amp; training</li> <li>Accidents</li> </ul>	<ul style="list-style-type: none"> <li>Annual security training, security exercises</li> </ul>	<ul style="list-style-type: none"> <li>AU, AT, PE, PS</li> </ul>

ASSET PROTECTED	THREATS	COUNTERMEASURES	CONTROL FAMILIES TO BE EVALUATED
	<ul style="list-style-type: none"> <li>• Fire, explosion</li> <li>• Malicious attacks</li> </ul>	<ul style="list-style-type: none"> <li>• Safety requirements, procedures</li> <li>• Physical security, monitoring and response</li> </ul>	

In addition to the technical and operational control families mitigating the threats identified in **Figure 2.5.2-2**, consideration must be applied to management aspects within the EIS Services RMF plan. Support elements identified within **Figure 2.5.2-3** identify areas under the service management area of responsibility.

**Figure 2.5.2.3. Management of Threats against Management Elements of Lumen**

MANAGEMENT COMPONENT	SUPPORT ELEMENT	CONTROL FAMILIES TO BE EVALUATED
<b>Maintenance &amp; Support</b>	<ul style="list-style-type: none"> <li>• Configuration Management</li> <li>• Service Maintenance</li> <li>• BCDR</li> </ul>	<ul style="list-style-type: none"> <li>• CM, MA, CP</li> </ul>
<b>Service Management</b>	<ul style="list-style-type: none"> <li>• Asset Management</li> <li>• Incident Response</li> <li>• Planning</li> <li>• Risk Assessment</li> <li>• Security Assessment</li> <li>• System &amp; Service Acquisition</li> <li>• Program Management</li> </ul>	<ul style="list-style-type: none"> <li>• PE, IR, PL, RA, PS, PM</li> </ul>

The evaluation of security controls for the EIS services and management of the services will establish the grounds for confidence that risks are identified and managed via specific control families and controls.

Consistent with RMF Task 2-3, Monitoring Strategy, Lumen will outline its strategy and approach for monitoring of each EIS Service. Because of the high degree of overlap of many of the services’ management platforms, we expect a high degree of commonality in the monitoring approach for many of the services.

We recognize the importance of RMF Task 2-4, Security Plan Approval, as a formal step to secure corporate-wide recognition and approval of security elements.

Lumen notes that partners will/could be involved in supporting or delivering a particular EIS service. As part of our agreements and relationships with all partners, as

---

needed they will work with Lumen to follow the RMF process to secure Authorization and Accreditation for their underlying services.

### **2.5.3 RMF Step 3: Implement Security Controls [L.29.3.a), C.1.8.7]**

The Tier 2 organizations supporting the Lumen enterprise services support the implementation of the services base risk management framework. Lumen has implemented industry and company specific security controls in the current operational environment.

In implementing security controls, Lumen adheres to the following set of internal guidelines for each control:

- **Description:** The control's implementation and how it satisfies the security requirement are described.
- **Responsibility:** The person(s) responsible for implementing and enforcing the control solution is named.
- **Review Policy:** The periodicity (daily, weekly, monthly, etc.) for reviewing the control and its implementation is specified. This information includes the naming of who conducts the review and what initiates it. The review initiation can be according to a schedule and/or an event.
- **Documentation:** Specify how reviews are documented and how we prove that the control is implemented and reviewed. If a published policy is the basis for the control's implementation, then that policy will be included with the documentation.

Alignment to NIST SP 800-53 controls will be demonstrated via the Authorization process.

### **2.5.4 RMF Step 4: Assess Security Controls [L.29.3.a), C.1.8.7]**

Should a service level RMF assessment be required within a given Task Order, Lumen Information System Security Officer (ISSO)/Information System Security Manager (ISSM) will execute an assessment of systems in the EIS services security boundary in compliance with NIST SP 800-53 and NIST SP 800-53A assessment procedures. The assessment will ensure the security controls were implemented as

---

designed and operating as expected prior to initiating EIS Security Authorization and Accreditation process. The following functional areas will be supported in our assessment process:

- Audit and Assessment:
  - Testing of access, identification, authentication and audit mechanisms
  - Testing of security configuration parameters
  - Testing of physical access controls
  - Conducting penetration testing of key service components
  - Testing backup and recovery controls
  - Testing incident response and contingency capabilities
- Mitigation and Remediation:
  - Controls or procedures within a control found to be inadequate or in need of adjustment will undergo a Plan of Action and Milestones (POA&M) - based corrective mitigation and remediation sequence
- Re-assessment:
  - Mitigated and remediated environments will be re-assessed for compliance
- Package Submission:
  - System Security Plan
  - Security Assessment Report
  - POA&M to address remaining vulnerabilities of a given EIS service

#### **2.5.5 RMF Step 5: Authorize Information System [L.29.3.a), C.1.8.7]**

Should a service level authorization be required, Lumen will follow the EIS Security Authorization and Accreditation process to obtain a formal ATO. Lumen will follow the EIS Security Authorization and Accreditation (Security A&A) process, as outlined in NIST SP 800-37 Revision 1 and GSA IT Security Procedural Guide 06-30, to obtain a formal ATO from the Government.

#### **2.5.6 RMF Step 6: Monitor Security Controls [L.29.3.a), C.1.8.7]**

Lumen follows a continuous monitoring strategy to ensure the EIS boundary is maintained and managed based on categorization definition. We will report on the

security state of the system to appropriate organizational officials via a quarterly POA&M as well as the annual assessment.

**2.6 Reference: FISMA Moderate (MOD) Impact Level Baseline Control Set [L.29.3.a), C.1.8.7]**

In NIST SP 800-53, Security and Privacy Controls for Federal Information Systems and Organizations, NIST presents the set of baseline controls for FISMA MOD impact level systems, the level specified for nearly all of the EIS services. As reference, we provide a summary of these baseline controls for the FISMA MOD impact level.

Baseline control sets are a starting point for control selection. Given the diversity of EIS services being offered by Lumen, we anticipate that controls selected will be tailored by specific EIS Service.

Figures 2.6-1 through 2.6-19 summarize the Control Families and specific controls of the FISMA Moderate impact baseline. No controls will apply to the Services Based RMF due to the obfuscation of Government information within the EIS Service IT environment.

**Figure 2.6-1. Access Control (AC) Controls Family**

CNTL NO.	CONTROL NAME	MOD BASELINE	COMMENTS
AC-1	Access Control Policy and Procedures	AC-1	Access controls establish the terms and conditions under which a person or process can access the system, and the controls placed on such access. EIS Service access controls will build upon Lumen’s stringent access control policies and approval procedures in place for many of our products.
AC-2	Account Management	AC-2 (1) (2) (3) (4)	
AC-3	Access Enforcement	AC-3	
AC-4	Information Flow Enforcement	AC-4	
AC-5	Separation of Duties	AC-5	
AC-6	Least Privilege	AC-6 (1) (2) (5) (9) (10)	
AC-7	Unsuccessful Logon Attempts	AC-7	
AC-8	System Use Notification	AC-8	
AC-11	Session Lock	AC-11 (1)	
AC-12	Session Termination	AC-12	
AC-14	Permitted Actions without Identification or Authentication	AC-14	
AC-17	Remote Access	AC-17 (1) (2) (3) (4)	
AC-18	Wireless Access	AC-18 (1)	
AC-19	Access Control for Mobile Devices	AC-19 (5)	

AC-20	Use of External Information Systems	AC-20 (1) (2)	
AC-21	Information Sharing	AC-21	
AC-22	Publicly Accessible Content	AC-22	

**Figure 2.6-2. Awareness and Training (AT) Controls Family**

CNTL NO.	CONTROL NAME	MOD BASELINE	COMMENTS
AT-1	Security Awareness and Training Policy and Procedures	AT-1	Will be derived from existing Training policies and procedures.
AT-2	Security Awareness Training	AT-2 (2)	
AT-3	Role-Based Security Training	AT-3	
AT-4	Security Training Records	AT-4	

**Figure 2.6-3. Audit and Accountability (AU) Controls Family**

CNTL NO.	CONTROL NAME	MOD BASELINE	COMMENTS
AU-1	Audit and Accountability Policy and Procedures	AU-1	AU controls are essential for security-related investigations and Lumen has AU controls in place for other security offerings. EIS Services will build upon the audit and accountability policies and approval procedures in place.
AU-2	Audit Events	AU-2 (3)	
AU-3	Content of Audit Records	AU-3 (1)	
AU-4	Audit Storage Capacity	AU-4	
AU-5	Response to Audit Processing Failures	AU-5	
AU-6	Audit Review, Analysis, and Reporting	AU-6 (1) (3)	
AU-7	Audit Reduction and Report Generation	AU-7 (1)	
AU-8	Time Stamps	AU-8 (1)	
AU-9	Protection of Audit Information	AU-9 (4)	
AU-11	Audit Record Retention	AU-11	
AU-12	Audit Generation	AU-12	

**Figure 2.6-4. Security Assessment and Authorization (CA) Controls Family**

CNTL NO.	CONTROL NAME	MOD BASELINE	COMMENTS
CA-1	Security Assessment and Authorization Policies and Procedures	CA-1	Lumen's existing commercial and Government security services themselves demand stringent CA controls. Accordingly, CA controls for EIS Services will be built upon our security assessment and authorization policies and
CA-2	Security Assessments	CA-2 (1)	
CA-3	System Interconnections	CA-3 (5)	
CA-5	Plan of Action and Milestones	CA-5	
CA-6	Security Authorization	CA-6	
CA-7	Continuous Monitoring	CA-7 (1)	
CA-9	Internal System Connections	CA-9	

			approval procedures already in place.
--	--	--	---------------------------------------

**Figure 2.6-5. Security Configuration Management (CM) Controls Family**

CNTL NO.	CONTROL NAME	MOD BASELINE	COMMENTS
CM-1	Configuration Management Policy and Procedures	CM-1	EIS Services' CM controls will be built upon Lumen's existing CM policies and approval procedures.
CM-2	Baseline Configuration	CM-2 (1) (3) (7)	
CM-3	Configuration Change Control	CM-3 (2)	
CM-4	Security Impact Analysis	CM-4	
CM-5	Access Restrictions for Change	CM-5	
CM-6	Configuration Settings	CM-6	
CM-7	Least Functionality	CM-7 (1) (2) (4)	
CM-8	Information System Component Inventory	CM-8 (1) (3) (5)	
CM-9	Configuration Management Plan	CM-9	
CM-10	Software Usage Restrictions	CM-10	
CM-11	User-Installed Software	CM-11	

**Figure 2.6-6. Contingency Planning (CP) Controls Family**

CNTL NO.	CONTROL NAME	MOD BASELINE	COMMENTS
CP-1	Contingency Planning Policy and Procedures	CP-1	Operating critical national infrastructure, Lumen has robust CP controls in place. EIS Services' CP controls will be built upon these existing CP policies and approval procedures.
CP-2	Contingency Plan	CP-2 (1) (3) (8)	
CP-3	Contingency Training	CP-3	
CP-4	Contingency Plan Testing	CP-4 (1)	
CP-6	Alternate Storage Site	CP-6 (1) (3)	
CP-7	Alternate Processing Site	CP-7 (1) (2) (3)	
CP-8	Telecommunications Services	CP-8 (1) (2)	
CP-9	Information System Backup	CP-9 (1)	
CP-10	Information System Recovery and Reconstitution	CP-10 (2)	

**Figure 2.6-7. Identification and Authorization (IA) Controls Family**

CNTL NO.	CONTROL NAME	MOD BASELINE	COMMENTS
IA-1	Identification and Authentication Policy and Procedures	IA-1	EIS Services' IA controls will be built upon Lumen's existing IA policies and approval procedures.
IA-2	Identification and Authentication (Organizational Users)	IA-2 (1) (2) (3) (8) (11) (12)	
IA-3	Device Identification and Authentication	IA-3	
IA-4	Identifier Management	IA-4	

IA-5	Authenticator Management	IA-5 (1) (2) (3) (11)	
IA-6	Authenticator Feedback	IA-6	
IA-7	Cryptographic Module Authentication	IA-7	
IA-8	Identification and Authentication (Non-Organizational Users)	IA-8 (1) (2) (3) (4)	

