Technical-Original

TECHNICAL PROPOSAL FOR:

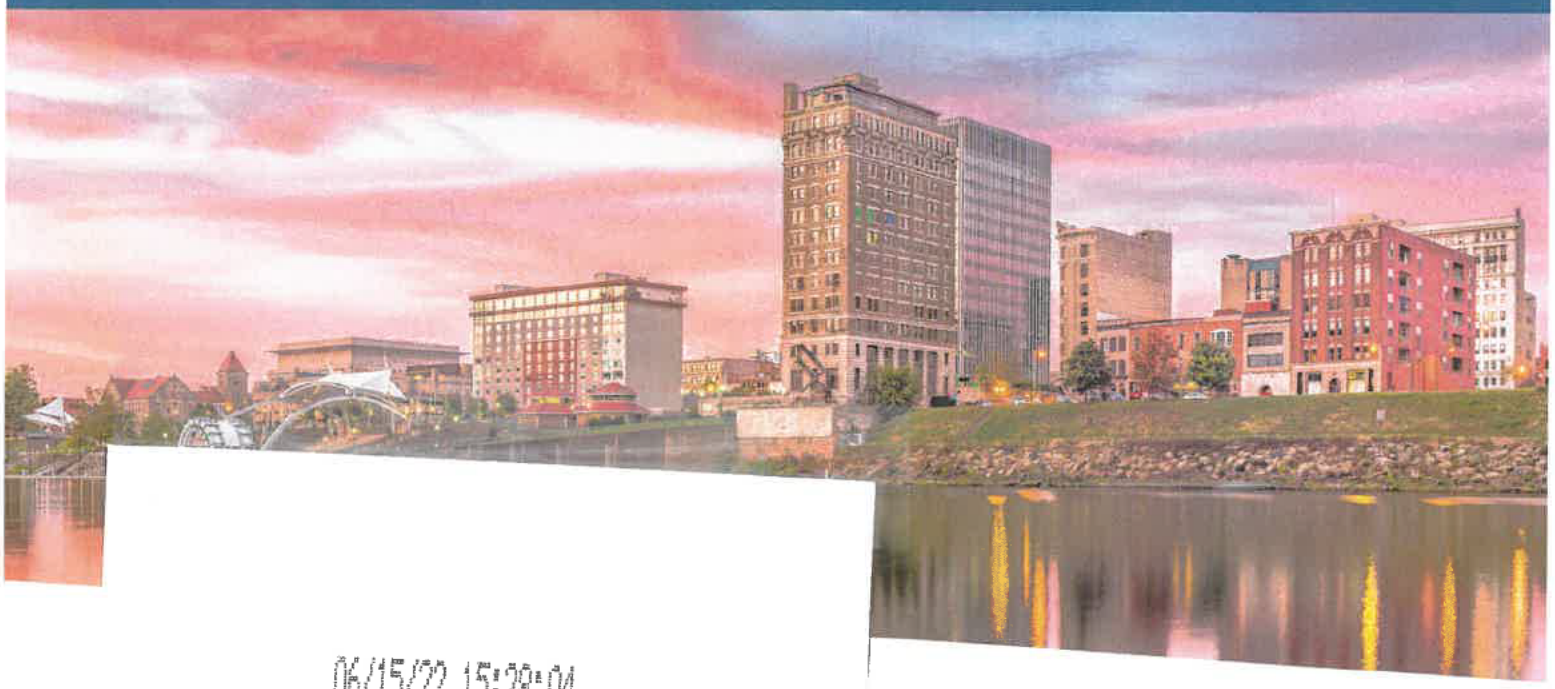
West Virginia Office of Technology (WVOT)

06/16/2022

Statewide Contract for Data Transport Services
CRFP 0212 SWC2200000001

PREPARED BY:

Gregory Florence
Government Account Executive II
Greg.Florence@segra.com (304) 414-0411



SEGRA℠

SEGRA.COM | 833.GO.SEGRA

Department of Administration
Purchasing Division
2019 Washington Street East
Post Office Box 50130
Charleston, WV 25305-0130

State of West Virginia
Centralized Request for Proposals
Info Technology

Folder: 1034853 **Doc Description:** Addendum #1 - Statewide Contract for Data Transport Services **Proc Type:** Statewide MA (Open End)			**Reason for Modification:** Addendum #1 is issued to change the bid opening date, attach vendor Q&A's, attach the Pre-Bid Sign-I..... See Page 2 for complete info
Date Issued	**Solicitation Closes**	**Solicitation No**	**Version**
2022-06-02	2022-06-16 13:30	CRFP 0212 SWC2200000001	2

BID RECEIVING LOCATION

BID CLERK
DEPARTMENT OF ADMINISTRATION
PURCHASING DIVISION
2019 WASHINGTON ST E
CHARLESTON WV 25305
US

VENDOR

Vendor Customer Code:
Vendor Name : Lumos Networks, LLC dba Segra
Address : 1200
Street : Greenbrier St
City : Charleston
State : WV **Country :** USA **Zip :** 25311
Principal Contact : Greg Florence
Vendor Contact Phone: 304-414-0411 **Extension:** NA

FOR INFORMATION CONTACT THE BUYER
Jessica L Hovanec
304-558-2314
jessica.l.hovanec@wv.gov

Vendor Signature X **FEIN#** 84-1452950 **DATE** 6/10/22

All offers subject to all terms and conditions contained in this solicitation

Reason for Modification:

Addendum #1 is issued to change the bid opening date, attach vendor Q&A's, attach the Pre-Bid Sign-In Sheet, and to attach a revised pricing page.

ADDITIONAL INFORMATION

Addendum #1 is issued to change the bid opening date, attach vendor Q&A's, attach the Pre-Bid Sign-In Sheet, and to attach a revised pricing page.

Bid Opening date changes from 06/09/2022 to 06/16/2022. Bid Opening time remains the same at 1:30 PM ET.

The West Virginia Purchasing Division is soliciting responses on behalf of the West Virginia Office of Technology (WVOT) to obtain Wide Area Network (WAN) services that will be utilized by the WVOT and other Statewide agencies, per the specifications and terms and conditions as attached hereto.

Mandatory Pre-Bid Meeting to be held on May 18, 2022 at 1:30 PM in the Executive Room at Building 7, WV Capitol Complex State Training Center, 1900 Kanawha Blvd E, Charleston, WV 25305

****ONLINE SUBMISSIONS FOR THIS REQUEST FOR PROPOSAL (RFP) ARE PROHIBITED****

****ADDITIONALLY, the Vendor should clearly separate and identify the cost proposal from the technical proposal in a separately sealed envelope.

INVOICE TO	SHIP TO
ALL STATE AGENCIES VARIOUS LOCATIONS AS INDICATED BY ORDER No City WV 99999 US	STATE OF WEST VIRGINIA VARIOUS LOCATIONS AS INDICATED BY ORDER No City WV 99999 US

Line	Comm Ln Desc	Qty	Unit of Measure	Unit Price	Total Price
1	Telecom/Data Transport Services - See Pricing Page	1.00000	EA		

Comm Code	Manufacturer	Specification	Model #
81161700			

Extended Description:

Telecom/Data Transport Services - See Pricing Page

SCHEDULE OF EVENTS

Line	Event	Event Date
1	Mandatory Pre-Bid Meeting on May 18, 2022 at 1:30 PM EDT	2022-05-18
2	Technical Questions due by May 25, 2022 at 10:00 AM EDT	2022-05-25

Technical Proposal

SEGRA℠

TECHNICAL PROPOSAL FOR:

West Virginia Office of Technology (WVOT)

06/16/2022

Statewide Contract for Data Transport Services
CRFP 0212 SWC2200000001

PREPARED BY:

Gregory Florence
Government Account Executive II
Greg.Florence@segra.com (304) 414-0411

SEGRA TABLE OF CONTENTS

SEGRA

June 16, 2022

Department of Administration, Purchasing Division
2019 Washington Street East
Charleston, WV 25305-0130

Buyer: Jessica L. Hovanec
Solicitation No.: CRFP 0212 SWC2200000001

Dear Jessica,

On behalf of the team at Segra, I would like to thank you and the West Virginia Office of Technology (WVOT) for the opportunity to respond to your solicitation for a Statewide Contract for Data Transport Services.

Segra is uniquely qualified to deliver this solution to the State of West Virginia:

- Segra is currently under contract with the WV Office of Technology providing Hosted Voice services to virtually every state agency. Such a working knowledge and contractual foundation allow Segra the unique familiarity with the State's procurement process, existing network, and specific needs to implement and support a solution that exceeds the State's expectations.
- Awarding Segra the network associated with Data Transport Services will enhance visibility into the Hosted Voice platform, improving the State's overall quality of service.
- Segra has developed a very close working relationship with the WVOT team working daily with your leadership, Intergovernmental Relationship Managers, and site contacts, which will help ensure timely installations, training, and potential troubleshooting for Data Transport Services.
- Segra currently has 118 of the State's locations on-net with Segra fiber and is proposing building fiber to approximately another 149 sites. On-net with Segra fiber or leased through another carrier, Segra owns the circuit and network performance with no finger pointing.
- Segra is more nimble and approachable than our larger competitors and has the technology, expertise, and financial strength to stand behind our services along with comprehensive support that will ensure the State's needs are met. From our CEO to the local account team, the State will have direct lines of communication to all levels of support within Segra and the financial backing of our parent company, Cox Communications, a $20 billion company.
- Segra has been the State of South Carolina's contracted provider for network services since 1996, long-distance voice provider since 1998, Internet service provider since 1999, and WAN service provider since 2003 serving approximately 588 locations across 114 municipalities and school districts. Segra also has been the Hosted Voice/VoIP service provider since 2008 (~32,000

seats) for the State of SC. We have proven we can deliver these services with accurate comprehensive billing, reporting, and responsive trouble management.

- Kyle Herron recently has joined Segra as our VP of Service Delivery. Kyle most recently was the CIO of the Citadel and prior to that he was the COO for the State of South Carolina. Kyle also previously consulted for Segra and was very engaged with the WVOT Hosted Voice solution. His industry experience, familiarity with the State of WV, unique experience as a customer, as a consultant, and now as an employee only strengthen Segra's ability to deliver your network.

In addition to the above, we have made every effort to meet or exceed all mandatory requirements as specified in your solicitation. We believe our proposed solution not only provides for your current needs, but is also designed with the scalability for future growth and the flexibility to mix and match services for the unique requirements of any individual location. Of course, the Segra network comes with the reliability and security the State of West Virginia requires.

We look forward to future discussions and the opportunity to answer any questions.

Sincerely,

Greg Florence
Government Account Executive II
1200 Greenbrier St
Charleston, WV 25311

Your future is our business.

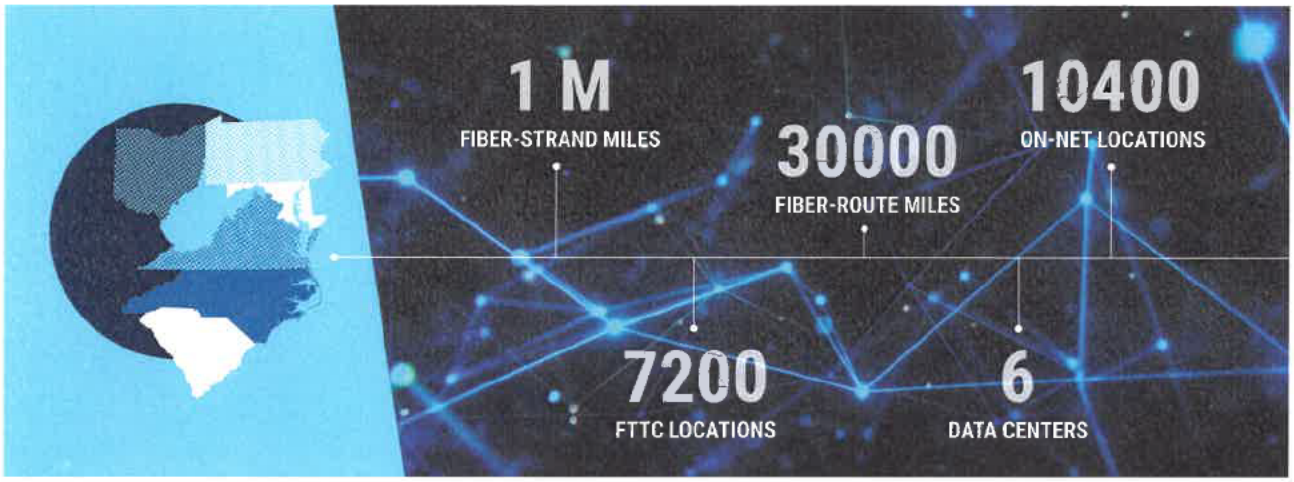
As one of the country's largest independent fiber networks, we're harnessing the latest technologies to power your potential. We're your partner, your advocate, your network connector.

The way we see it, we're in the business of you.

Welcome to Segra.

As one of the largest independent fiber network companies in the Eastern US, we provide a broad and dense service footprint across the Mid-Atlantic and Southeast. Our state-of-the-art voice and data technology solutions serve businesses of all sizes as well as some of the world's largest carriers.

But that's not what we're most proud of. What we work at day and night is delivering never-say-never customer service. In fact, we've re-engineered our entire operating model to ensure we deliver a delightful customer experience — every time.



OUR HISTORY

Segra was formed by the joining of Lumos Networks and Spirit Communications in 2018 and re-branded as Segra in 2019. We continue to build on the legacy of our two companies whose founders both had a passion for technology, communications, and product innovation.

OUR NAME

Our name "Segra" is derived from a Swedish verb meaning "to win." We chose this name carefully, knowing that a commitment to win expands far beyond our walls. This commitment translates into an ongoing partnership with our customers, giving them the freedom to grow and reach their potential.

Values that keep us focused on our customers.

We crafted our core values to reflect the deep sense of purpose and service that each of us brings to work every day. We refer to these values as our "Articles of Excellence."

Stay True.

We are honest with ourselves and with others. We earn their trust every day. We do what is right, we follow through, and we never compromise.

Be the Customer.

We know that without our customers, our company goes away. We listen, we have empathy, we show respect. We make every conversation count. We go the extra mile to make every experience memorable.

Build the Bonds.

1 + 1 = 3 is what makes us great. We seek the wisdom of others. We share our talents and we collaborate in continuum. We know that "command and control" never works. For it is only as a team that we achieve common goals.

Embrace Change.

We adjust and we evolve. We expect shifts and we find solutions. We are flexible, open-minded, and we iterate constantly. We celebrate the victories and we learn from the losses.

Light the Fire.

We empower ourselves through education and self-improvement. And we empower those around us to achieve their potential. We are responsible risk takers who seek information and search for the right tools.

Set the Pace.

In our quest for innovation, we are bold, competitive, and confident. We test boundaries, we question the status quo, and we push beyond expectations. We are unafraid of what lies ahead.

Choose to Win.

Whether we are laying new fiber routes, closing a million-dollar deal, or answering the phone, we take pride in all that we do. We study and understand the challenges. We strategize on a game plan. And then, we find a way to win.

Create a Legacy.

We create value for our customers, our employees, and our owners. By doing so, we establish a heritage of reliable infrastructure, constant innovation, and good stewardship.

At Segra, we're re-defining the delivery of communications services and solutions.

Every organization depends on reliable and safe connections. But there are differences in each industry, especially when it comes to communication. Even within an industry, no two companies are the same. We get it. That's why we've gone the extra mile to create solutions that are configured for the specifics of your industry and, more importantly, your company.

Below is an overview of the solutions we offer.

NETWORK SOLUTIONS

Reliability, reach, and fiber infrastructure that offer best-in-class connectivity.

- Dedicated Internet Access (DIA)
- Wide-Area Network (WAN)
- Long-Term Evolution (LTE)
- Dark Fiber
- Local Ring Enhancements (LRE)

VOICE SOLUTIONS

Flexible and streamlined voice solutions to keep your business connected 24/7.

- Hosted Voice
- Converged VoIP
- SIP Trunks
- IP Fax

MANAGED SERVICES

Customized communications solutions for workers in the office and out in the field.

- Software-Defined Wide Area Network (SD-WAN)
- Firewall Protection
- Distributed Denial of Service (DDoS) Protection
- Managed Local Area Network (LAN))

CLOUD SOLUTIONS

Security, data back-up, and disaster recovery for a world that's on the go.

- Infrastructure as a Service (IaaS)
- Disaster Recovery as a Service (DRaaS)
- Back-Up as a Service (BaaS)
- Data Centers

SEGRA®

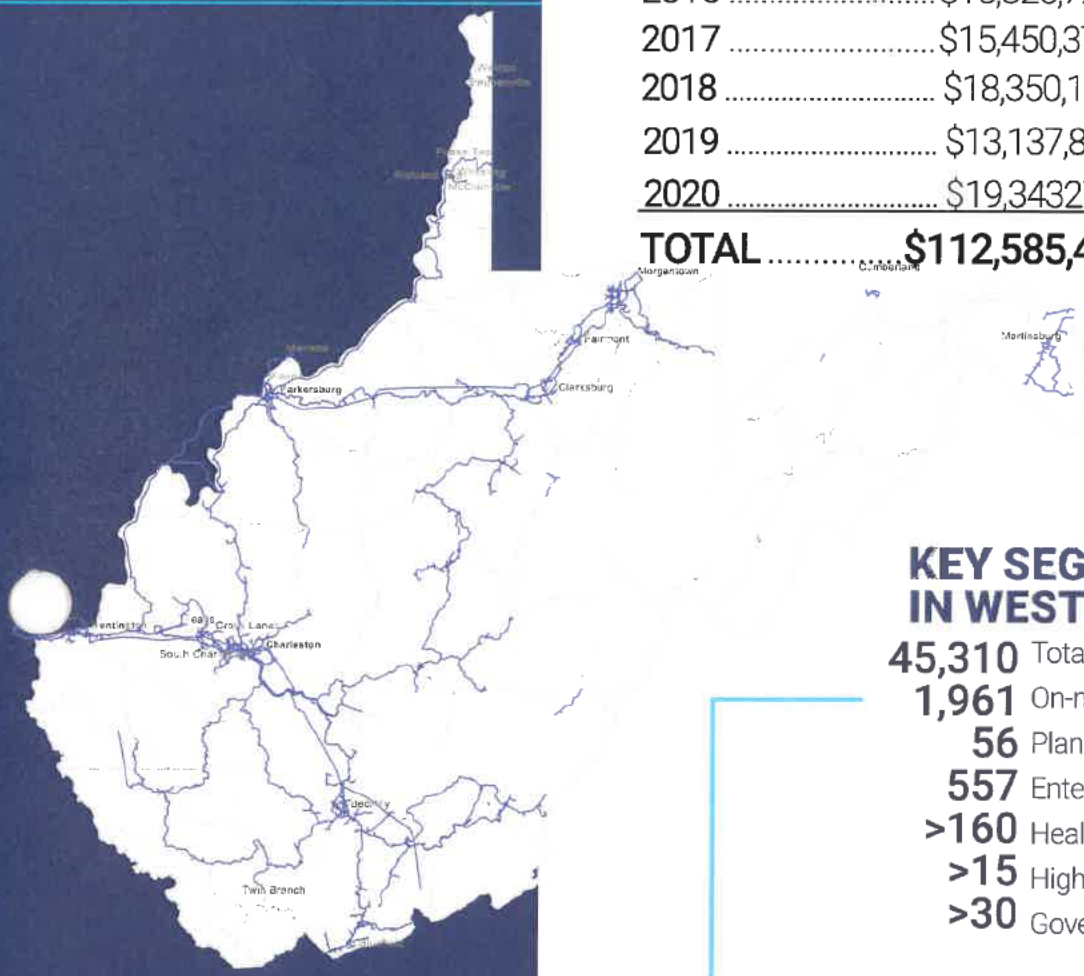
Our Commitment to West Virginia

WEST VIRGINIA STATISTICS

938 Fiber Route Miles

544 Fiber to the Cell Sites

2122 On-net Locations



SEGRA TOTAL STATISTICS

30000 Fiber Route Miles

1.7M Fiber Strand Miles

7200 Fiber to the Cell Sites

10400 On-net Locations

48 On-net Data Centers

9 States

CAPITAL INVESTMENT

2014	$13,237,768
2015	$16,240,290
2016	$16,825,728
2017	$15,450,379
2018	$18,350,152
2019	$13,137,857
2020	$19,343275
TOTAL	**$112,585,419**

TOTAL ROUTE MILES
3,736

KEY SEGRA STATS IN WEST VIRGINIA

45,310 Total Broadband Data Circuits
1,961 On-net Enterprise Sites
56 Planned On-net Enterprise Bldgs
557 Enterprise Customers
>160 Healthcare and Social Assistance
>15 Higher Education Institutions
>30 Government

ON-NET CELL TOWERS
544

WV EMPLOYEES
OVER 100

PROPERTY TAXES PAID
Over $1.3million in 2019

Voice & Collaboration

HOSTED IP VOICE
- HD Voice
- QoS Enabled Voice Policy (Segra Circuits)
- Voicemail
- Voicemail to Email
- Point to Point Video
- Soft Client
- Management Web Portal (for end users & administrators)
- On-Demand Dedicated Line Recording, by device
- Fax Messaging
- Segra Anywhere (Find Me, Follow Me)
- Instant Call Group
- Line Redirect for Disaster Recovery
- IP Fax

UNIFIED COLLABORATION
- HD Voice Calling from all device types
- Audio & Video Conferencing
- Instant Message & Chat
- Advanced Presence & Calendar Integration
- Dedicated Collaboration Space (via My Room)

ON-DEMAND CONFERENCE SERVICES
- Web Conferencing
- Audio Conferencing

CONTACT CENTER
- Call Queuing & ACD
- Agent Application
- Supervisor Application
- Dashboard for Monitoring and Reporting
- Portal for Administration of Contact Center
- Dedicated Call Recording
- Agent Hoteling (login on multiple devices)
- Enhanced Contact Center

HOSTED IP VOICE HANDSETS & ACCESSORIES
- Desktop phones
- Conference phones
- Cordless (SIP)
- Polycom and Yealink brands
- Video cameras (for Phones)
- Expansion Modules (Polycom & Yealink)

VOICE LINES/TRUNKS
- LFB Analog
- TDM PRI
- PRI over Ethernet
- Channelized T1
- DID Blocks
- SIP Trunks
- Voicemail
- Auto Attendant

WAN & Internet

ETHERNET (LAYER 2)
- Customer-managed WAN routing
- Support for E-Line, E-LAN, E-Tree topologies
- MEF certification
- Quality of Service (QoS) options
- Port Speeds:10Mbps, 100Mbps, 1Gbps, and 10Gbps
- Bandwidth Speeds: 3Mbps to 10Gbps
- SLAs

VPRN (LAYER 3)
- Support for fully meshed topologies
- Provider-managed WAN routing
- Quality of Service (QoS) options
- Port Speeds:10Mbps, 100Mbps, 1Gbps, and 10Gbps
- Bandwidth Speeds: 3Mbps to 10Gbps
- SLAs

REMOTE OFFICE LAN
- Supports Dual-Carriers
- Multiple Access Options
- 4G LTE Cat 18 Modem
- 5G Sub-6GHz Modular Modem

SD-WAN
- MPLS Extend
- MPLS Reach

EXPRESS CLOUD ACCESS
- Speeds up to 1Gbps
- MPLS Secure Connection
- Support for multiple Cloud Service Providers (CSP)

DEDICATED INTERNET ACCESS
- Scalable bandwidth
- Synchronous upload and download speeds
- Multiple resiliency mechanisms
- Automatic, real-time DDoS protection
- Multi-service support for network convergence

Managed Services & Security

SIMPLE LAN
- Router Options (up to 1 Gbps)
- Gigabit PoE Switches w/options of 10Gbps Switching
- CPE/IAD Circuit Management Equipment

MANAGED WI-FI
- Detailed pre-deployment study of Wi-Fi requirements
- Extensive site survey
- Wi-Fi Capacity Planner
- Predictive modeling
- Post-deployment survey
- Predicted vs actual Wireless LAN functioning

MANAGED FIREWALL
- Unified Threat Management with Next Gen Firewall
- Intrusion Prevention Service
- Anti-Virus/Anti-Malware
- Content/Web Filtering
- Security Information Management
- Cloud-based, hosted service
- Multiple solution packages
- Security Operations Center monitoring 24x7x365

DDOS
- Router Options (up to 1 Gbps)
- Gigabit PoE Switches w/options of 10Gbps Switching
- CPE/IAD Circuit Management Equipment
- Filters Internet traffic automatically
- Detects and stops attacks immediately
- Applies comprehensive protection analytics
- Operates with Segra DIA service

SOCAAS (SECURITY OPERATIONS CENTER AS A SERVICE)
- Real-time alerting
- Security and compliance out-of-the-box
- Cloud scale architecture
- Self-Learning Asset Inventory (CMDB)
- Exhaustive device support
- Event source monitoring

Data Center

IAAS (INFRASTRUCTURE AS A SERVICE)
- Dedicated hardware or secure virtual machines
- High-availability managed servers, switches and firewalls
- Tiered storage offerings
- IPS and DDoS protection
- Operating system monitoring and patching
- 24x7 support staff

DRAAS (DISASTER RECOVERY AS A SERVICE)
- Enterprise-grade data centers
- RPO of seconds and RTO of minutes
- Easy management with simplified UI (3 click failover)
- 99.99% solution availability
- Flash storage
- Continuous hypervisor replication with block-level replication
- Full orchestration w/ auto failover, and failback with tier 3 support
- Configurable protection options

BAAS (BACKUP AS A SERVICE)
- High availability, fault tolerant architecture
- Fully managed, monitored and supported 24x7x365
- Optional encryption
- Performance levels to match the Client's application
- Replication offered between a LDC data center and client data center

COLOCATION
- Rack Space Lease
- AC/DC Power Options
- 24/7/365 Remote Hands /Access
- Diverse Fiber Entry Points
- UPS and Generator Back-up
- Secured locations

Carrier

SMALL CELL FRONT-HAUL DARK FIBER
- Dark fiber availability on metro and long-haul footprints
- Expertly built fiber infrastructure
- Carrier Ethernet service to link your small-cell front-haul network

DARK FIBER
- Dark fiber availability on metro and long-haul footprints
- Expertly built fiber infrastructure
- Super-regional network available for carrier-managed services

LOCAL RING ENHANCEMENTS
- Access Ring Protection w/ a virtual or physical, private dedicated ring
- Non-Collapsed Lateral
- Dual Entrance Facility
- PoP Router Redundancy and Diversity
- Premise Router Redundancy
- Available with Segra on-net access

WAVELENGTHS

Segra's RFP In-Line Response

Speed and connectivity — backed by always-on customer service.

We're building the technology infrastructure of tomorrow to help you meet the challenges of today. Our state-of-the-art fiber network delivers superior voice, data, and cloud solutions to keep you ahead of the competition.

Department of Administration
Purchasing Division
2019 Washington Street East
Post Office Box 50130
Charleston, WV 25305-0130

State of West Virginia
Centralized Request for Proposals
Info Technology

Folder: 1034853	**Reason for Modification:**
Doc Description: Statewide Contract for Data Transport Services	
Proc Type: Statewide MA (Open End)	

Date Issued	Solicitation Closes	Solicitation No	Version
2022-04-29	2022-06-09 13:30	CRFP 0212 SWC2200000001	1

BID RECEIVING LOCATION

BID CLERK
DEPARTMENT OF ADMINISTRATION
PURCHASING DIVISION
2019 WASHINGTON ST E
CHARLESTON WV 25305
US

VENDOR

Vendor Customer Code:
Vendor Name : Lumos Networks, LLC dba Segra
Address : 1200
Street : Greenbrier St
City : Charleston
State : WV **Country :** USA **Zip :** 25311
Principal Contact : Greg Florence
Vendor Contact Phone: 304-414-0411 **Extension:** NA

FOR INFORMATION CONTACT THE BUYER
Jessica L Hovanec
304-558-2314
jessica.l.hovanec@wv.gov

Vendor Signature X **FEIN#** 84-1452950 **DATE** 6/8/22

All offers subject to all terms and conditions contained in this solicitation

ADDITIONAL INFORMATION

The West Virginia Purchasing Division is soliciting responses on behalf of the West Virginia Office of Technology (WVOT) to obtain Wide Area Network (WAN) services that will be utilized by the WVOT and other Statewide agencies, per the specifications and terms and conditions as attached hereto.

Mandatory Pre-Bid Meeting to be held on May 18, 2022 at 1:30 PM in the Executive Room at Building 7, WV Capitol Complex State Training Center, 1900 Kanawha Blvd E, Charleston, WV 25305

****ONLINE SUBMISSIONS FOR THIS REQUEST FOR PROPOSAL (RFP) ARE PROHIBITED****

****ADDITIONALLY, the Vendor should clearly separate and identify the cost proposal from the technical proposal in a separately sealed envelope.

INVOICE TO	SHIP TO
ALL STATE AGENCIES VARIOUS LOCATIONS AS INDICATED BY ORDER No City WV 99999 US	STATE OF WEST VIRGINIA VARIOUS LOCATIONS AS INDICATED BY ORDER No City WV 99999 US

Line	Comm Ln Desc	Qty	Unit of Measure	Unit Price	Total Price
1	Telecom/Data Transport Services - See Pricing Page	1.00000	EA		

Commodity Code	Manufacturer	Specification	Model #
81161700			

Extended Description:
Telecom/Data Transport Services - See Pricing Page

SCHEDULE OF EVENTS

Line	Event	Event Date
1	Mandatory Pre-Bid Meeting on May 18, 2022 at 1:30 PM EDT	2022-05-18
2	Technical Questions due by May 25, 2022 at 10:00 AM EDT	2022-05-25

TABLE OF CONTENTS

SECTION 1: GENERAL INFORMATION

1.1. Introduction:

The West Virginia Department of Administration, Purchasing Division (hereinafter referred to as the "Purchasing Division") is issuing this solicitation as a request for proposal ("RFP"), as authorized by W. Va. Code §5A-3-10b, for the West Virginia Office of Technology (hereinafter referred to as the "Agency") to provide statewide Wide Area Network (WAN) services.

The RFP is a procurement method in which vendors submit proposals in response to the request for proposal published by the Purchasing Division. It requires an award to the highest scoring vendor, rather than the lowest cost vendor, based upon a technical evaluation of the vendor's technical proposal and a cost evaluation. This is referred to as a best value procurement. Through their proposals, vendors offer a solution to the objectives, problem, or need specified in the RFP, and define how they intend to meet (or exceed) the RFP requirements.

Segra has read, understands, and will comply.

SECTION 2: INSTRUCTIONS TO VENDORS SUBMITTING BIDS

Instructions begin on next page.

INSTRUCTIONS TO VENDORS SUBMITTING BIDS

1. REVIEW DOCUMENTS THOROUGHLY: The attached documents contain a solicitation for bids. Please read these instructions and all documents attached in their entirety. These instructions provide critical information about requirements that if overlooked could lead to disqualification of a Vendor's bid. All bids must be submitted in accordance with the provisions contained in these instructions and the Solicitation. Failure to do so may result in disqualification of Vendor's bid.

Segra has read, understands, and will comply.

2. MANDATORY TERMS: The Solicitation may contain mandatory provisions identified by the use of the words "must," "will," and "shall." Failure to comply with a mandatory term in the Solicitation will result in bid disqualification.

Segra has read, understands, and will comply.

3. PREBID MEETING: The item identified below shall apply to this Solicitation.

☐ A pre-bid meeting will not be held prior to bid opening

☑ A **MANDATORY PRE-BID** meeting will be held at the following place and time:

When: Wednesday, May 18, 2022 at 1:30 PM EST

Location: Executive Room, Bldg 7, State Training Center
1900 Kanawha Blvd E
Charleston, WV 25305

All Vendors submitting a bid must attend the mandatory pre-bid meeting. Failure to attend the mandatory pre-bid meeting shall result in disqualification of the Vendor's bid. No one individual is permitted to represent more than one vendor at the pre-bid meeting. Any individual that does attempt to represent two or more vendors will be required to select one vendor to which the individual's attendance will be attributed. The vendors not selected will be deemed to have not attended the pre-bid meeting unless another individual attended on their behalf.

An attendance sheet provided at the pre-bid meeting shall serve as the official document verifying attendance. Any person attending the pre-bid meeting on behalf of a Vendor must list on the attendance sheet his or her name and the name of the Vendor he or she is representing.

Additionally, the person attending the pre-bid meeting should include the Vendor's E-Mail address, phone number, and Fax number on the attendance sheet. It is the Vendor's responsibility to locate the attendance sheet and provide the required information. Failure to complete the attendance sheet as required may result in disqualification of Vendor's bid.

All Vendors should arrive prior to the starting time for the pre-bid. Vendors who arrive after the starting time but prior to the end of the pre-bid will be permitted to sign in but are charged with knowing all matters discussed at the pre-bid.

Questions submitted at least five business days prior to a scheduled pre-bid will be discussed at the pre-bid meeting if possible. Any discussions or answers to questions at the pre-bid meeting are preliminary in nature and are non-binding. Official and binding answers to questions will be published in a written addendum to the Solicitation prior to bid opening.

Segra has read, understands, and will comply.

4. VENDOR QUESTION DEADLINE: Vendors may submit questions relating to this Solicitation to the Purchasing Division. Questions must be submitted in writing. All questions must be submitted on or before the date listed below and to the address listed below to be considered. A written response will be published in a Solicitation addendum if a response is possible and appropriate. Non-written discussions, conversations, or questions and answers regarding this Solicitation are preliminary in nature and are nonbinding.

Submitted emails should have the solicitation number in the subject line.

Question Submission Deadline: May 25, 2022 at 10:00 AM EST

Submit Questions to: Jessica L. Hovanec, Senior Buyer
2019 Washington Street, East
Charleston, WV 25305
Fax: (304) 558-3970
Email: Jessica.L.Hovanec@wv.gov

Segra has read, understands, and will comply.

5. VERBAL COMMUNICATION: Any verbal communication between the Vendor and any State personnel is not binding, including verbal communication at the mandatory pre-bid conference. Only information issued in writing and added to the Solicitation by an official written addendum by the Purchasing Division is binding.

Segra has read and understands.

6. BID SUBMISSION: All bids must be submitted on or before the date and time of the bid opening listed in section 7 below. Vendors can submit bids electronically through *wv*OASIS, in paper form delivered to the Purchasing Division at the address listed below either in person or by courier, or in facsimile form by faxing to the Purchasing Division at the number listed below. Notwithstanding the foregoing, the Purchasing Division may prohibit the submission of bids electronically through *wv*OASIS at its sole discretion. Such a prohibition will be contained and communicated in the *wv*OASIS system resulting in the Vendor's inability to submit bids through *wv*OASIS. The Purchasing Division will not accept bids, modification of bids, or addendum acknowledgment forms via email. Bids submitted in paper or facsimile form must contain a signature. Bids submitted in *wv*OASIS are deemed to be electronically signed.

Any bid received by the Purchasing Division staff is considered to be in the possession of the Purchasing Division and will not be returned for any reason.

For Request for Proposal ("RFP") Responses Only: Submission of a response to a Request for Proposal is not permitted in *wv*OASIS. In the event that Vendor is responding to a request for proposal, the Vendor shall submit one original technical and one original cost proposal prior to the bid opening date and time identified in Section 7 below, plus FIVE (5) convenience copies

of each to the Purchasing Division at the address shown below. Additionally, the Vendor should clearly identify and segregate the cost proposal from the technical proposal in a separately sealed envelope.

Bid Delivery Address and Fax Number:
Department of Administration, Purchasing Division
2019 Washington Street East
Charleston, WV 25305-0130
Fax: 304-558-3970

A bid submitted in paper or facsimile form should contain the information listed below on the face of the submission envelope or fax cover sheet. Otherwise, the bid may be rejected by the Purchasing Division.

VENDOR NAME:
BUYER: Jessica L. Hovanec
SOLICITATION NO.: CRFQ SWC2200000014
BID OPENING DATE: June 9, 2022
BID OPENING TIME: 1:30 PM EDT
FAX NUMBER: 304-558-3970

Segra has read, understands, and will comply.

7. BID OPENING: Bids submitted in response to this Solicitation will be opened at the location identified below on the date and time listed below. Delivery of a bid after the bid opening date and time will result in bid disqualification. For purposes of this Solicitation, a bid is considered delivered when confirmation of delivery is provided by *wv*OASIS (in the case of electronic submission) or when the bid is time stamped by the official Purchasing Division time clock (in the case of hand delivery).

Bid Opening Date and Time: June 9, 2022 at 1:30 PM EDT

Bid Opening Location: Department of Administration, Purchasing Division
2019 Washington Street East
Charleston, WV 25305-0130

Segra has read, understands, and will comply.

8. ADDENDUM ACKNOWLEDGEMENT: Changes or revisions to this Solicitation will be made by an official written addendum issued by the Purchasing Division. Vendor should acknowledge receipt of all addenda issued with this Solicitation by completing an Addendum Acknowledgment Form, a copy of which is included herewith. Failure to acknowledge addenda may result in bid disqualification. The addendum acknowledgement should be submitted with the bid to expedite document processing.

Segra has read, understands, and will comply.

9. BID FORMATTING: Vendor should type or electronically enter the information onto its bid to prevent errors in the evaluation. Failure to type or electronically enter the information may result in bid disqualification.

Segra has read, understands, and will comply.

10. ALTERNATE MODEL OR BRAND: Unless the box below is checked, any model, brand, or specification listed in this Solicitation establishes the acceptable level of quality only and is not intended to reflect a preference for, or in any way favor, a particular brand or vendor. Vendors may bid alternates to a listed model or brand provided that the alternate is at least equal to the model or brand and complies with the required specifications. The equality of any alternate being bid shall be determined by the State at its sole discretion. Any Vendor bidding an alternate model or brand should clearly identify the alternate items in its bid and should include manufacturer's specifications, industry literature, and/or any other relevant documentation demonstrating the equality of the alternate items. Failure to provide information for alternate items may be grounds for rejection of a Vendor's bid.

☐ This Solicitation is based upon a standardized commodity established under W. Va. Code § 5A-3-61. Vendors are expected to bid the standardized commodity identified. Failure to bid the standardized commodity will result in your firm's bid being rejected.

Segra has read, understands, and will comply.

11. EXCEPTIONS AND CLARIFICATIONS: The Solicitation contains the specifications that shall form the basis of a contractual agreement. Vendor shall clearly mark any exceptions, clarifications, or other proposed modifications in its bid. Exceptions to, clarifications of, or modifications of a requirement or term and condition of the Solicitation may result in bid disqualification.

Segra has read, understands, and will comply.

12. COMMUNICATION LIMITATIONS: In accordance with West Virginia Code of State Rules §148-1-6.6, communication with the State of West Virginia or any of its employees regarding this Solicitation during the solicitation, bid, evaluation or award periods, except through the Purchasing Division, is strictly prohibited without prior Purchasing Division approval. Purchasing Division approval for such communication is implied for all agency delegated and exempt purchases.

Segra has read, understands, and will comply.

13. REGISTRATION: Prior to Contract award, the apparent successful Vendor must be properly registered with the West Virginia Purchasing Division and must have paid the $125 fee, if applicable.

Segra has read, understands, and will comply.

14. UNIT PRICE: Unit prices shall prevail in cases of a discrepancy in the Vendor's bid.

Segra has read and understands.

15. PREFERENCE: Vendor Preference may be requested in purchases of motor vehicles or construction and maintenance equipment and machinery used in highway and other infrastructure projects. Any request for preference must be submitted in writing with the bid, must specifically identify the preference requested with reference to the applicable subsection of West Virginia Code § 5A-3-37, and must include with the bid any information necessary to evaluate and confirm the applicability of the requested preference. A request form to help facilitate the request can be found at: www.state.wv.us/admin/purchase/vrc/Venpref.pdf.

Segra has read, understands, and will comply.

15A. RECIPROCAL PREFERENCE: The State of West Virginia applies a reciprocal preference to all solicitations for commodities and printing in accordance with W. Va. Code § 5A-3-37(b). In effect, non-resident vendors receiving a preference in their home states, will see that same preference granted to West Virginia resident vendors bidding against them in West Virginia. Any request for reciprocal preference must include with the bid any information necessary to evaluate and confirm the applicability of the preference. A request form to help facilitate the request can be found at: www.state.wv.us/admin/purchase/vrc/Venpref.pdf.

Segra has read, understands, and will comply.

16. SMALL, WOMEN-OWNED, OR MINORITY-OWNED BUSINESSES: For any solicitations publicly advertised for bid, in accordance with West Virginia Code §5A-3-37(a)(7) and W. Va. CSR § 148-22-9, any non-resident vendor certified as a small, women-owned, or minority-owned business under W. Va. CSR § 148-22-9 shall be provided the same preference made available to any resident vendor. Any non-resident small, women-owned, or minority-owned business must identify itself as such in writing, must submit that writing to the Purchasing Division with its bid, and must be properly certified under W. Va. CSR § 148-22-9 prior to contract award to receive the preferences made available to resident vendors. Preference for a non-resident small, women-owned, or minority owned business shall be applied in accordance with W. Va. CSR § 148-22-9.

Segra has read, understands, and will comply. Segra is not a SWAM-owned business entity, or an underutilized business.

17. WAIVER OF MINOR IRREGULARITIES: The Director reserves the right to waive minor irregularities in bids or specifications in accordance with West Virginia Code of State Rules § 148-1-4.6.

Segra has read and understands.

18. ELECTRONIC FILE ACCESS RESTRICTIONS: Vendor must ensure that its submission in *wv*OASIS can be accessed and viewed by the Purchasing Division staff immediately upon bid opening. The Purchasing Division will consider any file that cannot be immediately accessed and viewed at the time of the bid opening (such as, encrypted files, password protected files, or incompatible files) to be blank or incomplete as context requires and are therefore unacceptable. A vendor will not be permitted to unencrypt files, remove password protections, or resubmit documents after bid opening to make a file viewable if those documents are required with the bid. A Vendor may be required to provide document passwords or remove access restrictions to allow the Purchasing Division to print or electronically save documents provided that those documents are viewable by the Purchasing Division prior to obtaining the password or removing the access restriction.

Segra has read, understands, and will comply.

19. NON-RESPONSIBLE: The Purchasing Division Director reserves the right to reject the bid of any vendor as Non-Responsible in accordance with W. Va. Code of State Rules § 148-1-5.3, when the Director determines that the vendor submitting the bid does not have the capability to fully perform or lacks the integrity and reliability to assure good-faith performance."

Segra has read and understands.

20. ACCEPTANCE/REJECTION: The State may accept or reject any bid in whole, or in part in accordance with W. Va. Code of State Rules § 148-1-4.5. and § 148-1-6.4.b."

Segra has read and understands.

21. YOUR SUBMISSION IS A PUBLIC DOCUMENT: Vendor's entire response to the Solicitation and the resulting Contract are public documents. As public documents, they will be disclosed to the public following the bid/proposal opening or award of the contract, as required by the competitive bidding laws of West Virginia Code §§ 5A-3-1 et seq., 5-22-1 et seq., and 5G-1-1 et seq. and the Freedom of Information Act West Virginia Code §§ 29B-1-1 et seq.

DO NOT SUBMIT MATERIAL YOU CONSIDER TO BE CONFIDENTIAL, A TRADE SECRET, OR OTHERWISE NOT SUBJECT TO PUBLIC DISCLOSURE.

Submission of any bid, proposal, or other document to the Purchasing Division constitutes your explicit consent to the subsequent public disclosure of the bid, proposal, or document. The Purchasing Division will disclose any document labeled "confidential," "proprietary," "trade secret," "private," or labeled with any other claim against public disclosure of the documents, to include any "trade secrets" as defined by West Virginia Code § 47-22-1 et seq. All submissions are subject to public disclosure without notice.

Segra has read, understands, and will comply.

22. WITH THE BID REQUIREMENTS: In instances where these specifications require documentation or other information with the bid, and a vendor fails to provide it with the bid, the Director of the Purchasing Division reserves the right to request those items after bid opening and prior to contract award pursuant to the authority to waive minor irregularities in bids or specifications under W. Va. CSR § 148-1-4.6. This authority does not apply to instances where state law mandates receipt with the bid.

Segra has read and understands.

23. EMAIL NOTIFICATION OF AWARD: The Purchasing Division will attempt to provide bidders with e-mail notification of contract award when a solicitation that the bidder participated in has been awarded. For notification purposes, bidders must provide the Purchasing Division with a valid email address in the bid response. Bidders may also monitor *wv*OASIS or the Purchasing Division's website to determine when a contract has been awarded.

Segra has read, understands, and will comply.

24. ISRAEL BOYCOTT CERTIFICATION: Vendor's act of submitting a bid in response to this solicitation shall be deemed a certification from bidder to the State that bidder is not currently engaged in, and will not for the duration of the contract, engage in a boycott of Israel. This certification is required by W. Va. Code § 5A-3-63.

Segra has read, understands, and will comply.

SECTION 3: GENERAL TERMS AND CONDITIONS

Terms and conditions begin on next page.

GENERAL TERMS AND CONDITIONS:

1. CONTRACTUAL AGREEMENT: Issuance of an Award Document signed by the Purchasing Division Director, or his designee, and approved as to form by the Attorney General's office constitutes acceptance by the State of this Contract made by and between the State of West Virginia and the Vendor. Vendor's signature on its bid, or on the Contract if the Contract is not the result of a bid solicitation, signifies Vendor's agreement to be bound by and accept the terms and conditions contained in this Contract.

Segra has reviewed, understands, and will comply.

2. DEFINITIONS: As used in this Solicitation/Contract, the following terms shall have the meanings attributed to them below. Additional definitions may be found in the specifications included with this Solicitation/Contract.

2.1. "Agency" or **"Agencies"** means the agency, board, commission, or other entity of the State of West Virginia that is identified on the first page of the Solicitation or any other public entity seeking to procure goods or services under this Contract.

2.2. "Bid" or **"Proposal"** means the vendors submitted response to this solicitation.

2.3. "Contract" means the binding agreement that is entered into between the State and the Vendor to provide the goods or services requested in the Solicitation.

2.4. "Director" means the Director of the West Virginia Department of Administration, Purchasing Division.

2.5. "Purchasing Division" means the West Virginia Department of Administration, Purchasing Division.

2.6. "Award Document" means the document signed by the Agency and the Purchasing Division, and approved as to form by the Attorney General, that identifies the Vendor as the contract holder.

2.7. "Solicitation" means the official notice of an opportunity to supply the State with goods or services that is published by the Purchasing Division.

2.8. "State" means the State of West Virginia and/or any of its agencies, commissions, boards, etc. as context requires.

2.9. "Vendor" or **"Vendors"** means any entity submitting a bid in response to the Solicitation, the entity that has been selected as the lowest responsible bidder, or the entity that has been awarded the Contract as context requires.

Segra has reviewed, understands, and will comply.

3. CONTRACT TERM; RENEWAL; EXTENSION: The term of this Contract shall be determined in accordance with the category that has been identified as applicable to this Contract below:

☑ **Term Contract**

Initial Contract Term: The Initial Contract Term will be for a period of THREE (3) YEARS . The Initial Contract Term becomes effective on the effective start date listed on the first page of this Contract and the Initial Contract Term ends on the effective end date also shown on the first page of this Contract.

Renewal Term: This Contract may be renewed upon the mutual written consent of the Agency, and the Vendor, with approval of the Purchasing Division and the Attorney General's office (Attorney General approval is as to form only). Any request for renewal should be delivered to the Agency and then submitted to the Purchasing Division thirty (30) days prior to the expiration date of the initial contract term or appropriate renewal term. A Contract renewal shall be in accordance with the terms and conditions of the original contract. Unless otherwise specified below, renewal of this Contract is limited to THREE (3) successive one (1) year periods or multiple renewal periods of less than one year, provided that the multiple renewal periods do not exceed the total number of months available in all renewal years combined. Automatic renewal of this Contract is prohibited. Renewals must be approved by the Vendor, Agency, Purchasing Division and Attorney General's office (Attorney General approval is as to form only)

☐ **Alternate Renewal Term** - This contract may be renewed for successive year periods or shorter periods provided that they do not exceed the total number of months contained in all available renewals. Automatic renewal of this Contract is prohibited. Renewals must be approved by the Vendor, Agency, Purchasing Division and Attorney General's office (Attorney General approval is as to form only)

Delivery Order Limitations: In the event that this contract permits delivery orders, a delivery order may only be issued during the time this Contract is in effect. Any delivery order issued within one year of the expiration of this Contract shall be effective for one year from the date the delivery order is issued. No delivery order may be extended beyond one year after this Contract has expired.

☐ **Fixed Period Contract:** This Contract becomes effective upon Vendor's receipt of the notice to proceed and must be completed within _____days.

☐ **Fixed Period Contract with Renewals:** This Contract becomes effective upon Vendor's receipt of the notice to proceed and part of the Contract more fully described in the attached specifications must be completed within days. Upon completion of the work covered by the preceding sentence, the vendor agrees that:

☐ the contract will continue for years;

☐ the contract may be renewed for successive year periods or shorter periods provided that they do not exceed the total number of months contained in all available renewals. Automatic renewal of this Contract is prohibited. Renewals must be approved by the Vendor, Agency, Purchasing Division and Attorney

General's Office (Attorney General approval is as to form only).

☐ **One-Time Purchase:** The term of this Contract shall run from the issuance of the Award Document until all of the goods contracted for have been delivered, but in no event will this Contract extend for more than one fiscal year.

☐ **Other:** Contract Term specified in _____

Segra has reviewed, understands, and will comply.

4. AUTHORITY TO PROCEED: Vendor is authorized to begin performance of this contract on the date of encumbrance listed on the front page of the Award Document unless either the box for "Fixed Period Contract" or "Fixed Period Contract with Renewals" has been checked in Section 3 above. If either "Fixed Period Contract" or "Fixed Period Contract with Renewals" has been checked, Vendor must not begin work until it receives a separate notice to proceed from the State. The notice to proceed will then be incorporated into the Contract via change order to memorialize the official date that work commenced.

Segra has reviewed, understands, and will comply.

5. QUANTITIES: The quantities required under this Contract shall be determined in accordance with the category that has been identified as applicable to this Contract below.

☑ **Open End Contract:** Quantities listed in this Solicitation/Award Document are approximations only, based on estimates supplied by the Agency. It is understood and agreed that the Contract shall cover the quantities actually ordered for delivery during the term of the Contract, whether more or less than the quantities shown.

☐ **Service:** The scope of the service to be provided will be more clearly defined in the specifications included herewith.

☐ **Combined Service and Goods:** The scope of the service and deliverable goods to be provided will be more clearly defined in the specifications included herewith.

☐ **One-Time Purchase:** This Contract is for the purchase of a set quantity of goods that are identified in the specifications included herewith. Once those items have been delivered, no additional goods may be procured under this Contract without an appropriate change order approved by the Vendor, Agency, Purchasing Division, and Attorney General's office.

Segra has reviewed, understands, and will comply.

6. EMERGENCY PURCHASES: The Purchasing Division Director may authorize the Agency to purchase goods or services in the open market that Vendor would otherwise provide under this Contract if those goods or services are for immediate or expedited delivery in an emergency. Emergencies shall include, but are not limited to, delays in transportation or an unanticipated increase in the volume of work. An emergency purchase in the open market, approved by the Purchasing Division Director, shall not constitute of breach of this Contract and shall not entitle the Vendor to any form of compensation or damages. This provision does not excuse the State from fulfilling its obligations under a One-Time Purchase contract.

Segra has reviewed, understands, and will comply.

7. REQUIRED DOCUMENTS: All of the items checked in this section must be provided to the Purchasing Division by the Vendor as specified:

☐ **BID BOND (Construction Only):** Pursuant to the requirements contained in W. Va. Code § 5-22-1(c), All Vendors submitting a bid on a construction project shall furnish a valid bid bond in the amount of five percent (5%) of the total amount of the bid protecting the State of West Virginia. The bid bond must be submitted with the bid.

☐ **PERFORMANCE BOND:** The apparent successful Vendor shall provide a performance bond in the amount of 100% of the contract. The performance bond must be received by the Purchasing Division prior to Contract award.

☐ **LABOR/MATERIAL PAYMENT BOND:** The apparent successful Vendor shall provide a labor/material payment bond in the amount of 100% of the Contract value. The labor/material payment bond must be delivered to the Purchasing Division prior to Contract award.

In lieu of the Bid Bond, Performance Bond, and Labor/Material Payment Bond, the Vendor may provide certified checks, cashier's checks, or irrevocable letters of credit. Any certified check, cashier's check, or irrevocable letter of credit provided in lieu of a bond must be of the same amount and delivered on the same schedule as the bond it replaces. A letter of credit submitted in lieu of a performance and labor/material payment bond will only be allowed for projects under $100,000. Personal or business checks are not acceptable. Notwithstanding the foregoing, West Virginia Code § 5-22-1 (d) mandates that a vendor provide a performance and labor/material payment bond for construction projects. Accordingly, substitutions for the performance and labor/material payment bonds for construction projects is not permitted.

☐ **MAINTENANCE BOND:** The apparent successful Vendor shall provide a two (2) year maintenance bond covering the roofing system. The maintenance bond must be issued and delivered to the Purchasing Division prior to Contract award.

☐ **LICENSE(S) / CERTIFICATIONS / PERMITS:** In addition to anything required under the Section of the General Terms and Conditions entitled Licensing, the apparent successful Vendor shall furnish proof of the following licenses, certifications, and/or permits upon request and in a form acceptable to the State. The request may be prior to or after contract award at the State's sole discretion.

☐

☐

☐

☐

The apparent successful Vendor shall also furnish proof of any additional licenses or certifications contained in the specifications regardless of whether or not that requirement is listed above.

Segra has reviewed, understands, and will comply.

8. INSURANCE: The apparent successful Vendor shall furnish proof of the insurance identified by a checkmark below and must include the State as an additional insured on each policy prior to Contract award. The insurance coverages identified below must be maintained throughout the life of this contract. Thirty (30) days prior to the expiration of the insurance policies, Vendor shall provide the Agency with proof that the insurance mandated herein has been continued. Vendor must also provide Agency with immediate notice of any changes in its insurance policies, including but not limited to, policy cancelation, policy reduction, or change in insurers. The apparent successful Vendor shall also furnish proof of any additional insurance requirements contained in the specifications prior to Contract award regardless of whether that insurance requirement is listed in this section.

Vendor must maintain:

☑ **Commercial General Liability Insurance** in at least an amount of: $1,000,000 per occurrence.

☑ **Automobile Liability Insurance** in at least an amount of: $1,000,000 per occurrence.

☐ **Professional/Malpractice/Errors and Omission Insurance** in at least an amount of: per occurrence. Notwithstanding the forgoing, Vendor's are not required to list the State as an additional insured for this type of policy.

☐ **Commercial Crime and Third Party Fidelity Insurance** in an amount of: per occurrence.

☑ **Cyber Liability Insurance** in an amount of: $3,000,000 per occurrence.

☐ **Builders Risk Insurance** in an amount equal to 100% of the amount of the Contract.

☐ **Pollution Insurance** in an amount of: per occurrence.

☐ **Aircraft Liability** in an amount of: per occurrence.

☐

☐

☐

☐

Notwithstanding anything contained in this section to the contrary, the Director of the Purchasing Division reserves the right to waive the requirement that the State be named as an additional insured on one or more of the Vendor's insurance policies if the Director finds that doing so is in the State's best interest.

Segra has read, understands, and will comply upon award.

Segra has appropriate insurance to support its obligations and liabilities in its customer agreements. We reserve the right to clarify such insurance support language in the final agreement.

9. WORKERS' COMPENSATION INSURANCE: Vendor shall comply with laws relating to workers compensation, shall maintain workers' compensation insurance when required, and shall furnish proof of workers' compensation insurance upon request.

Segra has reviewed, understands, and will comply.

10. [Reserved]

11. LIQUIDATED DAMAGES: This clause shall in no way be considered exclusive and shall not limit the State or Agency's right to pursue any other available remedy. Vendor shall pay liquidated damages in the amount specified below or as described in the specifications:

☑ $500 per day for Missed Installation Deadlines

☑ Liquidated Damages Contained in the Specifications.

☐ Liquidated Damages Are Not Included in this Contract.

Segra has full intention of delivering current on-net buildings within the 45-day time frame. Due to recent supply chain issues across the industry, we are mindful of delays that can occur out of our control as relates to supply availability of equipment. Although today we are not currently impeded by an issue with related equipment for the proposed solution, that would be the only unforeseen issue with committing/delivering to the 45-day timeframe. We would know this prior to taking related orders for desired locations to be converted.

12. ACCEPTANCE: Vendor's signature on its bid, or on the certification and signature page, constitutes an offer to the State that cannot be unilaterally withdrawn, signifies that the product or service proposed by vendor meets the mandatory requirements contained in the Solicitation for that product or service, unless otherwise indicated, and signifies acceptance of the terms and conditions contained in the Solicitation unless otherwise indicated.

Segra has reviewed, understands, and will comply.

13. PRICING: The pricing set forth herein is firm for the life of the Contract, unless specified elsewhere within this Solicitation/Contract by the State. A Vendor's inclusion of price adjustment provisions in its bid, without an express authorization from the State in the Solicitation to do so, may result in bid disqualification. Notwithstanding the foregoing, Vendor must extend any publicly advertised sale price to the State and invoice at the lower of the contract price or the publicly advertised sale price.

Segra has reviewed, understands, and will comply.

14. PAYMENT IN ARREARS: Payments for goods/services will be made in arrears only upon receipt of a proper invoice, detailing the goods/services provided or receipt of the goods/services, whichever is later. Notwithstanding the foregoing, payments for software maintenance, licenses, or subscriptions may be paid annually in advance.

Segra has reviewed, understands, and will comply.

15. PAYMENT METHODS: Vendor must accept payment by electronic funds transfer and P-Card. (The State of West Virginia's Purchasing Card program, administered under contract by a banking institution, processes payment for goods and services through state designated credit cards.)

Segra has reviewed, understands, and will comply.

16. TAXES: The Vendor shall pay any applicable sales, use, personal property or any other taxes arising out of this Contract and the transactions contemplated thereby. The State of West Virginia is exempt from federal and state taxes and will not pay or reimburse such taxes.

Segra has reviewed, understands, and will comply.

17. ADDITIONAL FEES: Vendor is not permitted to charge additional fees or assess additional charges that were not either expressly provided for in the solicitation published by the State of West Virginia, included in the Contract, or included in the unit price or lump sum bid amount that Vendor is required by the solicitation to provide. Including such fees or charges as notes to the solicitation may result in rejection of vendor's bid. Requesting such fees or charges be paid after the contract has been awarded may result in cancellation of the contract.

Segra has reviewed, understands, and will comply.

18. FUNDING: This Contract shall continue for the term stated herein, contingent upon funds being appropriated by the Legislature or otherwise being made available. In the event funds are not appropriated or otherwise made available, this Contract becomes void and of no effect beginning on July 1 of the fiscal year for which funding has not been appropriated or otherwise made available. If that occurs, the State may notify the Vendor that an alternative source of funding has been obtained and thereby avoid the automatic termination. Non-appropriation or non-funding shall not be considered an event of default.

Segra has reviewed, understands, and will comply.

19. CANCELLATION: The Purchasing Division Director reserves the right to cancel this Contract immediately upon written notice to the vendor if the materials or workmanship supplied do not conform to the specifications contained in the Contract. The Purchasing Division Director may also cancel any purchase or Contract upon 30 days written notice to the Vendor in accordance with West Virginia Code of State Rules § 148-1-5.2.b.

Segra has reviewed, understands, and will comply.

20. TIME: Time is of the essence regarding all matters of time and performance in this Contract.

Segra has reviewed and understands.

21. APPLICABLE LAW: This Contract is governed by and interpreted under West Virginia law without giving effect to its choice of law principles. Any information provided in specification manuals, or any other source, verbal or written, which contradicts or violates the West Virginia Constitution, West Virginia Code, or West Virginia Code of State Rules is void and of no effect.

Segra has reviewed, understands, and will comply.

22. COMPLIANCE WITH LAWS: Vendor shall comply with all applicable federal, state, and local laws, regulations and ordinances. By submitting a bid, Vendor acknowledges that it has reviewed, understands, and will comply with all applicable laws, regulations, and ordinances.

SUBCONTRACTOR COMPLIANCE: Vendor shall notify all subcontractors providing commodities or services related to this Contract that as subcontractors, they too are required to comply with all applicable laws, regulations, and ordinances. Notification under this provision must occur prior to the performance of any work under the contract by the subcontractor.

Segra has reviewed, understands, and will comply.

23. ARBITRATION: Any references made to arbitration contained in this Contract, Vendor's bid, or in any American Institute of Architects documents pertaining to this Contract are hereby deleted, void, and of no effect.

Segra has reviewed, understands, and will comply.

24. MODIFICATIONS: This writing is the parties' final expression of intent. Notwithstanding anything contained in this Contract to the contrary no modification of this Contract shall be binding without mutual written consent of the Agency, and the Vendor, with approval of the Purchasing Division and the Attorney General's office (Attorney General approval is as to form only). Any change to existing contracts that adds work or changes contract cost, and were not included in the original contract, must be approved by the Purchasing Division and the Attorney General's Office (as to form) prior to the implementation of the change or commencement of work affected by the change.

Segra has reviewed, understands, and will comply.

25. WAIVER: The failure of either party to insist upon a strict performance of any of the terms or provision of this Contract, or to exercise any option, right, or remedy herein contained, shall not be construed as a waiver or a relinquishment for the future of such term, provision, option, right, or remedy, but the same shall continue in full force and effect. Any waiver must be expressly stated in writing and signed by the waiving party.

Segra has reviewed, understands, and will comply.

26. SUBSEQUENT FORMS: The terms and conditions contained in this Contract shall supersede any and all subsequent terms and conditions which may appear on any form documents submitted by Vendor to the Agency or Purchasing Division such as price lists, order forms, invoices, sales agreements, or maintenance agreements, and includes internet websites or other electronic documents. Acceptance or use of Vendor's forms does not constitute acceptance of the terms and conditions contained thereon.

Segra has reviewed, understands, and will comply.

27. ASSIGNMENT: Neither this Contract nor any monies due, or to become due hereunder, may be assigned by the Vendor without the express written consent of the Agency, the Purchasing Division, the Attorney General's office (as to form only), and any other government agency or office that may be required to approve such assignments.

Segra has reviewed, understands, and will comply.

28. WARRANTY: The Vendor expressly warrants that the goods and/or services covered by this Contract will: (a) conform to the specifications, drawings, samples, or other description furnished or specified by the Agency; (b) be merchantable and fit for the purpose intended; and (c) be free from defect in material and workmanship.

Segra has reviewed, understands, and will comply.

29. STATE EMPLOYEES: State employees are not permitted to utilize this Contract for personal use and the Vendor is prohibited from permitting or facilitating the same.

Segra has reviewed, understands, and will comply.

30. PRIVACY, SECURITY, AND CONFIDENTIALITY: The Vendor agrees that it will not disclose to anyone, directly or indirectly, any such personally identifiable information or other confidential information gained from the Agency, unless the individual who is the subject of the information consents to the disclosure in writing or the disclosure is made pursuant to the Agency's policies, procedures, and rules. Vendor further agrees to comply with the Confidentiality Policies and Information Security Accountability Requirements, set forth in http://www.state.wv.us/admin/purchase/privacy/default.html.

Segra has reviewed, understands, and will comply.

31. YOUR SUBMISSION IS A PUBLIC DOCUMENT: Vendor's entire response to the Solicitation and the resulting Contract are public documents. As public documents, they will be disclosed to the public following the bid/proposal opening or award of the contract, as required by the competitive bidding laws of West Virginia Code §§ 5A-3-1 et seq., 5-22-1 et seq., and 5G-1-1 et seq. and the Freedom of Information Act West Virginia Code §§ 29B-1-1 et seq.

DO NOT SUBMIT MATERIAL YOU CONSIDER TO BE CONFIDENTIAL, A TRADE SECRET, OR OTHERWISE NOT SUBJECT TO PUBLIC DISCLOSURE.

Submission of any bid, proposal, or other document to the Purchasing Division constitutes your explicit consent to the subsequent public disclosure of the bid, proposal, or document. The Purchasing Division will disclose any document labeled "confidential," "proprietary," "trade secret," "private," or labeled with any other claim against public disclosure of the documents, to include any "trade secrets" as defined by West Virginia Code § 47-22-1 et seq. All submissions are subject to public disclosure without notice.

Segra has reviewed, understands, and will comply.

32. LICENSING: In accordance with West Virginia Code of State Rules § 148-1-6.1.e, Vendor must be licensed and in good standing in accordance with any and all state and local laws and requirements by any state or local agency of West Virginia, including, but not limited to, the West Virginia Secretary of State's Office, the West Virginia Tax Department, West Virginia Insurance Commission, or any other state agency or political subdivision. Obligations related to political subdivisions may include, but are not limited to, business licensing, business and occupation taxes, inspection compliance, permitting, etc. Upon request, the Vendor must

provide all necessary releases to obtain information to enable the Purchasing Division Director or the Agency to verify that the Vendor is licensed and in good standing with the above entities.

SUBCONTRACTOR COMPLIANCE: Vendor shall notify all subcontractors providing commodities or services related to this Contract that as subcontractors, they too are required to be licensed, in good standing, and up-to-date on all state and local obligations as described in this section. Obligations related to political subdivisions may include, but are not limited to, business licensing, business and occupation taxes, inspection compliance, permitting, etc. Notification under this provision must occur prior to the performance of any work under the contract by the subcontractor.

Segra has reviewed, understands, and will comply.

33. ANTITRUST: In submitting a bid to, signing a contract with, or accepting a Award Document from any agency of the State of West Virginia, the Vendor agrees to convey, sell, assign, or transfer to the State of West Virginia all rights, title, and interest in and to all causes of action it may now or hereafter acquire under the antitrust laws of the United States and the State of West Virginia for price fixing and/or unreasonable restraints of trade relating to the particular commodities or services purchased or acquired by the State of West Virginia. Such assignment shall be made and become effective at the time the purchasing agency tenders the initial payment to Vendor.

Segra has reviewed, understands, and will comply.

34. VENDOR CERTIFICATIONS: By signing its bid or entering into this Contract, Vendor certifies (1) that its bid or offer was made without prior understanding, agreement, or connection with any corporation, firm, limited liability company, partnership, person or entity submitting a bid or offer for the same material, supplies, equipment or services; (2) that its bid or offer is in all respects fair and without collusion or fraud; (3) that this Contract is accepted or entered into without any prior understanding, agreement, or connection to any other entity that could be considered a violation of law; and (4) that it has reviewed this Solicitation in its entirety; understands the requirements, terms and conditions, and other information contained herein.

Vendor's signature on its bid or offer also affirms that neither it nor its representatives have any interest, nor shall acquire any interest, direct or indirect, which would compromise the performance of its services hereunder. Any such interests shall be promptly presented in detail to the Agency. The individual signing this bid or offer on behalf of Vendor certifies that he or she is authorized by the Vendor to execute this bid or offer or any documents related thereto on Vendor's behalf; that he or she is authorized to bind the Vendor in a contractual relationship; and that, to the best of his or her knowledge, the Vendor has properly registered with any State agency that may require registration.

Segra has reviewed, understands, and will comply.

35. VENDOR RELATIONSHIP: The relationship of the Vendor to the State shall be that of an independent contractor and no principal-agent relationship or employer-employee relationship is contemplated or created by this Contract. The Vendor as an independent contractor is solely liable for the acts and omissions of its employees and agents. Vendor shall be responsible for selecting, supervising, and compensating any and all individuals employed pursuant to the terms of this Solicitation and resulting contract. Neither the Vendor, nor any employees or

subcontractors of the Vendor, shall be deemed to be employees of the State for any purpose whatsoever. Vendor shall be exclusively responsible for payment of employees and contractors for all wages and salaries, taxes, withholding payments, penalties, fees, fringe benefits, professional liability insurance premiums, contributions to insurance and pension, or other deferred compensation plans, including but not limited to, Workers' Compensation and Social Security obligations, licensing fees, etc. and the filing of all necessary documents, forms, and returns pertinent to all of the foregoing.

Vendor shall hold harmless the State, and shall provide the State and Agency with a defense against any and all claims including, but not limited to, the foregoing payments, withholdings, contributions, taxes, Social Security taxes, and employer income tax returns.

Segra has reviewed, understands, and will comply.

36. INDEMNIFICATION: The Vendor agrees to indemnify, defend, and hold harmless the State and the Agency, their officers, and employees from and against: (1) Any claims or losses for services rendered by any subcontractor, person, or firm performing or supplying services, materials, or supplies in connection with the performance of the Contract; (2) Any claims or losses resulting to any person or entity injured or damaged by the Vendor, its officers, employees, or subcontractors by the publication, translation, reproduction, delivery, performance, use, or disposition of any data used under the Contract in a manner not authorized by the Contract, or by Federal or State statutes or regulations; and (3) Any failure of the Vendor, its officers, employees, or subcontractors to observe State and Federal laws including, but not limited to, labor and wage and hour laws.

Segra has reviewed, understands, and will comply, excepting for claims or losses caused by gross negligence or willful misconduct by the State and the Agency, their officers, and employees.

37. NO DEBT CERTIFICATION: In accordance with West Virginia Code §§ 5A-3-10a and 5-22-1(i), the State is prohibited from awarding a contract to any bidder that owes a debt to the State or a political subdivision of the State. By submitting a bid, or entering into a contract with the State, Vendor is affirming that (1) for construction contracts, the Vendor is not in default on any monetary obligation owed to the state or a political subdivision of the state, and (2) for all other contracts, neither the Vendor nor any related party owe a debt as defined above, and neither the Vendor nor any related party are in employer default as defined in the statute cited above unless the debt or employer default is permitted under the statute.

Segra has reviewed, understands, and will comply.

38. CONFLICT OF INTEREST: Vendor, its officers or members or employees, shall not presently have or acquire an interest, direct or indirect, which would conflict with or compromise the performance of its obligations hereunder. Vendor shall periodically inquire of its officers, members and employees to ensure that a conflict of interest does not arise. Any conflict of interest discovered shall be promptly presented in detail to the Agency.

Segra has reviewed, understands, and will comply.

39. REPORTS: Vendor shall provide the Agency and/or the Purchasing Division with the following reports identified by a checked box below:

☑ Such reports as the Agency and/or the Purchasing Division may request. Requested reports may include, but are not limited to, quantities purchased, agencies utilizing the contract, total contract expenditures by agency, etc.

☐ Quarterly reports detailing the total quantity of purchases in units and dollars, along with a listing of purchases by agency. Quarterly reports should be delivered to the Purchasing Division via email at purchasing.division@wv.gov.

Segra has reviewed, understands, and will comply.

40. BACKGROUND CHECK: In accordance with W. Va. Code § 15-2D-3, the State reserves the right to prohibit a service provider's employees from accessing sensitive or critical information or to be present at the Capitol complex based upon results addressed from a criminal background check. Service providers should contact the West Virginia Division of Protective Services by phone at (304) 558-9911 for more information.

Segra has reviewed, understands, and will comply.