**Figure 2.6-8. Incident Response (IR) Controls Family**

CNTL NO.	CONTROL NAME	MOD BASELINE	COMMENTS
IR-1	Incident Response Policy and Procedures	IR-1	As for other control families, Lumen's existing commercial and Government security services themselves demand stringent IR controls. EIS Services' IR controls will be built upon Lumen's existing IR policies and approval procedures.
IR-2	Incident Response Training	IR-2	
IR-3	Incident Response Testing	IR-3 (2)	
IR-4	Incident Handling	IR-4 (1)	
IR-5	Incident Monitoring	IR-5 (1)	
IR-6	Incident Reporting	IR-6 (1)	
IR-7	Incident Response Assistance	IR-7 (1)	
IR-8	Incident Response Plan	IR-8	

**Figure 2.6-9. Maintenance (MA) Controls Family**

CNTL NO.	CONTROL NAME	MOD BASELINE	COMMENTS
MA-1	System Maintenance Policy and Procedures	MA-1	EIS Services' MA controls will be built upon Lumen's existing MA policies and approval procedures.
MA-2	Controlled Maintenance	MA-2	
MA-3	Maintenance Tools	MA-3 (1) (2)	
MA-4	Nonlocal Maintenance	MA-4 (2)	
MA-5	Maintenance Personnel	MA-5	
MA-6	Timely Maintenance	MA-6	

**Figure 2.6-10. Media Protection (MP) Controls Family**

CNTL NO.	CONTROL NAME	MOD BASELINE	COMMENTS
MP-1	Media Protection Policy and Procedures	MP-1	EIS Services' MP controls will be built upon Lumen's existing MA policies and approval procedures.
MP-2	Media Access	MP-2	
MP-3	Media Marking	MP-3	
MP-4	Media Storage	MP-4	
MP-5	Media Transport	MP-5 (4)	
MP-6	Media Sanitization	MP-6	
MP-7	Media Use	MP-7 (1)	

**Figure 2.6-11. Physical and Environmental Protection (PE) Controls Family**



CNTL NO.	CONTROL NAME	MOD BASELINE	COMMENTS
PE-1	Physical and Environmental Protection Policy and Procedures	PE-1	EIS Services' PE controls will be built upon Lumen's existing PE policies and approval procedures in place and will take advantage of the controls and capabilities of Lumen data centers.
PE-2	Physical Access Authorizations	PE-2	
PE-3	Physical Access Control	PE-3	
PE-4	Access Control for Transmission Medium	PE-4	
PE-5	Access Control for Output Devices	PE-5	
PE-6	Monitoring Physical Access	PE-6 (1)	
PE-8	Visitor Access Records	PE-8	
PE-9	Power Equipment and Cabling	PE-9	
PE-10	Emergency Shutoff	PE-10	
PE-11	Emergency Power	PE-11	
PE-12	Emergency Lighting	PE-12	
PE-13	Fire Protection	PE-13 (3)	
PE-14	Temperature and Humidity Controls	PE-14	
PE-15	Water Damage Protection	PE-15	
PE-16	Delivery and Removal	PE-16	
PE-17	Alternate Work Site	PE-17	

**Figure 2.6-12. Planning (PL) Controls Family**

CNTL NO.	CONTROL NAME	MOD BASELINE	COMMENTS
PL-1	Security Planning Policy and Procedures	PL-1	All EIS Services benefit from the Lumen product development process that incorporates feedback from all relevant parties, obtains executive support and funding approval, and leverages our internal Architectural Best Practices. The process also includes operations and support organizations, including the security organization, which will establish the planning controls.
PL-2	System Security Plan	PL-2 (3)	
PL-4	Rules of Behavior	PL-4 (1)	
PL-8	Information Security Architecture	PL-8	

**Figure 2.6-13. Personnel Security (PS) Controls Family**

CNTL NO.	CONTROL NAME	MOD BASELINE	COMMENTS
PS-1	Personnel Security Policy and Procedures	PS-1	For its existing security services, Lumen has many PS controls in place and they will serve as the baseline for the EIS
PS-2	Position Risk Designation	PS-2	
PS-3	Personnel Screening	PS-3	

PS-4	Personnel Termination	PS-4	Services PS controls.
PS-5	Personnel Transfer	PS-5	
PS-6	Access Agreements	PS-6	
PS-7	Third-Party Personnel Security	PS-7	
PS-8	Personnel Sanctions	PS-8	

**Figure 2.6-14. Risk Assessment (RA) Controls Family**

CNTL NO.	CONTROL NAME	MOD BASELINE	COMMENTS
RA-1	Risk Assessment Policy and Procedures	RA-1	EIS Services will build upon Lumen's Risk Assessment policies and approval procedures already in place.
RA-2	Security Categorization	RA-2	
RA-3	Risk Assessment	RA-3	
RA-5	Vulnerability Scanning	RA-5 (1) (2) (5)	

**Figure 2.6-15. System and Services Acquisition (SA) Controls Family**

CNTL NO.	CONTROL NAME	MOD BASELINE	COMMENTS
SA-1	System and Services Acquisition Policy and Procedures	SA-1	EIS Services will build upon the systems acquisition policies and budget approval procedures in place for Lumen and a SCRMM plan to meet these controls.
SA-2	Allocation of Resources	SA-2	
SA-3	System Development Lifecycle	SA-3	EIS Services already in place and those to be developed have been or will be designed per the Lumen Product Development Process in which all appropriate parties are included from the inception phase through operation and decommissioning. The security operations and compliance teams are involved, as well as the legal department, procurement and the executive team.
SA-4	Acquisition Process	SA-4 (1) (2) (9) (10)	
SA-5	Information System Documentation	SA-5	
SA-8	Security Engineering Principles	SA-8	Lumen employs Security Engineering principals consistent with a large telecommunications provider and as outlined in NIST SP 800-27. Such principals emphasize support for industry standards, global scale, and deny by default.
SA-9	External Information System Services	SA-9 (2)	
SA-10	Developer Configuration Management	SA-10	
SA-11	Developer Security Testing and Evaluation	SA-11	

**Figure 2.6-16. System and Communications Protection (SC) Controls Family**

CNTL NO.	CONTROL NAME	MOD BASELINE	COMMENTS
SC-1	System and Communications Protection Policy and Procedures	SC-1	As with so many other of the control families, EIS Services' SC controls will build upon Lumen's existing SC policies and approval procedures for our security services for commercial and Government customers. If and where required, FIPS certified cryptography will be used.
SC-2	Application Partitioning	SC-2	
SC-4	Information in Shared Resources	SC-4	
SC-5	Denial of Service Protection	SC-5	
SC-7	Boundary Protection	SC-7 (3) (4) (5) (7)	
SC-8	Transmission Confidentiality and Integrity	SC-8 (1)	
SC-10	Network Disconnect	SC-10	
SC-12	Cryptographic Key Establishment and Management	SC-12	
SC-13	Cryptographic Protection	SC-13	
SC-15	Collaborative Computing Devices	SC-15	
SC-17	Public Key Infrastructure Certificates	SC-17	
SC-18	Mobile Code	SC-18	
SC-19	Voice Over Internet Protocol	SC-19	
SC-20	Secure Name /Address Resolution Service (Authoritative Source)	SC-20	
SC-21	Secure Name /Address Resolution Service (Recursive or Caching Resolver)	SC-21	
SC-22	Architecture and Provisioning for Name/Address Resolution Service	SC-22	
SC-23	Session Authenticity	SC-23	
SC-28	Protection of Information at Rest	SC-28	
SC-39	Process Isolation	SC-39	

**Figure 2.6-17. System and Information Integrity (SI) Controls Family**

CNTL NO.	CONTROL NAME	MOD BASELINE	COMMENTS
SI-1	System and Information Integrity Policy and Procedures	SI-1	EIS Services will Leverage the System Integrity policies and approval procedures in place for Lumen. If and where required, FIPS certified cryptography will be used.
SI-2	Flaw Remediation	SI-2 (2)	
SI-3	Malicious Code Protection	SI-3 (1) (2)	
SI-4	Information System Monitoring	SI-4 (2) (4) (5)	
SI-5	Security Alerts, Advisories, and Directives	SI-5	
SI-7	Software, Firmware, and Information Integrity	SI-7 (1) (7)	
SI-8	Spam Protection	SI-8 (1) (2)	
SI-10	Information Input Validation	SI-10	
SI-11	Error Handling	SI-11	
SI-12	Information Handling and Retention	SI-12	

SI-16	Memory Protection	SI-16	
-------	-------------------	-------	--

NIST SP 800-53 Rev. 4 also defines controls that are independent of any system impact level such as those pertaining to Program Management (**Figure 2.6-18**). Lumen is very well positioned with a strong, security-aware program management organization.

**Figure 2.6-18. Program Management (PM) Controls Family**

CNTL NO.	CONTROL NAME	COMMENTS
PM-1	Information Security Program Plan	Lumen EIS Services have/will have a team of Lumen employees dedicated to the Services' support and success. Teams are tasked with developing the Information Security Program, as well as maintaining the POA&M and managing the interactions with the rest of the Lumen systems and processes.
PM-2	Senior Information Security Officer	
PM-3	Information Security Resources	
PM-4	Plan of Action and Milestones Process	
PM-5	Information System Inventory	
PM-6	Information Security Measures of Performance	
PM-7	Enterprise Architecture	
PM-8	Critical Infrastructure Plan	
PM-9	Risk Management Strategy	
PM-10	Security Authorization Process	
PM-11	Mission/Business Process Definition	
PM-12	Insider Threat Program	
PM-13	Information Security Workforce	
PM-14	Testing, Training, and Monitoring	
PM-15	Contacts with Security Groups and Associations	
PM-16	Threat Awareness Program	

Privacy Controls (**Figure 2.6-19**) are also defined as independent of any system impact level. Again, Lumen is very well positioned with well-established privacy controls that are required across much of our business.

**Figure 2.6-19. Privacy Controls**

ID	PRIVACY CONTROLS	ID	PRIVACY CONTROLS
AP	Authority and Purpose	DM-2	Data Retention and Disposal
AP-1	Authority to Collect	DM-3	Minimization of PII Used in Testing, Training, and Research

ID	PRIVACY CONTROLS	ID	PRIVACY CONTROLS
AP-2	Purpose Specification	IP	<b>Individual Participation and Redress</b>
AR	Accountability, Audit, and Risk Management	IP-1	Consent
AR-1	Governance and Privacy Program	IP-2	Individual Access
AR-2	Privacy Impact and Risk Assessment	IP-3	Redress
AR-3	Privacy Requirements for Contractors and Service Providers	IP-4	Complaint Management
AR-4	Privacy Monitoring and Auditing	SE	<b>Security</b>
AR-5	Privacy Awareness and Training	SE-1	Inventory of Personally Identifiable Information
AR-6	Privacy Reporting	SE-2	Privacy Incident Response
AR-7	Privacy-Enhanced System Design and Development	TR	<b>Transparency</b>
AR-8	Accounting of Disclosures	TR-1	Privacy Notice
DI	<b>Data Quality and Integrity</b>	TR-2	System of Records Notices and Privacy Act Statements
DI-1	Data Quality	TR-3	Dissemination of Privacy Program Information
DI-2	Data Integrity and Data Integrity Board	UL	<b>Use Limitation</b>
DM	<b>Data Minimization and Retention</b>	UL-1	Internal Use
DM-1	Minimization of Personally Identifiable Information	UL-2	Information Sharing with Third Parties

---

### **3.0 MTIPS Risk Management Framework Plan [L.29.3.b, C.2.8.4, C.2.8.4.5, C.2.8.4.5.4]**

## **STEP 1—DEFINE THE SECURITY SYSTEM**

### **TASK 1-1—SECURITY CATEGORIZATION**

The General Services Administration (GSA) assigned an information sensitivity category for Managed Trusted Internet Protocol Service (MTIPS) based on the federal government requirement and Federal Information Processing Standard (FIPS) 199. FIPS 199 requires MTIPS security to safeguard data and information from unauthorized disclosure, protect data from unauthorized modification, and ensure that services are available to meet mission requirements.