41. PREFERENCE FOR USE OF DOMESTIC STEEL PRODUCTS: Except when authorized by the Director of the Purchasing Division pursuant to W. Va. Code § 5A-3-56, no contractor may use or supply steel products for a State Contract Project other than those steel products made in the United States. A contractor who uses steel products in violation of this section may be subject to civil penalties pursuant to W. Va. Code § 5A-3-56. As used in this section:

a. "State Contract Project" means any erection or construction of, or any addition to, alteration of or other improvement to any building or structure, including, but not limited to, roads or highways, or the installation of any heating or cooling or ventilating plants or other equipment, or the supply of and materials for such projects, pursuant to a contract with the State of West Virginia for which bids were solicited on or after June 6, 2001.

b. "Steel Products" means products rolled, formed, shaped, drawn, extruded, forged, cast, fabricated or otherwise similarly processed, or processed by a combination of two or more or such operations, from steel made by the open heath, basic oxygen, electric furnace, Bessemer or other steel making process.

c. The Purchasing Division Director may, in writing, authorize the use of foreign steel products if:

   1. The cost for each contract item used does not exceed one tenth of one percent (.1%) of the total contract cost or two thousand five hundred dollars ($2,500.00), whichever is greater. For the purposes of this section, the cost is the value of the steel product as delivered to the project; or

   2. The Director of the Purchasing Division determines that specified steel materials are not produced in the United States in sufficient quantity or otherwise are not reasonably available to meet contract requirements.

Segra has reviewed, understands, and will comply.

42. PREFERENCE FOR USE OF DOMESTIC ALUMINUM, GLASS, AND STEEL: In Accordance with W. Va. Code § 5-19-1 et seq., and W. Va. CSR § 148-10-1 et seq., for every contract or subcontract, subject to the limitations contained herein, for the construction, reconstruction, alteration, repair, improvement or maintenance of public works or for the purchase of any item of machinery or equipment to be used at sites of public works, only domestic aluminum, glass or steel products shall be supplied unless the spending officer determines, in writing, after the receipt of offers or bids, (1) that the cost of domestic aluminum, glass or steel products is unreasonable or inconsistent with the public interest of the

State of West Virginia, (2) that domestic aluminum, glass or steel products are not produced in sufficient quantities to meet the contract requirements, or (3) the available domestic aluminum, glass, or steel do not meet the contract specifications. This provision only applies to public works contracts awarded in an amount more than fifty thousand dollars ($50,000) or public works contracts that require more than ten thousand pounds of steel products.

The cost of domestic aluminum, glass, or steel products may be unreasonable if the cost is more than twenty percent (20%) of the bid or offered price for foreign made aluminum, glass, or steel products. If the domestic aluminum, glass or steel products to be supplied or produced in a "substantial labor surplus area", as defined by the United States Department of Labor, the cost of domestic aluminum, glass, or steel products may be unreasonable if the cost is more than thirty percent (30%) of the bid or offered price for foreign made aluminum, glass, or steel products. This preference shall be applied to an item of machinery or equipment, as indicated above, when the item is a single unit of equipment or machinery manufactured primarily of aluminum, glass or steel, is part of a public works contract and has the sole purpose or of being a permanent part of a single public works project. This provision does not apply to equipment or machinery purchased by a spending unit for use by that spending unit and not as part of a single public works project.

All bids and offers including domestic aluminum, glass or steel products that exceed bid or offer prices including foreign aluminum, glass or steel products after application of the preferences provided in this provision may be reduced to a price equal to or lower than the lowest bid or offer price for foreign aluminum, glass or steel products plus the applicable preference. If the reduced bid or offer prices are made in writing and supersede the prior bid or offer prices, all bids or offers, including the reduced bid or offer prices, will be reevaluated in accordance with this rule.

Segra has reviewed, understands, and will comply.

43. INTERESTED PARTY SUPPLEMENTAL DISCLOSURE: W. Va. Code § 6D-1-2 requires that for contracts with an actual or estimated value of at least $1 million, the Vendor must submit to the Agency a disclosure of interested parties prior to beginning work under this Contract. Additionally, the Vendor must submit a supplemental disclosure of interested parties reflecting any new or differing interested parties to the contract, which were not included in the original pre-work interested party disclosure, within 30 days following the completion or termination of the contract. A copy of that form is included with this solicitation or can be obtained from the WV Ethics Commission. This requirement does not apply to publicly traded companies listed on a national or international stock exchange. A more detailed definition of interested parties can be obtained from the form referenced above.

Segra has reviewed, understands, and will comply. Please refer to Segra's completed **Disclosure of Interested Parties to Contracts**, included in our response on page 165.

44. PROHIBITION AGAINST USED OR REFURBISHED: Unless expressly permitted in the solicitation published by the State, Vendor must provide new, unused commodities, and is prohibited from supplying used or refurbished commodities, in fulfilling its responsibilities under this Contract.

Segra has reviewed, understands, and will comply.

45. VOID CONTRACT CLAUSES - This Contract is subject to the provisions of West Virginia Code § 5A-3-62, which automatically voids certain contract clauses that violate State law.

Segra has reviewed, understands, and will comply.

46. ISRAEL BOYCOTT: Bidder understands and agrees that, pursuant to W. Va. Code § 5A-3-63, it is prohibited from engaging in a boycott of Israel during the term of this contract.

Segra has reviewed, understands, and will comply.

Segra suggests that the below Force Majeure provision be incorporated into the Terms and Conditions, to be discussed with the State when appropriate.

47. FORCE MAJEURE: Segra is not liable for any failure of performance hereunder due to causes beyond its reasonable control including, but not limited to, acts of third parties not under the direction or actual control of the party delayed or unable to perform, acts of God, fire, explosion, vandalism, cable or fiber cut, flood, storm, epidemic, or other similar catastrophe, any law, order, regulation, direction, action, or request of the government, or any department, agency, commission, court, or bureau of a government, or any civil or military authority, national emergency, insurrection, riot, war, strike, lockout, or work stoppage (each, a "Force Majeure Event"). The party claiming relief due to a Force Majeure Event shall notify the other party of the occurrence or existence of the Force Majeure Event and of the termination of such event.

DESIGNATED CONTACT: Vendor appoints the individual identified in this Section as the Contract Administrator and the initial point of contact for matters relating to this Contract.

(Name, Title) 

(Printed Name and Title) Greg Florence, Government Account Executive II

(Address) 1200 Greenbrier St, Charleston, WV 25311

(Phone Number) / (Fax Number) Phone number: (304) 414-0411 / Fax number: N/A

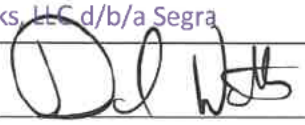
(email address) Greg.Florence@segra.com

CERTIFICATION AND SIGNATURE: By signing below, or submitting documentation through *wv*OASIS, I certify that: I have reviewed this Solicitation/Contract in its entirety; that I understand the requirements, terms and conditions, and other information contained herein; that this bid, offer or proposal constitutes an offer to the State that cannot be unilaterally withdrawn; that the product or service proposed meets the mandatory requirements contained in the Solicitation/Contract for that product or service, unless otherwise stated herein; that the Vendor accepts the terms and conditions contained in the Solicitation, unless otherwise stated herein; that I am submitting this bid, offer or proposal for review and consideration; that I am authorized by the vendor to execute and submit this bid, offer, or proposal, or any documents related thereto on vendor's behalf; that I am authorized to bind the vendor in a contractual relationship; and that to the best of my knowledge, the vendor has properly registered with any State agency that may require registration.

By signing below, I further certify that I understand this Contract is subject to the provisions of West Virginia Code § 5A-3-62, which automatically voids certain contract clauses that violate State law; and that pursuant to W. Va. Code 5A-3-63, the entity entering into this contract is prohibited from engaging in a boycott against Israel.

Lumos Networks, LLC d/b/a Segra

(Company)



(Authorized Signature) (Representative Name, Title)

Dan Watts, Chief Operating Officer 6/10/2022

(Printed Name and Title of Authorized Representative) (Date)

Phone number: (803) 888-3106 / Fax number: N/A

(Phone Number) (Fax Number)

Dan.Watts@segra.com

(Email Address)

SECTION 4: PROJECT SPECIFICATIONS

4.1. Background and Current Operating Environment:

The State of West Virginia operates and maintains statewide networks for data, video and voice transmission that are shared between government and education entities including state agencies, higher education, K-12 schools, libraries, and county/municipal units of government.

The next-generation statewide Wide Area Network (WAN) known as Data Transport 2.0, has been designed to enable a single vendor to provide secure, flexible, reliable, and cost-effective services including Ethernet WAN services and dedicated Internet access, and to enable value-added support services from the Vendor. The current WAN services contract is set to expire on June 30, 2022.

The services will be brokered and/or managed by the West Virginia Office of Technology (WVOT), where applicable. It is the State's intent that Data Transport 2.0 leverage the cost efficiencies of shared services (centralized billing, ordering, technology support, network services, and cybersecurity services).

There are approximately 1000 WAN circuits and services installed statewide under existing telecommunications contracts. The winning Vendor will be expected to provide services to existing sites and at new sites, if requested, during the contract term. (see Exhibit B) There is no guarantee that existing sites detailed in this RFP will require services under the new Vendor contract, since the State is continually opening and closing sites.

The Vendor will be required to work with other technology service provider(s), where necessary, for both the transition from legacy WAN services and for the installation of new WAN services defined in this RFP at various locations across the state. The State's goal is to award a contract to a single Vendor, who will leverage a variety of technology solutions and partner with other technology companies to provide the most secure, robust, reliable, and comprehensive WAN solution for the State. Other technology companies may include (but are not limited to) cellular/wireless carriers, Internet Service Providers (ISPs), Wireless Internet Service Providers (WISPs), and Cable TV companies.

The contract resulting from this RFP is intended to provide a comprehensive procurement vehicle for all listed services and value-added solutions defined in this RFP. The Vendor awarded the contract will be the single responsible party for coordination and installation as well as ongoing maintenance and billing for all of their services and will include all service from the Vendor's technology subcontracting partners.

Segra has read, understands, and will comply.

4.2. DEFINITIONS and ACRONYMS: The terms and abbreviations listed below shall have the meanings assigned to them below.

- **"AS"** means Autonomous System
- **"ASN"** means Autonomous System Number
- **"BGP"** means Border Gateway Protocol
- **"Contract Item"** or **"Contract Items"** means the services defined in Section Four.
- **"DDOS"** means Distributed Denial of Service Attack
- "**Dedicated Internet Access**" (DIA) means a private connection to the Internet that is exclusively dedicated to a business or government for their use.

"

- **"DHCP"** means Dynamic Host Configuration Protocol
- **"DIA"** means Dedicated Internet Access
- "**Distributed Denial of Service Attack**" (DDOS) means a malicious attempt to disrupt the normal traffic of a targeted server, service or network by overwhelming the target or its surrounding infrastructure with a flood of Internet traffic.
- **"DNS"** means Domain Name Services
- **"Edge Router"** means a specialized router located at a network boundary that enables an internal network (LAN) to connect to external networks (WAN).
- **"ESL"** means Eligible Services List
- **"Ethernet WAN Service"** means a service delivered by network and telecom vendors that provides a high-speed connection between sites utilizing a standardized Ethernet connection.
- **"ETP"** means Eligible Telecommunications Provider
- **"FCC"** means Federal Communications Commission
- **"FCDL"** means Funding Commitment Decision Letter
- **"Force Majeure"** means an extraordinary event or circumstance beyond the control of the parties involved.
- **"FRN"** means Funding Request Number
- **"Gbps"** means Gigabits, or one billion bits per second.
- **"GETS"** means Government Emergency Telecommunications Service
- **"IEEE"** means Institute of Electrical and Electronic Engineers
- **"ILEC"** means Incumbent Local Exchange Carrier
- **"IPv4"** means Internet Protocol Version 4
- **"IPv6"** means Internet Protocol Version 6
- **"LAN"** means a Local Area Network (LAN) that connects network devices over a relatively short distance. A networked office building, school, or home usually contains a single LAN, though sometimes one building will contain a few small LANs.
- **"LCP"** means Lowest Corresponding Price
- **"Mbps"** means Megabits, or one million bits per second.
- **"MTTR"** means Mean Time To Repair
- **"Non-Recurring"** means one-time or installation costs for service, requested in the Exhibit A (Pricing Page).
- **"PIA"** means Program Integrity Assurance
- **"Point of Presence (PoP)"** means a point of presence that is an access point to a carrier's network at a building or facility. It may be housed either in the facilities of a telecommunications provider (building entrance or closet) or a location separate from the telecommunications provider (extended PoP).
- "**Postalized**" means rates or prices that are structured so that they are not distance or location sensitive but are dependent on other factors such as type of service, speed of service, etc.
- **"Pricing Section"** means the pricing evaluation sheets where the types and quantities of services are identified. The Vendor should provide pricing per type of transport. Exhibit A is the Pricing Page to be completed for each type of transport that the Vendor is proposing.

- **"Quality of Service" (QOS)** means a set of technologies that work on a network to guarantee its ability to dependably run high-priority applications and traffic under limited network capacity. QoS technologies accomplish this by providing differentiated handling and capacity allocation to specific flows in network traffic.
- **"Recurring"** means monthly recurring costs for solicited services, requested per Exhibit A (Pricing Page).
- **"SD-WAN"** means Software Defined Wide Area Network
- **"SLD"** means Schools and Libraries Division
- **"SLA"** means Service Level Agreement
- **"Solicitation"** means the official notice of an opportunity to supply the State with goods or services that is published by the Purchasing Division.
- **"Special Construction"** means when there are no existing telecommunications facilities to fulfill the need for a new service installation to a physical location and new physical network facilities will need to be built to accommodate the new services requested or to accommodate new service requirements.
- **"SPIN"** means Service Provider Identification Number
- **"TCR"** means Telecommunications Request Form
- **"TSP"** means Telecommunications Service Priority
- **"USAC"** means Universal Service Administrative Company
- **"USF"** means Universal Service Fund
- "**Vendor Response Sheet**" means the information sheet where the Vendor provides details about its company and provides references that match the services being proposed within this solicitation.
- **"VLAN"** means Virtual Local Area Network
- **"VOIP"** means Voice Over Internet Protocol
- **"VPN"** means Virtual Private Network
- **"WAN"** means Wide Area Network, a computer network that covers a large geographical area. WAN includes the technologies to transmit data, image, audio and video information over long distances and among different LANs.
- "**Wireless 4G/5G service**" means a cellular wireless broadband communication service leveraging 4G (4th generation) or 5G (5th Generation) protocols and equipment.
- **"Wireless Bandwidth Throttling"** means that a cellular wireless carrier artificially limits the bandwidth availability for their service
- **"WVOT"** means West Virginia Office of Technology
- **"WVDA"** means West Virginia Department of Administration
- **"WVDE"** means West Virginia Department of Education
- **"WVLC"** means West Virginia Library Commission

Segra has read, understands, and will comply.

4.3. Project Desirables and Goals, and Mandatory Requirements:

The State of West Virginia's goal is to award a contract to a single Vendor, who will leverage a variety of technology solutions and partner with other technology companies when required to provide the most secure, robust, reliable, and comprehensive WAN and Dedicated Internet Access services for the State.

Vendor should describe its approach and methodology to providing their services by addressing the mandatory requirements as well as the goals and objectives identified below. Mandatory requirements relate to the goals and objectives and must be met by the Vendor as a part of its submitted proposal. Vendor should describe how it will comply with the mandatory requirements and include any areas where its proposed solution exceeds the mandatory requirement. Failure to comply with mandatory requirements will lead to disqualification, but the approach/methodology that the vendor uses to comply, and areas where the mandatory requirements are exceeded, will be included in technical scores where appropriate.

Vendor's response should include any information about how the proposed approach is superior to other possible approaches as well as identify areas where the proposed solution exceeds the project expectations.

The State has divided this RFP into four major parts, each with their own mandatory requirements and goals and objectives.

- Part 1: Technology Service and Solution for Ethernet WAN, DIA and 4G/5G Services
- Part 2: Ethernet WAN Service Migration Approach
- Part 3: Service and Support for WAN and DIA and 4G/5G Services
- Part 4: Security for WAN and DIA Services

Segra has read, understands, and will comply.

4.3.1. Goals and Objectives

4.3.1.1. Part 1: Technology Service and Solution for Ethernet WAN, DIA and 4G/5G Services

4.3.1.1.1. Ethernet WAN Service

4.3.1.1.1.1. The State desires that the Vendor have an online performance management and support portal that, at a minimum, the State can use to enter and track new trouble tickets, review pending trouble tickets and the performance statistics of installed services. The State desires that the Vendor have an online performance management and support portal that at minimum the State can use to enter and track new trouble tickets, review pending trouble tickets and the performance statistics of installed services.

Please describe your solution's ability to provide an online portal for Ethernet WAN services that meets or exceeds this goal.

Your dedicated Account Manager, in conjunction with Segra Customer Care specialists, will support WVOT for new orders and non-service related items. In addition, Segra offers a customer ticket portal for moves/adds/changes and opening trouble tickets.

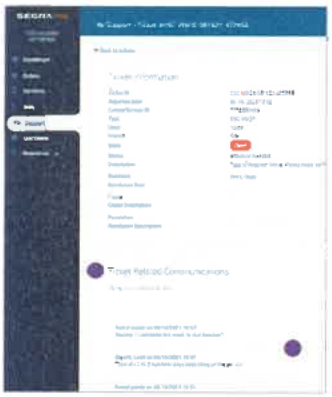
Segra will provide WVOT access to our new Segra360 online customer portal for trouble ticketing. This portal is available 24x7x365 and allows users to engage with us and interact directly with the services we provide.

Segra360 will be the gateway to providing real-time digital communications along with future self-service transactions under a single pane of glass. Users will be able to submit, track, and manage inquiries.

The latest Segra360 release includes in-app messaging that customers can use to discuss support tickets with Segra. This release also provides resolution information for closed tickets.

In-App Messaging for Support Tickets

Start, review or continue a discussion about a support ticket using messaging provided in the Support module.



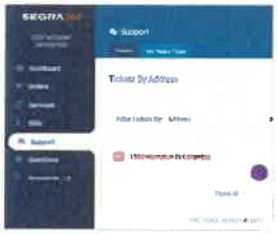
Messages are color-coded for easy tracking. Customer messages appear in green and Segra messages in blue.

Submit, check on, and discuss Segra support tickets, all without leaving the portal.

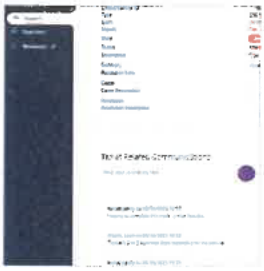
In-App Messaging for Support Tickets: How It Works

From the Support Module, click on a site.

Click a ticket ID.



View the ticket's messages



Enter a message and click Reply to submit it.

Resolution Information for Closed Support Tickets

View the date a ticket was resolved, the action taken to resolve it, and more.

Convenient access to ticket-resolution details

Viewing Ticket Resolution Information: How It Works

From the Support Module, click on a site.

Click the ID of a closed ticket.

View the resolution information.

4.3.1.1.1.2. The State desires that the Vendor provide Ethernet WAN services that utilize SD-WAN overlay services as defined in the Metro Ethernet Forum (MEF) 3.0 standards. https://www.mef.net/service-standards/overlay-services/sd- wan/. Please describe your company's ability to meet this goal.

The Segra SD-WAN design provides customers with a highly available solution by bonding Segra's primary service to secondary and back-up WAN options (private fiber based, public fiber based, broadband, bonded T1s, LTE, Ethernet over Copper). This approach will allow the customer to customize the WAN applications and policies by site, via our online portal.

Please refer to **Segra's SD-WAN Solution Exhibit**, included in our response on page 168.

4.3.1.1.2. Dedicated Internet Access Service (DIA)

4.3.1.1.2.1. The State desires that the Vendor have an online performance management and support portal that, at

a minimum, the State can use to enter and track new trouble tickets, review pending trouble tickets and the performance statistics of installed services. Please describe your solution's ability to provide an online portal for DIA services that meets or exceeds this goal.

Your dedicated Account Manager, in conjunction with Segra Customer Care specialists, will support WVOT for new orders and non-service related items. In addition, Segra offers a customer ticket portal for moves/adds/changes and opening trouble tickets.

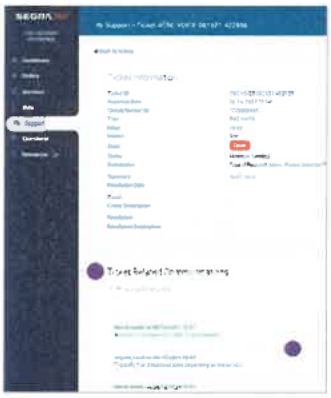
Segra will provide WVOT access to our new Segra360 online customer portal for trouble ticketing. This portal is available 24x7x365 and allows users to engage with us and interact directly with the services we provide.

Segra360 will be the gateway to providing real-time digital communications along with future self-service transactions under a single pane of glass. Users will be able to submit, track, and manage inquiries.

The latest Segra360 release includes in-app messaging that customers can use to discuss support tickets with Segra. This release also provides resolution information for closed tickets.

In-App Messaging for Support Tickets

Start, review or continue a discussion about a support ticket using messaging provided in the Support module.

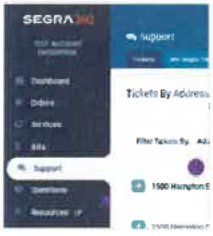


Messages are color-coded for easy tracking. Customer messages appear in green and Segra messages in blue.

Submit, check on, and discuss Segra support tickets, all without leaving the portal.

In-App Messaging for Support Tickets: How It Works

From the Support Module, click on a site.



Click a ticket ID.

View the ticket's messages

Enter a message and click Reply to submit it.

Resolution Information for Closed Support Tickets

View the date a ticket was resolved, the action taken to resolve it, and more.

Convenient access to ticket-resolution details

Viewing Ticket Resolution Information: How It Works

From the Support Module, click on a site.

Click the ID of a closed ticket.

View the resolution information.

4.3.1.1.3. 4G/5G Wireless Service

4.3.1.1.3.1. State desires a single bill from Vendor that includes wireless service as well as Ethernet WAN and DIA services. Please describe your solution's ability to provide an integrated services bill that meets or exceeds this goal.

Segra has read, understands, and will comply. Segra can provide a single invoice for wireless, WAN, and DIA services.

4.3.1.2.Part 2: Vendor Ethernet WAN Services Migration Plan

4.3.1.2.1. The State desires a finalized and agreed upon an Operations Plan within sixty (60) calendar days of contract effective date for the management, support, and maintenance of the State's current WAN infrastructure. Please describe your company's ability to deliver the finalized Operations Plan to the State within sixty (60) calendar days of contract effective date with scheduling the appropriate meetings, making changes after State input, and meeting deadlines.

Segra has read, understands, and will comply.

WVOT will be assigned a dedicated project manager to oversee the implementation of the services proposed in this RFP. Upon contract award, your project manager will create a schedule to bring all sites online based on the Project Plan below.

The goal of Segra's project management team is to provide a superior, seamless experience for our customers by establishing a single point of accountability for service implementation projects. Your project manager will ensure expedites, escalations, and jeopardies are handled appropriately and that all critical project dates are met. Your project manager will also coordinate the activities of individual team members across all Segra departments (as well as the customer's vendors if the customer concurs) and will ensure that all field personnel are assigned as needed based on the location and scope of the project. Throughout the project, your project manager will be able to provide status reports, identify, assign, and track to closure all project issues and action items, and reach an agreement on all changes to the project scope.

Project Plan

Segra's Project Plan methodology involves the use of recognized Project Management tools, as listed in Table 1 below, to ensure that projects are carefully planned, successfully executed, and closed out with the customer's concurrence that commitments have been met.

Table 1 – Project Management Tools

Initiating and Planning the Project	Executing, Monitoring, and Controlling the Project	Closing the Phase/Project
Project Scope and Charter	Change Request Form	Project Close-Out Checklist
Project Schedule	Change Control Log	Quality Review Plan
Risk Analysis and Mitigation Plan	Issue Log	Close-Out Package
Work Breakdown Structure (WBS)	Action Item Log	
Communication Plan	Project Status Reports	
Project Team Contact List		
Contract/Vendor Management Plan		

Executing, Monitoring, and Controlling the Project

Once the order is submitted, the Segra Project Manager will ensure that expedites, escalations, and jeopardies are handled appropriately and that all critical project dates are met. The Project Manager will coordinate the activities of individual project team members across all Segra departments (as well as the customer's vendors if the customer concurs) and will ensure that all field personnel are assigned as needed based on the location and scope of the project. Throughout the project, the Segra Project Manager will be responsible for:

- Managing Change Control processes, including changes in scope and variations in the Statement of Work (SOW);
- Tracking timelines, deliverables, action items, and outcomes associated with the project;
- Managing the Risk Mitigation plan, including identifying new risks associated with schedule and quality as they arise, and working with the customer and the project team to create action plans that address and/or mitigate potential issues; and

- Scheduling and running project status meetings and acting as the primary interface between the customer and the Segra implementation team.

The Project Manager will also meet with the customer at regularly scheduled intervals, as mutually agreed upon. The purpose of the meetings will be to provide status reports to the customer, to identify, assign, and track to closure all project issues and action items, and to reach an agreement on all changes to the project scope. These meetings will be held as often as necessary, but at least monthly. The timing and location of these meetings will be established with the customer during the project-planning phase, and the meetings may be in person or via conference call as deemed necessary by both parties.

Closing the Project

After installation is complete and service has been activated and tested, signed customer acceptance will be obtained, scanned, and saved to the appropriate customer project file. After completion of the project, a Segra representative will conduct a First Bill Review, including a financial audit, to review and clarify any discrepancies between the original contract and the actual billing. Project close-out activities will also include knowledge transfer and the release of project resources.

Project Implementation

The normal installation interval for fiber-based WAN services is approximately 90 to 180 business days from the date that Segra receives a clean order.

Segra follows the Project Management Body of Knowledge (PMBOK) process for project implementation. Throughout the implementation process, the various teams follow the steps listed below:

Section	Description	Activity
1.	Project Management	
	1.	Manage overall implementation process.
	2.	Track baseline and variation timelines.
	3.	Track Action Items.
	4.	Track project deliverables.
	5.	Implement Communications Plan.
	6.	Provide consistent updates to all project team members.
	7.	Ensure consistent compliance with completion of prerequisite tasks.
	8.	Regularly and consistently monitor the implementation and integration of the solution.
	9.	PM will act as the primary escalation point for technical and non-technical issues and will obtain the necessary resources to resolve any issues.
	10.	Define assigned points of contact and team escalation points for the entirety of the solution implementation.
2.	Planning and Preparation	
2.1	Readiness Assessment	
	1.	Detailed assessment of applications to help determine the bandwidth needed at

Section	Description	Activity
		each site. Specific address, telephone, and contact information gathered for service inquiries. Information to be obtained through a combination of interviews with appropriate personnel and network assessment tools.
	2.	Review and analyze the data collected in order to determine the suitability of the network elements and links to support desired bandwidth. Identify areas that require improvements and provide recommendations in order for the affected network to be rectified to handle WAN access.
2.2	Operations Planning	
	1.	Assess current operational and maintenance processes and methods of procedures.
	2.	Develop or redefine operational and maintenance processes as needed.
	3.	Define interface and flow requirements between WVOT and Segra CNOC or other organizations as appropriate.
	4.	Identify appropriate personnel necessary to develop interface agreements.
	5.	Provide interface documentation and train all necessary personnel on plan.
	6.	Define escalation procedures.
3.	Initial Set-Up Verification	
	1.	Complete user profiles and billing information.
	2.	Receive, in writing, customer's decision on bandwidth needs.
4.	Training	
	1.	Define training requirements for different platforms.
	2.	Develop training delivery schedules.
	3.	Identify and reserve training locations.
	4.	Provide end user training material for use during rollout.
5.	General Prerequisites	
	1.	Develop a customer document containing service information, processes, escalation, and contact information.
	2.	Perform Operational Readiness Test.
6.	Performance Management	
	1.	Establish performance standards.
	2.	Identify standard report requirements.
	3.	Define required reports.
	4.	Collect and analyze data.
	5.	Generate reports.

Section	Description	Activity
	6.	Perform trend analysis.
	7.	Distribute reports.
	8.	Review Internet Conferencing utilization periodically.
7.	Service Provisioning	
	1.	Issue order for fiber access and service.
	2.	Order is tracked. Segra Project Manager will provide status updates to the customer throughout the provisioning process.
	3.	Project Manager will direct, assist, and manage premise equipment activities associated with orders.
	4.	Complete fiber installation and send test ticket to Segra Operations for testing (2 days).
	5.	Upon completion of final operations task, an automatic email notification is generated to the customer stating that the service is ready. Circuit information is included in this email.
	6.	Segra Project Manager will work with the customer to schedule a date for the cut to the new service.
	7.	Segra Project Manager will email an Outlook invitation to the customer and Segra Installations/Operations with confirmed cut date.
8.	Project Close-Out	
	1.	Develop project findings with the customer.
	2.	Produce reports of surveys and performance information as necessary.
	3.	Review project documentation with the customer.

4.3.1.2.2. The State desires all sites listed in Appendix A be migrated to vendor Ethernet WAN service within 365 calendar days from contract effective date. The State reserves the right to reprioritize this list as necessary. Please describe your company's plan to accomplish these migrations. Please describe your company's ability to migrate all sites listed in Appendix A within 365 calendar days from contract effective date.

Segra has read, understands, and will comply.

We anticipate the installation interval to be approximately 90 to 180 days for sites requiring special construction. If a site requires a 45-day installation, a 4G/5G, broadband solution or an alternative access circuit may be installed to mitigate delays. With effective planning and communication, Segra will be able to migrate within the 365 calendar day requirement outlined.

A dedicated project manager will be assigned to oversee the implementation of the services proposed in this RFP. The goal of Segra's project management team is to provide a superior, seamless experience for our customers by

establishing a single point of accountability for service implementation projects. The project manager will ensure expedites, escalations, and jeopardies are all handled appropriately and that all critical project dates are met.

For further information on Segra's implementation plan, please refer to our **Project Methodology**, included in our response on page 94.

4.3.1.3. Part 3: Service and Support for WAN and DIA and 4G/5G Services

4.3.1.3.1. If the Vendor's work requires them to be at a State site, the Vendor should provide Agency at least 72 hours' notice before arriving at the site and comply with State law and all Agency policies, including but not limited to background checks for contractors, vendors, and visitors. Please describe your approach and methodology in your solution/response.

Segra has read, understands, and will comply.

Testing and Acceptance after Site Turn-Up

Segra will assume that access to the State of West Virginia and related Agency facilities for verification testing will require, at a minimum, the following information:

- State of West Virginia facility location (physical address);
- Procedures for physical access to the State of West Virginia facility (including point of contact for access);
- A list of Segra personnel requiring access;
- The dates when access is required;
- Test cases to be performed at the State of West Virginia facility; and
- Equipment required at the facility to complete the verification testing.

4.3.1.3.2. Vendor should describe their company's ability to hold regular meetings on each of these topics, as well as their company's implementation plans for starting these discussions:

4.3.1.3.2.1. Architecture and Design
4.3.1.3.2.2. Implementation
4.3.1.3.2.3. Ordering and Billing
4.3.1.3.2.4. Service and Support
4.3.1.3.2.5. Project Management

Segra has read, understands, and will comply.

Segra has a robust Project Management Team, which is led by Dan Watts, Chief Operating Officer (22 years) and Cheryl Thibodeaux, Director Project Management (24 years). Cheryl's department consists of thirty-two (32) Project Managers with most having ten (10) plus years of experience managing projects.

A certified dedicated project manager will be assigned to each government agency to oversee the implementation of the services proposed in this RFP. The goal of Segra's project management team is to provide a superior, seamless experience for our customers by establishing a single point of accountability for service implementation projects. Your project manager will ensure expedites, escalations, and jeopardies are handled appropriately and that all critical project dates are met. Your project manager will also coordinate the activities of individual team members across all Segra departments, as well as the customer's vendors if the customer concurs, and will ensure that all field personnel

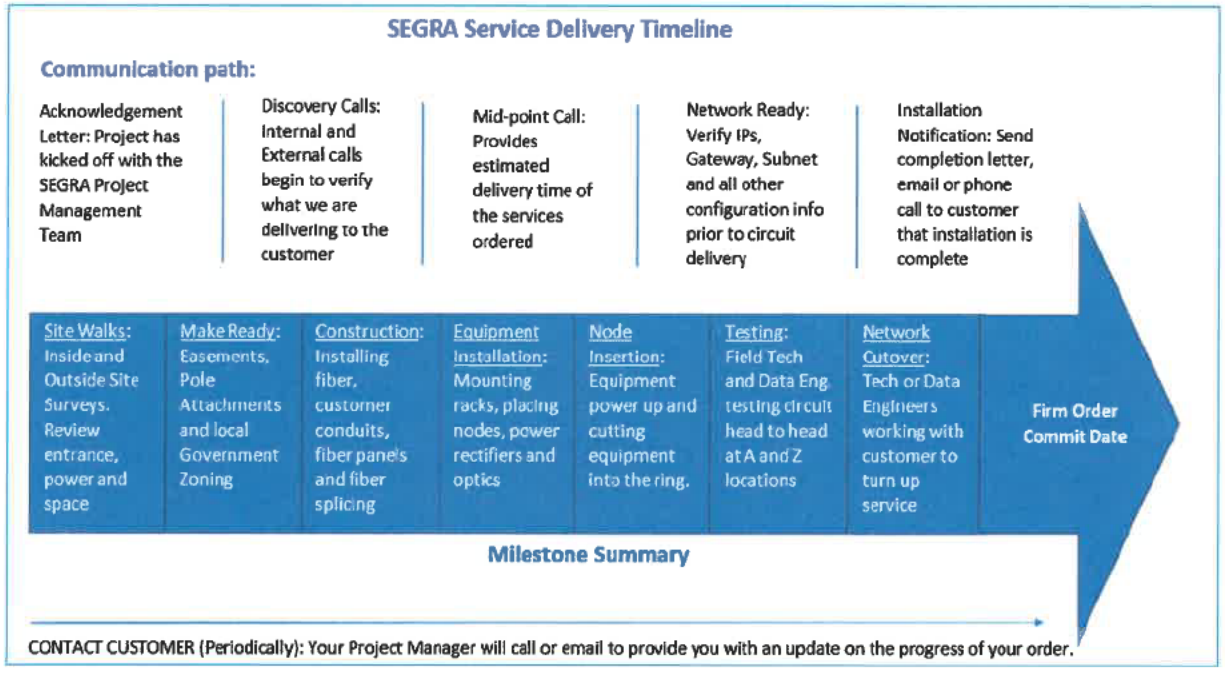
are assigned as needed based on the location and scope of the project. Throughout the project, your project manager will be responsible for:

- Managing the Change Control processes, including changes in scope and variation in the Statement of Work (SoW);
- Tracking timelines, deliverables, action items, and outcomes associated with the project;
- Managing the Risk Mitigation Plan, including identifying new risks associated with the schedule and quality as they arise, and working directly with the customer and project team to crate action plans that address and/or mitigate potential issues; and
- Scheduling and running project status meetings and acting as the primary interface between the customer and the Segra implementation team.

The Project Manager will also meet with the specific government agency at regularly scheduled intervals. The purpose of these meetings will be to provide status reports, identify and track to closure any project issues and action items, and to reach agreement on all changes to the project scope.

Project Schedule

Segra uses specific project management teams and assigns specific project managers on each project who are responsible for coordinating all aspects and interactions to ensure accurate and timely completion. Additionally, we keep a KPI (Key Performance Indicator) at Segra for On Time Delivery by the month. We use the Initial FOC (Firm Order Commitment date), which is an agreed upon date by Segra and the customer. This date does not change, and we track to completion for On Time or Earlier. We have a testing and acceptance team that is responsible for end-to-end testing and issuing a certificate that the circuit is ready to hand off. Following testing, a coordinated Activation of Services is scheduled with Segra technicians and the customer's vendor support for completion.



4.3.1.3.3. The State desires a service order tracking web portal, including real-time updates for new and pending service orders. The State desires details including the following data elements:

- **4.3.1.3.3.1.** Telecommunications Change Request (TCR) Form Number
- **4.3.1.3.3.2.** Date order was received
- **4.3.1.3.3.3.** Department/Agency Name where service is being installed
- **4.3.1.3.3.4.** Department/Agency where service is being installed address
- **4.3.1.3.3.5.** Projected due date
- **4.3.1.3.3.6.** Rate element identifier (circuit ID or other)
- **4.3.1.3.3.7.** Additional order details

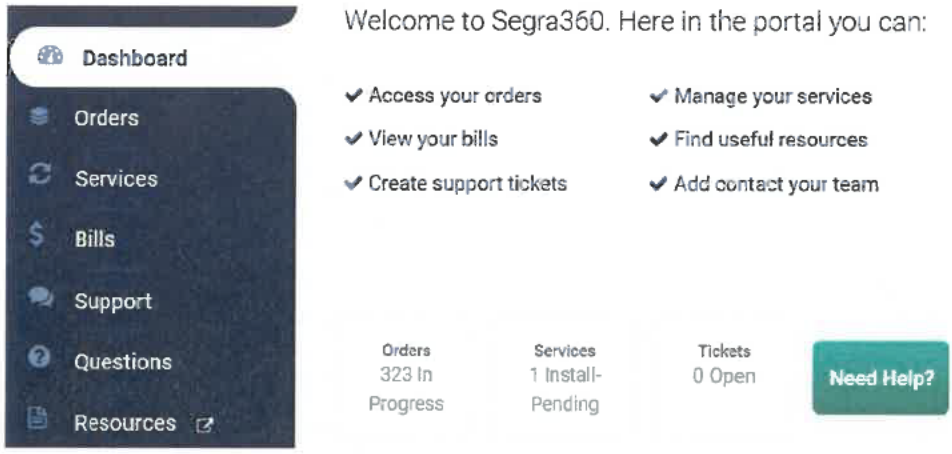
The State will place orders, disconnects, and changes through its established TCR process; however, the State desires this portal to provide more transparency and faster updates without the need to contact the Vendor. Please describe your company's ability to provide this portal, as well as any requirements from the State needed to implement such a program.

Segra has read, understands, and will comply with having its Service Desk accepting incident notifications and service requests from WVOT by means of voice calls, email submissions, and through the required web portal.

Segra is pleased to offer Segra360, our new online web portal, as a way for our customers to engage with us and interact directly with the services we provide. This portal is the gateway to providing real-time communications along with future self-service transactions and online order requests under a single pane of glass. Segra360 will provide WVOT or any State Agency with the ability to request new service, change existing service, track the status of the provisioning process as well as view services from an account dashboard, view and download bills, and create and review support tickets.

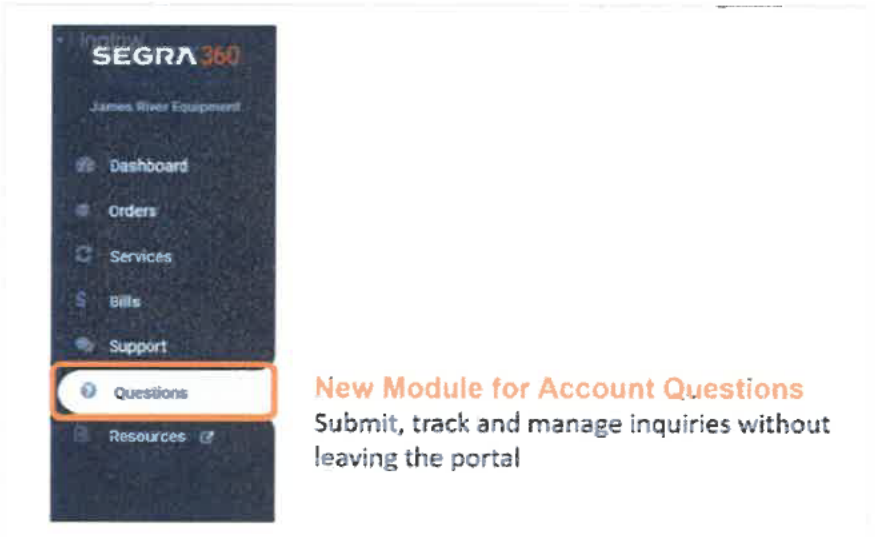
Segra360 is available 24x7x365 and can be accessed from a link on our home page at www.segra.com or directly from www.segra360.com.

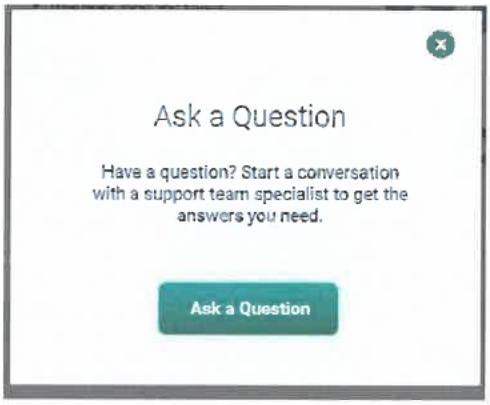
Registered Segra360 users can submit an Inquiry/Question or Support Ticket without leaving the portal using the portal's **'Need Help?'** option on the **Dashboard** or through the **Questions** module. In addition, Segra360 includes in-app messaging that customers can use to communicate with Segra. Alternatively, Customer Care can be reached by phone or email at 833.GO.SEGRA (833.467.3472) or customercare@segra.com.



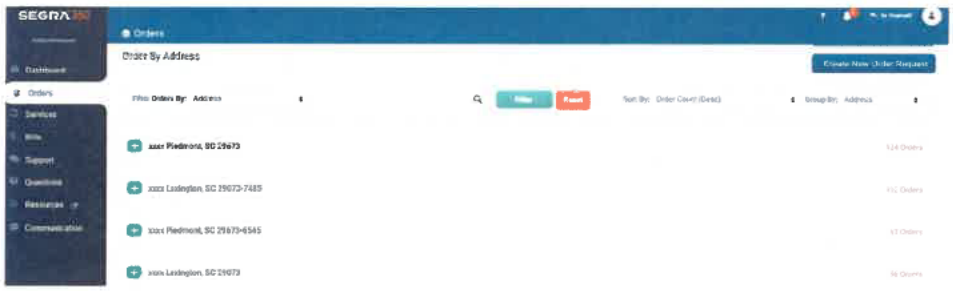
INQUIRY MANAGEMENT

Submit, track and manage inquiries without leaving the portal

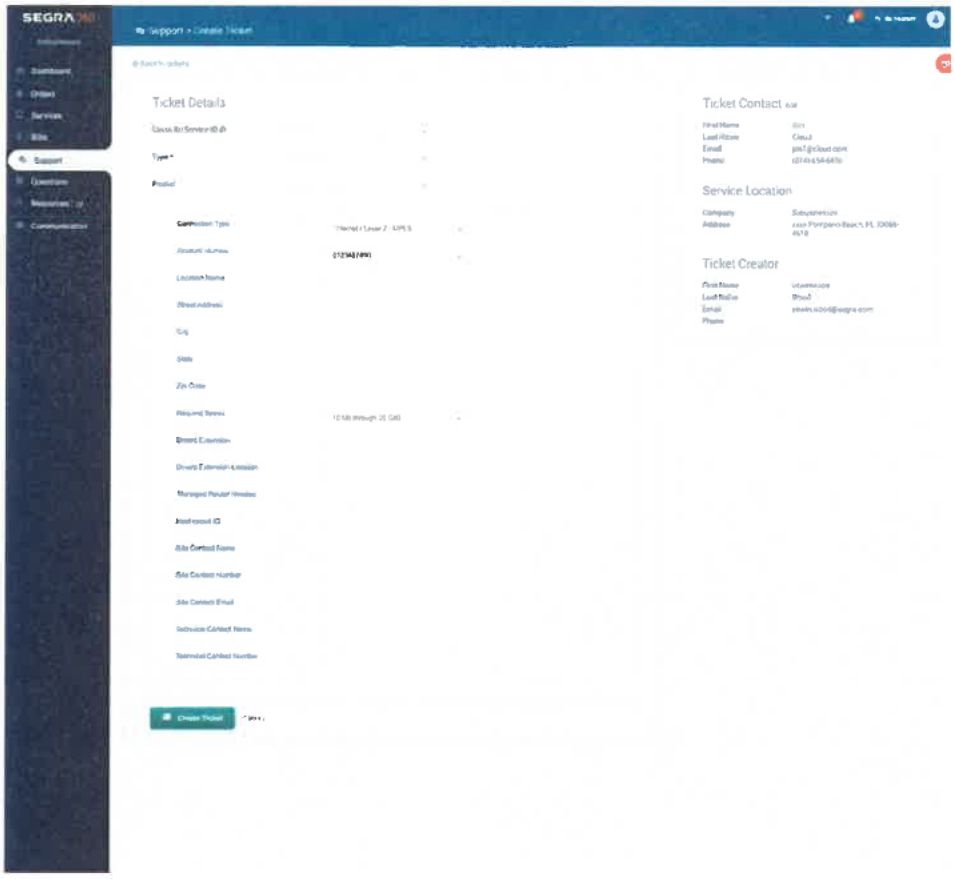




From the **Orders** module, customers are able to create new orders as well as filter, sort, or group data by Address, Order ID, Status, Charges, and Due Date. This feature will be restricted so that orders can only be placed on contracted services.



Customer Order Detail Information – Creating a ticket to request a NEW order

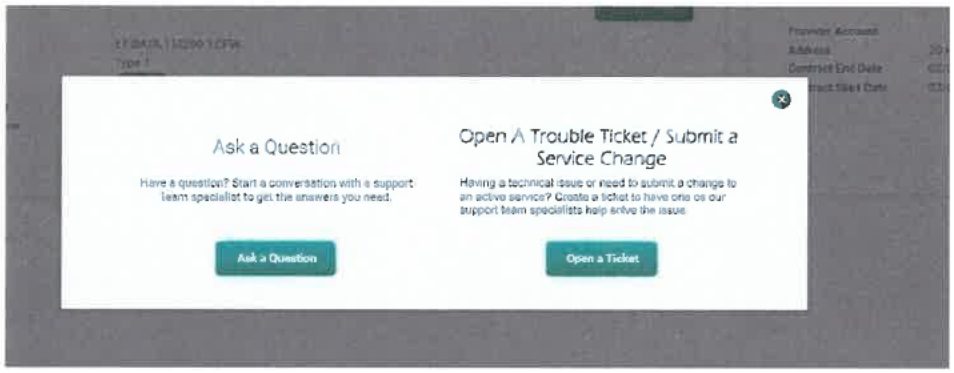


ORDERS MODULE: EASIER ACCESS TO ORDER INFORMATION

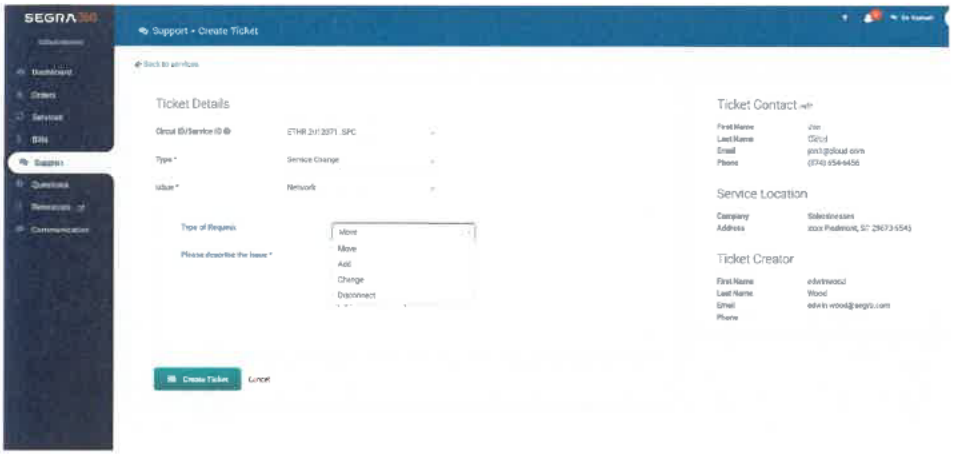
Shows Customer Orders with Ability to Filter, Sort, and Group Data

From the **Services** module, customers are able to create change orders (i.e., upgrades or disconnects) on existing services.

Submitting an Issue or Change to a Service

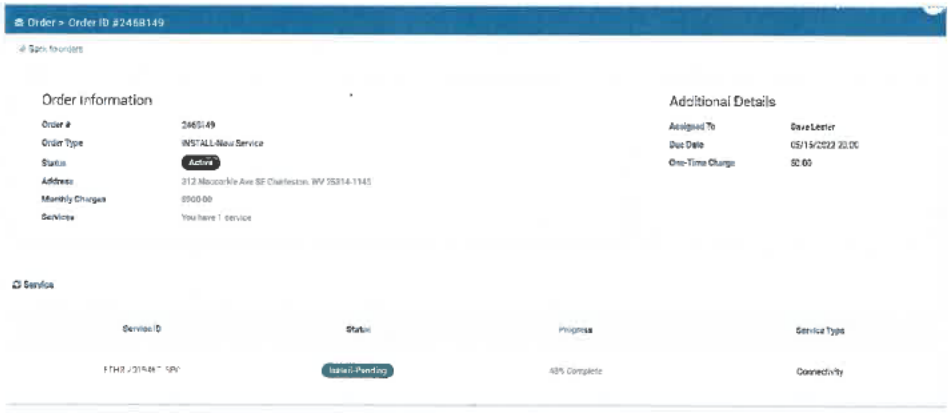


Service Change Detail



Once the request is submitted, the user will receive an email confirmation of the ticket number. Notifications will also be emailed when the ticket is updated and/or closed. Open tickets are also displayed on the user's Dashboard as shown below.

A detailed order status is also available, which shows the order completion progress.



4.3.1.3.4. Vendor should contact the State's engineering points of contact by phone within thirty (30) minutes of a Vendor network outage that affects multiple sites on the State's network. This verbal notification should be followed with a written report that provides an explanation of the problem, the cause of the problem, the solution to the problem, the estimated time for recovery, and the steps taken or to be taken to prevent a reoccurrence. The Vendor should provide onsite staff to the location, as necessary, within twelve (12) hours of the outage. To that end, please describe your company's notification procedures in the case of an outage.

Segra had read, understands, and will comply.

Segra has 70+ technicians and engineers who work in the support centers covering three shifts to assure around the clock support for customers. The following list details performance objectives for the Segra Network Operations Center. Staffing is designed to meet the objectives listed below.

ELEMENT	OBJECTIVE
NOC Availability	24 hours per day, 365 days per year
Average Speed of Answer	15 seconds
Answer Time	90% answered within 15 seconds
Customer Status (Priority 1)	1 hour interval 95% on-time
Account Team Notification	Within 15 minutes of Priority 1 ticket generation

4.3.1.3.5. Vendor should provide written notification of ten (10) business days or more in advance of any planned upgrades, modifications, etc. that may affect the State's customers to the State's engineering points of contact. Please describe your company's notification process for planned maintenance.

For purposes of notification, maintenance will be designated as one of two types — **Scheduled Maintenance** and **Emergency Maintenance**.

Scheduled Maintenance is any maintenance at Segra to which the customer's circuit is connected that is performed between 12:00 AM and 6:00 AM or if possible otherwise scheduled according to the customer's or company's request and is mutually agreed upon by both parties. The customer will receive at least **7 days'** advance notice of service-impacting Scheduled Maintenance.

Emergency Maintenance is performed in order to promptly respond to and resolve emergency issues associated with service-affecting conditions. The customer will be contacted when Emergency Maintenance has been performed on service-impacting work. Segra's goal is to inform the customer of emergency maintenance at least 48 hours in advance; however, at times it may be of a critical impact that the duration may be shorter.

In the case of Emergencies, Acts of God, Natural Disasters, etc.: Segra will, if practical due to the nature and scale of the emergency, make an attempt at notification. If, however, the Segra NOC receives equipment degradation or failure alarms that will require future repair or replacement, Segra will notify the customer of the imminent activity and estimated time of repair.

MTTR

Mean Time to Repair (MTTR) is the average time required to repair service to an operational condition if service(s) are not active or the customer is experiencing consistent service degradation. The MTTR objective is four (4) hours for outages due to electronic equipment failure and fiber optic facilities failure and ten (10) hours for outages due to fiber cuts.

Please refer to **Segra's Service Level Agreement (SLA)**, included in our response on page 186.

4.3.1.3.6. Vendor should provide notification of three (3) business days or more in advance of emergency maintenance. While the State understands emergency outages and/or unplanned maintenance windows occur, it is expected that these situations are kept to a minimum. Please describe your company's notification process for emergency maintenance and outages.

For purposes of notification, maintenance will be designated as one of two types — **Scheduled Maintenance** and **Emergency Maintenance**.

Scheduled Maintenance is any maintenance at Segra to which the customer's circuit is connected that is performed between 12:00 AM and 6:00 AM or if possible otherwise scheduled according to the customer's or company's request and is mutually agreed upon by both parties. The customer will receive at least **7 days'** advance notice of service-impacting Scheduled Maintenance.

Emergency Maintenance is performed in order to promptly respond to and resolve emergency issues associated with service-affecting conditions. The customer will be contacted when Emergency Maintenance has been performed on

service-impacting work. Segra's goal is to inform the customer of emergency maintenance at least 48 hours in advance; however, at times it may be of a critical impact that the duration may be shorter.

In the case of Emergencies, Acts of God, Natural Disasters, etc.: Segra will, if practical due to the nature and scale of the emergency, make an attempt at notification. If, however, the Segra NOC receives equipment degradation or failure alarms that will require future repair or replacement, Segra will notify the customer of the imminent activity and estimated time of repair.

MTTR

Mean Time to Repair (MTTR) is the average time required to repair service to an operational condition if service(s) are not active or the customer is experiencing consistent service degradation. The MTTR objective is four (4) hours for outages due to electronic equipment failure and fiber optic facilities failure and ten (10) hours for outages due to fiber cuts.

Please refer to **Segra's Service Level Agreement (SLA)**, included in our response on page 186.

4.3.1.3.7. The Vendor's solution should include a documented support and escalation structure to address outages. The State prefers the severity of the issue/support problem to determine the average problem resolution response time, as outlined below:

4.3.1.3.7.1. Severity Level 1 is defined as an urgent situation, where the customer's services are unavailable, and the customer is unable to use/access the network. The Vendor should resolve Severity Level 1 problems as quickly as possible, which on average should not exceed two (2) business hours. If repair inside the 2-hour window is not feasible, then regular 1-hour updates are desired.

Please refer to **Segra's Escalation Contacts and Contact Information**, and **Segra's Service Level Agreement (SLA)**, included in our response on pages 190 and 186, respectively.

Network Operations Center (NOC)

Segra's Network Operations Center has certified personnel accessible 24x7x365 to ensure your service is monitored and well looked after.

Segra supports our customers with geo-redundant network operations centers located in Waynesboro, VA and Columbia, SC. Segra's geo-redundant centers operate on a 24x7x365 basis.

Details of Segra's capabilities:

Issue Resolution and Maintenance

Segra has two 24/7/365 geo-redundant Network Operations Centers in Columbia, SC and Waynesboro, VA. Segra Field Operations Support teams are also located strategically in the markets served. Fiber restoration crews are also dispersed throughout our markets.

Segra's Enterprise Repair Team (ERT) is composed of a team of dedicated W-2 Segra engineers who are responsible for monitoring, troubleshooting, and maintaining the entire Segra network and the services provided. As the first point of contact for our customers, the ERT is responsible for generating trouble tickets on all issues, dispatching technicians if necessary, isolating the problem, keeping customers updated, and driving all troubles to completion. Quick trouble resolution with a sense of urgency is our priority, and we are available 24x7x365.

The Network Operations Center (NOC) manages all change management network events (high-risk maintenance activities) along with delivering on SLA parameters for mission critical services.

The Segra NOC tracks all events via trouble ticket(s). Customer event updates are provided via phone calls or emails directly from our ticketing system.

If an outage occurs, Segra has Ethernet test heads strategically placed throughout the network to perform RFC 2544 testing on demand, which supports our ability to meet the four-hour MTTR objective in our Service Level Agreement (SLA).

For any maintenance related activities, the Change Management group will notify customers via email of any service impacting scheduled work. Segra strives to give all customers at least seven (7) days' advance notice for all regularly scheduled maintenance. These events take place between the hours of 12:01AM and 5:59AM. Segra reserves the right to perform emergency maintenance during service impacting events.

Mean Time to Repair Objective is Four (4) Hours

Mean Time to Repair (MTTR) is the average time required to repair service to an operational condition if service(s) are not active or the customer is experiencing consistent service degradation. The MTTR objective is four (4) hours for normal circuit outages, and ten (10) hours for fiber damages.

If an outage occurs, Segra has Ethernet test heads strategically placed throughout the network to perform RFC 2544 testing on demand, which supports our ability to meet the four-hour MTTR in our Service Level Agreement (SLA).

Segra has two 24/7/365 geo-diverse Network Operations Centers in Columbia, SC and Waynesboro, VA. Segra Field Operations Support teams are also located strategically in the markets served. Fiber restoration crews are also dispersed throughout our markets.

The severity/priority levels and escalation procedures are identical for all traffic types. The management escalation procedures for each severity/priority level are as follows:

- **Critical** - A critical ticket is defined as a service outage that has a severe impact on customer business operations with no workaround available. This condition includes a critical work stoppage during the customer's normal working hours that affects multiple customer sites and/or affects a critical component or function of the customer's business. Segra and its vendor-partners will commit substantial resources around the clock to resolve the situation. Examples of critical outages include an agency host major outage or 10% or greater of the current agency node count in production status.

  - Critical – Escalation Interval
    - Immediate: CNOC Manager & Director
    - 2 Hours: Vice President
- **Major** - A major ticket describes a condition where a partial service outage occurs or the service is severely degraded, which has a significant impact on customer business operations, with no adequate workaround available. This condition includes a partial work stoppage or severe performance degradation during the customer's normal working hours, which affects a customer site. Segra and vendor-partners will commit full time resources during business hours or around the clock as necessary to resolve the situation.
  - Major – Escalation Interval
    - Immediate: Tier 3 CNOC Analyst
    - 1 Hour: Floor Manager
    - 2 Hours: CNOC Manager
    - 3 Hours: Director
    - 5 Hours: Vice President
  - Escalations can be made at the customer's request
- **Minor** - A minor ticket describes conditions where difficulties are experienced with a transport service, but do not cause a work stoppage; there is a workaround, but performance and/or system functionality may be degraded or limited. This condition includes degraded service performance and impaired service functionality, but most business operations continue. Workarounds are established, implemented, and documented for problems with this priority level. Segra will commit resources during business hours as required to resolve problems with this severity level.
- **Informational** - An informational ticket describes conditions that are not urgent, and/or are not problems, and/or that do not impact customer business operations. Informational tickets are for the CNOC. This priority level is most appropriate for:
  - Minor alarms and informational alarms
  - Escalations can be made at the customer's request

4.3.1.3.7.2. Severity Level 2 is defined as significant outages and/or repeated failures resulting in limited effective use by the customer. The service may operate but is severely restricted (i.e., slow response, intermittent but repeated inaccessibility, etc.). The Vendor should resolve Severity Level 2 problems as quickly as possible, which on average should not exceed four (4) business hours. If repair inside the 4-hour window is not feasible, then regular 2-hour updates are desired.

Segra has read, understands, and will comply.

Please refer to **Segra's Escalation Contacts and Contact Information** and **Segra's Service Level Agreement (SLA)**, included in our response on pages 190 and 186, respectively.

Network Operations Center (NOC)

Segra's Network Operations Center has certified personnel accessible 24x7x365 to ensure your service is monitored and well looked after.

Segra supports our customers with geo-redundant network operations centers located in Waynesboro, VA and Columbia, SC. Segra's geo-redundant centers operate on a 24x7x365 basis.

Details of Segra's capabilities:

Issue Resolution and Maintenance
Segra has two 24/7/365 geo-redundant Network Operations Centers in Columbia, SC and Waynesboro, VA. Segra Field Operations Support teams are also located strategically in the markets served. Fiber restoration crews are also dispersed throughout our markets.

Segra's Enterprise Repair Team (ERT) is composed of a team of dedicated W-2 Segra engineers who are responsible for monitoring, troubleshooting, and maintaining the entire Segra network and the services provided. As the first point of contact for our customers, the ERT is responsible for generating trouble tickets on all issues, dispatching technicians if necessary, isolating the problem, keeping customers updated, and driving all troubles to completion. Quick trouble resolution with a sense of urgency is our priority, and we are available 24x7x365.

The Network Operations Center (NOC) manages all change management network events (high-risk maintenance activities) along with delivering on SLA parameters for mission critical services.

The Segra NOC tracks all events via trouble ticket(s). Customer event updates are provided via phone calls or emails directly from our ticketing system.

If an outage occurs, Segra has Ethernet test heads strategically placed throughout the network to perform RFC 2544 testing on demand, which supports our ability to meet the four-hour MTTR objective in our Service Level Agreement (SLA).

For any maintenance related activities, the Change Management group will notify customers via email of any service impacting scheduled work. Segra strives to give all customers at least seven (7) days' advance notice for all regularly scheduled maintenance. These events take place between the hours of 12:01AM and 5:59AM. Segra reserves the right to perform emergency maintenance during service impacting events.

Mean Time to Repair Objective is Four (4) Hours
Mean Time to Repair (MTTR) is the average time required to repair service to an operational condition if service(s) are not active or the customer is experiencing consistent service degradation. The MTTR objective is four (4) hours for normal circuit outages, and ten (10) hours for fiber damages.

If an outage occurs, Segra has Ethernet test heads strategically placed throughout the network to perform RFC 2544 testing on demand, which supports our ability to meet the four-hour MTTR in our Service Level Agreement (SLA).

Segra has two 24/7/365 geo-diverse Network Operations Centers in Columbia, SC and Waynesboro, VA. Segra Field Operations Support teams are also located strategically in the markets served. Fiber restoration crews are also dispersed throughout our markets.

The severity/priority levels and escalation procedures are identical for all traffic types. The management escalation procedures for each severity/priority level are as follows:

- **Critical** - A critical ticket is defined as a service outage that has a severe impact on customer business operations with no workaround available. This condition includes a critical work stoppage during the customer's normal working hours that affects multiple customer sites and/or affects a critical component or function of the customer's business. Segra and its vendor-partners will commit substantial resources around the clock to resolve the situation. Examples of critical outages include an agency host major outage or 10% or greater of the current agency node count in production status.
    - Critical – Escalation Interval
        - Immediate: CNOC Manager & Director
        - 2 Hours: Vice President
- **Major** - A major ticket describes a condition where a partial service outage occurs or the service is severely degraded, which has a significant impact on customer business operations, with no adequate workaround available. This condition includes a partial work stoppage or severe performance degradation during the customer's normal working hours, which affects a customer site. Segra and vendor-partners will commit full time resources during business hours or around the clock as necessary to resolve the situation.
    - Major – Escalation Interval
        - Immediate: Tier 3 CNOC Analyst
        - 1 Hour: Floor Manager
        - 2 Hours: CNOC Manager
        - 3 Hours: Director
        - 5 Hours: Vice President
    - Escalations can be made at the customer's request
- **Minor** - A minor ticket describes conditions where difficulties are experienced with a transport service, but do not cause a work stoppage; there is a workaround, but performance and/or system functionality may be degraded or limited. This condition includes degraded service performance and impaired service functionality, but most business operations continue. Workarounds are established, implemented, and documented for problems with this priority level. Segra will commit resources during business hours as required to resolve problems with this severity level.
- **Informational** - An informational ticket describes conditions that are not urgent, and/or are not problems, and/or that do not impact customer business operations. Informational tickets are for the CNOC. This priority level is most appropriate for:
    - Minor alarms and informational alarms
    - Escalations can be made at the customer's request

4.3.1.3.7.3. Severity Level 3 is defined as a minor problem that exists with the service, but most of the functions are still usable, and some circumvention may be required to provide service. The Vendor should resolve Severity Level 3 problems as quickly as possible, which on average should not exceed ten (10) business hours. If repair inside the 10-hour window is not feasible, then updates are desired at the start of the next business day and every day thereafter until repairs are complete.

Please refer to **Segra's Escalation Contacts and Contact Information** and **Segra's Service Level Agreement (SLA)**, included in our response on pages 190 and 186, respectively.

Network Operations Center (NOC)

Segra's Network Operations Center has certified personnel accessible 24x7x365 to ensure your service is monitored and well looked after.

Segra supports our customers with geo-redundant network operations centers located in Waynesboro, VA and Columbia, SC. Segra's geo-redundant centers operate on a 24x7x365 basis.

Details of Segra's capabilities:

Issue Resolution and Maintenance
Segra has two 24/7/365 geo-redundant Network Operations Centers in Columbia, SC and Waynesboro, VA. Segra Field Operations Support teams are also located strategically in the markets served. Fiber restoration crews are also dispersed throughout our markets.

Segra's Enterprise Repair Team (ERT) is composed of a team of dedicated W-2 Segra engineers who are responsible for monitoring, troubleshooting, and maintaining the entire Segra network and the services provided. As the first point of contact for our customers, the ERT is responsible for generating trouble tickets on all issues, dispatching technicians if necessary, isolating the problem, keeping customers updated, and driving all troubles to completion. Quick trouble resolution with a sense of urgency is our priority, and we are available 24x7x365.

The Network Operations Center (NOC) manages all change management network events (high-risk maintenance activities) along with delivering on SLA parameters for mission critical services.

The Segra NOC tracks all events via trouble ticket(s). Customer event updates are provided via phone calls or emails directly from our ticketing system.

If an outage occurs, Segra has Ethernet test heads strategically placed throughout the network to perform RFC 2544 testing on demand, which supports our ability to meet the four-hour MTTR objective in our Service Level Agreement (SLA).

For any maintenance related activities, the Change Management group will notify customers via email of any service impacting scheduled work. Segra strives to give all customers at least seven (7) days' advance notice for all regularly scheduled maintenance. These events take place between the hours of 12:01AM and 5:59AM. Segra reserves the right to perform emergency maintenance during service impacting events.

Mean Time to Repair Objective is Four (4) Hours
Mean Time to Repair (MTTR) is the average time required to repair service to an operational condition if service(s) are not active or the customer is experiencing consistent service degradation. The MTTR objective is four (4) hours for normal circuit outages, and ten (10) hours for fiber damages.

If an outage occurs, Segra has Ethernet test heads strategically placed throughout the network to perform RFC 2544 testing on demand, which supports our ability to meet the four-hour MTTR in our Service Level Agreement (SLA).

Segra has two 24/7/365 geo-diverse Network Operations Centers in Columbia, SC and Waynesboro, VA. Segra Field Operations Support teams are also located strategically in the markets served. Fiber restoration crews are also dispersed throughout our markets.

The severity/priority levels and escalation procedures are identical for all traffic types. The management escalation procedures for each severity/priority level are as follows:

- **Critical** - A critical ticket is defined as a service outage that has a severe impact on customer business operations with no workaround available. This condition includes a critical work stoppage during the customer's normal working hours that affects multiple customer sites and/or affects a critical component or function of the customer's business. Segra and its vendor-partners will commit substantial resources around the clock to resolve the situation. Examples of critical outages include an agency host major outage or 10% or greater of the current agency node count in production status.
    - Critical – Escalation Interval
        - Immediate: CNOC Manager & Director
        - 2 Hours: Vice President
- **Major** - A major ticket describes a condition where a partial service outage occurs or the service is severely degraded, which has a significant impact on customer business operations, with no adequate workaround available. This condition includes a partial work stoppage or severe performance degradation during the customer's normal working hours, which affects a customer site. Segra and vendor-partners will commit full time resources during business hours or around the clock as necessary to resolve the situation.
    - Major – Escalation Interval
        - Immediate: Tier 3 CNOC Analyst
        - 1 Hour: Floor Manager
        - 2 Hours: CNOC Manager
        - 3 Hours: Director
        - 5 Hours: Vice President
    - Escalations can be made at the customer's request
- **Minor** - A minor ticket describes conditions where difficulties are experienced with a transport service, but do not cause a work stoppage; there is a workaround, but performance and/or system functionality may be degraded or limited. This condition includes degraded service performance and impaired service functionality, but most business operations continue. Workarounds are established, implemented, and documented for problems with this priority level. Segra will commit resources during business hours as required to resolve problems with this severity level.
- **Informational** - An informational ticket describes conditions that are not urgent, and/or are not problems, and/or that do not impact customer business operations. Informational tickets are for the CNOC. This priority level is most appropriate for:
    - Minor alarms and informational alarms
    - Escalations can be made at the customer's request

4.3.1.3.8. The Vendor's network operation support center should provide: all tiers of support, advanced technical expertise, be staffed with resources that are proficient in spoken and written English, maintain and take responsibility for trouble tickets reported by the State until resolved, and provide a tiered support escalation process. Please describe your network operation support center's structure, processes, and procedures for handling trouble tickets, resolving those tickets, and reporting back to the State's point of contacts.

Segra supports our customers with geo-redundant network operation centers located in Columbia, SC and Waynesboro, VA. Segra's NOC consists of the Segra Customer Network Operations Center (CNOC), Network Operations Center (NOC), and Security Operations Center (SOC). Each organization is composed of a team of dedicated Tier 1 and Tier 2 trained technicians who are responsible for monitoring, troubleshooting, and maintaining the entire Segra network and the services provided. Segra field operations support teams are located strategically in the markets served, and fiber restoration crews are also dispersed throughout our markets.

The following list details performance objectives for the Segra CNOC, NOC, and SOC. Staffing is designed to meet the objectives listed below.

ELEMENT	OBJECTIVE
NOC Availability	24 hours per day, 365 days per year
Average Speed of Answer	15 seconds
Answer Time	90% answered within 15 seconds
Customer Status (Priority 1)	1 hour interval 95% on-time
Account Team Notification	Within 15 minutes of Priority 1 ticket generation

The CNOC was established so Segra could have a direct focus on our end-user customers. This support organization, whose sole responsibility is working customer driven issues, operates in a contact center environment. As the first point of contact for our customers, the CNOC is responsible for generating trouble tickets on all issues, dispatching technicians if necessary, isolating the problem, keeping customers updated, and driving all troubles to completion. This team owns the issue, isolation, repair, and communications back to the customer. CNOC technician responsibilities are:

- Receiving all incoming customer trouble calls;
- Creating tickets in Segra's trouble ticketing system;
- Providing timely updates to customers; and
- Working tickets and escalating when necessary.

Quick trouble resolution with a sense of urgency is our priority, and we are available 24x7x365 at 833.GO.SEGRA. Segra also offers a web-based trouble reporting tool for opening trouble tickets, service inquiries, and status reports online at www.segra.com (click on 'Request Support'). Segra's online trouble ticketing allows real-time updates via email as major milestones are accomplished in the ticket triage process. This allows our customers to be abreast of all ticket activity. Furthermore, it is available to all support personnel needed to update the customer via telephone.