Protection ratings are determined for each of these three categories:

- Confidentiality: MTIPS contains information that requires protection from unauthorized disclosure
- Integrity: MTIPS contains information that must be protected from unauthorized, unanticipated, or unintentional modification
- Availability: MTIPS contains information or provides services that must be available on a timely basis to meet mission requirements, or to avoid substantial losses

MTIPS is rated as one of the following:

- High: the loss of confidentiality, integrity, or availability could expect to have a severe or catastrophic adverse effect on organization operations, organizational assets, or individuals
- Moderate: the loss of confidentiality, integrity, or availability could expect to have a serious adverse effect on organizational operations, organizational assets, or individuals

- Low: the loss of confidentiality, integrity, or availability could expect to have limited adverse effect on organizational operations, organizational assets, or individuals

To determine the information types that MTIPS will potentially handle, GSA used National Institute of Standards and Technology (NIST) Special Publication (SP) 800-60 Volume 1 Revision 1, *Guide for Mapping Types of Information and Information Systems to Security Categories*, and Volume 2 Revision 1, *Appendices to Guide for Mapping Types of Information and Information Systems to Security Categories*. Following the Office of Management and Budget’s (OMB) Federal Enterprise Architecture (FEA) Business Reference Model (BRM), GSA determined that the MTIPS business areas will deliver services and manage resources, serving in a supportive role to an agency’s mission but not directly processing any agency mission-based information types.

The information types that MTIPS will potentially handle with associated provisional impact levels, due to loss of any of the three security objectives (confidentiality, integrity, and availability), are shown in **Table 1**. The high watermark method was used to determine the overall information categorization.

**Table 1. MTIPS Information Type Categorization**

Information Type	Confidentiality	Integrity	Availability
Contingency planning	Low	Low	High
Continuity of operations	Low	Low	High
Service recovery	Low	Low	High
Goods acquisition	Low	Moderate	Low
Inventory control	Low	Moderate	Low
Logistics management	Low	Moderate	Low
Services acquisition	Moderate	Moderate	Low
System development	Moderate	Moderate	Low
Life cycle/change management	Low	Moderate	Moderate
System maintenance	High	Moderate	Moderate
Information technology (IT) infrastructure maintenance	High	High	High
MTIPS security	Moderate	Moderate	High
Record retention	Moderate	High	Low

Information management	Moderate	Moderate	Moderate
System and network monitoring	High	High	High
Information sharing	Moderate	Moderate	Moderate
Overall information categorization	High	High	High

As part of the MTIPS system development life cycle (SDLC) and security assessment and authorization (A&A) processes, Lumen periodically reviews the list of information types to add and remove data types, as necessary, and update the impact to the above security objectives.

In summary, the MTIPS overall sensitivity rating is high based on the following:

- Requirements for confidentiality, integrity, and availability protections
- Related level of sensitivity
- Highest magnitude of harm directly resulting from loss, misuse, modification to, or unauthorized access to information on MTIPS

**Information System Owner**

**GSA**

**Name:** Kevin Gallo  
**Title:** GSA System Owner  
**Agency:** GSA  
**Address:** 1800 F Street NW, Washington, DC 20450  
**Email Address:** kevin.gallo@gsa.gov  
**Phone Number:** 703-306-6616

**Lumen**

**Name:** [REDACTED]  
**Title:** [REDACTED]  
**Agency:** [REDACTED]



**General Services Administration (GSA)**  
*Enterprise Infrastructure Solutions (EIS)*

Contract # GS00Q17NSD3006  
Mod #: P00310  
Submission #: CL01001.01a

---

**Address:**

[REDACTED]

**Email Address:**

[REDACTED]

**Phone Number:**

[REDACTED]

---

## TASK 1-2—INFORMATION SYSTEM DESCRIPTION

Lumen MTIPS portals function as OMB-approved multi-agency Trusted Internet Connection Access Provider (TICAP) connection points capable of hosting, managing and correlating multiple independent traffic streams for each subscribing agency. Since 2009, Lumen has maintained its Authority to Operate (ATO) MTIPS with the GSA. The system boundary includes the following components: Trusted Internet Connection (TIC) access points in [REDACTED]

[REDACTED] Lumen complies with the capabilities published by the OMB, as part of the TIC initiative; and participates in the National Cyber Protection System (NCPS) program. The TICAP has a minimum of three qualified people with Top Secret/Sensitive Compartmented Information (TS/SCI) clearance available within two (2) hours, 24x7x365, with authority to report, acknowledge and initiate action based on TS/SCI-level information, including tear line information, with United States Computer Emergency Readiness Team (US-CERT). Authorized personnel with TS/SCI clearances have 24x7x365 access to an Intelligence Community Directive (ICD) 705-accredited Sensitive Compartment Information Facility (SCIF) including the following TS/SCI communications channels: Secure telephone (STE/STU) and card authorized for TS/SCI; and Secure FAX machine.

The Lumen MTIPS system has also passed the Department of Homeland Security (DHS) TIC initiative Cybersecurity Capability Validation (CCV) assessment, annually, since 2009, certifying that Lumen MTIPS meets all necessary criteria according to OMB TIC Initiative in Memorandum M-08-05, announced in November 2007, in support of Homeland Security Presidential Directive (HSPD) 23. HSPD-23 and the Comprehensive National Security Initiative (CNSI) addressed the need to make the United States (U.S.) more secure against cyber threats and established a national strategy to protect the Nation's Information Technology Infrastructure. As a follow-up, OMB Memorandum M-10-28 further defined DHS' responsibility, in coordination with OMB, to certify and

---

enforce agency implementation of network security operational standards and best practices, and to ensure agencies comply with Federal standards and policies. Lumen also supports OMB Memorandum M-08-27 by complying with the capabilities published by OMB as part of the TIC Initiative; and participating in the National Cyber Protection System (NCPS) program. The DHS Federal Network Resilience (FNR) Division's Cybersecurity Assurance Branch (CAB) annually assesses the state of operational readiness and cybersecurity risk of unclassified networks and systems across the Federal Civilian Executive Branch.

MTIPS allows agencies to physically connect to the public Internet or other external connections, as the agency requires, in full compliance with the OMB's TIC initiative (M-08-05). MTIPS facilitates the reduction of the number of Internet connections in government networks and provides standard security services to all government users.

MTIPS has the network infrastructure to transport Internet Protocol (IP) traffic between the agency enterprise wide area network (WAN) and the TIC portal; together they create an agency TIC trusted domain (DMZ) for IP traffic.

MTIPS provides event collection, correlation, and reporting using [REDACTED] [REDACTED] to support the Lumen MTIPS TIC portal connectivity that insulates an agency's internal network from the Internet and other external networks. [REDACTED] devices housed in the Lumen MTIPS TIC portal facility collect log/event data. The Lumen Multiprotocol Label Switching (MPLS) virtual local area network (VLAN) pushes data through the SOC and stores it [REDACTED] infrastructure that is dedicated to MTIPS TIC support. Lumen MTIPS TIC portal connectivity is firewalled off and isolated from other components within the SOC. Lumen cybersecurity analysts and managers access the information and provide event reporting as required.

MTIPS takes a tiered approach to support and incident/event escalation. Tier 1 is the basic level of support and typically the first contact on a call. Tier 2 is comprised of more

---

experienced personnel who handle more complex issues. Tier 3 is comprised of senior engineering personnel who are the subject matter experts (SMEs).

MTIPS enables the government to react more effectively to cybersecurity attacks, reducing malicious penetrations and theft of critical data. An integral MTIPS SOC closely monitors the exchange of information through the TIC portal to protect agency IP traffic.

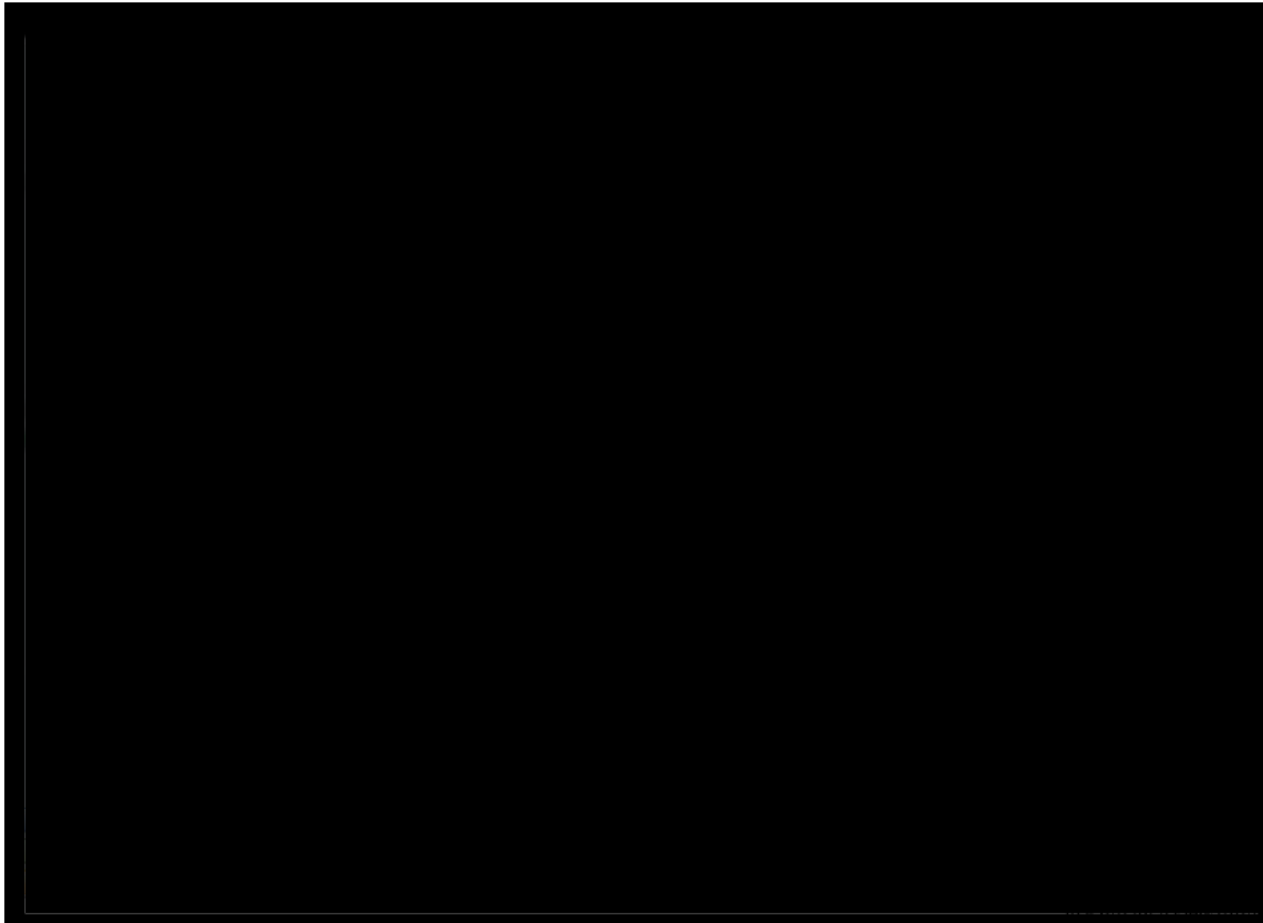
The MTIPS-provided transport will serve as a collection network for TIC portal connectivity to insulate an agency's internal network from the Internet and other external networks.

The TIC portal will function as an OMB-approved multi-service TICAP, capable of hosting multiple agencies and managing and correlating multiple independent traffic streams for each subscribing agency. The TIC portal shall provide security services to multiple clients but allow for specific controls based on agency coordination, when necessary.