The severity/priority levels and escalation procedures are identical for all traffic types. The management escalation procedures for each severity/priority level are as follows:

Critical - A critical ticket is defined as a service outage that has a severe impact on customer business operations with no workaround available. This condition includes a critical work stoppage during the customer's normal working hours that affects multiple customer sites and/or affects a critical component or function of the customer's business. Segra and its vendor-partners will commit substantial resources around the clock to resolve the situation. Examples of critical outages include an agency host major outage or 10% or greater of the current agency node count in production status.

Critical – Escalation Interval

- Immediate: CNOC Manager & Director
- 2 Hours: Vice President

Major - A major ticket describes a condition where a partial service outage occurs or the service is severely degraded, which has a significant impact on customer business operations, with no adequate workaround available. This condition includes a partial work stoppage or severe performance degradation during the customer's normal working hours, which affects a customer site. Segra and vendor-partners will commit full-time resources during business hours or around the clock as necessary to resolve the situation.

Major – Escalation Interval

- Immediate: Tier 3 CNOC Analyst
- 1 Hour: Floor Manager
- 2 Hours: CNOC Manager
- 3 Hours: Director
- 5 Hours: Vice President
- Escalations can be made at the customer's request

Minor - A minor ticket describes conditions where difficulties are experienced with a transport service, but do not cause a work stoppage; there is a workaround, but performance and/or system functionality may be degraded or limited. This condition includes degraded service performance and/or impaired service functionality, but most business operations continue. Workarounds are established, implemented, and documented for problems with this priority level. Segra will commit resources during business hours as required to resolve problems with this severity level.

Informational - An informational ticket describes conditions that are not urgent and/or are not problems and/or that do not impact customer business operations. Informational tickets are for the CNOC. This priority level is most appropriate for:

Minor Alarms and Informational Alarms

- Escalations can be made at the customer's request.

The management team makes the decision for technical resource escalations as necessary, as there is no formal timeline for the need for the appropriate technical resource. The following is the technical escalation path and the corresponding skill set of each organization:

- Tier II Support Analyst (CCNA);
- Tier III Support Analyst (CCNA through written CCIE);
- Network Technical Assistance Center (CCNA through CCIE);
- Engineering – Architectural and Sustaining Engineers as required.

If at any time you feel the normal trouble repair process does not meet your needs, please use the following escalation procedures:

1. Call the CNOC Manager and identify yourself and the trouble about which you are inquiring (trouble ticket number).
2. Explain the steps that have been taken. The manager will be able to discuss the status of your trouble report and provide you with additional information regarding the completion of the repair.
3. If at any time you are not satisfied with the progress, please escalate to the next level.

A copy of **Segra's Escalation Contacts and Contact Information** is included in our response on page 190.

The Segra NOC is responsible for ensuring that Segra's core and access networks are performing as designed. The NOC manages all change management network events (high-risk maintenance activities) along with delivering on SLA parameters for mission critical services. The NOC is composed of transport, IP/security, voice, and web services technicians and responsible for the following:

- Network surveillance;
- Environmental alarms;
- Maintenance notifications;
- Working tickets and escalating when necessary.

Segra's NOC is equipped with many different Element Management Systems (EMS) that monitor specific vendors and technologies. These EMS monitor a specific set of equipment manufacturers in real time and provide visual fault indicators when an alarm is present within the infrastructure or backbone. If an outage occurs, Segra has Ethernet test heads strategically placed throughout the network to perform RFC 2544 testing on demand, which supports our ability to meet the four-hour MTTR in our Service Level Agreement (SLA).

Mean Time To Repair (MTTR) is the average time required to repair service to an operational condition if service(s) are not active or the customer is experiencing consistent service degradation. The MTTR objective is four (4) hours for outages due to electronic equipment failure and fiber optic facilities failure, and ten (10) hours for outages due to fiber cuts.

Segra's CNOC Escalation List

ENTERPRISE REPAIR ESCALATION LIST (CNOC)

MONDAY - FRIDAY		
1st Level	On-Duty Technical Support Analyst	1.833.467.3472 (option 2)
2nd Level	On-Duty (7 a.m.- 12 a.m.) Enterprise Repair Escalations Manager	800.304.1498
3rd Level	Andrea Redfern Sr. Manager, Voice	800.304.0320 andrea.redfern@segra.com
3rd Level	Scott Dunham Sr. Manager, Elite CNOC	844.733.4318 scott.dunham@segra.com
4th Level	Fred Christian Sr. Director, Enterprise Repair	888.696.0408 fred.christian@segra.com
SATURDAY - SUNDAY		
1st Level	On-Duty Technical Support Analyst	1.833.467.3472 (option 2)
2nd Level	On-Duty Enterprise Repair Escalation Manager	800.304.1498
3rd Level	Fred Christian Sr. Director, Enterprise Repair	888.696.0408 fred.christian@segra.com

4.3.1.4. Part 4: Security for WAN and DIA Services

4.3.1.4.1. The Vendor should support customer evaluation of security incidents and compliance verification evaluations, as deemed necessary by the customer.

Segra has read, understands, and will comply.

As part of Segra's security assessment policy, we hire independent third-party companies to conduct a very defined security audit. This audit contains various penetration tests both internally and externally. DDoS prevention is done in real time on all of our peering connections. Segra utilizes a robust hardware-based appliance that can "scrub" traffic in real time at line rates. 99% of DDoS events are mitigated automatically without intervention from the WVOT or Segra's SOC. The system inherently inspects traffic and can quickly identify both volumetric and/or signature-based attacks and discard the traffic before it enters Segra's core internet backbone. This process is highly effective although there can be a "zero day" attack without a predefined signature in which Segra's SOC can write a flex rule to mitigate the attack. Once this is done, the new signature is added to the signature database preventing it from occurring again.

4.3.1.4.2. The Vendor should have an established and documented policy governing personnel security to include the validation of employee trustworthiness.

As part of our information security program, Segra performs dual control procedures, segregation of duties, and employee background checks, including drug testing, for employees with responsibilities for, or access to, sensitive information.

All Segra employees are required to have a background check, including drug testing prior to employment.

Please refer to **Segra's Drug and Alcohol Use Policy**, included in our response on page 194.

4.3.1.4.3. The Vendor should describe its company's cyber security and privacy management program including an overview of the governance structure, cyber security strategy, and the experience of personnel in key security and privacy roles.

Segra's information security policies cover multiple areas.

The most common security policy documents requested are attached and cover access control, network segmentation, physical security, risk management, incident response, vendor risk, and our employee acceptable use policy.

Please refer to the following seven (7) documents, included in our response:

- Access Control Policy (page 199)
- Physical and Environmental Security Policy (page 208)
- Network Communications Policy (page 216)
- Supplier Relationships Security Policy (page 223)
- Information Systems Acceptable Use Standard (page 232)
- Security Incident Response (page 242)
- Security Risk Management (page 250)

Segra's internal information security program is based on the NIST Cyber Security Framework, using the NIST 800-53 and ISO 27002 as control references.

4.3.2. Mandatory Requirements

4.3.2.1. Part 1: Technology Service and Solution for Ethernet WAN, DIA and 4G/5G Services

4.3.2.1.1. Ethernet WAN Service

4.3.2.1.1.1. The Vendor must provide Ethernet WAN services that will terminate into existing State network equipment.

Segra has read, understands, and will comply.

Segra is proposing an SD-WAN solution that will allow for WVOT to migrate from the current WAN environment to a hybrid MPLS/SD-WAN solution allowing for symmetrical dedicated private links to natively communicate with sites that are connected via DIA, Broadband, or 4G/LTE. Segra's co-managed SD-WAN Edge device allows for a turn-key ease of deployment, enabling remote locations to be online and communicating back to the private network with ease.

Prior to the Segra proposed solution being deployed, Segra will work with WVOT to talk through options of transitioning from the existing network to the new solution via strategic locations with firewalls acting as the gateways between the two networks.

4.3.2.1.1.2. The State requires the Vendor to provide standard Ethernet interface options to include 10/100/1000 and 4G/5G.

Segra has read, understands, and will comply.

4.3.2.1.1.3. Vendor must propose service options that range between 5Mbps through 40Gbps.

Segra has read, understands, and will comply.

4.3.2.1.1.4. The Vendor will be responsible for all service continuity associated with their WAN service, whether issues are within the Vendor's networks, alternative local-loop vendors, 4G/5G vendors, WISPS, Cable TV vendors or other technology vendors engaged to provide WAN services to the State. The Vendor must be able to coordinate, test and troubleshoot the service continuity and integrity end-to-end.

Segra has read, understands, and will comply.

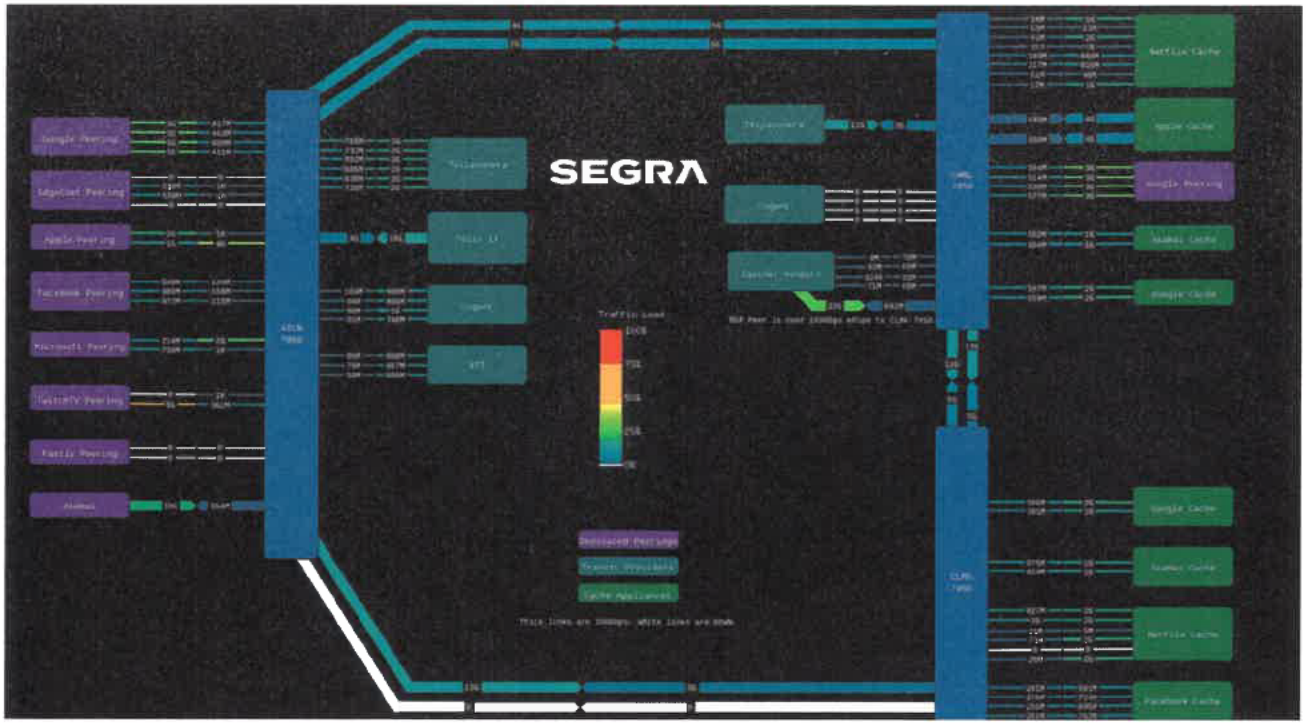
4.3.2.1.1.5. The Vendor must provide services capable of supporting dynamic routing and sharing routes between autonomous systems (AS) on provider networks as well as other public and private networks.

Segra has read, understands, and will comply. Segra will work with WVOT on any BGP advertisement set-up and changes, ranging from multi-home configurations, upstream advertisements, private and public networks, ASN learning and adjustments.

Segra's IP backbone consists of multiple 100 Gigabit transport circuits with full redundancy and multiple transit points to other national Tier 1 Internet providers.

Segra has connectivity to the following upstream internet service providers: Telia (Tier 1), Cogent (Tier 2), and NTT (Tier 1).

Below is a 'weather map' snapshot of Segra IP transit, outlining peering partners (turquois colored, upstream providers) as well as dedicated on-net caching servers (green colored), IX exchanges (turquois as well, IP Internet exchanges with multiple collective providers and tech companies), and direct peering (purple color). The thicker links indicate 100 Gb circuits, and all thinner links are 10 Gb circuits.



Backbone

Our IP network core is powered by Nokia 7950 XRS-20 routers. The 7950 XRS-20 is a 16 Terabit per second core router that can deliver 80 100GE interfaces in a single rack (5x more than the current norm). It can be upgraded to 7950 XRS-40 and/or multi-chassis configurations as demand requires, and is designed to accommodate up to 2 Terabits per slot.

Segra has deployed the Nokia 7950 XRS routing platform at three core locations where our public and private peering connections are routed. These strategic locations are Columbia, SC, Atlanta, GA, and Charlotte, NC. The 7950 XRS-20 are interconnected with 100 Gigabit per second (100G) links over diverse and redundant connections.

100 gigabit per second (100G) links serve as the foundation of our IP transport backbone network. As these link speeds evolve to 400 Gb and Terabit speeds, our 7950 XRS core routing platform is already in place to accelerate the deployment of next-generation high-speed connections.

Segra utilizes fully meshed Nokia 7750 SR-12e as distribution routers to reach our customers. The Nokia 7750 SR series delivers high-performance routing and an extensive range of IP applications. The 7750 SR scales system capacity to 9.6 Terabits per second and is equipped with high-density Gigabit Ethernet (GE), 10GE, 40GE, and 100GE interfaces.

Segra has deployed Nokia 7750 SR12-e routers in Columbia, Greenville, Florence, Charleston, Charlotte, and Atlanta. These routers are interconnected with multiple 10 Gigabit Ethernet links that are diverse and redundant over the Segra-owned DWDM fiber backbone throughout the Carolinas.

Public Peering

Segra utilizes a strategy of maintaining public peering points and private IP transit connections with multiple Tier 1 providers. The current Internet exchange point aggregates thousands of peering sessions onto the shared fabric. Public peering points are AtlantaIX, Ashburn, VA, and Los Angeles, CA. Each public and private peer supports dual-stack IPv4 and IPv6.

The public peering point located in Ashburn, VA is a global Internet exchange facility that utilizes IP peering via an Ethernet switching fabric. These interconnections are designed on a centralized Ethernet switching fabric and the necessary supporting infrastructure to support multiple 10 Gbps connections.

The public peering point in Atlanta is located at the AtlantaIX exchange facility. This Internet exchange is a neutral, high-performance Internet peering fabric for participants. The AtlantaIX public peering point is designed on a centralized Ethernet switching fabric and the necessary supporting infrastructure to support multiple 10 Gbps connections.

The public peering point in Los Angeles is located at the CoreSite-Any2 LA1 international Internet exchange point. This public peering is located at one of the most interconnected buildings on Earth — One Wilshire at 624 S. Grand — with interconnections to Telehouse's LAIIX, located at 626 Wilshire Blvd. These interconnections are designed on a centralized Ethernet switching fabric and the necessary supporting infrastructure to support multiple 10 Gbps connections.

These strategic public peering points give Segra and our customers a nationwide presence to the Internet with enhanced end-to-end network performance, speed, and reliability.

Private IP Transit Peering

Segra also maintains private IP transit connections with other Tier 1 global Internet providers to augment our public peers and provide additional global reach for our customers.

Segra runs BGP (IPV4 & IPV6) with these IP transit providers to optimize routing entering and leaving the Segra Autonomous Systems (AS). All providers allow Segra to manipulate traffic in their AS, which gives a lot of power and traffic manageability to Segra.

Each private IP transit connection consists of multiple 10 Gigabit peering connections and terminates into our core 7950 XRS IP routers. These connections are located in Atlanta, GA and Charlotte, NC.

This public and private peering strategy has provided our customers with the utmost in networking performance and reliability.

Caching Services

Segra hosts large Akamai caching environments/content distribution networks located in Columbia, SC and Charlotte, NC. These content caching servers are used to improve performance for high-bandwidth intensive content applications such as streaming video and operating system updates. When content is requested from companies like Netflix, Microsoft, Apple, Facebook, Twitter, and Google, the information is not necessarily returned from that company's website or data center. Instead, the information is returned from the Akamai web cache or Google content distribution server located at the Segra POP(s) listed above.

In K-12 environments, this is increasingly important as so much content is now stored in the Cloud. By caching content like YouTube for Schools, streaming educational videos and web-based testing environments results in faster and more reliable networking performance. The users are just milliseconds away from the content they need to access.

4.3.2.1.1.6. The proposed WAN services must support the transport of existing applications and services currently being utilized by the State of West Virginia. The Vendor proposed solution must allow existing or future 3rd party applications and services (example: Google Cloud, AWS, Azure) to be accessed or to function in a robust, secure, and reliable manner from the vendors core network. Some existing applications and services include, but are not limited to:

- **4.3.2.1.1.6.1.** Unified Communication services including VOIP and Video
- **4.3.2.1.1.6.2.** Commodity Internet access
- **4.3.2.1.1.6.3.** Internet 2 access
- **4.3.2.1.1.6.4.** High Volume Database transmissions
- **4.3.2.1.1.6.5.** Desktop Virtualization
- **4.3.2.1.1.6.6.** Server Synchronization

4.3.2.1.1.6.7. Network Monitoring (not an application)

4.3.2.1.1.6.8. Security Monitoring (not an application)

4.3.2.1.1.6.9. Content Filtering (not an application)

4.3.2.1.1.6.10. Virtual Private Networking

4.3.2.1.1.6.11. Cloud hosted platforms like the Google Workspace for Business

Segra has read, understands, and will comply.

Segra hosts a good majority of voice services for the State of West Virginia today. The troubleshooting and visibility of Segra hosted SIP, Hosted Voice, and Unified Communications become increasingly easier to manage (Quality of Service) and monitor (Jitter, Packet Loss, Latency) if Segra is the provider of WAN services.

Segra currently provides onboarding of multiple colleges and universities to Internet 2/Lambda Rail Network and is able to expand connectivity to additional customers.

Segra offers IPv4 and IPv6 addressing to its customers. Segra's network is optimized to allow for Quality of Service mindful services such as desktop virtualization, database and server synchronization, as well as high-capacity and low-latency connectivity to a vast amount of Cloud service providers.

4.3.2.1.2. Dedicated Internet Access

4.3.2.1.2.1. Vendor must provide dedicated DIA services purchased from the State demarcation point to the Internet backbone.

Segra has read, understands, and will comply.

4.3.2.1.2.2. Vendor must provide DIA Service Level Agreements (SLAs) that meet or exceed the following service categories and associated benchmarks:

4.3.2.1.2.2.1. Service Availability: Vendor DIA Service will be available 99.999% of the time.

The objective for our Network Availability is 99.999%.

Please refer to **Segra's Service Level Agreement (SLA)**, included in our response on page 186.

4.3.2.1.2.2.2. Denial of Service: Vendor must respond to Denial of Service attacks reported by State within 15 minutes of State opening a trouble ticket.

Segra has read, understands, and will comply. Segra's solution to WVOT is an inline, always on, automated DDoS detection and mitigation tool that is deployed at Segra peering points, resolving/mitigating attacks prior to making their way to a customer's network.

Segra utilizes the Corero SmartWall Threat Defense System (TDS) as the core of our managed security service offering DDoS Edge Protect. Segra's DDoS Edge Protect is a managed security service that eliminates cyber threats in real time. It provides comprehensive DDoS protection capable of mitigating a wide range of DDoS attacks all while maintaining full connectivity to avoid disrupting the delivery of legitimate traffic.

It is designed to handle large network-based DDoS attacks or floods, reflective amplified spoof attacks, as well as application layer attacks that are typically too low to be detected by out of band solutions. This DDoS Edge Protect product protects where firewalls cannot since the protection occurs prior to reaching the customer's network at the Internet peer source.

Segra supports our customers with geo-redundant network operation centers located in Waynesboro, VA and Columbia, SC. Segra's geo-redundant centers operate on a 24x7x365 basis.

DDoS mitigation is one attribute that sets Segra ahead of the competition, and is included as a standard feature with our dedicated Internet fiber services.

Segra implements DDoS protection at the Internet gateways. The DDoS appliances are capable of wire-speed inspection and enable mitigation of an identified DDoS attack at the very edge of the Segra network. This strategy not only protects the target customer, but also limits the attack's impact to overall Segra network performance. Threat/attack intelligence information on in-progress DDoS attacks from a network of global Tier 1 and Tier 2 providers is used to preemptively block DDoS attacks as they propagate globally. This approach to DDoS attacks provides Segra customers with both a proactive and a reactive DDoS attack threat response.

Please refer to **Segra's DDoS Edge** product sheet, included in our response on page 258. Please also refer to **Segra's Escalation Contacts and Contact Information** and **Segra's Service Level Agreement (SLA)**, included in our response on pages 190 and 186, respectively.

DDoS

DDoS protection appliances are located at high-volume entry points on the Segra core network where attacks are most likely to occur, such as public transit connections. The appliances automatically inspect all traffic as soon as it arrives at an entry point, immediately discarding malicious packets while sending legitimate packets to their destination. During this process, other network services continue to operate without interruption, even latency-sensitive applications like voice and video.

FAST

The protection capability is purpose-built for speed and low latency, so attacks are detected and mitigated immediately without impacting network performance.

EFFECTIVE

The protection is comprehensive, identifying both existing and newly discovered attack types, and preventing direct attacks as well as their side effects.

RISK REDUCTION

The fast, effective protection included in the Segra DIA service significantly minimizes the risk of DDoS attacks from the public Internet.

REAL-TIME FILTERING

Inspection, detection, and scrubbing occur as soon as traffic arrives at the Segra network.

AUTOMATIC PROCESSING

All filtering functions are performed automatically, without the requirement for regular human intervention and/or delay.

IN-LINE OPERATION

Traffic stays on the Segra network during filtering instead of being physically and/or logically diverted for processing, minimizing latency.

COMPREHENSIVE PROTECTION ANALYTICS

Inherent analytics detect a variety of attack types and are updated continually with the latest intelligence on DDoS threats.

CORE FUNCTIONALITY

DDoS protection is required as a standard, core function of the Segra DIA service. Taking this approach protects the entire Segra network path from DDoS attacks, and in turn, the entire Segra DIA customer base. The approach also complements any local DDoS solution a customer may implement since a local solution cannot protect the Segra network path.

SCALABILITY

The DDoS protection appliances are designed and located to easily keep pace with growth in the Segra footprint and the customer networks we serve. Any site a customer adds to the Segra network is automatically protected from DDoS attacks without configuration changes.

4.3.2.1.2.2.3. Latency: Vendor service must provide for average round-trip transmissions of 45 milliseconds or less between their regional core backbone routers and the State designated core routers.

Segra has read, understands, and will comply. Segra understands latency is important to WVOT. Our objective for average latency is to not be greater than 8 milliseconds inside a metropolitan area. The goal for average latency is to not be greater than 30 milliseconds between metropolitan markets. For any month in which the objective is not met, the customer will receive a credit, which may be applied towards the customer's monthly invoice, equal to 1/30 of the monthly recurring charges for the services.

$$\text{Latency} = \frac{\text{Sum of the roundtrip delay measurements for an On-Net Service}}{\text{Total \# of measurements for an On-Net Service}}$$

"Average Latency" is the monthly average round-trip latency from a core network node to any other designated core network node on the Segra network, determined by measuring round-trip network responses over such portions of the network.

Please refer to **Segra's Service Level Agreement (SLA)**, included in our response on page 186.

4.3.2.1.2.2.4. Network Packet Delivery: Vendor service must provide for a monthly packet delivery of 99.5% or greater between Vendor designated regional core backbone routers and the State designated core routers.

Segra has read, understands, and will comply. "Packet Loss" or "Frame Loss Ratio" is defined as the percentage of frames that are not successfully received compared to the total frames that are sent in a calendar month, except where any packet or frame loss is the result of an Excluded Disruption. The percentage calculation is based on frames that are transmitted from a network origination point and received at a network destination point (Segra network hub to Segra network hub). Packet Loss / Frame Loss Ratio is calculated as follows:

Packet Loss / Frame Loss (%) = 100 (%) – Frames Received (%)

Please refer to **Segra's Service Level Agreement (SLA)**, included in our response on page 186.

4.3.2.1.2.3. Vendor must supply IP address blocks up to and including a full Class-C block.

Segra has read, understands, and will comply.

4.3.2.1.2.4. Vendor must provide bandwidth pricing for the following levels of Service:

4.3.2.1.2.4.1.	50mbps
4.3.2.1.2.4.2.	100mbps
4.3.2.1.2.4.3.	500mbps
4.3.2.1.2.4.4.	1Gbps
4.3.2.1.2.4.5.	2Gbps
4.3.2.1.2.4.6.	5Gbps
4.3.2.1.2.4.7.	10Gbps
4.3.2.1.2.4.8.	25Gbps
4.3.2.1.2.4.9.	40Gbps

Segra has read, understands, and will comply. Please refer to Segra's completed **Exhibit A - Pricing Page**, included in our response starting on page 8.

4.3.2.1.3. E-Rate

The Universal Service Fund (USF) was established as the result of the Telecommunications Act of 1996, when Congress directed the Federal Communications Commission (FCC) to "establish competitively neutral rules to enhance, to the extent technically feasible and economically

reasonable, access to advanced telecommunication and information services for all public and non-profit elementary and secondary school classrooms and libraries." The FCC then empowered the Universal Service Administrative Company (USAC) to administer the program. A division within USAC, later to become known as the Schools and Libraries Division (SLD), now administers the approximate $4.9 billion (annual) program known as E-Rate. Schools and libraries must apply for eligible services from eligible service providers every year. The eligible services fall into the following categories:

4.3.2.1.3.1. Category 1: Telecommunications, Telecommunications Services & Internet Access

4.3.2.1.3.2. Category 2: LAN and WLAN Internal Connections & Basic Maintenance of Internal Connections

4.3.2.1.3.3. General E-Rate Requirements

Segra has read and understands.

Segra has extensive experience working with school districts on E-Rate funding projects. Segra directly employs an E-Rate funding team consisting of coordinators and billing specialists. Many have held this position since the original funding years of 1999-2000 of the E-Rate funding program. They are the Segra subject matter experts on all issues pertaining to E-Rate funding. Segra's E-Rate funding team is here to assist, provide guidance, and serve as contacts for questions regarding services that are being delivered.

4.3.2.1.3.3.1. The Vendor must comply with the requirements of the Universal Service Fund (USF) program. E-Rate eligible entities utilizing the contract(s) resulting from this solicitation reserve the right to proceed with orders prior to receiving any funding commitments from the USF. They also reserve the right to proceed or not to proceed regardless of the outcome of USF funding commitments.

Segra has read, understands, and will comply.

4.3.2.1.3.3.2. All services and products requested within this solicitation will be made available to schools, RESAs,

consortia, and libraries statewide and therefore must meet all E-Rate guidelines for eligible services and products, service providers, and contracts.

Segra has read, understands, and will comply.

4.3.2.1.3.3.3. The Vendor must prove eligibility for E-Rate by providing its Service Provider Identification Number (SPIN) in the RFP Response.

Segra has read, understands, and will comply. Lumos Networks, LLC d/b/a Segra's SPIN number is **143024848**.

4.3.2.1.3.3.4. The Vendor must meet all required participation guidelines.

Segra has read, understands, and will comply.

4.3.2.1.3.3.5. The Vendor must provide eligible entities the "Lowest Corresponding Price" (LCP) for services (refer to FCC 47 CFR § 54.500(f) and 47 CFR § 54.511(b)).

Segra has read, understands, and will comply.

4.3.2.1.3.3.6. Service providers shall offer schools and libraries services at the lowest corresponding prices throughout its geographic service areas that include all non-residential customer offerings that are similarly situated to a school or library. The "geographic service area" shall be the area in which a service provider Vendor is seeking to serve customers with any of its E-Rate services.

Segra has read, understands, and will comply.

4.3.2.1.3.3.7. The FCC will only permit service providers to offer schools and libraries prices above prices

charged to other similarly situated customers when those Vendors can show that they face demonstrably and significantly higher costs to serve the school or library seeking service. Factors that could affect the cost of service include volume, mileage from facility, and length of contract.

Segra has read, understands, and will comply.

4.3.2.1.3.3.8. Vendor must operate within Rule 47 CFR § 54.511(b) which states that the provider of eligible services shall not charge schools, school districts, libraries, library consortia, or consortia including any of these entities a price above the Lowest Corresponding Price (LCP) for supported services, unless the FCC, with respect to interstate services or the state commission with respect to intrastate services, finds that the Lowest Corresponding Price is not compensatory.

Segra has read, understands, and will comply.

4.3.2.1.3.3.9. The Vendor, regardless of the size of the company, must provide LCP for a school or library. A service provider's obligation to provide the LCP shall not be tied to a response to an FCC Form 470 or this solicitation and should carry over throughout the billing life of the contract, as well.

Segra has read, understands, and will comply.

4.3.2.1.3.3.10. The Vendor must agree to abide by all E-Rate rules, regulations, and limitations as described by FCC, USAC, and SLD. For a complete program overview, the Vendor can visit the following link: http://www.universalservice.org /SL/d efault.aspx.

Segra has read, understands, and will comply.

4.3.2.1.3.3.11. Successful Vendor of telecommunication services must meet certain qualifications to be eligible to provide the services and receive USAC reimbursement.

Segra has read, understands, and will comply.

4.3.2.1.3.3.12. Must contribute to the Universal Service Fund

Segra has read, understands, and will comply.

4.3.2.1.3.3.13. Must provide telecommunications services on a common carrier basis

Segra has read, understands, and will comply.

4.3.2.1.3.3.14. Must file an FCC Form 498, Service Provider Information Form and obtain a Service Provider Identification Number (SPIN), providing that number as part of this bid response, and an FCC Registration number tied to their IEN tax ID number

Segra has read, understands, and will comply. Please refer to **Segra's FCC Form 498**, included in our response on page 274.

Lumos Networks, LLC d/b/a Segra's SPIN number is **143024848**, and Segra's FCC Registration number is **0003771011**. Furthermore, Segra's FEIN is **84-1452950**.

4.3.2.1.3.3.15. Must file an FCC Form 473, Service Provider Annual Certification Form, on an annual basis

Segra has read, understands, and will comply. Please refer to Segra's **FCC Form 473**, included in our response on page 285.

4.3.2.1.3.3.16. Must file an FCC Form 499-A, Annual Telecommunications Reporting Worksheet, on an annual basis.

Segra has read, understands, and will comply.

4.3.2.1.3.3.17. Must complete the FCC Forms 949- A,/Q (Annual and Quarterly Telecommunications Reporting Worksheets) and receive a Filer ID. The FCC Forms 499-A/Q Filer ID will be tied to your SPIN. Certain service providers are not required to file or complete all items on an FCC Forms 499-A/Q, either because the company has a de minimis status or meets one of the exceptions noted in the "Filing Requirements and General Instructions" section of the instructions on the Contributors Forms page.

Segra has read, understands, and will comply.

4.3.2.1.3.3.18. You can refer to the Service Providers section or the Contributors section of the USAC website for more detailed information on these forms and instructions.

Segra has read, understands, and will comply.

4.3.2.1.3.3.19. The Vendor must work with the applicant to ensure that all services for which E-Rate discounts are being requested under the contracts resulting

from this solicitation, are indeed eligible services as described in the Eligible Services List (ESL) which can be found at the link provided below: http://www.universalservice.org/sl/applicants/beforeyoubegin/eligible- services-list.aspx

Segra has read, understands, and will comply.

4.3.2.1.3.3.20. Prior to the contract award, the Vendor must specify the name, phone number, fax number, and e-mail address of the person responsible for E-Rate within the Vendor's company. The Vendor must provide updated information should that contact information change, and must do so within 7 days of the change.

Segra has read, understands, and will comply. Please refer to the requested information below.

Anthony Stroman
E-RATE/Rural Health Care Program Coordinator
Email: Anthony.Stroman@segra.com
Phone: (803) 726-4074
Fax: N/A

4.3.2.1.3.3.21. The Red Light Rule states that the FCC shall withhold action on any request for benefits made by any applicant or service provider that is delinquent in its non-tax debts owed to the FCC. USAC shall dismiss any outstanding requests for funding if a service provider (or applicant) has not paid the outstanding debt, or made otherwise satisfactory arrangements, within 30 days of being notified

Segra has read and understands. Segra confirms that it is in good standing with the FCC and that it will comply with this requirement.

4.3.2.1.3.3.22. The result of a Red Light could be that all payments are stopped on all Funding Request Numbers (FRN) for that service provider (or applicant) and no invoices will be paid.

Segra has read, understands, and will comply.

4.3.2.1.3.3.23. The Vendor must agree to notify the State of West Virginia, WVDE and WVLC within 24 hours in the event the Vendor/Service Provider has been subjected to the "Red Light Rule".

Segra has read, understands, and will comply.

4.3.2.1.3.3.24. In the event of an E-Rate audit or Program Integrity Assurance (PIA) review, the Vendor must respond within 3 calendar days for 7 day deadline reviews and 7 calendar days for 15 day deadline reviews to any and all questions associated with its contracts, proposals, or processes.

Segra has read, understands, and will comply.

4.3.2.1.3.3.25. The Vendor must maintain all bids, quotes, records, correspondence, receipts, vouchers, delivery information, and other data relating to the Vendor's services to the eligible entities in the State of West Virginia. All such records must be retained for ten (10) years after last date of service or whatever retention period is required by the rules in effect at the time that services are delivered and shall be subject to inspection and audit by the customer.

Segra has read, understands, and will comply. At time of award, Segra would like to review this policy as our normal record retention is for a period of five years.

4.3.2.1.3.3.26. The Vendor must have an internal audit process in place to ensure compliance with E-Rate program rules and regulations.

Segra has read, understands, and will comply.

4.3.2.1.3.3.27. If requested by an applicant, service providers must use the Service Provider Invoice (SPI) method for invoicing the applicant. It is understood that should a provider extend this service to an applicant, that the applicant will be responsible for the discounted portion of those invoices should E-Rate funding be denied; however, applicants will not be responsible for any discounted portion that is the direct result of negligence or error in the SPI invoicing process on the part of the service provider.

Segra has read, understands, and will comply.

Segra supports both Service Provider Invoice (SPI) to request reimbursement from USAC for the discounted amount for eligible services and equipment provided to the applicant, and Billed Entity Applicant Reimbursement (BEAR), in which the applicant will request reimbursement from USAC for eligible services and equipment paid in full.

4.3.2.1.3.3.28. The Vendor must commit to work with the E-rate eligible entities using the resulting contract regarding E-rate discounts and billing.

Segra has read, understands, and will comply.

4.3.2.1.4. 4G/5G Wireless Service

As part of its WAN solution, Vendor must provide 4G or 5G wireless service. Upon request from the State, 4G or 5G service will be installed at locations where wireless service is available and satisfies the location bandwidth requirements. The state plans to utilize 4G/5G service as a full time or interim WAN service, or to provide back-up/redundant service for a sites Ethernet WAN service.

Segra has read, understands, and will comply.

4.3.2.1.4.1. Vendor will be responsible for coordination of the installation and ongoing management of the 4G/5G wireless service.

Segra has read, understands, and will comply.

Segra has over 1,300 similar customer-managed 4G/5G modems/routers today. Segra currently deploys CradlePoint 100Es for its customers' 4G/5G needs, whether it is called for as a standalone, failover, or temporary solution. The CradlePoint 100E allows for flexible dual SIM deployment, and Segra utilizes both AT&T and Verizon Wireless Network for its design options.

Our customers are provisioned in unique MPLS networks that are available through DMNR protocol. This service will scale x10 with the evolution of 5G in North American markets. LTE Secure Access is a fully managed service to ensure seamless failover and failback of primary IP services via BGP protocol.

4.3.2.1.4.2. State requires that both 4G/5G wireless service options include unlimited data.

Segra has read, understands, and will comply.

4.3.2.1.4.3. Throttling of 4G/5G wireless data is strictly and wholly prohibited.

Segra has read, understands, and will comply.

4.3.2.2. Part 2: Vendor Ethernet WAN Services Migration Plan

4.3.2.2.1. The Vendor must provide a detailed project plan and Project Manager for transitioning the legacy installed WAN services to its Ethernet WAN services.

Segra has read, understands, and will comply.

WVOT will be assigned a dedicated project manager to oversee the implementation of the services proposed in this RFP. Upon contract award, your project manager will create a schedule to bring all sites online based on the Project Plan below.

The goal of Segra's project management team is to provide a superior, seamless experience for our customers by establishing a single point of accountability for service implementation projects. Your project manager will ensure expedites, escalations, and jeopardies are handled appropriately and that all critical project dates are met. Your project manager will also coordinate the activities of individual team members across all Segra departments (as well as the customer's vendors if the customer concurs) and will ensure that all field personnel are assigned as needed based on the location and scope of the project. Throughout the project, your project manager will be able to provide status reports, identify, assign, and track to closure all project issues and action items, and reach an agreement on all changes to the project scope.

Project Plan

Segra's Project Plan methodology involves the use of recognized Project Management tools, as listed in Table 1 below, to ensure that projects are carefully planned, successfully executed, and closed out with the customer's concurrence that commitments have been met.

Table 1 – Project Management Tools

Initiating and Planning the Project	Executing, Monitoring, and Controlling the Project	Closing the Phase/Project
Project Scope and Charter	Change Request Form	Project Close-Out Checklist
Project Schedule	Change Control Log	Quality Review Plan
Risk Analysis and Mitigation Plan	Issue Log	Close-Out Package
Work Breakdown Structure (WBS)	Action Item Log	
Communication Plan	Project Status Reports	
Project Team Contact List		
Contract/Vendor Management Plan		

Executing, Monitoring, and Controlling the Project

Once the order is submitted, the Segra Project Manager will ensure that expedites, escalations, and jeopardies are handled appropriately and that all critical project dates are met. The Project Manager will coordinate the activities of individual project team members across all Segra departments (as well as the customer's vendors if the customer concurs) and will ensure that all field personnel are assigned as needed based on the location and scope of the project. Throughout the project, the Segra Project Manager will be responsible for:

- Managing Change Control processes, including changes in scope and variations in the Statement of Work (SOW);
- Tracking timeline, deliverables, action items, and outcomes associated with the project;
- Managing the Risk Mitigation plan, including identifying new risks associated with schedule and quality as they arise, and working with the customer and the project team to create action plans that address and/or mitigate potential issues; and
- Scheduling and running project status meetings and acting as the primary interface between the customer and the Segra implementation team.

The Project Manager will also meet with the customer at regularly scheduled intervals, as mutually agreed upon. The purpose of the meetings will be to provide status reports to the customer, to identify, assign, and track to closure all project issues and action items, and to reach an agreement on all changes to the project scope. These meetings will be held as often as necessary, but at least monthly. The timing and location of these meetings will be established with the customer during the project-planning phase, and the meetings may be in person or via conference call as deemed necessary by both parties.

Closing the Project

After installation is complete and service has been activated and tested, signed customer acceptance will be obtained, scanned, and saved to the appropriate customer project file. After completion of the project, a Segra representative will conduct a First Bill Review, including a financial audit, to review and clarify any discrepancies between the original contract and the actual billing. Project close-out activities will also include knowledge transfer and the release of project resources.

Project Implementation

The normal installation interval for fiber-based WAN services is approximately 90 to 180 business days from the date that Segra receives a clean order.

Segra follows the Project Management Body of Knowledge (PMBOK) process for project implementation. Throughout the implementation process, the various teams follow the steps listed below.

Section	Description	Activity
1.	Project Management	
	1.	Manage overall implementation process.
	2.	Track baseline and variation timelines.
	3.	Track Action Items.
	4.	Track project deliverables.
	5.	Implement Communications Plan.
	6.	Provide consistent updates to all project team members.
	7.	Ensure consistent compliance with the completion of prerequisite tasks.
	8.	Regularly and consistently monitor the implementation and integration of the solution.
	9.	PM will act as the primary escalation point for technical and non-technical issues and will obtain the necessary resources to resolve any issues.
	10.	Define assigned points of contact and team escalation points for the entirety of the solution implementation.
2.	Planning and Preparation	
2.1	Readiness Assessment	
	1.	Detailed assessment of applications to help determine the bandwidth needed at each site. Specific address, telephone, and contact information gathered for service inquiries. Information to be obtained through a combination of interviews with appropriate personnel and network assessment tools.
	2.	Review and analyze the data collected in order to determine the suitability of the network elements and links to support desired bandwidth. Identify areas that require improvements and provide recommendations in order for the affected network to be rectified to handle WAN access.
2.2	Operations Planning	
	1.	Assess current operational and maintenance processes and methods of procedures.
	2.	Develop or redefine operational and maintenance processes as needed.
	3.	Define interface and flow requirements between WVOT and Segra CNOC or other organizations as appropriate.
	4.	Identify appropriate personnel necessary to develop interface agreements.
	5.	Provide interface documentation and train all necessary personnel on the plan.
	6.	Define escalation procedures.

Section	Description	Activity
3.	Initial Set-Up Verification	
	1.	Complete user profiles and billing information.
	2.	Receive, in writing, the customer's decision on bandwidth needs.
4.	Training	
	1.	Define training requirements for different platforms.
	2.	Develop training delivery schedules.
	3.	Identify and reserve training locations.
	4.	Provide end-user training material for use during rollout.
5.	General Prerequisites	
	1.	Develop a customer document containing service information, processes, escalation, and contact information.
	2.	Perform Operational Readiness Test.
6.	Performance Management	
	1.	Establish performance standards.
	2.	Identify standard report requirements.
	3.	Define required reports.
	4.	Collect and analyze data.
	5.	Generate reports.
	6.	Perform trend analysis.
	7.	Distribute reports.
	8.	Review Internet Conferencing utilization periodically.
7.	Service Provisioning	
	1.	Issue order for fiber access and service.
	2.	Order is tracked. Segra Project Manager will provide status updates to the customer throughout the provisioning process.
	3.	Project Manager will direct, assist, and manage premise equipment activities associated with orders.
	4.	Complete fiber installation and send test ticket to Segra Operations for testing (2 days).
	5.	Upon completion of final operations task, an automatic email notification is generated to the customer stating that the service is ready. Circuit information is included in this email.
	6.	Segra Project Manager will work with the customer to schedule a date for the cut to the new service.

Section	Description	Activity
	7.	Segra Project Manager will email an Outlook invitation to the customer and Segra Installations/Operations with confirmed cut date.
8.	Project Close-Out	
	1.	Develop project findings with customer.
	2.	Produce reports of surveys and performance information as necessary.
	3.	Review project documentation with customer.

4.3.2.2.2. Vendor project plan must include details on how it will coordinate service migrations with WVOT and include details for their plan to mitigate any gaps in service (interruption of service).

Segra has read, understands, and will comply.

Segra has a robust Project Management Team, which is led by Dan Watts, Chief Operating Officer (22 years) and Cheryl Thibodeaux, Director Project Management (24 years). Cheryl's department consists of thirty-two (32) Project Managers with most having ten (10) plus years of experience managing projects.

A certified dedicated project manager will be assigned to each government agency to oversee the implementation of the services proposed in this RFP. The goal of Segra's project management team is to provide a superior, seamless experience for our customers by establishing a single point of accountability for service implementation projects. Your project manager will ensure expedites, escalations, and jeopardies are handled appropriately and that all critical project dates are met. Your project manager will also coordinate the activities of individual team members across all Segra departments, as well as the customer's vendors if the customer concurs, and will ensure that all field personnel are assigned as needed based on the location and scope of the project. Throughout the project, your project manager will be responsible for:

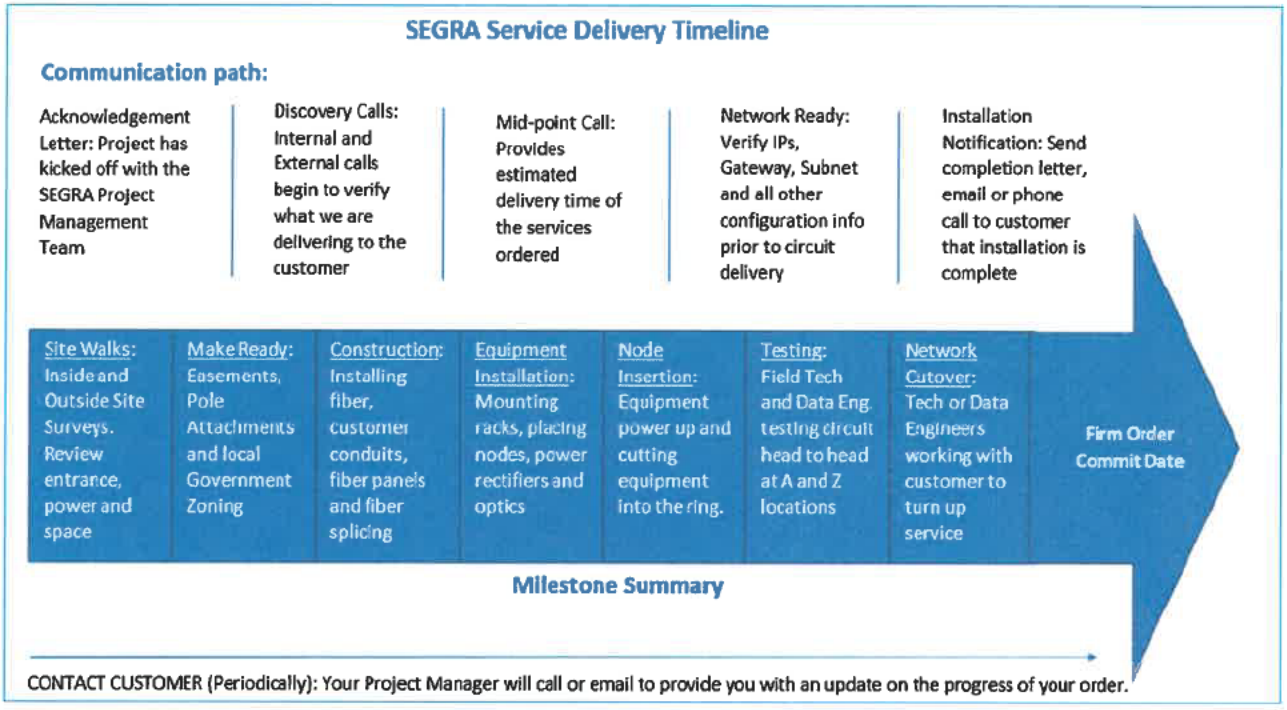
- Managing the Change Control processes, including changes in scope and variation in the Statement of Work (SoW);
- Tracking timelines, deliverables, action items, and outcomes associated with the project;
- Managing the Risk Mitigation Plan, including identifying new risks associated with the schedule and quality as they arise, and working directly with the customer and project team to crate action plans that address and/or mitigate potential issues; and
- Scheduling and running project status meetings and acting as the primary interface between the customer and the Segra implementation team.

The Project Manager will also meet with the specific government agency at regularly scheduled intervals. The purpose of these meetings will be to provide status reports, identify and track to closure any project issues and action items, and to reach agreement on all changes to the project scope.

Project Schedule

Segra uses specific project management teams and assigns specific project managers on each project who are responsible for coordinating all aspects and interactions to ensure accurate and timely completion. Additionally, we keep a KPI (Key Performance Indicator) at Segra for On Time Delivery by the month. We use the Initial FOC (Firm

Order Commitment date), which is an agreed upon date by Segra and the customer. This date does not change, and we track to completion for On Time or Earlier. We have a testing and acceptance team that is responsible for end-to-end testing and issuing a certificate that the circuit is ready to hand off. Following testing, a coordinated Activation of Services is scheduled with Segra technicians and the customer's vendor support for completion.



4.3.2.2.3. Vendor must coordinate new services acceptance and billing for new services with WVOT in a manner that eliminates any duplicate billing between legacy services and new Vendor services.

Segra has read, understands, and will comply.

Segra will coordinate all pending installation dates with the Office of Technology/State of West Virginia so that the pertinent disconnects can be placed with the current provider, in order to lessen, and even eliminate, duplicate billing when possible. Any services billed in error will be reviewed and addressed by Segra's Billing Support team.

4.3.2.2.4. Vendor must assign an experienced and skilled Project Manager who will provide a high-level project management plan including key components such as a project charter, issue tracking, statements of work (SOW), work breakdown structures (WBS), implementation schedules, etc. in accordance with the Project Management Body of Knowledge (PMBOK) or other industry standard project management methodology stated in West Virginia State Code (§5A-6-4b). The link can be found at:

http://www.legis.state.wv.us/WVCODE/Code.cfm?chap= 05a&art=6#06

Segra has read, understands, and will comply. In addition to the below, please also refer to **Segra's Detailed Work Breakdown Structure**, included in our response on page 290.

WVOT will be assigned a dedicated project manager to oversee the implementation of the services proposed in this RFP. Upon contract award, your project manager will create a schedule to bring all sites online based on the Project Plan below.

The goal of Segra's project management team is to provide a superior, seamless experience for our customers by establishing a single point of accountability for service implementation projects. Your project manager will ensure expedites, escalations, and jeopardies are handled appropriately and that all critical project dates are met. Your project manager will also coordinate the activities of individual team members across all Segra departments (as well as the customer's vendors if the customer concurs) and will ensure that all field personnel are assigned as needed based on the location and scope of the project. Throughout the project, your project manager will be able to provide status reports, identify, assign, and track to closure all project issues and action items, and reach an agreement on all changes to the project scope.

Project Plan

Segra's Project Plan methodology involves the use of recognized Project Management tools, as listed in Table 1 below, to ensure that projects are carefully planned, successfully executed, and closed out with the customer's concurrence that commitments have been met.

Table 1 – Project Management Tools

Initiating and Planning the Project	Executing, Monitoring, and Controlling the Project	Closing the Phase/Project
Project Scope and Charter	Change Request Form	Project Close-Out Checklist
Project Schedule	Change Control Log	Quality Review Plan
Risk Analysis and Mitigation Plan	Issue Log	Close-Out Package
Work Breakdown Structure (WBS)	Action Item Log	
Communication Plan	Project Status Reports	
Project Team Contact List		
Contract/Vendor Management Plan		

Executing, Monitoring, and Controlling the Project

Once the order is submitted, the Segra Project Manager will ensure that expedites, escalations, and jeopardies are handled appropriately and that all critical project dates are met. The Project Manager will coordinate the activities of individual project team members across all Segra departments (as well as the customer's vendors if the customer concurs) and will ensure that all field personnel are assigned as needed based on the location and scope of the project. Throughout the project, the Segra Project Manager will be responsible for:

- Managing Change Control processes, including changes in scope and variations in the Statement of Work (SOW);
- Tracking timeline, deliverables, action items, and outcomes associated with the project;
- Managing the Risk Mitigation plan, including identifying new risks associated with schedule and quality as they arise, and working with the customer and the project team to create action plans that address and/or mitigate

potential issues; and

- Scheduling and running project status meetings and acting as the primary interface between the customer and the Segra implementation team.

The Project Manager will also meet with the customer at regularly scheduled intervals, as mutually agreed upon. The purpose of the meetings will be to provide status reports to the customer, to identify, assign, and track to closure all project issues and action items, and to reach an agreement on all changes to the project scope. These meetings will be held as often as necessary, but at least monthly. The timing and location of these meetings will be established with the customer during the project-planning phase, and the meetings may be in person or via conference call as deemed necessary by both parties.

Closing the Project

After installation is complete and service has been activated and tested, signed customer acceptance will be obtained, scanned, and saved to the appropriate customer project file. After completion of the project, a Segra representative will conduct a First Bill Review, including a financial audit, to review and clarify any discrepancies between the original contract and the actual billing. Project close-out activities will also include knowledge transfer and the release of project resources.

Project Implementation

The normal installation interval for fiber-based WAN services is approximately 90 to 180 business days from the date that Segra receives a clean order.

Segra follows the Project Management Body of Knowledge (PMBOK) process for project implementation. Throughout the implementation process, the various teams follow the steps listed below.

Section	Description	Activity
1.	Project Management	
	1.	Manage overall implementation process.
	2.	Track baseline and variation timelines.
	3.	Track Action Items.
	4.	Track project deliverables.
	5.	Implement Communications Plan.
	6.	Provide consistent updates to all project team members.
	7.	Ensure consistent compliance with the completion of prerequisite tasks.
	8.	Regularly and consistently monitor the implementation and integration of the solution.
	9.	PM will act as the primary escalation point for technical and non-technical issues and will obtain the necessary resources to resolve any issues.
	10.	Define assigned points of contact and team escalation points for the entirety of the solution implementation.
2.	Planning and Preparation	

Section	Description	Activity
2.1	Readiness Assessment	
	1.	Detailed assessment of applications to help determine the bandwidth needed at each site. Specific address, telephone, and contact information gathered for service inquiries. Information to be obtained through a combination of interviews with appropriate personnel and network assessment tools.
	2.	Review and analyze the data collected in order to determine the suitability of the network elements and links to support desired bandwidth. Identify areas that require improvements and provide recommendations in order for the affected network to be rectified to handle WAN access.
2.2	Operations Planning	
	1.	Assess current operational and maintenance processes and methods of procedures.
	2.	Develop or redefine operational and maintenance processes as needed.
	3.	Define interface and flow requirements between WVOT and Segra CNOC or other organizations as appropriate.
	4.	Identify appropriate personnel necessary to develop interface agreements.
	5.	Provide interface documentation and train all necessary personnel on the plan.
	6.	Define escalation procedures.
3.	Initial Set-Up Verification	
	1.	Complete user profiles and billing information.
	2.	Receive, in writing, the customer's decision on bandwidth needs.
4.	Training	
	1.	Define training requirements for different platforms.
	2.	Develop training delivery schedules.
	3.	Identify and reserve training locations.
	4.	Provide end-user training material for use during rollout.
5.	General Prerequisites	
	1.	Develop a customer document containing service information, processes, escalation, and contact information.
	2.	Perform Operational Readiness Test.
6.	Performance Management	

Section	Description	Activity
	1.	Establish performance standards.
	2.	Identify standard report requirements.
	3.	Define required reports.
	4.	Collect and analyze data.
	5.	Generate reports.
	6.	Perform trend analysis.
	7.	Distribute reports.
	8.	Review Internet Conferencing utilization periodically.
7.	Service Provisioning	
	1.	Issue order for fiber access and service.
	2.	Order is tracked. Segra Project Manager will provide status updates to the customer throughout the provisioning process.
	3.	Project Manager will direct, assist, and manage premise equipment activities associated with orders.
	4.	Complete fiber installation and send test ticket to Segra Operations for testing (2 days).
	5.	Upon completion of final operations task, an automatic email notification is generated to the customer stating that the service is ready. Circuit information is included in this email.
	6.	Segra Project Manager will work with the customer to schedule a date for the cut to the new service.
	7.	Segra Project Manager will email an Outlook invitation to the customer and Segra Installations/Operations with confirmed cut date.
8.	Project Close-Out	
	1.	Develop project findings with customer.
	2.	Produce reports of surveys and performance information as necessary.
	3.	Review project documentation with customer.

4.3.2.2.5. The project management plan must be submitted and approved by the WVOT Project Management Office (PMO) prior to engaging the first agency for Ethernet WAN services implementation.

Segra has read, understands, and will comply.

4.3.2.2.6. The successful Vendor's Project Manager must track and report (via written status reports) the

following: schedule, scope, budget, issues, risks, specified performance indicators, and other metrics determined appropriate throughout the project and each site implementation.

Segra has read, understands, and will comply.

4.3.2.3. Part 3: Service and Support for WAN and DIA and 4G/5G Services

4.3.2.3.1. Vendor must provide a network operation support center(s) for all tiers of support that is available 24x7x365 and is accessible via a toll-free number.

Please refer to **Segra's Escalation Contacts and Contact Information**, and **Segra's Service Level Agreement (SLA)**, included in our response on pages 190 and 186, respectively.

Network Operations Center (NOC)

Segra's Network Operations Center has certified personnel accessible 24x7x365 at 833.GO.SEGRA to ensure your service is monitored and well looked after.

Segra supports our customers with geo-redundant network operations centers located in Waynesboro, VA and Columbia, SC. Segra's geo-redundant centers operate on a 24x7x365 basis.

Details of Segra's capabilities:

Issue Resolution and Maintenance
Segra has two 24/7/365 geo-redundant Network Operations Centers in Columbia, SC and Waynesboro, VA. Segra Field Operations Support teams are also located strategically in the markets served. Fiber restoration crews are also dispersed throughout our markets.

Segra's Enterprise Repair Team (ERT) is composed of a team of dedicated W-2 Segra engineers who are responsible for monitoring, troubleshooting, and maintaining the entire Segra network and the services provided. As the first point of contact for our customers, the ERT is responsible for generating trouble tickets on all issues, dispatching technicians if necessary, isolating the problem, keeping customers updated, and driving all troubles to completion. Quick trouble resolution with a sense of urgency is our priority, and we are available 24x7x365.

The Network Operations Center (NOC) manages all change management network events (high-risk maintenance activities) along with delivering on SLA parameters for mission critical services.

The Segra NOC tracks all events via trouble ticket(s). Customer event updates are provided via phone calls or emails directly from our ticketing system.

If an outage occurs, Segra has Ethernet test heads strategically placed throughout the network to perform RFC 2544 testing on demand, which supports our ability to meet the four-hour MTTR objective in our Service Level Agreement (SLA).

For any maintenance related activities, the Change Management group will notify customers via email of any service impacting scheduled work. Segra strives to give all customers at least seven (7) days' advance notice for all regularly

scheduled maintenance. These events take place between the hours of 12:01AM and 5:59AM. Segra reserves the right to perform emergency maintenance during service impacting events.

Mean Time to Repair Objective is Four (4) Hours

Mean Time to Repair (MTTR) is the average time required to repair service to an operational condition if service(s) are not active or the customer is experiencing consistent service degradation. The MTTR objective is four (4) hours for normal circuit outages, and ten (10) hours for fiber damages.

If an outage occurs, Segra has Ethernet test heads strategically placed throughout the network to perform RFC 2544 testing on demand, which supports our ability to meet the four-hour MTTR in our Service Level Agreement (SLA).

Segra has two 24/7/365 geo-diverse Network Operations Centers in Columbia, SC and Waynesboro, VA. Segra Field Operations Support teams are also located strategically in the markets served. Fiber restoration crews are also dispersed throughout our markets.

The severity/priority levels and escalation procedures are identical for all traffic types. The management escalation procedures for each severity/priority level are as follows:

- **Critical** - A critical ticket is defined as a service outage that has a severe impact on customer business operations with no workaround available. This condition includes a critical work stoppage during the customer's normal working hours that affects multiple customer sites and/or affects a critical component or function of the customer's business. Segra and its vendor-partners will commit substantial resources around the clock to resolve the situation. Examples of critical outages include an agency host major outage or 10% or greater of the current agency node count in production status.
    - Critical – Escalation Interval
        - Immediate: CNOC Manager & Director
        - 2 Hours: Vice President
- **Major** - A major ticket describes a condition where a partial service outage occurs or the service is severely degraded, which has a significant impact on customer business operations, with no adequate workaround available. This condition includes a partial work stoppage or severe performance degradation during the customer's normal working hours, which affects a customer site. Segra and vendor-partners will commit full time resources during business hours or around the clock as necessary to resolve the situation.
    - Major – Escalation Interval
        - Immediate: Tier 3 CNOC Analyst
        - 1 Hour: Floor Manager
        - 2 Hours: CNOC Manager
        - 3 Hours: Director
        - 5 Hours: Vice President
    - Escalations can be made at the customer's request
- **Minor** - A minor ticket describes conditions where difficulties are experienced with a transport service, but do not cause a work stoppage; there is a workaround, but performance and/or system functionality may be degraded or limited. This condition includes degraded service performance and impaired service functionality, but most business operations continue. Workarounds are established, implemented, and documented for problems with this priority level. Segra will commit resources during business hours as required to resolve problems with this severity level.
- **Informational** - An informational ticket describes conditions that are not urgent, and/or are not problems, and/or that do not impact customer business operations. Informational tickets are for the CNOC. This priority level is most appropriate for:

- Minor alarms and informational alarms
- Escalations can be made at the customer's request

4.3.2.3.2. Vendor must work with the WVOT using the established Telecommunications Change Request (TCR) procedures for ordering and implementing these telecommunications services.

Segra has reviewed, understands, and will comply.

4.3.2.3.3. For auditing, billing, and support purposes, the State requires any service with an associated rate to be identified on its monthly bill. As such, the State must be provided, at a minimum, the following:

4.3.2.3.3.1. Billing Month
4.3.2.3.3.2. Billed Entity Name
4.3.2.3.3.3. Customer Name/Account (if different from billed entity)
4.3.2.3.3.4. Service Location
4.3.2.3.3.5. Service Period
4.3.2.3.3.6. Circuit or Service ID
4.3.2.3.3.7. Price Sheet Billing Component (Ex. Ethernet WAN 10MB)
4.3.2.3.3.8. Itemized Cost for Individual Billing Components
4.3.2.3.3.9. Itemized Cost for Any One-Time or Non-Recurring Charges
4.3.2.3.3.10. Itemized Cost for Any Surcharges and Total Cost
4.3.2.3.3.11. The cost identified in the bill must match the contract rates for the specified services.

Segra has read, understands, and will comply.

4.3.2.3.4. The Vendor must provide the State's monthly bill in an editable format such as Excel and/or csv, and the State must be able to open the file in Google Sheets without the need for modifications. The Vendor's bill must be received within ten (10) business days from the end of the billing cycle. The Vendor should provide a copy of their bill as part of their response.

Segra has read, understands, and will comply. Segra can deliver billing detail in a .csv file. Invoice will be delivered within 10 days from the end of the billing cycle. Please refer to **Segra's Sample Bill**, included in our response on page 302.

4.3.2.3.5. The Vendor must invoice on a consistent monthly billing cycle across all services. Services installed or disconnected for a partial month must be prorated based on the date the service is accepted by the State or by the disconnect due date on the TCR. For new services, the Vendor must not bill the State until the State has accepted the services as functional. The Vendor shall not bill the State for services after the disconnect due date listed on the submitted TCR.

Segra has reviewed, understands, and will comply.

4.3.2.3.6. If a billing error is discovered by the State, the State shall notify the Vendor, in writing, of the errors and the errors must be corrected prior to the next billing cycle. Vendor billing errors must be credited back to the State from the effective date of the error. The State reserves the right to withhold payment, in part or in full, until credit is received.

Segra has read, understands, and will comply.

It is requested that the customer submit written notice of the claim with sufficient detail including, but not limited to: (a) the items on the invoices in dispute; (b) the nature of the dispute; (c) documentation of Customer filing a trouble report, including the Seller ticket number or order number; and (d) any other relevant information reasonably requested by Seller with respect to the affected Service(s) or the disputed amount. All claims must be submitted to Seller in writing within thirty (30) days from the date of the invoice for those Services or they are waived. If Customer has provided sufficient detail for investigation of the dispute, Seller will use reasonable efforts to resolve and communicate its resolution of the dispute within thirty (30) days of its receipt of the dispute notice.

4.3.2.3.7. If the Vendor has multiple contracts with the State of West Virginia, the Vendor must provide separate billing for each contract.

Segra has reviewed, understands, and will comply.

4.3.2.3.8. The Vendor must provide and update a weekly status report using the provided TCR log and agree to meetings to discuss as needed.

Segra has reviewed, understands, and will comply.

4.3.2.3.9. All unplanned service outages at the individual circuit level must be fully resolved within 24 hours. For each day beyond the initial 24-hour outage that an individual service is not fully functional, one day of credit will be applied to the State's bill. Credit shall be received starting at Hour 25 and no partial-day credits will be accepted. Service credit will be defined as monthly service cost divided by the number of days in that month. Service outage credits must not be averaged across all State installed services. Service outage credits must be applied against the individual site/service where the outage occurred.

Segra has read, understands, and will comply.

4.3.2.3.10. The State requires an Account team (including Account Support Representative, Technical Support Representative, Solution Implementation Support Representative, Contract Manager, Billing Support Representative, Security/Compliance Specialist, and Project Manager) for the winning solution and life of the contract. Vendor must describe in detail the responsibilities of key roles and staff's experience in working in these roles. The State reserves the right to request, and the Vendor must provide, a new employee for any reason.

Segra has read, understands, and will comply.

Segra employs over 870 full-time W-2 employees across our organization, with approximately 80 full-time W-2 employees based in West Virginia. Segra will have a series of personnel who will be dedicated to ensuring the requirements of this RFP are not only met, but exceeded.

ACCOUNT TEAM

Segra's dedicated Mid-Atlantic Government Account Team will be responsible for ensuring the overall satisfaction of WVOT for the services provided as a result of this RFP. These team members are located in West Virginia and Virginia and are extremely experienced in working with state agencies, local municipalities, universities, and K-12 entities on many government contracted services.

This tenured core team is led by Gary Crocco, Director - Government Sales, who began working with Segra as a Sales Director in 2017. As Director, Gary manages the support of all government accounts and continues to interact with customers and all internal departments for coordination, implementation, and escalation of services. He also serves as the procurement contact for all of Segra's government contracts with the State of West Virginia.

Segra's account team works closely each day with our customers on ordering, provisioning, and cross-functional teams to ensure the timely and successful delivery of services to meet their needs. Because there is an assigned account executive dedicated to each customer, strong and positive relationships have been developed with these users. The account team consists of:

- Kyle Herron, **VP of Service Delivery** (35 Years Telecom Experience - Former CIO of The Citadel and COO for the State of South Carolina)
- Gregory Florence, **Government Account Executive** (32 Years Telecom Experience - 15 of those with Segra)
- Michael Brisson, **Strategic Account Specialist** (15 Years Telecom Experience - 2 of those with Segra)
- David Jones, **Technical Support Representative** (30 Years Telecom Experience - 9 of those with Segra)
- Kelly Demattia, **Account Support Representative** (20 Years Telecom Experience - 15 of those with Segra)
- Bob Berry, **Senior Manager Technical Support** (26 Years Telecom Experience - 23 of those with Segra)
- Michael DeHart, **Team Lead, Technical Customer Solutions Center**, (38 Years Telecom Experience - 6 of those with Segra)
- Cheryl Thibodeaux, **Project Management and Implementation Support** (25 Years Telecom Experience - 5 of those with Segra)
- Teresa Bright, **Billing Support** (15 Years Telecom Experience - 14 of those with Segra)
- Amanda Folk, **Contract Management** (25 Years Telecom Experience - 13 of those with Segra)
- Jim Mundy, **Security/Compliance** (38 Years Telecom Experience - 7 of those with Segra)

TECHNICAL GUIDANCE AND SOLUTION DESIGN

The Segra Sales Engineering Team will serve as a technical resource for the services provided in this RFP and be fully engaged in supporting the project. This 27-member team is led by our Director of Sales Engineering, Kerry Grueneich (8 years of experience). David Jones, Senior Sales Engineer - Government, located in Pennsylvania, is dedicated to supporting the Government Sales Team in West Virginia and will serve as the primary engineering contact.

PROJECT MANAGEMENT

Segra has a robust Project Management Team, which is led by Dan Watts, Chief Operating Officer (22 years of experience) and Cheryl Thibodeaux, Senior Director of Project Management (24 years of experience). Cheryl's

department consists of thirty-two (32) Project Managers with most having over ten (10) years of experience managing projects.

A dedicated project manager will be assigned to WVOT to oversee the implementation of the services proposed in this RFP. The goal of Segra's project management team is to provide a superior, seamless experience for our customers by establishing a single point of accountability for service implementation projects. Your project manager will ensure expedites, escalations, and jeopardies are handled appropriately and that all critical project dates are met. Your project manager will also coordinate the activities of individual team members across all Segra departments, as well as the customer's vendors if the customer concurs, and will ensure that all field personnel are assigned as needed based on the location and scope of the project.

INSTALLATION

Segra's talented Field Operations team performs network installations and extensive equipment and facility maintenance, and provides timely service delivery with exceptional technical support to all of our customers. Our Field Operations support teams are located strategically in the markets served, and fiber restoration crews are also dispersed throughout our markets. Kyle Herron, Segra VP of Service Delivery, has over 35 years of telecommunications experience. Prior to joining Segra, he was the CIO at The Citadel and prior to that, he was the COO for the State of South Carolina.

PRODUCT MANAGEMENT/TRAINING

Segra's Product Management Department is headed by Jim Jones, Director of Product Management (3 years of experience). This department, with a current headcount of nine (9), is composed of a team of Product Managers as well as a dedicated Customer Onboarding Team to provide effective and comprehensive customer training for all Segra products and services.

HELP DESK AND OPERATIONAL SUPPORT

Segra supports our customers 24x7x365 with geo-redundant Network Operation Centers (NOC) located in Columbia, SC and Waynesboro, VA. Segra's NOC consists of the Customer Network Operations Center (CNOC), Network Operations Center (NOC), and Security Operations Center (SOC). Each organization consists of a team of dedicated Tier 1 and Tier 2 trained technicians who are responsible for monitoring, troubleshooting, and maintaining the entire Segra network and the services provided. Segra Field Operations Support teams are located strategically in the markets served, and fiber restoration crews are also dispersed throughout our markets.

The CNOC was established so Segra could have a direct focus on our end user customers. The CNOC is led by Scott Dunham, Senior Manager - Elite CNOC (2 years of experience) and Andrea Redfern, Senior Manager - Voice Enterprise Repair (10 years of experience), and staffed by 24 analysts operating in a contact center environment and serving as the single point of contact responsible for engaging the necessary resources to resolve customer issues. This team receives all incoming calls, creates trouble tickets, works the issue to resolution or escalates to respective support groups or vendors as necessary, and communicates back to the customer.

Segra will also provide a direct contact to a dedicated support manager who can triage any service related item. If needed once triage is complete, one of our strategically located Field Operations Support Technicians will be deployed to the customer premise.

The NOC, staffed by 31 engineers, is led by Cory Stringer, Director of the Network Operations Center (9 years of experience) and is responsible for ensuring that Segra's core and access networks are performing as they have been designed to do. This team is responsible for network surveillance, environmental alarms, maintenance notifications, and working ticket escalations when necessary.

Segra's SOC, led by James Mundy, Senior Manager - Security Operations (7 years of experience), brings together the people, technology, and process to identify threats in real time and take immediate action. In partnership with our Network Operations Center, our network is monitored 24x7x365. The SOC team consists of security specialists who are responsible for identifying real-time threats, triaging and mitigating through automation and manual investigation and remediation, and ensuring that all traffic is scrubbed against the latest threat intelligence so that they never reach a customer's facility.

CUSTOMER SOLUTIONS CENTER

In addition to the dedicated Government Account Team, Segra offers a Customer Solutions Center (CSC) located in Columbia, SC. Segra prides itself in Customer Service, the personal way. When you call Segra's Customer Care, you speak directly with one of our 20 representatives in Columbia, SC or Waynesboro, VA – not to another country and not to automated prompts or recordings.

The CSC is Segra's Tier 1 customer support group and is responsible for handling and triaging all incoming requests. Our highly trained professionals provide outstanding customer support and do their utmost to deliver first call resolution and assistance with product information, service ordering, and billing inquires. Segra's CSC can be reached at 1-800-686-7671 or customercare@segra.com.