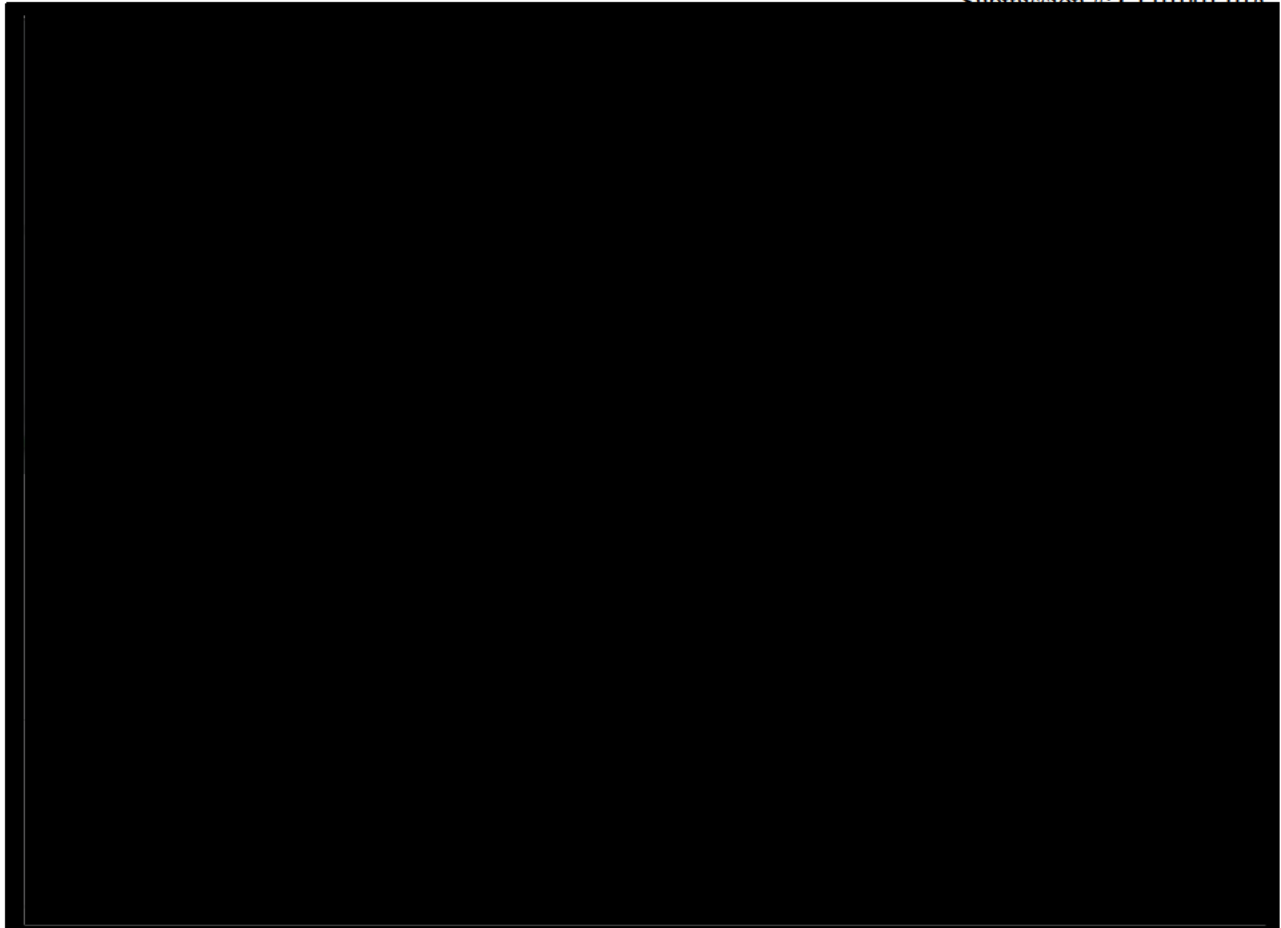
The following figures provide logical and physical details of the MTIPS and SOC sites:

- Depict the MTIPS security A&A boundary (also known as the security assessment boundary as set forth in RFP Section C.2.8.4.5.4(2)).
  - Figure 1. MTIPS 2.0 Standard Portal A&A Boundary
  - Figure 2. MTIPS 2.0 Augment A&A Boundary
- Depict how information is transferred in MTIPS environments
  - Figure 3. MTIPS 2.0 Standard Portal Traffic Flow
  - Figure 4. MTIPS 2.0 Augment Traffic Flow
- Depicts site logical detail and information security systems described within the system environment: Figure 5. SOC Site Logical Detail

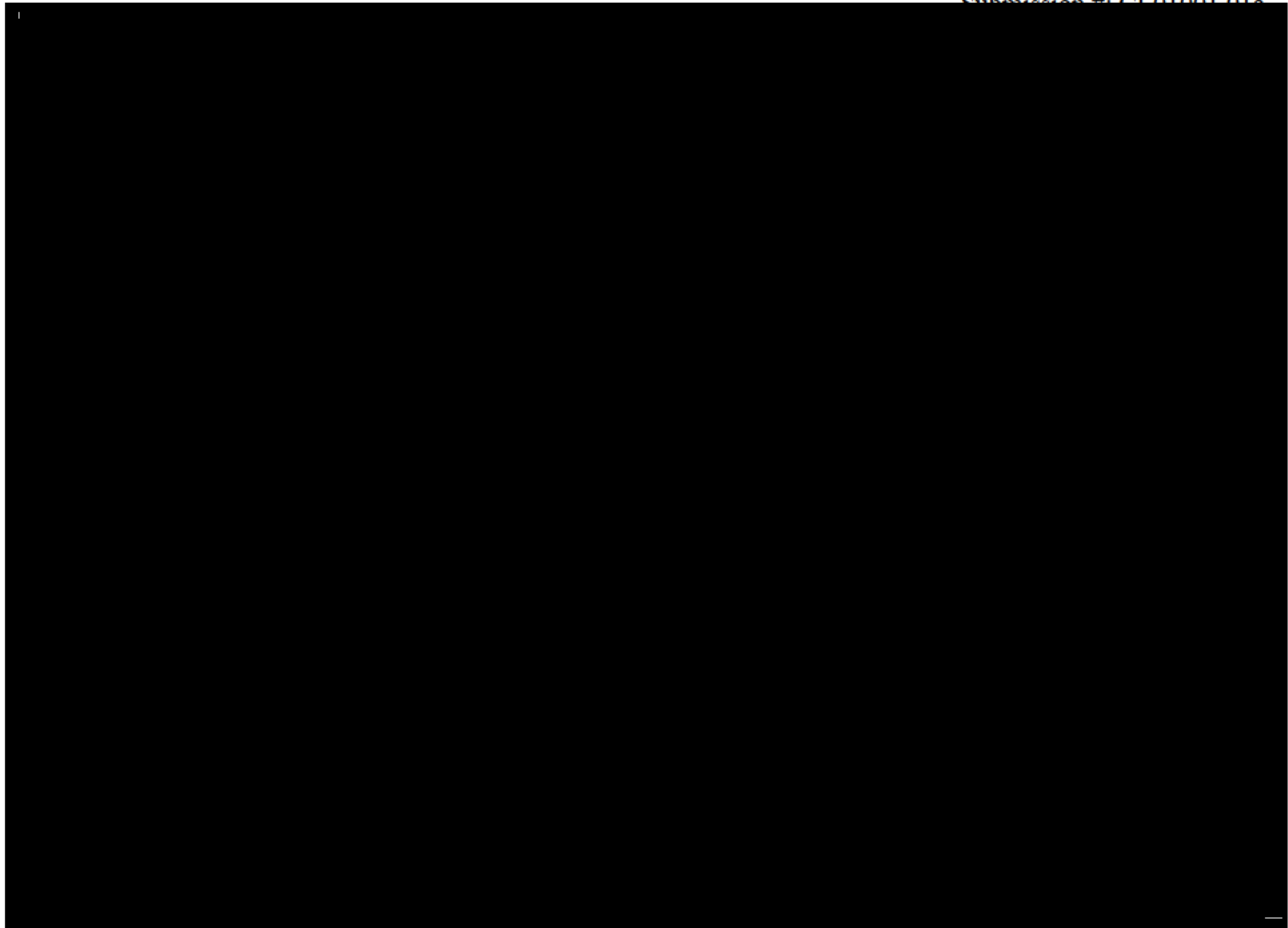
**System Environment**



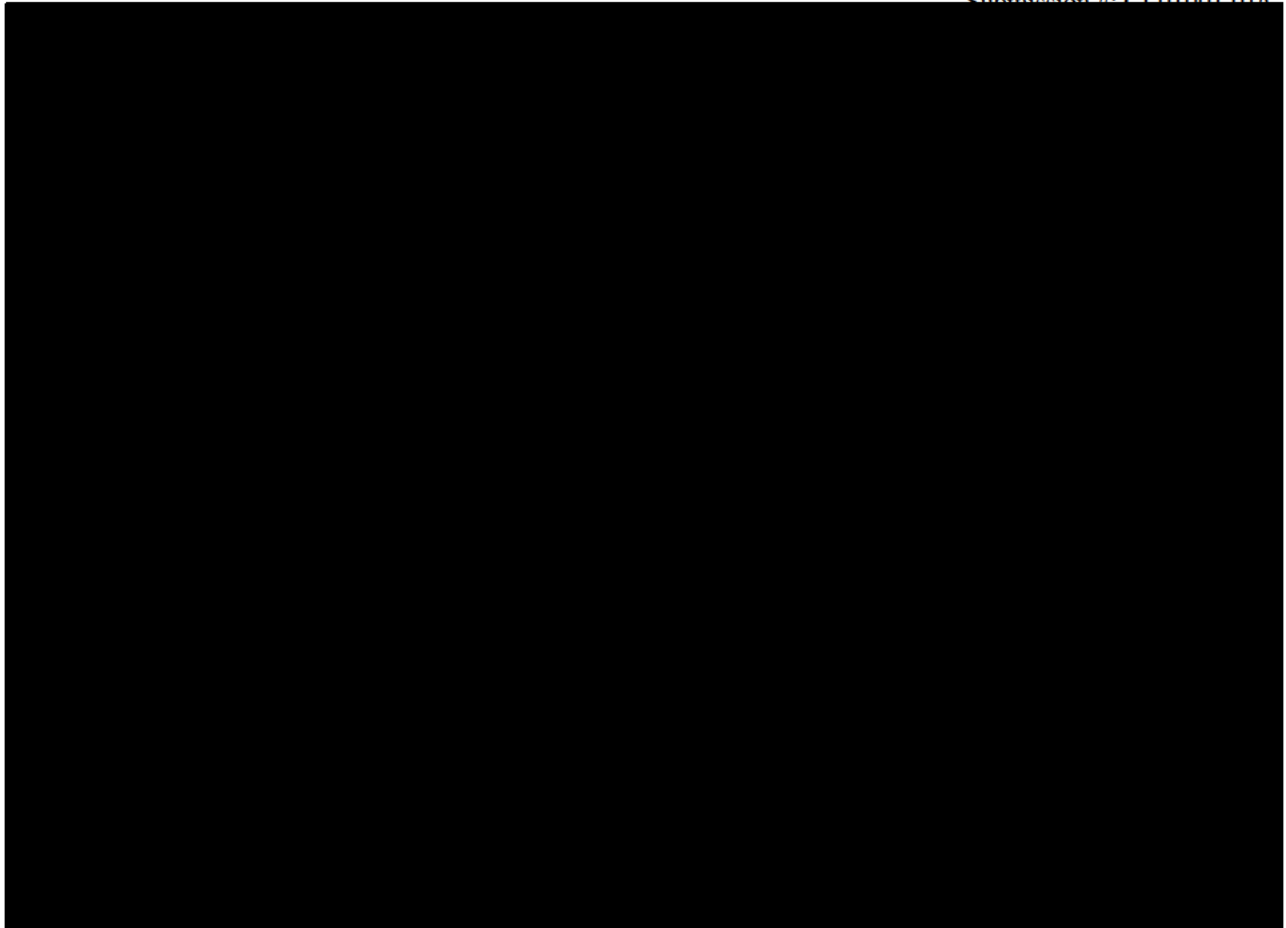
**Figure 1. MTIPS 2.0 Standard Portal A&A Boundary**