Segra's CSC consists of two (2) specialized departments - Billing, which is led by Teresa Bright, Manager of Billing Support (14 years of experience), and Technical, which is led by Cheryl Morlan (2 years of experience), with overall responsibility falling under Nicole Smart, Senior Director of Customer Service (26 years of experience).

CONTRACT MANAGEMENT

The Legal Team provides invaluable expertise to support Segra's goal to offer state-of-the-art industry solutions to our customers. Segra's Legal Team is led by our Chief Legal Counsel and supported by the Associate General Counsel, the VP of Business & Legal Affairs, the Director of Strategic Contracts, the Manager of Strategic Contracts, the Regulatory Manager, and the Contract & Real Estate Specialist. The Legal Team is responsible for all contracts, litigation, real estate matters, and maintaining regulatory compliance with all federal, state, and local regulations.

4.3.2.3.11. The Vendor's bill must show E-rate discounts per Funding Request Number (FRN) on the bill for E-rate eligible entities.

Segra's bill will include the applicable E-Rate discount for all eligible services.

4.3.2.3.12. The State expects full, complete, and timely cooperation in disentangling the relationship in the event that the Agreement expires or terminates for any reason. In the event of expiration or termination, the State expects that the Vendor shall, among other things: return all State data and documentation to the State, including but not limited to configuration information; transfer ownership of all leased equipment at no cost to the State (other than the payments already received by the Vendor under the Agreement); and, allow the State or the replacement provider(s) continued access to all billing, ordering, and trouble ticketing systems, and processes that have been employed in servicing the State, in accordance with methods and procedures to be agreed

upon and established in the Agreement. Please acknowledge your acceptance of this in your RFP response.

Segra has reviewed, understands, and will comply.

4.3.2.3.13. If, as part of its proposal, the Vendor submits appendices or other supplemental materials, the Vendor must denote specifically in those materials where the relevant information is located.

Segra has read, understands, and will comply.

4.3.2.3.14. The Vendor's installation services must include all required products and services needed to install a functional service. This includes planning/engineering, termination, cross-connects, splices, terminating hardware setup, programming, mounting, and related documentation.

Segra has read, understands, and will comply.

Please refer to **Segra Environmental-Electronic Requirements for Fiber Projects**, included in our response on page 307, for space, power, and environmental requirements.

Also, please refer to **Segra's Remediation Guide**, included in our response on page 309, as an example of common installation. Segra's installation methodology is meant to ensure maximum assurance and service availability of 99.999%.

4.3.2.3.15. The Vendor must be capable of extending the service to the required termination location beyond the minimum point of entry. The additional cost for the extension of service must be provided in the Pricing Page (Exhibit A – line 54).

Segra has read, understands, and will comply. Please refer to **Exhibit A - Pricing Page**, included in our **Cost Proposal** on page 8. Please note: the pricing listed on the Pricing Page only applies for DEMARC extensions 200 feet and beyond. There is no charge for any DEMARC extension under 200 feet.

4.3.2.3.16. The Vendor must clearly label demarcation points with the site-specific service identification information, including demarcation extensions to the location of customer equipment where applicable. along with the identification of whether the Vendor or subcontractor will be providing the extension.

Segra has read, understands, and will comply.

Segra's demarcation point is the NID (Network Interface Device) or smart jack. Depending on existing or new demarcation needs, the NID may be outdoors (in a weatherproof box) or indoors. Segra would get an agreement from WVOT on demarcation location prior to any work being performed. Segra will specify the equipment, point of demarcation, rack space (if necessary) or wallboard needs, power, and any physical requirements of the Offeror's equipment to WVOT.

Segra will make known and has flexibility in the interface hand-off types that will be available for WVOT to connect WVOT's network to Segra's service. Extending the demarcation is an available request to WVOT as part of the installation service.

Segra is responsible for incurring the cost of all construction, cabling, and labor to install or otherwise extend the SDP to the location specified by WVOT.

Please refer to the environmental requirements in **Segra Environmental-Electronic Requirements for Fiber Projects**, included in our response on page 307.

4.3.2.3.17. The Vendor must comply with all applicable codes, licenses, certifications, and standards in the State of West Virginia as it relates to the proposed installation services.

Segra has read, understands, and will comply.

4.3.2.3.18. The Vendor must perform adequate testing after installation services are performed to ensure services are operating properly when turned up for the customer. The Vendor may be required to provide documentation of test results if so requested.

Segra has read, understands, and will comply.

Please see the testing plan/process utilized for circuit and internet service delivery:

Y.1564 and RFC 2544 Testing Requirements for E-Access Orders

Purpose
Address Y.1564 and RFC 2544 test, its purpose, and the components involved in the test.

Guidelines
Service providers must rely on testing in order to assure customers that their subscribed services are functioning as contracted. To this end, most service providers are using Y.1564 and RFC 2544 testing to establish three baseline parameters on the service:

- Throughput
- Latency
- Frame Loss

Remember that layer 2 tests are for layer 2 services (E-Line and E-Lan) and layer 3 tests are for layer 3 services (Dedicated Internet Access and Virtual Private Routed Networks). In both layer 2 and 3 tests, there is a certain amount of overhead inherent in both layer 2 frame headers and layer 3 IP headers.

One of the first pieces of information we will examine is the Test Loop types that are available to test to.

Loops and Loop Types
In RFC testing, we must point a testing device towards a loop of some sort. These loops can take on the form of a small cable looped back on itself physically, a logical loop where the internal hardware of the switch performs a process known as MAC Swapping/Bridging Loop, and, last but not least, is another test unit. There are pros and cons to each of these.

- **Physical Loop** - This requires additional hardware such as optics, cables, and even light pads. This is perhaps the most straightforward method of performing an end-to-end test. No additional configuration is needed to make this loop happen.
- **Logical Loop** - Some switches and routers have the ability to loop the information sent on the service back at the

sender with an intentional switching loop. This does not usually require additional hardware, but does require reconfiguration (if available) of hardware to accomplish and is the most cost effective/time saving of the three approaches.

- **Head-To-Head / Test Unit** - Many of the test head manufacturers have designed their test units to be able to link up automatically with like units and test available throughput more easily. This does require two test units and two technicians to operate the units. They also require optics and cabling to make this scenario work. This is the most effective, but costly (man-hours/equipment) method of the three.

Throughput

Testing Overhead

Part of testing the throughput of a circuit is testing how the circuit transports layer 2 / 3 data units of various sizes.

Drops/Frame loss due to frame size limitations will show up in RFC tests almost immediately and will not produce a passing test result. Technicians can usually tell when the test is going to fail by the way the meter is acting / reading during the test. In testing a layer 2 tunnel, we have the following protocols headers that we have to account for in the size of each frame:

- Ethernet - 14 Bytes
- 801.1q VLAN - 4 Bytes
- 802.1ad QinQ - 4 Bytes

The Metro Ethernet Forum (MEF) standard for a Maximum Transmission Unit (MTU) is around 1560. Most service providers these days allow for an MTU of up to 9000 on their own backbone.

Please note, some customer IGP traffic (specifically EIGRP) on layer 2 services may require an MTU higher than 1560.

As you can see, we can have up to 22 bytes in every frame occupied with header information alone. While this is not generally an issue with circuit tests, the overhead can be a major factor in testing a circuit that is close to the line speed of the port. For instance: Testing a circuit that is traversing a 100 Mbps service being handed off on a 100 Mbps port will only yield a 95-97 Mbps test. With a 1 Gbps service on a 1 Gbps port, you'll only get about 950-970 Mbps. Any test performed for <=90% of the port/line speed should be able to run cleanly with just the policers.

The same overhead is present in layer 3 packets as well, except we have IPv4 headers included in the packet, which is roughly 20 additional bytes. As you can see, the overhead increases significantly at layer 3.

Frame Sizes

In the RFC test, a variety of frame sizes are usually defined for testing by the test operator. The standard frame sizes available are:

- 68
- 132
- 260
- 516
- 1028
- 1284
- 1522
- Jumbo (9114)

As the test progresses, the test operator should be able to monitor the successful test of each frame size. If any one frame size fails, a new test will have to be initiated.

Latency

Latency is one of the more important statistics in the RFC test and can have a major effect on voice services. Each customer contract should have a maximum latency negotiated/agreed upon. Latency increases as the data flow increases in physical distance and active pass-throughs/routers.

Sources of Latency

In a vacuum, signals between computers travel at the speed of light, or 186,000 miles per second. In a fiber-optic cable, they slow down closer to 122,000 miles per second. The loss of speed measures roughly 8.2 microseconds per mile, or 0.82 milliseconds per 100 miles. The latency increases if the data packet must pass through a router or a switch, or your network uses NAT: network address translation, a system for sending network packets to your router's address.

Significance

Network latency matters more with small data packages than with big chunks of information. On big, slow-moving packets, the added drag of a millisecond or two remains all but imperceptible. With small data packets that should move swiftly, the added time can make a significant difference. In real-time voice or video communications, high latency becomes particularly noticeable, especially when it interrupts conversations.

Distance

Reduce the miles a signal must cross and you reduce data latency as well. A single mile of cable produces 0.5 percent of the delay introduced by a 200-mile stretch of cable. If you're planning a new location for an office that will become part of a wide area network, minimize its distance from the next node or the hub of the network. When you can't choose geographic locations to favor network traffic, consider alternative solutions.

Frame Loss

*"**Frame Loss Ratio (FLR)** is a characterization of the portion of lost Service Frames between the ingress External Interface (EI) and the egress External Interface (EI). Frame Loss Ratio is expressed as a percentage."* - MEF Definitions
In the RFC 2544 test, there should be little to no frame loss in the test. Frame loss of more that 0.1% could indicate problems in the flow path that will need to be examined. This could also indicate a problem with the policers in the path being too restrictive.

Testing

Once all testing is complete, the activations engineer will review test results. If it's passing, the engineer will normalize the circuit and prep for release to the customer with a copy of the test results. If the test results show failing, Segra will investigate accordingly, isolate the root cause, and retest after remedial actions are taken.

4.3.2.3.19. The Vendor must agree to the following installation timelines:

4.3.2.3.19.1. Forty-five days (45) where no special construction is required.

Segra has read, understands, and will comply. In addition to the 118 sites currently on-net, Segra is proposing building to an additional 149 locations that require special construction at no charge to the State of West Virginia. We anticipate the installation interval to be approximately 90 to 180 days for sites requiring special construction. If a

site requires a 45-day installation, a 4G/5G, broadband solution or an alternative access circuit may be installed to mitigate delays.

4.3.2.3.19.1.1. For each day beyond the forty-five (45) day installation intervals defined or agreed to above, where the new service is not installed within the installation timelines, liquidated damages of $500 per day will be assessed at the State's discretion.

Segra has read, understands, and will comply.

4.3.2.3.19.1.2. Where special construction is required, Vendor must provide installation timeline which must be approved by the state.

Segra has read, understands, and will comply.

4.3.2.3.20. The Vendor must provide a cost associated with expediting a service installation request on the Pricing Page (Exhibit A).

Segra has read, understands, and will comply. Please refer to **Exhibit A - Pricing Page**, included in our **Cost Proposal** on page 8.

4.3.2.3.20.1. The vendor will refund in full service expedite fee should agree upon expedite date not being met.

Segra has read, understands, and will comply.

4.3.2.3.21. The State will only pay special construction costs for new or legacy sites if other options (e.g.: 4G/5G wireless or other service provider facilities) are not available or if increased State bandwidth requirements cannot be met by existing telecommunication carrier facilities at the location. Special construction shall be approved at the State's discretion.

Segra has reviewed, understands, and will comply.

4.3.2.3.22. The Vendor must provide the following two value- added installation and managed service options.

4.3.2.3.22.1. Leased Router:

4.3.2.3.22.1.1. Vendor provided edge router

(Cisco or equal) will be leased by the state and must support access speed of service.

Segra has read, understands, and will comply.

4.3.2.3.22.1.2. Vendor retains ownership of the Router and is responsible for all licensing fees and maintenance costs.

Segra has read, understands, and will comply.

4.3.2.3.22.1.3. Vendor must replace/upgrade the Router within 24-months following the Cisco End of Support notification in order to maintain support and software update eligibility.

Segra's intention with the proposal and design being proposed is to replace the current Cisco equipment with an equivalent (with enhancements) VeloCloud Edge SD-WAN Router.

4.3.2.3.22.1.4. Vendor is required to provide replacement router upon failure within 8x5xNext Business Day.

Segra has read, understands, and will comply.

4.3.2.3.22.1.5. Vendor must replace/upgrade Router as requested by the State to support increased bandwidth demands and provide adequate throughput.

Segra has read, understands, and will comply.

4.3.2.3.22.1.6. WVOT retains management responsibility of the Router including configuration, installation, and monitoring.

Segra has read, understands, and will comply.

Segra touts its SD-WAN solution as being a co-managed solution.

4.3.2.3.22.2. Managed Internet Service

4.3.2.3.22.2.1. Vendor provides a bundled rate for managed services inclusive of the following:

4.3.2.3.22.2.1.1. Circuit, Edge router and Internet access

4.3.2.3.22.2.1.2. Installation and ongoing support for bundled service

Segra has read, understands, and will comply. Please refer to **Exhibit A - Pricing Page**, included in our **Cost Proposal** on page 8.

4.3.2.3.22.2.2. Vendor retains ownership of the Router and is responsible for all licensing fees and maintenance costs.

Segra has read, understands, and will comply.

4.3.2.3.22.2.3. Vendor must replace/upgrade the Router within 24-months following the Cisco End of Support notification in order to maintain support and software update eligibility.

Segra's intention with the proposal and design being proposed is to replace the current Cisco equipment with an equivalent (with enhancements) VeloCloud Edge SD-WAN Router.

4.3.2.3.22.2.4. Vendor is required to provide replacement router upon failure within 8x5xNext Business Day.

Segra has read, understands, and will comply.

4.3.2.3.22.2.5. Vendor must replace/upgrade Router as requested by the State to support increased bandwidth demands and provide adequate throughput.

Segra has read, understands, and will comply.

4.3.2.4. Part 4: Security for WAN and DIA Services

4.3.2.4.1. The Vendor will be responsible for the physical and cyber security of the network infrastructure that provides services to the State.

Segra has read, understands, and will comply. Segra's solution to WVOT is an inline, always on, automated DDoS detection and mitigation tool that is deployed at Segra peering points, resolving/mitigating attacks prior to making their way to a customer's network.

Segra utilizes the Corero SmartWall Threat Defense System (TDS) as the core of our managed security service offering DDoS Edge Protect. Segra's DDoS Edge Protect is a managed security service that eliminates cyber threats in real time. It provides comprehensive DDoS protection capable of mitigating a wide range of DDoS attacks all while maintaining full connectivity to avoid disrupting the delivery of legitimate traffic.

It is designed to handle large network-based DDoS attacks or floods, reflective amplified spoof attacks, as well as application layer attacks that are typically too low to be detected by out of band solutions. This DDoS Edge Protect product protects where firewalls cannot since the protection occurs prior to reaching the customer's network at the Internet peer source.

Segra supports our customers with geo-redundant network operation centers located in Waynesboro, VA and Columbia, SC. Segra's geo-redundant centers operate on a 24x7x365 basis.

DDoS mitigation is one attribute that sets Segra ahead of the competition, and is included as a standard feature with our dedicated Internet fiber services.

Segra implements DDoS protection at the Internet gateways. The DDoS appliances are capable of wire-speed inspection and enable mitigation of an identified DDoS attack at the very edge of the Segra network. This strategy not only protects the target customer, but also limits the attack's impact to overall Segra network performance. Threat/attack intelligence information on in-progress DDoS attacks from a network of global Tier 1 and Tier 2 providers is used to preemptively block DDoS attacks as they propagate globally. This approach to DDoS attacks provides Segra customers with both a proactive and a reactive DDoS attack threat response.

Please refer to **Segra's DDoS Edge** product sheet, included in our response on page 258. Please also refer to **Segra's Escalation Contacts and Contact Information** and **Segra's Service Level Agreement (SLA)**, included in our response on pages 190 and 186, respectively.

DDoS

DDoS protection appliances are located at high-volume entry points on the Segra core network where attacks are most likely to occur, such as public transit connections. The appliances automatically inspect all traffic as soon as it arrives at an entry point, immediately discarding malicious packets while sending legitimate packets to their destination. During this process, other network services continue to operate without interruption, even latency-sensitive applications like voice and video.

FAST

The protection capability is purpose-built for speed and low latency, so attacks are detected and mitigated immediately without impacting network performance.

EFFECTIVE

The protection is comprehensive, identifying both existing and newly discovered attack types, and preventing direct attacks as well as their side effects.

RISK REDUCTION

The fast, effective protection included in the Segra DIA service significantly minimizes the risk of DDoS attacks from the public Internet.

REAL-TIME FILTERING

Inspection, detection, and scrubbing occur as soon as traffic arrives at the Segra network.

AUTOMATIC PROCESSING

All filtering functions are performed automatically, without the requirement for regular human intervention and/or delay.

IN-LINE OPERATION

Traffic stays on the Segra network during filtering instead of being physically and/or logically diverted for processing, minimizing latency.

COMPREHENSIVE PROTECTION ANALYTICS

Inherent analytics detect a variety of attack types and are updated continually with the latest intelligence on DDoS threats.

CORE FUNCTIONALITY

DDoS protection is required as a standard, core function of the Segra DIA service. Taking this approach protects the entire Segra network path from DDoS attacks, and in turn, the entire Segra DIA customer base. The approach also complements any local DDoS solution a customer may implement since a local solution cannot protect the Segra network path.

SCALABILITY

The DDoS protection appliances are designed and located to easily keep pace with growth in the Segra footprint and the customer networks we serve. Any site a customer adds to the Segra network is automatically protected from DDoS attacks without configuration changes.

4.3.2.4.2. The Vendor will be responsible for resolving all security vulnerabilities that may affect equipment or transmission services provided to the customer.

Segra has read, understands, and will comply.

Please refer to the following Segra documentation, included in our response:

- Security Risk Management (page 250)
- Security Incident Response (page 242)
- Network Communications Policy (page 216)
- Physical and Environmental Security Policy (page 208)
- 2022 Pentest Results Summary (page 314)

4.3.2.4.3. The Vendor's policies, services, processes, or employees cannot create conflicts with the State's standard security policy requirements. In the event of a standard security policy conflict, the State's policy will prevail. (Policies available at http://www.technology.wv.gov)

Segra has reviewed, understands, and will comply with applicable policies. In the event of a conflict identified by the State, Segra will work with the State to determine an acceptable resolution. Please also refer to **Segra's Systems and**

Organization Controls (SOC 2) Type II Report for the covered services outlining relevant controls, included in our response on page 316.

4.4. Qualifications and Experience: Vendor should provide information and documentation regarding its qualifications and experience in providing services similar to those requested in this RFP. Information and documentation should include, but is not limited to, copies of any staff certifications or degrees applicable to this project, proposed staffing plans, descriptions of past projects completed (descriptions should include the location of the project, project manager name and contact information, type of project, and what the project goals and objectives where and how they were met.), references for prior projects, and any other information that vendor deems relevant to the items identified as desirable or mandatory below.

HISTORY OF SEGRA

Background

Segra has been serving customers since 1897 with the founding of CFW (Clifton Forge – Waynesboro), R&B Communications, PalmettoNet, and Spirt Telecom. Segra was formed by the joining of Lumos Networks and Spirit Communications when EQT Partners, a Swedish private equity group, purchased a majority stake in both companies in 2018. In 2019, the company was re-branded as "Segra," which is derived from a Swedish verb meaning "to win." We chose this name carefully, knowing that a commitment to win expands far beyond our walls. This commitment translates into an ongoing partnership with our customers, giving them the freedom to grow and reach their potential.

We continue to build on the legacy of our two companies, whose founders both had a passion for technology, communications, and product innovation. Segra is one of the largest independent fiber infrastructure bandwidth companies in the eastern U.S. We own and operate an advanced fiber infrastructure network throughout nine Mid-Atlantic and Southeastern states. Our state-of-the-art fiber network covers over 30,000 fiber-route miles that connect more than 10,400 on-net locations and 9 data centers and is delivered with our industry-leading service and reliability. Segra provides Ethernet, MPLS, dark fiber, advanced data center services, IP and managed services, voice and cloud solutions, all backed by its industry-leading service and reliability. Customers include carriers, enterprises, governments, higher education, and healthcare organizations.

In April of 2021, Cox Communications announced that it had entered into a definitive agreement to acquire the commercial services segment of Segra, which includes the enterprise and wholesale carrier services business. In

October of 2021, Cox Communications acquired Segra, which will continue to operate as a stand-alone business within the Cox family of businesses.

Segra currently employs approximately 870 full-time W-2 employees across our organization.

Segra's Headquarters:
11215 North Community House Road, Suite 1000
Charlotte, NC 28277

Segra Sales Office in West Virginia:
1200 Greenbrier Street, Charleston, WV 25311

Experience

Segra (legacy Lumos Networks and Spirit Communications) is celebrating over 30 years in business and has been offering the following services:

- Long Distance and Private Line Services - 30 Years
- Internet Service - 25 Years
- Data Network Service - 25 Years
- Local Service - 21 Years
- SS7 and ANSI Services - 25 Years
- IP Telephony Services - 19 Years
- 4G LTE Private IP NeMo Service - 10 Years

Segra has the technology, expertise, and financial strength to stand behind our services with comprehensive support and a local sales team who will ensure your needs are met. Segra has been the State of South Carolina's contracted provider for network services since 1996, long-distance voice provider since 1998, Internet service provider since 1999, K-12 Ethernet service provider since 2003, and Hosted Voice/VoIP service provider since 2008. We have proven we can deliver these services with accurate comprehensive billing, reporting, and responsive trouble management.

Segra has extensive experience working with government agencies and school districts. Segra directly employs an E-Rate funding team consisting of coordinators and billing specialists. Many have held this position since the original funding years of 1999-2000 of the E-Rate funding program. They are the Segra subject matter experts on all issues pertaining to E-Rate funding. Segra's E-Rate funding team is here to assist, provide guidance, and serve as contacts for questions regarding services that are being delivered. In addition to what's noted below, please also refer to section **4.4.1. Qualification and Experience Information**, included in our response on page 118, for additional qualifications, experience, and references.

Loudoun County School District, VA
Department of Digital Innovation
21000 Education Court, Suite 316
Ashburn, VA 20148

Aaron M. Smith, CETL, PMP, CSM
Interim Assistant Superintendent for Digital Innovation
(571) 252-1230
aaron.smith@lcps.org

Description of Work:
The Segra contract award established a multiple term contract to provide a Wide Area Network (WAN) solution for all campuses and facilities for Loudoun County Public Schools referred to as "LCPS".
The contract award provides connectivity for: 1) each LCPS facility to the backbone network of nine (9) Aggregation Sites (Hub Sites), 2) connectivity from each hub site to the DC Aggregation Site and to the Technology Center, and 3) an option to provide connectivity from the Aggregation Site and Technology Center to the Data Center at QTS.

Contract Period:
The award was for a Leased Lit fiber service contract for a period of ten (10) years with the option to renew for one (1) additional ten (10) year period and with the ability to upgrade to additional bandwidth.

Summary of deliverables by Segra:
- Dark Fiber to all LCPS sites in Loudoun County
- Segra providing an Elite Care team for LCPS
- 102 LCPS sites connected by Segra Dark Fiber
- 1,373 fiber route miles

State of West Virginia
Capitol Complex, Building 5, 10th Floor
1900 Kanawha Blvd E, Charleston, WV 25305

Joshua D. Spence, CISSP-CTO
Chief Information Officer
(304) 957-8100
Joshua.D.Spence@wv.gov

Description of Work:
In West Virginia, the use of Segra is not mandated for public sector institutions. However, we are implementing ten thousand VoIP seats in phase one of an ongoing operation. Phase two includes a second round of ten thousand seats. Segra has a dedicated team of account managers, project managers, and engineers working with various public sector agencies, including state agencies, universities, municipalities, and K-12 groups across the state.

The following table lists references for services similar to those described in this RFP:

Institution	Length of Service	Contact Name	Contact Email	Contact Phone
Virginia Community College System	9 Years	Ralph Lucia	rlucia@vccs.edu	(804) 423-6755
Virginia Military Institute	5 Years	Wes Robinson	robinsonwl@vmi.edu	(540) 464-7036
Washington and Lee University	18 Years	Matt Fitzgerald	mfitzgerald@wlu.edu	(540) 462-7036
Roanoke College	9 Years	Mark Poore	poore@roanoke.edu	(540) 375-2403
Bridgewater College	19 Years	Aaron Kein	aaron@bridgewater.edu	(540) 828-5646
Christopher Newport University	5 Years	Brian Foran	brian@cnu.edu	(757) 594-8620
Liberty University	9 Years	John Dalton	jjdalton@liberty.edu	(434) 592-6979

Institution	Length of Service	Contact Name	Contact Email	Contact Phone
Lynchburg College	6 Years	Bob Driskill	driskall.b@lynchburg.edu	(434) 544-8100
Norfolk State University	3 Years	Ronald King	raking@nsu.edu	(757) 823-2916
Radford University	9 Years	Ed Oakes	eoakes@radford.edu	(540) 831-7515
ECPI University	3 Years	Julian Aiken	jaiken@ecpi.edu	(757) 213-3522
Randolph-Macon College	1 Year	Kirk Baumbach	KirkBaumbach@rmc.edu	(804) 752-7263

Segra has the ability in all respects to fully perform the contract requirements of this Request for Proposal. Segra has a successful history of completing projects of the same size and scope as those outlined in this RFP. As a current contracted vendor of Internet Services for the State of South Carolina, Segra has been working with governmental units since 1999 to assist with their Internet service needs. Segra has also been the sole Internet Service provider for the K-12 Schools and Library community since 2016. Segra has the technology, expertise, and financial strength to stand behind our services with comprehensive support and an account team who will ensure your needs are met.

In addition to the government account team, Segra will have a series of personnel who will be dedicated to ensuring the requirements of this RFP are not only met but exceeded. The following table lists the key support contacts:

Support Area	Key Contact	Role
Account Management	Gary Crocco, Director of Mid-Atlantic Government	Gary has over 25 years of sales leadership experience in the telecommunications industry. Prior to joining Segra, Gary worked for Level 3/CenturyLink where he led the sales efforts of a broad range of technology based solutions to SLED organizations, large local enterprise, and multi-national corporations. Prior to that, Gary served as Regional Sales Vice President at Frontier Communications leading a multi-state, government, and commercial sales force. For the previous 12 years, Gary was employed by Cavalier Telephone where he served in various sales leadership roles, ultimately rising to SVP of Commercial Sales and Retention where he led all government, direct, indirect, and retention sales channels for the company. Gary started his telecommunications career with AT&T where he led various commercial sales teams within AT&T Business Services and AT&T Broadband. Gary is a graduate of the College of William and Mary and lives in Richmond with his wife and four children.
Account Management	Greg Florence, Government Account Executive	Greg Florence is a Major Account Manager who has been with Segra over 15 years. Greg has managed accounts in the Commercial, Government, Higher Education, Financial, and Healthcare market segments. Greg has worked in the telecom industry for over 30 years. Greg is a graduate of WVU, has 3 sons, and lives in Charleston, WV with his wife.
Sales Engineer	David A. Jones, Senior Sales Engineer	David A. Jones is the Senior Sales Engineer who will be supporting the project. He has been with Segra for over 9 years. David has extensive experience designing and implementing cost effective solutions for Ethernet wide area networks for educational and non-educational customers consistent with industry standards. He has been working in the telecom industry for over 30 years. His experience includes supporting Ethernet, SIP,

Support Area	Key Contact	Role
		DWDM, SONET, and legacy voice and data services. This experience also includes obtaining certifications with Lucent, Fujitsu, AT&T, Tellabs, and Carrier Access networking equipment. David supports Sales Account Directors with the technical solution and network design. David lives in Warriors Mark, PA and covers the Mid-Atlantic area. David holds a B.A. in Computing and Information Science from St. Vincent College in Latrobe, PA.
Installation	Kyle Herron, VP of Service Delivery	Kyle has over 35 years of telecommunications experience. Kyle and his team are responsible for ensuring that the installation process of all services is delivered on time, accurately, and completely. Prior to joining Segra, Kyle was most recently the CIO of The Citadel. Prior to The Citadel, Kyle was the COO for the State of South Carolina. Kyle recently joined Segra, but has been in a consulting role for Segra the past 5 years. In his role as consultant, Kyle played a key role in the Hosted Voice Services Contract currently in place between the State of WV and Segra. His many years of experience, relationship with key personnel, and overall familiarity and ongoing commitment to the State of WV will ensure a successful delivery of the Segra solution for the State.
Project Management	Cheryl Thibodeaux, Director of Customer Implementation Advocacy	Cheryl's team's responsibility is to provide superior customer support throughout the service implementation process. They ensure that expedites, escalations, and jeopardies are handled appropriately and that all critical project dates are met. They will coordinate the activities of individual project team members across all Segra departments, as well as the customer's vendors if the customer concurs, and will ensure that all field personnel are assigned as needed based on the location and scope of the project. Throughout the project, Cheryl will be able to provide status reports, identify, assign, and track to closure all project issues and action items, and to reach agreement on all changes to project scope.
Operational Support	Walt Cole, Senior Manager, Technical Support	Walt Cole began his career at Segra in July 2013. In his current role as Technical Service Manager, Walt provides you with an internal contact for all support issues. He is the liaison between Segra's CNOC, sales, and our customers.
Billing	Teresa Bright, Manager – Customer Solutions Center – Billing Support	Teresa has 14 years of billing experience with Segra and 12 years managing the Billing Team. Teresa and her team are responsible for handling and triaging incoming billing requests to ensure all instances are resolved promptly and properly.

4.4.1. Qualification and Experience Information: Vendor should describe in its proposal how it meets the desirable qualification and experience requirements listed below.

4.4.1.1. Vendor should provide three (3) examples demonstrating at least three (3) years of experience in providing state-wide or region-wide Ethernet Wan Services of a similar size and scope as this project, with at least one example being a public entity. Vendor should

provide a summarization of each project including goals and objectives, total number of circuits deployed, length of time deployment took, if still in service, and reference for each example.

Segra brings a wealth of experience and expertise in serving the public sector throughout our entire service area. K-12, higher education, federal, state, and local government agencies of all sizes enjoy Segra's unsurpassed customer service, as well as premium technology and data protection services uniquely designed for their specific needs.

Loudoun County Public Schools (LCPS), serving the third largest county in Virginia, selected Segra to deploy network services throughout its school system. Segra's Wide Area Network (WAN) solution was chosen for the connectivity, reliability, security, and performance that LCPS need to support online learning, virtual classrooms, and the expected population growth of the region.

Segra's solution for LCPS provides connectivity between several network hub sites to over 100 LCPS facilities and data centers. Segra's world-class fiber network, along with an updated network architecture design, offers greater reliability and increased performance. In addition, the WAN is deployed with the technology necessary to support advanced communication and data services, and to scale with the county's population growth and increased demand for bandwidth. Segra's WAN provides diverse fiber routes for redundant connectivity to ensure continuity of operations in the event of a natural disaster or other catastrophic events. Deployment took approximately one year.

The partnership between Segra and LCPS represents a significant investment by Segra in the network infrastructure of the region and a major expansion of its world-class fiber network to a growing part of the state seeking alternative, high-bandwidth providers. This network expansion, in one of the largest counties in Virginia, provides the infrastructure needed to support the massive demand for connectivity. In addition to the LCPS, Loudoun County also selected Segra to provide its WAN solution to approximately 100 sites. This decision was made in large part due to the approach and methodology Segra incorporated into the implementation plan for LCPS and our proven ability to deliver upon the mandatory project requirements.

Segra provides Dark Fiber along with Hosted Voice, WAN, and Internet Services to 86 school districts across the State of South Carolina, providing Hosted IP Voice service since 2008, WAN for all 86 school districts to include Layer 2, Layer 3, and Leased Dark Fiber since 2003, and Dedicated Internet service to all 86 school districts from 10M to 10G since 1999. Segra was awarded as the single Hosted Voice over IP Contracted Service Provider from 2008 through today. Every public agency in the State of South Carolina that implements hosted voice must purchase through Segra via this state contract. Currently, Segra provides over 32,000 Hosted Voice over IP seats to virtually every state agency across South Carolina, which includes 588 service locations across 114 municipalities and K-12 school divisions riding over the Segra network. Deployment has been ongoing, but new circuits typically have taken six months.

DISH Wireless L.L.C, which operates Boost Mobile, is another Segra customer. DISH Wireless is a subsidiary of DISH Network Corporation (NASDAQ: DISH), headquartered in Denver, CO. In 2020, DISH became a nationwide U.S. wireless carrier through the acquisition of Boost Mobile. DISH continues to innovate in wireless, building the nation's first virtualized standalone 5G broadband network. Segra is providing Fiber Data Connectivity to hundreds of towers as DISH rolls out its wireless service options. DISH has many hard set delivery dates mandated by the FCC for population and geographic coverage areas, and Segra has been a key partner in ensuring DISH makes appropriate delivery dates.

The above customers are all still in service and growing with Segra.

Loudoun County Public Schools
Aaron M. Smith, CETL, PMP, CSM
Interim Assistant Superintendent for Digital Innovation
(571) 252-1230
aaron.smith@lcps.org

State of South Carolina
Charlie Zeberlein
Current Network Manager for the South Carolina Department of Transportation
Former State of South Carolina Network Design and Infrastructure Manager
(803) 896-0381
Charlie.zeberlein@admin.sc.gov

Dish Network
Josh Graham
Head of Transport
(281) 235-0851
Joshua2.Graham@dish.com

4.4.1.2. The State desires an Account Team (including Account Support Representative, Technical Support Representative, Solution Implementation Support Representative, Contract Manager, Billing Support Representative, Security/Compliance Specialist, and Project Manager) for the winning solution and life of the contract. Vendor should describe in detail the responsibilities of key roles and staff's experience in working in these roles.

Segra has read, understands, and will comply.

Segra employs over 870 full-time W-2 employees across our organization, with approximately 80 full-time W-2 employees based in West Virginia. Segra will have a series of personnel who will be dedicated to ensuring the requirements of this RFP are not only met, but exceeded.

ACCOUNT TEAM

Segra's dedicated Mid-Atlantic Government Account Team will be responsible for ensuring the overall satisfaction of WVOT for the services provided as a result of this RFP. These team members are located in West Virginia and Virginia and are extremely experienced in working with state agencies, local municipalities, universities, and K-12 entities on many government contracted services.

This tenured core team is led by Gary Crocco, Director - Government Sales, who began working with Segra as a Sales Director in 2017. As Director, Gary manages the support of all government accounts and continues to interact with customers and all internal departments for coordination, implementation, and escalation of services. He also serves as the procurement contact for all of Segra's government contracts with the State of West Virginia.