**Figure 2. MTIPS 2.0 Augment Portal A&A Boundary**



**Figure 3. MTIPS 2.0 Standard Portal Traffic Flow.**

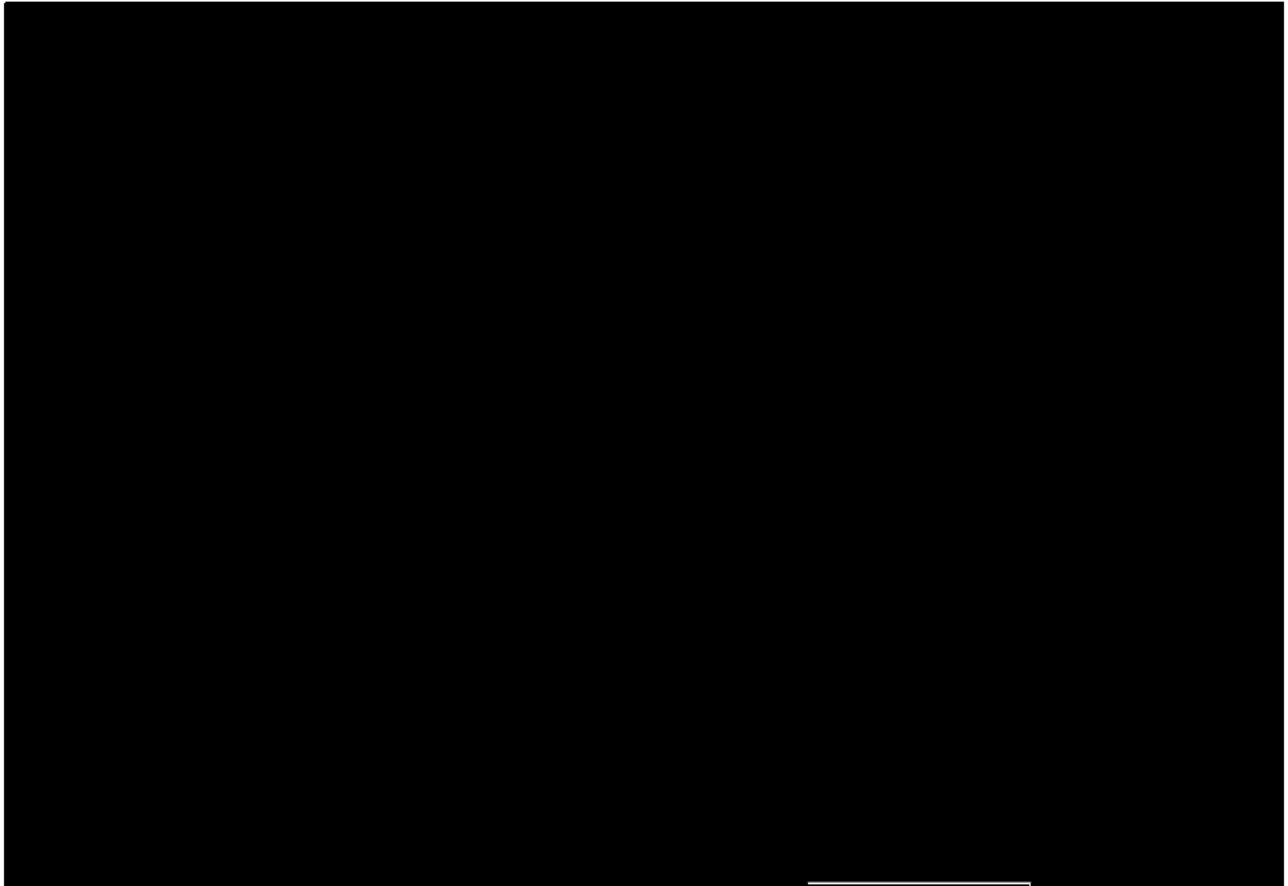


**Figure 4. MTIPS 2.0 Augment Portal Traffic Flow**

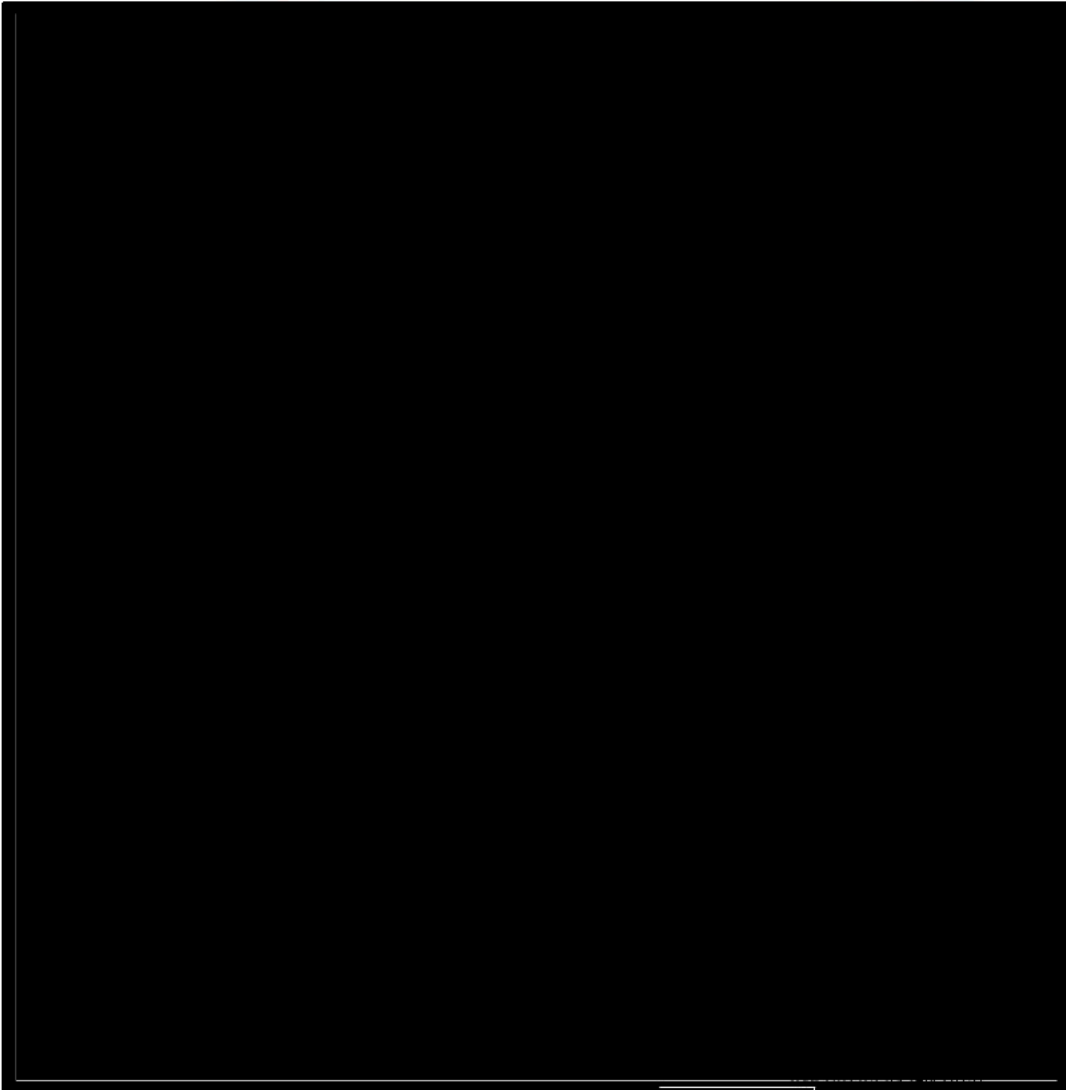




**Figure 5. SOC Site 1 Logical Detail**



**Figure 6. SOC Site 2 Logical Detail**



**Figure 7. Site Physical Detail** [REDACTED]

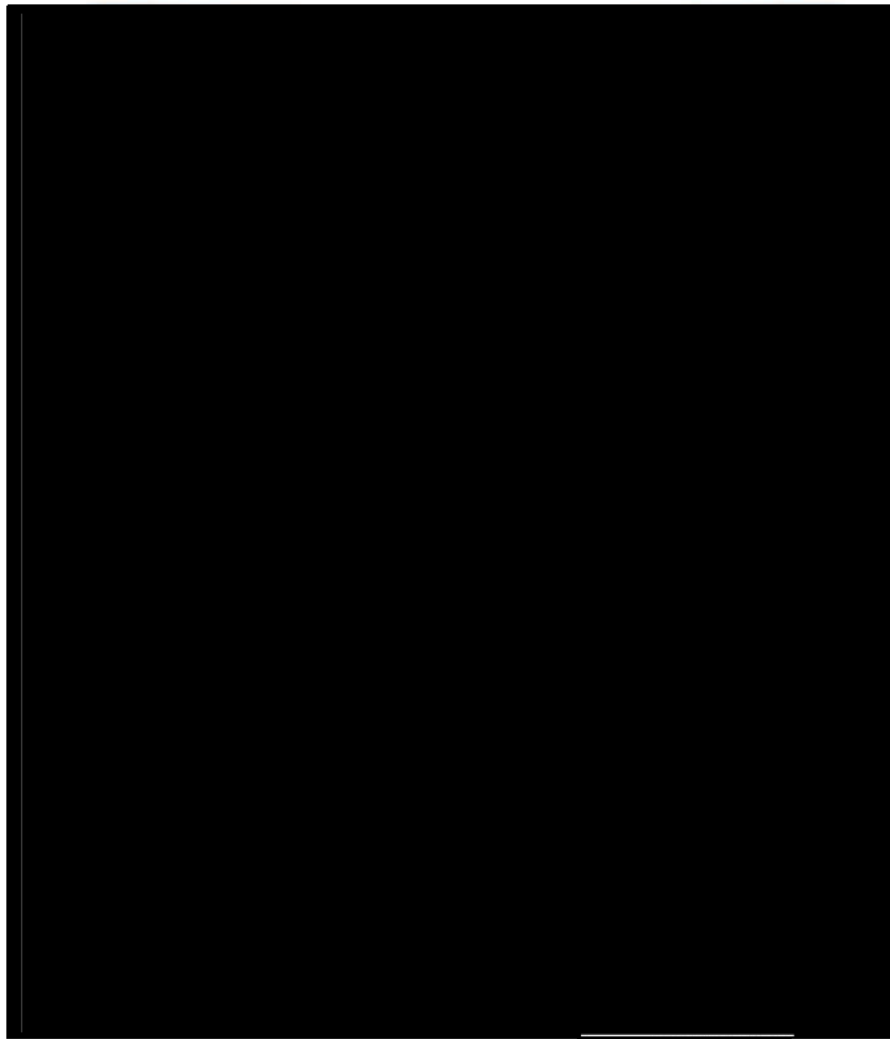


Figure 8. Site Physical Detail [redacted]

[redacted]

MTIPS physical locations:

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

---

MTIPS architecture consists of multi-active connections to security portal functions:

- MFS: managed firewall (FortiNet)
- AVMS: anti-virus management (FortiNet)
- IDPS: intrusion detection and prevention (FortiNet)
- INRS: incident response
- SMEMS: secure managed email (FortiMail)
- VSS: vulnerability scanning (Nessus, AppScan)
- MTSS: managed tiered security
- MEAS: managed e-authentication
- CHS: colocated hosting
- IPS: Internet protocol service

Each MTIPS TIC portal facility contains two portals: an MTIPS 2.0 standard portal for agencies requiring moderate bandwidth services and an MTIPS 2.0 augment portal for customers requiring higher bandwidth services.

The MTIPS architecture is separated into three zones. These zones are designated for purposes of describing the security layers of the A&A boundary (see **Figures 5 & 6**).



Lumen monitors and controls communications at the external boundary of the MTIPS network and key internal boundaries within this network through [REDACTED]



Connections to the Internet, or other external networks or information systems, occur through a managed router with all traffic passing through one or more unified threat management (UTM) firewalls.

[Redacted text block]

[Redacted text block]

[Redacted text block]

[Redacted text block]

[Redacted text block]

[Redacted text block]



---

The authorization boundary includes the resources and components identified in the system description and the accompanying architectural drawings.

### **TASK 1-3—INFORMATION SYSTEM REGISTRATION**

The registration process will begin with the definition of the A&A (or authorization) boundary in the *Security Assessment Boundary and Scope Document (BSD)*, as referenced in RFP Section C.2.8.4.5.4 (2). This section identifies the information system and subsystems in the system inventory and establishes a relationship between the information system and the parent or governing organization that owns, manages, and/or controls the system.

The information system owner has primary responsibility for registering each EIS information system that supports network services and network management systems.

#### **Primary Responsibility:** *Lumen Information System Owner*

**Name:** [REDACTED]  
**Title:** [REDACTED]  
**Agency:** Lumen Technologies Government Solutions, Inc.  
**Address:** 4250 N Fairfax Drive, Arlington, VA 22203  
**Email Address:** [REDACTED]  
**Phone Number:** [REDACTED]

#### **Supporting Roles:** *Lumen Information Systems Security Officer (ISSO)*

**Name:** [REDACTED]  
**Title:** Information System Security Officer (ISSO)  
**Agency:** Lumen Technologies Government Solutions, Inc.  
**Address:** 1 Solutions Pkwy, Town and Country, MO 63017  
**Email Address:** [REDACTED]



---

**Phone Number:** [REDACTED]

*GSA Information System Security Manager (ISSM)*

**Name:** David Trzcinski  
**Title:** Information Systems Security Manager  
**Agency:** GSA  
**Address:** 1800 F Street, NW, Washington, DC 20405  
**Email Address:** [david.trzcinski@gsa.gov](mailto:david.trzcinski@gsa.gov)  
**Phone Number:** 703-306-6354

*GSA ISSO*

**Name:** William Olson  
**Title:** Systems and Security Program Manager  
**Agency:** GSA  
**Address:** 1800 F Street, NW, Washington, DC 20405  
**Email Address:** [william.olson@gsa.gov](mailto:william.olson@gsa.gov)  
**Phone Number:** 703-306-6393

GSA personnel have performed the security categorization of the MTIPS information systems, which are determined to be FIPS 199 high impact.

## **STEP 2—SELECT SECURITY CONTROLS**

### **TASK 2-1—COMMON CONTROL IDENTIFICATION**

Common controls inherited within the MTIPS system authorization boundary will include

- Physical security controls
- Environmental controls

- 
- Centralized authentication mechanisms
    - SecurID
    - Active directory
  - Continuous monitoring systems
    - Log aggregators and alarming systems
    - Centralized configuration control monitoring systems
    - Centralized file integrity monitoring systems
    - Centralized access monitoring systems
    - Network intrusion detection and prevention systems (IDS/IPS)

A team of Lumen personnel, including the information system owner, ISSO, and personnel from network engineering, network operations, IT architecture, IT development, and information assurance (IA) will design common controls, including specific security products, hardware, software, and processes applied within the MTIPS system authorization boundary.

Regarding overall common controls inherited by MTIPS systems and other services provided under the EIS contract, Lumen follows industry-leading information security standards and best practices to ensure the integrity and confidentiality of customer and company information in support of our services. Comprehensive security policies and standards guide these practices which include extensive controls in the areas of personnel, systems, and facility security. Lumen maintains a hierarchy of information security-related policies and standards, using NIST SP 800 series as underlying guidance. Authority for these policies is founded in the Lumen code of conduct (available on the public Internet under our corporate governance page), and the Lumen Board of Directors sponsored and authorized corporate ethics and compliance program. Lumen has a comprehensive physical security program that includes centrally managed exterior and interior card access controls and video surveillance systems that supplement standard facility features, including power backup systems, fire control systems, and physical access controls.

---

Lumen's information security teams develop and maintain processes designed to identify new risks and monitor and respond to known security risks. These processes include both process and technical controls such as:

- IDS/IPS
- DLP systems
- Ongoing security assessment of systems, software, and network environments
- Partnering with audit teams to ensure Lumen systems and processes are in compliance with information security policies and standards

As part of our enterprise security program, Lumen's cyber defense team maintains a centralized cyber incident response process with specific criteria for identifying and responding to events in the operational environment, including customer notification, as appropriate. The cyber incident response process is closely integrated with Lumen's overall disaster preparedness and emergency response programs. In addition to real time event management, specific post-event analysis and continuous-improvement activities are completed for each incident.

Lumen has a fully documented, comprehensive disaster preparedness program, ensuring that all business units have business continuity (BC), disaster recovery (DR) and emergency response plans for all critical functions and processes. These plans are reviewed, updated, and tested on an annual basis to ensure (at a minimum) their effectiveness. Lumen's corporate compliance policy mandates this program while a full-time staff of certified business continuity professionals manages it.

### **Inherited Controls**

Controls inherited within the MTIPS security authentication boundary will include centralized authentication mechanisms:

- SecurID
- Active directory
- Personal digital certificates

- Continuous monitoring systems
  - Log aggregators and alarming systems
  - Centralized configuration control monitoring systems
  - Centralized file integrity monitoring systems
  - Centralized access monitoring systems

Lumen personnel, including the information system owner, ISSO, and personnel from network engineering, network operations, IT architecture, IT development, and IA design and select the specific security products, hardware, software, and processes that are implemented according to the applicable and appropriate security controls.

### Overall Lumen Infrastructure

Securing the overall Lumen infrastructure—whether within corporate environments, customer-facing networks, or the infrastructure that links them—requires collaboration on risk assessment, policies, threat remediation, and implementation of best practices. Information security-related functions are performed in collaboration with Lumen’s operations organizations as follows:

- **Corporate security/(InfoSec):** Provides end-to-end governance, policy making, compliance assurance, risk assessment, vulnerability management, incident response, identity management, and security monitoring.
- **Operations/corporate infrastructure and systems sphere:** Operational teams focus on IT areas, including internal Lumen computing and network components.
- **Operations/customer-facing sphere:** Operational teams provide element access control and security-related response and other functions in both the public-switched telephone network (PSTN) and the transport services area (IP-based, dedicated facilities, Internet service provider (ISP) services, etc.).

Lumen’s security management provides customers with a strong, dedicated partner that understands the security challenges they face. Lumen’s numerous well established security policies, standards, and processes demonstrate our experience.

---

## Process

The following Lumen processes, distributed across the organization, are currently used to identify and manage security risk:

- **Corporate Security:** Maintains comprehensive processes to measure information security risk and manage those risks within acceptable levels through clear policy-setting, assessments, and compliance management.
- **Business continuity planning:** Provides planning efforts, including facilitating the development, testing and training of business continuity and disaster recovery plans to ensure that Lumen and our customers are prepared to effectively manage disaster situations.
- **Vulnerability management:** Maintains a risk inventory, highlighting the risk and potential exposure status for key infrastructure elements, including extensive monitoring and analysis of numerous sources for newly published vulnerabilities. Monitors compliance with Lumen policies and standards, using key industry and international standards as guidance (e.g., International Organization for Standardization (ISO) 2700x, industry associations, or regulating agencies). Lumen conducts ongoing risk assessments of individual systems and network elements. End-to-end system testing is also a normal part of Lumen's security processes.
- **Strategic security planning with hardware and software suppliers:** Reveals risk dependencies between systems and risk pinch points. Establishes strong relationships for vulnerability notification and remediation.
- **Building compliance-based security into Lumen networks:** Records and track risk remediation activity. Collects and collates data about incidents affecting information systems, highlighting root causes and business impact with appropriate follow-up.

---

## **Mechanisms and Controls**

Lumen uses numerous mechanisms and controls in the Lumen network to protect the infrastructure and services:

- Risk management (assessment and mitigation)
- Access control
- Testing
- Mature, formal operational processes including event management
- Anti-spam
- Anti-malicious software (malware)

## **Mechanisms to Ensure Protection of Lumen's Infrastructure**

Logical and physical security measures protect Lumen's network in an in-depth defense approach. These measures include IDS, firewalls and access controls administered through the operations group, and automated access controls on routers, servers, and other network elements in accordance with Lumen information security policies and industry best practices. In addition, Lumen uses procedures outlined in widely accepted security policies and guidelines to protect the network infrastructure.

## **Mechanisms to Provide Security for the Services Offered to Lumen's Customers**

Lumen provides customers with award-winning and industry-recognized products that aid chief information officers (CIOs) in complying with their own audit and risk management requirements. Lumen specifically assists organizations in the following areas:

- Performance and availability management: monitor, manage, and report on service levels, application performance, and systems capacity
- Security management: identify, track, and resolve security incidents in real time
- Operational change control: ensure that changes are properly authorized and tested offline before they are put into production to protect sensitive databases and information

- Configuration and vulnerability management: audit and enforce system compliance with organizational configuration policies
- Authentication, authorization, and accounting (AAA): centralized AAA services enforce strong authentication and a least privilege authorization model
- Best common practices: implement best common security practices from Internet Engineering Task Force (IETF), North American Electric Reliability Corporation (NERC), NIST, and suppliers

### **Customer Service Security Technical Controls**

Lumen offers a variety of technical controls as products to enhance the customer's information security posture:

- Incident response
- Vulnerability scanning
- Managed firewall
- Managed network
- Intrusion detection
- Anti-virus management

### **Tools and Methods**

As part of Lumen's broad security monitoring and risk management program, Lumen has deployed additional IA measures to safeguard critical network backbone services and infrastructure against cyber attacks. These include, but are not limited to, denial-of-service (DoS) attack detection and mitigation, DNS redundancy, pinhole firewalls protecting H.323 and media gateway control protocol (MGCP), protection against Signaling System 7 (SS7) attacks, anti-spoofing mechanisms, and MD5 authentication for routing updates to prevent routing table corruption.

The following tools and methods provide specific protections against cyber attacks:

- **Configuration management controls**

- 
- Network element configurations and software images that conform to suppliers' and industry best common practices and recommendations
  - Configuration management board to review all changes to network elements
  - Element management, network management, operational support, and business support tools and systems all actively managed and each network technology supported by equivalent security practices
  - **User and protocol access controls**
    - Restricted access controls to the management and control planes of the network elements including FIPS 140-2-compliant encryption, and two-factor authentication methods.
    - Rate limiting and blocking of protocols specifically directed to the network elements
    - Restricted access to the management and control planes of network elements permitted only from a small set of trusted sources
    - Core privatization architecture that limits outside visibility to key network elements using MPLS tunneling
    - Deployment of session border controllers for dynamic pinhole firewall controls for signaling and bearer voice over IP (VoIP) traffic on Session Initiation Protocol (SIP), H.323, and MGCP protocols
    - Defense in depth architecture with multiple layers, including firewalls, proxies and rate limiters to protect the SS7 infrastructure from cyber attacks
    - Dynamic routing prefix filtering at all carrier and customer interconnects to prevent accidental or malicious route corruption
  - **IP spoofing prevention measures**
    - Implementation of anti-spoofing technologies on the majority of our edge and border routers to prevent spoofed network attacks from entering the Lumen network
    - Routing protocol message integrity checks using MD5 authentication



- 
- **Comprehensive monitoring and alarming of infrastructure components:**  
Real-time monitoring of network elements with alarm notifications to the Lumen Network Management Center (24/7)
  - **DoS/DDoS monitoring and mitigation measures**
    - DoS and distributed DoS (DDoS) flow monitoring across border routers to provide proactive attack identification and mitigation
    - Lumen and customer-initiated IP address black hole filtering
    - DNS URL blackhole filtering and redirect for mitigation of phishing attacks and malware distribution
    - Monitoring, notification and turndown of malware-infected customers on the public Lumen IP network
    - Network based Layer 3-7 data scrubbing capabilities for DoS/DDoS mitigation
  - **Protection of SS7**
    - The Lumen SS7 network is provisioned using closed, dedicated circuit pathways across physically and geographically diverse transport facilities
    - Message throttling is accomplished using standard ANSI and Telcordia SS7 congestion control mechanisms
    - All SS7 connections to external SS7 networks use SS7 gateways
    - All incoming messages are screened for proper origination, destination and service indicator (type)
  - **In-depth certification testing**
    - Comprehensive hardening, testing, and ongoing auditing of network elements including routers, switches and servers.
  - **Robustness and failover of IP traffic and backbone services.**
    - Sub-50ms failover provided on the Lumen IP backbone using MPLS fast reroute and on the Lumen domestic private line network using Synchronous Optical Network (SONET) four-fiber bi-directional switched rings

- 
- Two independent recursive DNS anycast systems that provide a highly geographically redundant DNS service
  - Redundant router and circuit links in each point of presence (POP)
  - Enhanced backbone traffic separation for different risk domains

### **Lumen Enterprise Malware Protection**

Lumen actively manages virus protection and anti-malware controls. Lumen standards cover all Lumen computing assets and apply to all employees, contractors and suppliers who are responsible for operating, installing, deploying, or administering computing systems within Lumen. Lumen has implemented a comprehensive anti-virus and anti-spam posture within its infrastructure. Mandatory controls at multiple levels (including email, desktop and server) are implemented and constantly updated. These controls, coupled with a formal incident response process, create an environment in which impact on Lumen operations by malware events is extremely rare. Over 99 percent of the spam directed to the Lumen domain is blocked.

### **Lumen Cyber Incident Response Team (CIRT)**

Lumen maintains a corporate-level CIRT and corresponding processes. These processes incorporate specific criteria and procedures for engaging operational groups and escalation to Lumen's corporate-level emergency response team. Specific event criteria define Lumen senior management engagement. An assessment is made for internal and external communication to various customers, critical infrastructure and national security information-sharing groups, and other external communication points. Once the risk exposure is remediated (or mitigation is in place), the CIRT and security management meet to ascertain the depth to which the system may have been breached and what, if any, customer data may have been exposed; determine any employee compliance findings; perform a gap analysis; and determine follow-up steps to ensure continuous process improvement. Key stakeholders are advised of the outcome, and any follow-up, including notifications and communications, are tracked to completion.

---

## **Security Enhancements**

Lumen takes a lead role in developing standards, working with suppliers to implement new, innovative approaches that improve our products, including security services. Lumen maintains relationships with key network equipment suppliers to create a dialogue on best security practices and new feature development and maintains membership and participation in a variety of industry and standards forums. Examples of network security enhancements are given below.

### **Enhancements to Privatization of Network**

Lumen deployed a set of tools and portals that allow customers to check connectivity through our MPLS network.

### **DoS/DDoS Data-Scrubbing Technologies**

For select customers, Lumen implements IP data scrubbing, a mechanism that reduces the effect of DoS/DDoS attacks. The mechanism redirects traffic to data scrubbers, which drop the attack traffic and tunnel the clean traffic to the proper customer locations. Data scrubbing can be provided as a service for an individual customer agency or as a service shared among customer agencies. It can be implemented inside and/or outside Lumen's TIC gateways. Lumen will continue to monitor the industry for DDoS solutions or alternatives to eliminate jitter and latency as a result of DDoS prevention technology.

### **Black Hole Filtering**

For select customers and high-visibility events, Lumen implements IP data scrubbing, a mechanism that effectively reduces the effect of DoS/DDoS attacks. The mechanism redirects traffic to data scrubbers, which drop the attack traffic and tunnel the clean traffic to the proper customer locations. Data scrubbing can be provided as a service for an individual customer agency or as a service shared among customer agencies. It can be implemented inside and/or outside Lumen's TIC gateways.

---

Lumen strongly implements destination black hole filtering, including customer-initiated remote destination black hole filtering, where customers can proactively inject Border Gateway Protocol (BGP) routes into Lumen-managed IP routers outside of their gateways. Targeted bad traffic is then dropped in the Lumen backbone and never reaches customer gateways.

**BGP Flowspec Deployment**

[Redacted]

**Generic Time-to-Live (TTL) Security Enhancement**

Lumen works with IETF and other standards bodies to encourage suppliers to support the TTL security enhancements.

**MD5 Service Authentication**

Lumen uses TTL security enhancements and other configuration options to mitigate DoS attack methods related to MD5 authentication.

[Redacted]

[REDACTED]

**TASK 2-2—SECURITY CONTROL SELECTION**

Select the security controls for the information system and document the controls in the security plan.

A team of Lumen personnel, including the information system owner, ISSO, and personnel from network engineering, network operations, IT architecture, IT development, and IA, design and select specific security products, hardware, software, and processes. Controls will be based on NIST SP 800-53 Rev 4, at the FIPS 199 security impact level (high impact) determined by GSA.

**TASK 2-3—MONITORING STRATEGY**

IDS/IPS is deployed throughout our national and international networks at inside and outside locations across the Lumen network boundary, as well as at strategic locations within corporate networks. Sensors report to centralized security information and event management (SIEM) systems, which the MTIPS network and SOC, NOC, and Lumen’s corporate cyber defense teams manage and monitor.

Automated, continuous monitoring of EIS systems is centralized in SIEM systems for access monitoring, file integrity monitoring, and configuration monitoring. Monitoring

---

detects potential unauthorized use of systems. Network traffic for malware signatures or unusual behavior

- Successful and unsuccessful access attempts Unauthorized changes to configuration files, security-related files, and other files that should not change except during a software release or system maintenance activity
- Devices that appear on the network or drop from the network (automated inventory monitoring)
- Security vulnerability scanning

Certain activities trigger alerts within the SIEM systems and network elements at network borders:

- Series of unsuccessful access attempts
- Unauthorized or unexpected changes in configuration files
- Unexpected changes to inventory (automated inventory monitoring)
- Traffic that matches known malware signatures
- Traffic that matches known malware behavior
- DoS attacks

## Access Monitoring

The continuous monitoring process includes all operating systems that report successful and unsuccessful access attempts, and MTIPS SOC management and monitoring of other operating system activity to [REDACTED] log aggregation/correlation and alerting system. Access monitoring in the FedNOC environment is centralized in a Tripwire log center system.

## File Integrity and Configuration Monitoring

The continuous monitoring process includes all FedNOC systems reporting to a centralized Tripwire Log Center instance that monitors for unauthorized changes to configuration files and other files that should not change except during a software release or operating system maintenance activity.

Lumen's managed security services staff monitors for alerts regarding changes and compares them to active service tickets to ensure that the changes were planned and expected. Changes that occur without applicable service tickets trigger notifications to Lumen's Network IA group.

File integrity and configuration monitoring in the SOC management network is performed using [REDACTED]. Lumen maintains System Configuration Settings utilizing centralized configuration management systems (see RFP Section C.2.8.4.5.4 (14)). Our system configuration settings policy will be included in the Configuration Management Plan and will be updated on an annual basis.

## Network Monitoring

Network monitoring systems are deployed within the MTIPS SOC and FedNOC environments to look for anomalous traffic that could signal network performance issues, malware, and unauthorized behavior on the network.

Network monitoring systems are also deployed at inside and outside locations across the Lumen network boundary and at strategic locations within the corporate network and our national networks. Lumen's cyber incident response team manages and monitors the IDS systems report to the SIEM.

## Automated Inventory Monitoring

Lumen's managed security services staff implement port up/down monitoring on MTIPS routers and switches. As devices are added to or dropped from the network, the Tripwire log center instance sends and raises alerts.

## Real-Time Alerts

FedNOC and SOC MTIPS-supporting systems provide near real time alerts when the following indications of actual or potential compromise occur:

- Protected system files or directories have been modified without notification from the appropriate change/configuration management channels

- 
- System performance indicates resource consumption that is inconsistent with expected operating conditions
  - Audit or log records have been deleted or modified without explanation
  - The system is raising alerts or faults in a manner that indicates the presence of an abnormal condition (syslog information is sent remotely to a centralized SIEM)
  - The system reports failed logins or password changes for administrative or key service accounts
  - Processes and services are running that are outside of the baseline system profile
  - Utilities, tools, or scripts have been saved or installed on production systems without clear indication of their use or purpose

Lumen's network operations and CIRTs manage and monitor SIEMs that aggregate and correlate input from firewalls, gateways, switches, routers, and IDS, in addition to the specific EIS systems.

Lumen's SOC and our cyber defense organization investigate alerts. Investigations are documented as security incidents in the incident tracking tools. Monitoring tools, engineers' discovery through network monitoring, or notifications or questions from customers, business partners, or internal organizations can trigger incident investigations following an alert.

### **Security Vulnerability Scanning**

Lumen performs authenticated security vulnerability scans of MTIPS systems, databases, and web applications at least quarterly, and typically every week. Additional scans are manually performed in test environments and in production to examine recent updates and patches when new, critical vulnerability alerts are released.

### **Security Penetration Testing (C.2.8.4.5.4 (20, 22))**

Lumen annually engages an independent firm to conduct an assessment of the security controls in MTIPS environments and to perform detailed internal and external



---

penetration tests of the system. The resulting Internal and External Independent Penetration Test Reports are integrated into our continuous monitoring programs.

### **Government Assessment/Testing (C.2.8.4.5.4 (22))**

We will continue to allow GSA employees (or GSA-designated third-party contractors) to conduct security A&A activities to include control reviews in accordance with NIST SP 800-53 R4/800-53A R4 and GSA IT Security Procedural Guide 06-30, “Managing Enterprise Risk.” Such activities can include, but are not limited to, operating system vulnerability scanning, web application scanning, and database scanning of applicable systems that support the processing, transportation, storage, or security of government information. GSA’s security scans may run unauthenticated or be configured to use authentication credentials of a user with elevated privileges.

### **TASK 2-4—SECURITY PLAN APPROVAL**

Lumen’s ISSO and Information Security System Manager (ISSM) review the system security plan and its attachments before submitting them to GSA’s ISSO for review and approval, which ultimately includes a GSA authorizing official or designated representative.

Security controls applied to MTIPS systems subject to Federal Information Security Management Act (FISMA) requirements are itemized according to control type (specific, hybrid, or common) in their respective system security plans. Lumen’s risk assessment processes inform and guide security control selection processes to achieve the necessary level of security and compliance for MTIPS.

## **STEP 3—IMPLEMENT SECURITY CONTROLS**

### **TASK 3-1—SECURITY CONTROL IMPLEMENTATION**

**Implement the security controls specified in the security plan.**

Appropriate teams across diverse platforms implement security platforms, including national networks, corporate networks, customer networks, IT systems, databases, and applications. Lumen’s IA staff connects with each team, communicates security

requirements, and facilitates implementations. IA staff also integrates with service providers to ensure security compliance across provider-managed systems.

[REDACTED]

### **Lumen’s Continuous Monitoring Strategy**

Lumen employs a comprehensive continuous monitoring strategy:

- Security vulnerability scanning is performed across operating systems, databases, and web applications, in both authenticated and non-authenticated modes to provide a complete view.
- Security penetration testing: Independent third-party security firms are used to provide additional security assessments and penetration testing of Lumen systems.
- Access monitoring: Centralized logging and alerting systems are used to monitor access attempts to systems, databases, and applications, activating alerts for unusual behavior such as a series of unsuccessful login attempts or attempts to gain privileged access through an unauthorized channel.
- Configuration monitoring and file integrity monitoring: Agents such as Tripwire monitor configuration and application files where applicable, sending alerts to centralized SIEM monitoring and alerting systems. Other agents monitor configuration parameters and report noncompliance with baseline configurations to centralized configuration management systems. Configurations of network elements (e.g., firewalls, routers, switches, and load balancers) are monitored

---

and controlled through network-specific centralized configuration management systems.

- Network monitoring: Lumen uses network IDS/IPS deployed throughout our national and international networks, at locations inside and outside the Lumen network boundary and at strategic locations within corporate and customer networks. Both our network security management and Lumen cyber defense teams manage and monitor sensor reports to centralized SIEM systems.
- DLP: Lumen incorporates DLP systems into its network perimeter architecture, monitoring data entering and leaving corporate networks for unauthorized content.

## **TASK 3-2—SECURITY CONTROL DOCUMENTATION**

IA personnel document security control implementations in the system security plan and supporting documentation. Operations teams provide artifacts (i.e., documentation deliverables) to demonstrate security compliance on systems they manage. IA personnel assemble artifacts for audit and assessment purposes. Security control documentation will be provided to GSA as itemized in Task 5-2.

## **STEP 4—ASSESS SECURITY CONTROLS**

### **TASK 4-1—ASSESSMENT PREPARATION**

**Develop, review, and approve a plan to assess the security controls.**

Lumen's IA team continually assesses the system's security with help from our cyber defense team, NOC/SOC personnel, and subcontractors such as security penetration testing firms. Those same teams coordinate to prepare for outside assessments, such as periodic authorization to operate assessments performed by GSA, since 2009.

---

## **TASK 4-2—SECURITY CONTROL ASSESSMENT**

**Assess the security controls in accordance with procedures defined in the security assessment plan.**

Our IA, SOC, and corporate cyber defense teams, internally assess security controls on Lumen systems, in addition to government systems that receive periodic security assessments from our government customers and independent third party assessment firms. Each year, the DHS Cybersecurity Assurance Branch (CAB) assesses «longname»'s compliance with the TIC Initiative. The GSA's Security Services Division reviews and assesses Lumen's MTIPS Security Systems through quarterly and annual deliverables, as well as initial and three year ATO assessments. Commercial customers and business partners also perform security audits of services provided to them, and our overall corporate security program.

## **TASK 4-3—SECURITY ASSESSMENT REPORT (C.2.8.4.5.4 (19))**

Security assessment details are provided in quarterly plans of action and milestones (POA&Ms) that are delivered to government customers quarterly. Raw reports of security vulnerability scans and penetration test reports are included. Scans include all networking components that fall within the security accreditation boundary. The appropriate vulnerability scans are submitted with the initial security A&A package. An annual information system user certification/authorization review is annotated on the POA&M.

## **TASK 4-4—REMEDIATION ACTIONS**

In the event of security vulnerabilities or weaknesses, IA personnel open service tickets and are directed to the appropriate engineering or operations groups. The ticketing system tracks the testing, implementation, and resolution of the findings. Security vulnerability scans or other applicable methods verify any resolutions.

---

## **STEP 5—AUTHORIZE INFORMATION SYSTEM**

### **TASK 5-1—PLAN OF ACTION AND MILESTONES**

IA personnel prepare quarterly POA&Ms for delivery to GSA.

### **TASK 5-2—SECURITY AUTHORIZATION PACKAGE (C.2.8.4.5.3, C.2.8.4.5.4 (1 THROUGH 27))**

Lumen develops and maintains the necessary documentation required for maintain the ATO. IA personnel produce the security A&A package and submit it to the appropriate authorizing official for adjudication.

The typical security A&A package and deliverables include the following:

- Security Assessment Boundary (aka Security Authorization Boundary) and Scope Document (BSD) (C.2.8.4.5.4 (2))
- System Security Plan (SSP) (C.2.8.4.5.4 (1))
- Rules of Behavior (RoB) (C.2.8.4.5.4 (6))
- Privacy Impact Assessment (PIA) (C.2.8.4.5.4 (11))
- 800-53 Control Tailoring Workbook (CTW) (C.2.8.4.5.4 (4))
- 800-53 Control Summary Table (C.2.8.4.5.4 (5))
- System Inventory (hardware, software, and related information) (C.2.8.4.5.4 (7))
- Security Incident Response Plan (IRP) (C.2.8.4.5.4 (15))
- Security Incident Response Test Plan
- Security Incident Response Test Report (C.2.8.4.5.4 (16))
- Supply Chain Risk Management (SCRM) Plan ((C.2.8.4.5.4 (17))
- Contingency Plan (CP), including the Disaster Recovery Plan (DRP) and Business Impact Assessment (BIA) (C.2.8.4.5.4 (8))
- Contingency Plan Test Plan (CPTP) (C.2.8.4.5.4 (9))
- Contingency Plan Test Report (CPTPR) (C.2.8.4.5.4 (10))

- 
- Interconnection Security Agreements (ISA) (C.2.8.4.5.4 (3))
  - Configuration Management Plan (CMP) (C.2.8.4.5.4 (12))
  - Systems Baseline Configuration Standard Document (C.2.8.4.5.4 (13))
  - Audit Monitoring Program
  - Continuous Monitoring Program (security risk mitigation) (C.2.8.4.5.4 (18))
    - Access monitoring
    - Configuration Monitoring
    - Vulnerability Monitoring (Scanning)
    - Third-Party Penetration Test Report
    - Automated reporting to customer (if customer is prepared for it)
  - Continuous Monitoring Plan
  - e-Authentication documents
    - e-Authentication Executive Summary
    - e-Authentication Detail Report
    - e-Authentication Risk and Requirements Assessment Tool (database file)
  - Independent External Penetration Test and Report (C.2.8.4.5.4 (20))
  - User Access Authorization and Management Process
  - Personnel Security Procedures
  - Suitability Report (employee background investigation report)
  - Security Test and Evaluation Plan (ST&E Plan)
  - Security Test and Evaluation Report (ST&E Report) or Security Assessment Report (SAR) (C.2.8.4.5.4 (6))
  - Annual FISMA Assessment (conducted per GSA CIO IT Security Procedural Guide 04-26, “FISMA Implementation.”) (C.2.8.4.5.4 (25))

---

In addition to the items above that are already included in our security A&A package or as deliverables, Lumen will include the following in its EIS MTIPS security A&A package or provide as deliverables:

- Code Review Report (if applicable) (C.2.8.4.5.4 (21))
- Monthly Reports on SCAP Common Configuration Enumerations (CCE) (NIST SP 800-53 R4: CM-6) (C.2.8.4.5.4 (26))

Monthly Reports on SCAP Common Platform Enumeration (CPE) (NIST SP 800-53 R4: CM-8) (C.2.8.4.5.4 (26))

- Monthly Reports on SCAP Common Vulnerabilities and Exposures (CVE) (NIST SP 800-53 R4: CM-8) (C.2.8.4.5.4 (26))
- Independent Internal Penetration Test and Report (C.2.8.4.5.4 (20))

#### **Document Management (C.2.8.4.5.4 (27))**

Lumen develops and maintains all current policy and procedure documents, as outlined in the specified NIST documents and applicable GSA IT Security Procedural Guides. For EIS, they will be verified and reviewed during the initial security assessment, and updates will be provided to the GSA Contracting Officer's Representative (COR)/ISSO/ISSM biennially to include the following.

- Access Control Policy and Procedures (NIST SP 800-53 R4: AC-1)
- Security Awareness and Training Policy and Procedures (NIST SP 800-53 R4: AT-1)
- Audit and Accountability Policy and Procedures (NIST SP 800-53 R4: AU-1)
- Security Assessment and Authorization Policies and Procedures (NIST SP 800-53 R4: CA-1)
- Configuration and Management Policy and Procedures (NIST SP 800-53 R4: CM-1)
- Contingency Planning Policy and Procedures (NIST SP 800-53 R4: CP-1)

- 
- Identification and Authentication Policy and Procedures (NIST SP 800-53 R4: IA-1)
  - Incident Response Policy and Procedures (NIST SP 800-53 R4: IR-1)
  - System Maintenance Policy and Procedures (NIST SP 800-53 R4: MA-1)
  - Media Protection Policy and Procedures (NIST SP 800-53 R4: MP-1)
  - Physical and Environmental Policy and Procedures (NIST SP 800-53 R4: PE-1)
  - Security Planning Policy and Procedures (NIST SP 800-53 R4: PL-1)
  - Personnel Security Policy and Procedures (NIST SP 800-53 R4: PS-1)
  - Risk Assessment Policy and Procedures (NISTSP 800-53 R4: RA-1)
  - Systems and Services Acquisition Policy and Procedures (NIST SP 800-53 R4: SA-1)
  - System and Communication Protection Policy and Procedures (NIST SP 800-53 R4: SC-1)
  - System and Information Integrity Policy and Procedures (NIST SP 800-53 R4: SI-1)

### **TASK 5-3—RISK DETERMINATION**

System risk is assessed for newly proposed systems and changes to existing systems. Lumen change management standard operating procedures provide detailed processes and procedures to identify, review, approve, and implement change requests to systems and operational baselines. At a high level, the change control processes consist of the following basic steps:

- Identify and classify a change to system architecture
- Evaluate what components in the current configuration need to be changed
- Test or model the impact of the change upon the current system or network
- Implement the change if it is approved



---

Lumen's configuration control boards (CCBs) are committees that coordinate and provide oversight of changes to system architecture and changes that could impact the security of systems or operations. The scope includes additions and removals of hardware and software, configuration changes, and process changes related to specific system environments.

Lumen's information security teams develop and maintain processes designed to identify new risks and monitor and respond to known security risks. These processes include both process and technical controls:

- IDS/IPS
- DLP systems
- Ongoing security assessment of systems, software, and network environments
- Partnering with audit teams to ensure Lumen systems and processes are in compliance with information security policies and standards

## **TASK 5-4—RISK ACCEPTANCE**

When a specific security vulnerability or finding cannot be completely resolved without compensating controls or mitigating controls, IA personnel author an acceptance of risk request and submit it to the customer's ISSO for an authorizing official's assessment and an exception decision.

## **STEP 6—MONITOR SECURITY CONTROLS**

### **TASK 6-1—INFORMATION SYSTEM AND ENVIRONMENT CHANGES**

**Determine the security impact of proposed or actual changes to the information system and its environment of operation.**

The applicable Change Control Board addresses changes proposed for a government system before implementation. A proposal for a significant change in architecture or operations prompts a formal Security Risk Assessment that documents the potential impacts and benefits of the change.

---

Detailed changes to configurations of systems and network elements go through formalized, documented change management processes that control which changes can be made and when. These processes ensure that the appropriate personnel review each proposed change and minimize the chance for a negative outcome.

## **TASK 6-2—ONGOING SECURITY CONTROL ASSESSMENTS**

Security controls are assessed on a continual basis, with weekly security vulnerability scans of operating systems, databases, and web applications.

The Lumen Chief Technology Officer (CTO) for new products and services ensures network elements are rigorously evaluated prior to use in our networks. This includes extensive security testing based on suppliers' implementations of requirements in IETF rfc3871, specifically developed for the technologies incorporated in each platform.

Once a system has been deployed, patch management, ongoing monitoring, and security testing of new features key security prevention measures.

Additionally, Lumen depends on third-party certification services such as NSS labs, ICSA, UC APL, Common Criteria, FIPS, and VB antispam testing.

[http://www.fortinet.com/resource\\_center/whitepapers/nss\\_labs\\_firewall\\_product\\_analysis.html](http://www.fortinet.com/resource_center/whitepapers/nss_labs_firewall_product_analysis.html)

[http://www.fortinet.com/aboutus/fortinet\\_advantages/certifications.html](http://www.fortinet.com/aboutus/fortinet_advantages/certifications.html)

Vulnerability management practices maintain a risk inventory, highlighting the risk and potential exposure status for key infrastructure elements including extensive monitoring and analysis of numerous sources for newly-published vulnerabilities. We monitor compliance with Lumen policies and standards along with key industry and international standards used as underlying guidance (e.g., International Organization for Standardization (ISO) 17799, industry associations or regulating agencies). Security controls are assessed on a continual basis, with weekly security vulnerability scans of operating systems, databases, and web applications. End-to-end system testing is also a normal part of Lumen's security processes.

---

### **TASK 6-3—ONGOING REMEDIATION ACTIONS (C.2.8.4.5.4 (24))**

Remediation actions are initiated as soon as security vulnerabilities are known. Actions are typically initiated with service tickets assigned to the appropriate management team.

Lumen will mitigate all security risks found during the security A&A and continuous monitoring activities. All critical and high-risk vulnerabilities will be mitigated within 30 days and all moderate risk vulnerabilities will be mitigated within 90 days from the date vulnerabilities are formally identified. Updates on the status of all critical and high vulnerabilities that have not been closed within 30 days will be provided on a monthly basis.

### **TASK 6-4—KEY UPDATES**

System security plans and supporting documents are updated as systems evolve, and they are included with quarterly POA&Ms as appropriate.

### **TASK 6-5—SECURITY STATUS REPORTING**

The security status of each information system is reported to the authorizing official and customer ISSO on a quarterly basis through the POA&M and supporting documentation. More continuous security status reporting and automated, continuous security monitoring data streams are provided to government customers in accordance with their prescribed monitoring strategy.

### **TASK 6-6—ONGOING RISK DETERMINATION AND ACCEPTANCE**

Authorizing officials review the reported security status of information systems on an ongoing basis in accordance with the monitoring strategy to determine whether the risk to organizational operations, organizational assets, individuals, other organizations, and the nation remains acceptable.

---

**TASK 6-7—INFORMATION SYSTEM REMOVAL AND DECOMMISSIONING**

Lumen follows a system-removal and decommissioning policy and procedures that ensure all data are securely erased or destroyed before storage elements leave Lumen premises.