Segra's account team works closely each day with our customers on ordering, provisioning, and cross-functional teams to ensure the timely and successful delivery of services to meet their needs. Because there is an assigned account executive dedicated to each customer, strong and positive relationships have been developed with these users. The account team consists of:

- Kyle Herron, **VP of Service Delivery** (35 Years Telecom Experience - Former CIO of The Citadel and COO for the State of South Carolina)
- Gregory Florence, **Government Account Executive** (32 Years Telecom Experience - 15 of those with Segra)
- Michael Brisson, **Strategic Account Specialist** (15 Years Telecom Experience - 2 of those with Segra)
- David Jones, **Technical Support Representative** (30 Years Telecom Experience - 9 of those with Segra)
- Kelly Demattia, **Account Support Representative** (20 Years Telecom Experience - 15 of those with Segra)
- Bob Berry, **Senior Manager Technical Support** (26 Years Telecom Experience - 23 of those with Segra)
- Michael DeHart, **Team Lead, Technical Customer Solutions Center**, (38 Years Telecom Experience - 6 of those with Segra)
- Cheryl Thibodeaux, **Project Management and Implementation Support** (25 Years Telecom Experience - 5 of those with Segra)
- Teresa Bright, **Billing Support** (15 Years Telecom Experience - 14 of those with Segra)
- Amanda Folk, **Contract Management** (25 Years Telecom Experience - 13 of those with Segra)
- Jim Mundy, **Security/Compliance** (38 Years Telecom Experience - 7 of those with Segra)

TECHNICAL GUIDANCE AND SOLUTION DESIGN

The Segra Sales Engineering Team will serve as a technical resource for the services provided in this RFP and be fully engaged in supporting the project. This 27-member team is led by our Director of Sales Engineering, Kerry Grueneich (8 years of experience). David Jones, Senior Sales Engineer - Government, located in Pennsylvania, is dedicated to supporting the Government Sales Team in West Virginia and will serve as the primary engineering contact.

PROJECT MANAGEMENT

Segra has a robust Project Management Team, which is led by Dan Watts, Chief Operating Officer (22 years of experience) and Cheryl Thibodeaux, Senior Director of Project Management (24 years of experience). Cheryl's department consists of thirty-two (32) Project Managers with most having over ten (10) years of experience managing projects.

A dedicated project manager will be assigned to WVOT to oversee the implementation of the services proposed in this RFP. The goal of Segra's project management team is to provide a superior, seamless experience for our customers by establishing a single point of accountability for service implementation projects. Your project manager will ensure expedites, escalations, and jeopardies are handled appropriately and that all critical project dates are met. Your project manager will also coordinate the activities of individual team members across all Segra departments, as well as the customer's vendors if the customer concurs, and will ensure that all field personnel are assigned as needed based on the location and scope of the project.

INSTALLATION

Segra's talented Field Operations team performs network installations and extensive equipment and facility maintenance, and provides timely service delivery with exceptional technical support to all of our customers. Our Field Operations support teams are located strategically in the markets served, and fiber restoration crews are also dispersed throughout our markets. Kyle Herron, Segra VP of Service Delivery, has over 35 years of telecommunications experience. Prior to joining Segra, he was the CIO at The Citadel and prior to that, he was the COO for the State of South Carolina.

PRODUCT MANAGEMENT/TRAINING

Segra's Product Management Department is headed by Jim Jones, Director of Product Management (3 years of experience). This department, with a current headcount of nine (9), is composed of a team of Product Managers as

well as a dedicated Customer Onboarding Team to provide effective and comprehensive customer training for all Segra products and services.

HELP DESK AND OPERATIONAL SUPPORT

Segra supports our customers 24x7x365 with geo-redundant Network Operation Centers (NOC) located in Columbia, SC and Waynesboro, VA. Segra's NOC consists of the Customer Network Operations Center (CNOC), Network Operations Center (NOC), and Security Operations Center (SOC). Each organization consists of a team of dedicated Tier 1 and Tier 2 trained technicians who are responsible for monitoring, troubleshooting, and maintaining the entire Segra network and the services provided. Segra Field Operations Support teams are located strategically in the markets served, and fiber restoration crews are also dispersed throughout our markets.

The CNOC was established so Segra could have a direct focus on our end user customers. The CNOC is led by Scott Dunham, Senior Manager - Elite CNOC (2 years of experience) and Andrea Redfern, Senior Manager - Voice Enterprise Repair (10 years of experience), and staffed by 24 analysts operating in a contact center environment and serving as the single point of contact responsible for engaging the necessary resources to resolve customer issues. This team receives all incoming calls, creates trouble tickets, works the issue to resolution or escalates to respective support groups or vendors as necessary, and communicates back to the customer.

Segra will also provide a direct contact to a dedicated support manager who can triage any service related item. If needed once triage is complete, one of our strategically located Field Operations Support Technicians will be deployed to the customer premise.

The NOC, staffed by 31 engineers, is led by Cory Stringer, Director of the Network Operations Center (9 years of experience) and is responsible for ensuring that Segra's core and access networks are performing as they have been designed to do. This team is responsible for network surveillance, environmental alarms, maintenance notifications, and working ticket escalations when necessary.

Segra's SOC, led by James Mundy, Senior Manager - Security Operations (7 years of experience), brings together the people, technology, and process to identify threats in real time and take immediate action. In partnership with our Network Operations Center, our network is monitored 24x7x365. The SOC team consists of security specialists who are responsible for identifying real-time threats, triaging and mitigating through automation and manual investigation and remediation, and ensuring that all traffic is scrubbed against the latest threat intelligence so that they never reach a customer's facility.

CUSTOMER SOLUTIONS CENTER

In addition to the dedicated Government Account Team, Segra offers a Customer Solutions Center (CSC) located in Columbia, SC. Segra prides itself in Customer Service, the personal way. When you call Segra's Customer Care, you speak directly with one of our 20 representatives in Columbia, SC or Waynesboro, VA – not to another country and not to automated prompts or recordings.

The CSC is Segra's Tier 1 customer support group and is responsible for handling and triaging all incoming requests. Our highly trained professionals provide outstanding customer support and do their utmost to deliver first call resolution and assistance with product information, service ordering, and billing inquires. Segra's CSC can be reached at 1-800-686-7671 or customercare@segra.com.

Segra's CSC consists of two (2) specialized departments - Billing, which is led by Teresa Bright, Manager of Billing Support (14 years of experience), and Technical, which is led by Cheryl Morlan (2 years of experience), with overall responsibility falling under Nicole Smart, Senior Director of Customer Service (26 years of experience).

CONTRACT MANAGEMENT

The Legal Team provides invaluable expertise to support Segra's goal to offer state-of-the-art industry solutions to our customers. Segra's Legal Team is led by our Chief Legal Counsel and supported by the Associate General Counsel, the VP of Business & Legal Affairs, the Director of Strategic Contracts, the Manager of Strategic Contracts, the Regulatory Manager, and the Contract & Real Estate Specialist. The Legal Team is responsible for all contracts, litigation, real estate matters, and maintaining regulatory compliance with all federal, state, and local regulations.

4.4.1.3. Vendor should describe its experience and provide an overview of their incident management process and cyber threat intelligence sharing process for incidents associated with the vendor provided solution.

Please refer to Segra's **Security Incident Response** policy, included in our response on page 242.

4.5. **Oral Presentations (Agency Option):** The Agency has the option of requiring oral presentations of all Vendors participating in the RFP process. If this option is exercised, points will be allocated in Section 6.2 below at the time the RFP is issued, or via addendum prior to technical bid opening. During oral presentations, Vendors may not alter or add to their submitted proposal, but only clarify information. A description of the materials and information to be presented is provided below:

Segra has read, understands, and will comply. Segra welcomes the opportunity to participate in an oral presentation to discuss the benefits of our proposal.

Materials and Information Requested at Oral Presentation:

4.5.1. Vendor will give an overview of its bid response, explaining its approach and methodology to providing the services outlined in the RFP, as well as provide information regarding its experience.

Segra has read, understands, and will comply.

4.5.2. The State of West Virginia will ask clarifying questions regarding the submission.

Segra has read, understands, and will comply.

SECTION 5: VENDOR PROPOSAL

5. **Economy of Preparation:** Proposals should be prepared simply and economically providing a concise description of the items requested in Section 4. Emphasis should be placed on completeness and clarity of the content.

Segra has read, understands, and will comply.

5.1. **Incurring Cost:** Neither the State nor any of its employees or officers shall be held liable for any expenses incurred by any Vendor responding to this RFP, including but not limited to preparation, delivery, or travel.

Segra has read, understands, and will comply.

5.2. Proposal Format: Vendors should provide responses in the format listed below:

5.2.1. Two-Part Submission: Vendors must submit proposals in two distinct parts: technical and cost. Technical proposals must not contain any cost information relating to the project. Cost proposal must contain all cost information and must be sealed in a separate envelope from the technical proposal to facilitate a secondary cost proposal opening.

Segra has read, understands, and will comply.

5.2.2. Title Page: State the RFP subject, number, Vendor's name, business address, telephone number, fax number, name of contact person, e-mail address, and Vendor signature and date.

Segra has read, understands, and will comply.

5.2.3. Table of Contents: Clearly identify the material by section and page number.

Segra has read, understands, and will comply.

5.2.4. Response Reference: Vendor's response should clearly reference how the information provided applies to the RFP request. For example, listing the RFP number and restating the RFP request as a header in the proposal would be considered a clear reference.

Segra has read, understands, and will comply.

5.2.5. Proposal Submission: All proposals (both technical and cost) must be submitted to the Purchasing Division prior to the date and time listed in Section 2, Instructions to Vendors Submitting Bids as the bid opening date and time.

Segra has read, understands, and will comply.

SECTION 6: EVALUATION AND AWARD

6. **Evaluation Process:** Proposals will be evaluated in two parts by a committee of three (3) or more individuals. The first evaluation will be of the technical proposal and the second is an evaluation of the cost proposal. The Vendor who demonstrates that it meets all of the mandatory specifications required, attains the minimum acceptable score and attains the highest overall point score of all Vendors shall be awarded the contract.

Segra has read and understands.

6.1. **Evaluation Criteria:** Proposals will be evaluated based on criteria set forth in the solicitation and information contained in the proposals submitted in response to the solicitation. The technical evaluation will be based upon the point allocations designated below for a total of 70 of the 100 points. Cost represents 30 of the 100 total points.

Evaluation Point Allocation:

Project Goals and Proposed Approach (§ 4.2)

• Approach & Methodology to Goals/Objectives (§ 4.2.1)	50 Points Possible
Part 1: Technology Service & Solution for Ethernet WAN, DIA & 4G/5G Services	25 Points Possible
Part 2: Vendor Ethernet WAN Services Migration Plan	5 Points Possible
Part 3: Service and Support for WAN and DIA & 4G/5G Services	10 Points Possible
Part 4: Security for WAN & DIA Services	10 Points Possible
• Approach & Methodology to Compliance with Mandatory Project Requirements (§ 4.2.2)	5 Points Possible

Qualifications and experience (§ 4.3)

• Qualifications and Experience Generally (§ 4.3.1)	10 Points Possible
(Oral interview, if applicable) (§ 4.4)	5 Points Possible
Total Technical Score:	70 Points Possible
Total Cost Score:	30 Points Possible
Total Proposal Score:	**100 Points Possible**

Segra has read and understands.

6.2. **Technical Bid Opening:** At the technical bid opening, the Purchasing Division will open and announce the technical proposals received prior to the bid opening deadline. Once opened, the technical proposals will be provided to the Agency evaluation committee for technical evaluation.

Segra has read and understands.

6.3. **Technical Evaluation:** The Agency evaluation committee will review the technical proposals, assign points where appropriate, and make a final written recommendation to the Purchasing Division.

Segra has read and understands.

6.4. **Proposal Disqualification:**

6.4.1. **Minimum Acceptable Score ("MAS"):** Vendors must score a minimum of 70% (49 points) of the total technical points possible in order to move past the technical evaluation and have their cost proposal evaluated. All vendor proposals not attaining the MAS will be disqualified.

Segra has read and understands.

6.4.2. **Failure to Meet Mandatory Requirement:** Vendors must meet or exceed all mandatory requirements in order to move past the technical evaluation and have their cost proposals evaluated. Proposals failing to meet one or more mandatory requirements of the RFP will be disqualified.

Segra has read and understands.

6.5. **Cost Bid Opening:** The Purchasing Division will schedule a date and time to publicly open and announce cost proposals after technical evaluation has been completed and the Purchasing Division has approved the technical recommendation of the evaluation committee. All cost bids received will be opened. Cost bids for disqualified proposals will be opened for record keeping purposes only and will not be evaluated or considered. Once opened, the cost proposals will be provided to the Agency evaluation committee for cost evaluation.

The Purchasing Division reserves the right to disqualify a proposal based upon deficiencies in the technical proposal even after the cost evaluation.

Segra has read and understands.

6.6. **Cost Evaluation:** The Agency evaluation committee will review the cost proposals, assign points in accordance with the cost evaluation formula contained herein and make a final recommendation to the Purchasing Division.

Segra has read and understands.

Cost Evaluation Formula: Each cost proposal will have points assigned using the following formula for all Vendors not disqualified during the technical evaluation. The lowest cost of all proposals is divided by the cost of the proposal being evaluated to generate a cost score percentage. That percentage is then multiplied by the points attributable to the cost proposal to determine the number of points allocated to the cost proposal being evaluated.

Step 1: Lowest Cost of All Proposals / Cost of Proposal Being Evaluated = Cost Score Percentage

Step 2: Cost Score Percentage X Points Allocated to Cost Proposal = **Total Cost Score**

Example:

Proposal 1 Cost is $1,000,000
Proposal 2 Cost is $1,100,000
Points Allocated to Cost Proposal is 30

Proposal 1: Step 1 – $1,000,000 / $1,000,000 = Cost Score Percentage of 1 (100%)
Step 2 – 1 X 30 = Total Cost Score of 30

Proposal 2: Step 1– $1,000,000 / $1,100,000 = Cost Score Percentage of 0.909091 (90.9091%)
Step 2 – 0.909091 X 30 = Total Cost Score of 27.27273

Segra has read and understands.

6.7. Availability of Information: Proposal submissions become public and are available for review immediately after opening pursuant to West Virginia Code §5A-3-11(h). All other information associated with the RFP, including but not limited to, technical scores and reasons for disqualification, will not be available until after the contract has been awarded pursuant to West Virginia Code of State Rules §148-1-6.3.d.

Segra has read and understands.

By signing below, I certify that I have reviewed this Request for Proposal in its entirety; understand the requirements, terms and conditions, and other information contained herein; that I am submitting this proposal for review and consideration; that I am authorized by the bidder to execute this bid or any documents related thereto on bidder's behalf; that I am authorized to bind the bidder in a contractual relationship; and that, to the best of my knowledge, the bidder has properly registered with any State agency that may require registration.

Lumos Networks, LLC d/b/a Segra
(Company)

Dan Watts,
Chief Operating Officer
(Representative Name, Title)

Contact Phone: (803) 888-3106 / Fax Number: N/A
(Contact Phone/Fax Number)

6/10/2022
(Date)

Revised 07/01/2021

Exhibit A: Pricing Page

Please refer to **Exhibit A - Pricing Page**, included in our **Cost Proposal** on page 8.

EXHIBIT A: Pricing Page **CRFP SWC2200000001**

Company Name

1) The quantities indicated below (Column B) are the best estimate of network inventory near the time of release.
2) If the inventory changed after data capture or was missed during the data capture, it does not change the evaluation.
3) The evaluation will be based on the quantities represented in this section. Vendors must provide costs for each Service, including $0 if applicable.
4) If there were not any current installations of a circuit type being requested under this RFP, it was represented with a quantity of 1 for evaluation purposes.
5) If a current circuit type was not being requested under this RFP, it was not included in this evaluation, but was left in the inventory for vendor reference regarding a potential installation site.
6) Column D is calculated by multiplying twelve (12) months by Column B and Column C.
7) Column F is calculated by multiplying Column B and Column E to show the total cost for Non-Recurring.
8) Column G is calculated by adding Column D and Column F to show the total cost for both Annual and Non-recurring costs.

A	B	C	D	E	F	G
Description of Service	**Qty**	**Monthly Recurring Cost (MRC) - Vendor Response**	**Annual Cost - -Calculated (12 * B * C)**	**Non-Recurring Cost (NRC) - Vendor Response**	**Total NRC - -Calculated (B * E)**	**Total Cost - - - - Calculated (D + F)**
Ethernet WAN Service 5Mbps	40					
Ethernet WAN Service 10Mbps	200					
Ethernet WAN Service 25Mbps	40					
Ethernet WAN Service 50Mbps	40					
Ethernet WAN Service 100Mbps	50					
Ethernet WAN Service 200Mbps	1					

Description of Service	Qty	Monthly Recurring Cost (MRC) - Vendor Response	Annual Cost - -Calculated (12 * B * C)	Non-Recurring Cost (NRC) - Vendor Response	Total NRC - -Calculated (B * E)	Total Cost - - - - Calculated (D + F)
Ethernet WAN Service 300Mbps	5					
Ethernet WAN Service 500Mbps	1					
Ethernet WAN Service 1Gbps	5					
Ethernet WAN Service 2Gbps	1					
Ethernet WAN Service 3Gbps	1					
Ethernet WAN Service 5Gbps	1					
Ethernet WAN Service 7Gbps	1					
Ethernet WAN Service 10Gbps	1					
Ethernet WAN Service 20Gbps	1					
Ethernet WAN Service 40Gbps	1					
Dedicated Internet Access 50Mbps	1					
Dedicated Internet Access 100Mbps	1					
Dedicated Internet Access 500Mbps	1					
Dedicated Internet Access 1Gbps	1					
Dedicated Internet Access 2Gbps	1					

Description of Service	Qty	Monthly Recurring Cost (MRC) - Vendor Response	Annual Cost - -Calculated (12 * B * C)	Non-Recurring Cost (NRC) - Vendor Response	Total NRC - -Calculated (B * E)	Total Cost - - - - Calculated (D + F)
Dedicated Internet Access 5Gbps	1					
Dedicated Internet Access 10Gbps	1					
Dedicated Internet Access 25Gbps	1					
Dedicated Internet Access 40Gbps	1					
4G/5G Wireless Service (*Unlimited Data, no data throttling*)	1					
Leased Router (5mbps Service)	1					
Leased Router (10mbps Service)	1					
Leased Router (25mbps Service)	1					
Leased Router (50mbps Service)	1					
Leased Router (100mbps Service)	1					
Leased Router (200mbps Service)	1					
Leased Router (300mbps Service)	1					
Leased Router (500mbps Service)	1					
Leased Router (1Gbps Service)	1					

Description of Service	Qty	Monthly Recurring Cost (MRC) - Vendor Response	Annual Cost - -Calculated (12 * B * C)	Non-Recurring Cost (NRC) - Vendor Response	Total NRC - -Calculated (B * E)	Total Cost - - - - Calculated (D + F)
Dedicated Internet Access 5Gbps	1					
Dedicated Internet Access 10Gbps	1					
Dedicated Internet Access 25Gbps	1					
Dedicated Internet Access 40Gbps	1					
4G/5G Wireless Service (*Unlimited Data, no data throttling*)	1					
Leased Router (5mbps Service)	1					
Leased Router (10mbps Service)	1					
Leased Router (25mbps Service)	1					
Leased Router (50mbps Service)	1					
Leased Router (100mbps Service)	1					
Leased Router (200mbps Service)	1					
Leased Router (300mbps Service)	1					
Leased Router (500mbps Service)	1					
Leased Router (1Gbps Service)	1					

Description of Service	Qty	Monthly Recurring Cost (MRC) - Vendor Response	Annual Cost - -Calculated (12 * B * C)	Non-Recurring Cost (NRC) - Vendor Response	Total NRC - -Calculated (B * E)	Total Cost ---- Calculated (D + F)
Leased Router (2Gbps Service)	1					
Leased Router (3Gbps Service)	1					
Leased Router (5Gbps Service)	1					
Leased Router (7Gbps Service)	1					
Leased Router (10Gbps Service)	1					
Leased Router (20Gbps Service)	1					
Leased Router (40Gbps Service)	1					
Managed Internet Service (50Mbps)	1					
Managed Internet Service (100Mbps)	1					
Managed Internet Service (500Mbps)	1					
Managed Internet Service (1Gbps)	1					
Managed Internet Service (2Gbps)	1					
Managed Internet Service (5Gbps)	1					
Managed Internet Service (10Gbps)	1					
Managed Internet Service (40Gbps)	1					

Description of Service	Qty	Monthly Recurring Cost (MRC) - Vendor Response	Annual Cost - -Calculated (12 * B * C)	Non-Recurring Cost (NRC) - Vendor Response	Total NRC - -Calculated (B * E)	Total Cost - - - - Calculated (D + F)
Total Annual Costs and Non-Recurring Costs						

Miscellaneous Costs and information

	Provided by		Hourly Rate	Estimate of Hours	Total Cost
	Vendor (Y or N)	Subcontractor (Y or N)			
Extension of Circuit demarcation				100	

	Cost per Circuit Expedited	Estimate of Requests	Total Cost
Expedite Charge		100	

Overall Cost Summary

Total Annual Costs and Non-Recurring Costs	
Extension of Circuit demarcation	
Expedite Charge	
Total Cost for Evaluation	

Exhibit B: Site List

Segra has read, understands, and will comply.

EXHIBIT B - List of Sites

Street Address	Speed in MBPS
1 DEPOT ST, ROMNEY, WV 26757	10
1 DOT DR, MOUNDSVILLE, WV 26041	100
1 FREEDOMS WAY, CLARKSBURG, WV 26301	100
1 LOIS LN, GREENWOOD, WV 26415	50
1 LORY PL, ,JULIAN, WV 25529	20
1 MOUNTAINSIDE WAY, MOUNT OLIVE, WV 25185	100
1 O HANLAN PL, BARBOURSVILLE, WV 25504	10
1 O HANLAN PL, BARBOURSVILLE, WV 25504	50
1 PLAYERS CLUB DR, CHARLESTON, WV 25311	10
1 W VIRGINIA 97, MULLENS, WV 25882	10
1 WALDEN ROUSH WAY, POINT PLEASANT, WV 25550	10
10 MCJUNKIN RD, NITRO, WV 25143	300
100 COURT ST N, RIPLEY, WV 25271	20
100 DEE DR, CHARLESTON, WV 25311	100
100 MARKET PLACE MALL, WESTON, WV 26452	10
100 MUNICIPAL PLZ, WEIRTON, WV 26062	10
100 THORN CREEK RD, FRANKLIN, WV 26807	10
1000 CHAPLINE ST, WHEELING, WV 26003	20
1000 CONFERENCE CENTER DR, LOGAN, WV 25601	10
1001 ARMY RD, KINGWOOD, WV 26537	100
1001 CENTRE WAY, CHARLESTON, WV 25309	50
101 BEECH ST, GRAFTON, WV 26354	10
1012 KANAWHA BLVD E, CHARLESTON, WV 25301	10
1014 S RALEIGH ST, MARTINSBURG, WV 25401	20
1018 KANAWHA BLVD E, CHARLESTON, WV 25301	10
1019 PICKENS RD, PICKENS, WV 26230	5
102 3RD ST, LOGAN, WV 25601	10
102 N MAIN ST, KEYSER, WV 26726	10
1020 BROAD ST, SUMMERSVILLE, WV 26651	3
1023 N RANDOLPH AVE, ELKINS, WV 26241	10
1025 MAIN ST, WHEELING, WV 26003	10
1025 N RANDOLPH AVE, ELKINS, WV 26241	10
1027 N RANDOLPH AVE, ELKINS, WV 26241	50
1029 N RANDOLPH AVE, ELKINS, WV 26241	10
103 ACADEMY DR, GLENVILLE, WV 26351	50
103 E MAIN ST, BRIDGEPORT, WV 26330	10
105 S EISENHOWER DR, BECKLEY, WV 25801	100
105 S RAILROAD ST, PHILIPPI, WV 26416	10
106 MARTIN DR, MOUNT HOPE, WV 25880	20
106 SAND MINE RD, BERKELEY SPRINGS, WV 25411	10
106B DEER VIEW DR, CHARLESTON, WV 25312	10
107 CAPITOL ST, CHARLESTON, WV 25301	100
107 DAVIS ST, ELKINS, WV 26241	10
107 E 4TH AVE, RANSON, WV 25438	10
107 PINECREST DR, BECKLEY, WV 25801	10
108 BACK VALLEY RD, LINDSIDE, WV 24951	10
108 LEE ST E, CHARLESTON, WV 25301	10
1081 COUNTRY CLUB RD, FAIRMONT, WV 26554	10
109 HCC BLVD, HUTTONSVILLE, WV 26273	100
109 TAVERN RD, MARTINSBURG, WV 25401	10
11 COMMERCE DR, WESTOVER, WV 26501	10

Street Address	Speed in MBPS
110 N MAIN ST, WEBSTER SPRINGS, WV 26288	20
110 N MAIN ST ,WEBSTER SPRINGS, WV 26288	10
110 PARK AVE, WELCH, WV 24801	10
110 STOCKTON ST, CHARLESTON, WV 25387	10
1101 GEORGE KOSTAS DR, LOGAN, WV 25601	300
1101 N RANDOLPH AVE, ELKINS, WV 26241	100
1106 RAILROAD ST, FARMINGTON, WV 26571	10
111 S EISENHOWER DR, BECKLEY, WV 25801	50
1110 RAILROAD ST, FARMINGTON, WV 26571	10
1116 SMITH ST ,CHARLESTON, WV 25301	10
112 NORTHERN REG CORRECTIONAL DR	50
1124 SMITH ST, CHARLESTON, WV 25301	500
11264 OHIO RIVER RD, WEST COLUMBIA, WV 25287	100
113 RANDOLPH ST, BECKLEY, WV 25801	5
1139 I 70 W, WHEELING, WV 26003	3
114 GRACE ST, DELBARTON, WV 25670	10
114 S HIGH ST, MORGANTOWN, WV 26501	10
115 AIKENS CTR, MARTINSBURG, WV 25404	10
115 CHURCH ST, SPENCER, WV 25276	10
11522 OHIO RIVER RD, WEST COLUMBIA, WV 25287	100
1159 NICK RAHALL GREENWAY, FAYETTEVILLE, WV	300
116 LIBERTY SQ, HURRICANE, WV 25526	10
1163 WILDLIFE RD, POINT PLEASANT, WV 25550	10
117 COURT ST N, RIPLEY, WV 25271	10
118 ADAMS ST, FAIRMONT, WV 26554	20
1186 N MILDRED ST, RANSON, WV 25438	10
119 RAILCROSS RD, CLARKSBURG, WV 26301	10
11923 CHARLESTON RD, RED HOUSE, WV 25168	5
120 WATER PLANT DR, MOOREFIELD, WV 26836	10
1200 AIRPORT RD, BEAVER, WV 25813	10
1200 HARRISON AVE, ELKINS, WV 26241	10
1201 DUNBAR AVE, DUNBAR, WV 25064	10
1201 GREENBRIER ST, CHARLESTON, WV 25311	100
1207 QUARRIER ST, CHARLESTON, WV 25301	20
1236 N STATE ROUTE 2, NEW MARTINSVILLE, WV 26155	20
1236 N STATE ROUTE 2, NEW MARTINSVILLE, WV 26155	50
124 COURT ST, ELIZABETH, WV 26143	20
124 MCGRAW ST, RIPLEY, WV 25271	10
1240 PAUL E MALONE RD, GRAFTON, WV 26354	10
1249 PRICHARD RD, PRICHARD, WV 25555	3
125 W MAIN ST, HARRISVILLE, WV 26362	10
12531 WINFIELD RD ,WINFIELD, WV 25213	20
1255 DYER HILL RD, SUTTON, WV 26601	50
1275 WARWOOD AVE, WHEELING, WV 26003	10
130 ACADEMY DR, DUNBAR, WV 25064	5
130 STRATTON ST, LOGAN, WV 25601	100
1300 GASTON CAPERTON DR, HOLDEN, WV 25625	50
1301 34TH ST, VIENNA, WV 26105	10
1301 OLD LEETOWN PIKE, KEARNEYSVILLE, WV 25430	10
131 HIGHLAND DR, WESTON, WV 26452	100
1317 HANSFORD ST, CHARLESTON, WV 25301	10
131A PENINSULA ST, WHEELING, WV 26003	50
1321 PLAZA E, CHARLESTON, WV 25301	100

Street Address	Speed in MBPS
1324 CHAPLINE ST, WHEELING, WV 26003	10
1325 COOK PKWY, OCEANA, WV 24870	10
13285 MOUNTAINEER DR, RIVERTON, WV 26814	5
1339 PLAZA E, CHARLESTON, WV 25301	10
1343 N PRESTON HWY ,KINGWOOD, WV 26537	10
1356 HANSFORD ST, CHARLESTON, WV 25301	50
137 PEACH CT, DANVILLE, WV 25053	10
1385 LOCUST AVE, FAIRMONT, WV 26554	10
14 COMMERCE DR, WESTOVER, WV 26501	50
140 SCHOOL ST, OAK HILL, WV 25901	5
1400 12TH ST, VIENNA, WV 26105	10
1400 VIRGINIA ST, OAK HILL, WV 25901	50
1406 KANAWHA ST ,POINT PLEASANT, WV 25550	10
1408 KANAWHA ST, POINT PLEASANT, WV 25550	10
141 FORESTRY CAMP RD, DAVIS, WV 26260	20
1411 N WALKER ST, PRINCETON, WV 24740	10
14115 N PRESTON HWY, BRUCETON MILLS, WV 26525	5
1415 EARL L CORE RD, MORGANTOWN, WV 26505	10
1439 MANSFIELD DR, PHILIPPI, WV 26416	5
144 JERRY LN, AUGUSTA, WV 26704	20
145 PILGRIM ST, INWOOD, WV 25428	10
146 STONEHOUSE RD, LEWISBURG, WV 24901	100
1471 WV HIGHWAY 5 E, GLENVILLE, WV 26351	10
148 MAPLEWOOD AVE, LEWISBURG, WV 24901	10
149 ROBERT C BYRD INDUSTRIAL PARK, MOOREFIELD,	10
1493 WV HIGHWAY 5 E, GLENVILLE, WV 26351	10
150 HOPEMONT DR, TERRA ALTA, WV 26764	20
150 ROBERT C. BYRD INDUSTRIAL PARK, MOOREFIELD,	10
1501 EOFF ST, WHEELING, WV 26003	50
151 ROBERT C BYRD INDUSTRIAL PARK, MOOREFIELD,	10
1513 HARRISON AVE, ELKINS, WV 26241	10
1520 WINCHESTER AVE, MARTINSBURG, WV 25405	10
1525 DECKERS CREEK BLVD, MORGANTOWN, WV 26505	10
153 W MAIN ST, CLARKSBURG, WV 26301	20
1530 NORWAY AVE, HUNTINGTON, WV 25705	100
156 RESOURCE LN, FOSTER, WV 25081	50
159 DAVIS ST, PRINCETON, WV 24739	10
15933 APPALACHIAN HWY, THOMAS, WV 26292	5
1600 HARPER RD, BECKLEY, WV 25801	10
162 ARKWRIGHT AVE, MORGANTOWN, WV 26505	1000
163 WILDLIFE RD, FRENCH CREEK, WV 26218	10
1655 S PLEASANTS HWY, SAINT MARYS, WV 26170	10
166 DOH LN, BERKELEY SPRINGS, WV 25411	10
167 11TH AVE, SOUTH CHARLESTON, WV 25303	100
16964 CACAPON RD, GREAT CACAPON, WV 25422	3
17 MCDOWELL ST, WELCH, WV 24801	10
1700 MACCORKLE AVE SE, CHARLESTON, WV 25314	50
1701 5TH AVE, CHARLESTON, WV 25387	20
1703 COONSKIN DR, CHARLESTON, WV 25311	20
1740 UNION CARBIDE DR, SOUTH CHARLESTON, WV	20
1767 BEARHOLE RD, PINEVILLE, WV 24874	20
18 N TORNADO WAY, KEYSER, WV 26726	10
180 ASSOCIATION DR, CHARLESTON, WV 25311	10

Street Address	Speed in MBPS
1822 MAIN ST E, OAK HILL, WV 25901	10
1824 MURDOCH AVE, PARKERSBURG, WV 26101	10
18351 VETERANS MEMORIAL HWY, KINGWOOD, WV	10
186 HOSPITAL DR, GRANTSVILLE, WV 26147	10
1867 ROCK CLIFF DR, MARTINSBURG, WV 25401	10
19 CIRCLE DR, LOGAN, WV 25601	3
19 PUTNAM VILLAGE DR, HURRICANE, WV 25526	10
1900 KANAWHA BLVD E, CHARLESTON, WV 25305	100
1900 KANAWHA BLVD E, CHARLESTON, WV 25305	100
1900 KANAWHA BLVD E, CHARLESTON, WV 25305	100
1900 KANAWHA BLVD E, CHARLESTON, WV 25305	1000
1900 KANAWHA BLVD E, CHARLESTON, WV 25305	100
1900 KANAWHA BLVD E, CHARLESTON, WV 25305	5000
1900 KANAWHA BLVD E, CHARLESTON, WV 25305	100
192 INDUSTRIAL PARK LN, BEECH BOTTOM, WV 26030	10
1948 WILTSHIRE RD, KEARNEYSVILLE, WV 25430	10
195 DAVIS ST, PRINCETON, WV 24739	10
195 DAVIS ST, PRINCETON, WV 24739	10
196 N TORNADO WAY, KEYSER, WV 26726	10
198 DAVIS ST, PRINCETON, WV 24739	10
1993 SMITHTON RD, WEST UNION, WV 26456	10
2 ARMORY WAY, SUMMERSVILLE, WV 26651	10
2 BROWN AVE, WESTON, WV 26452	10
2 O HANLAN PL, BARBOURSVILLE, WV 25504	20
200 ARLINGTON ST, CHELSEA, MA 02150-2375	500
200 DAVIS ST, PRINCETON, WV 24739	20
200 MAIN ST, SPENCER, WV 25276	10
200 N COURT ST, LEWISBURG, WV 24901	10
200 NEW RIVER TOWN CTR, BECKLEY, WV 25801	10
200 S VIKING WAY, MARTINSBURG, WV 25401	10
200 SAMARITAN DR, SHADY SPRING, WV 25918	10
200 STATE ST, MADISON, WV 25130	100
200 W MAIN ST, CLARKSBURG, WV 26301	10
2006 ROBERT C BYRD DR, BECKLEY, WV 25801	10
2006 TRAP SPRINGS RD, GRAFTON, WV 26354	50
2020 UNION CARBIDE DR, SOUTH CHARLESTON, WV	1000
203 DOH GARAGE RD, DANVILLE, WV 25053	10
203 E 3RD AVE, WILLIAMSON, WV 25661	10
203 KENOVA AVE, WAYNE, WV 25570	20
2031 PLEASANT VALLEY RD, FAIRMONT, WV 26554	50
206 SENIOR LN, PARSONS, WV 26287	10
209 MARION SQ, FAIRMONT, WV 26554	10
210 BROOKS ST, CHARLESTON, WV 25301	10
210 MAIN ST, MIDDLEBOURNE, WV 26149	10
211 6TH ST, PARKERSBURG, WV 26101	50
211 E 5TH AVE, RANSON, WV 25438	10
211 VALHALLA LN, MARLINTON, WV 24954	10
212 E MAIN ST, GLENVILLE, WV 26351	10
2120 NORTHWESTERN TPKE, BURLINGTON, WV 26710	100
213 KENMORE DR, DANVILLE, WV 25053	10
215 W MAIN ST, CLARKSBURG, WV 26301	10
22 HERBERT AVE, SMITHBURG, WV 26436	20
220 W MAIN ST, HARRISVILLE, WV 26362	10

Street Address	Speed in MBPS
222 PAYNE ST, HILLSBORO, WV 24946	50
222 S VIKING WAY, MARTINSBURG, WV 25401	10
22278 NORTHWESTERN PIKE, ROMNEY, WV 26757	10
22288 NORTHWESTERN PIKE, ROMNEY, WV 26757	10
22445 ALLEGHENY HWY, HARMAN, WV 26270	5
225 E 3RD AVE, WILLIAMSON, WV 25661	10
225 HOLIDAY HILLS DR, PARKERSBURG, WV 26104	50
2266 PENNSYLVANIA AVE, CHARLESTON, WV 25302	5
229 E MARTIN ST, MARTINSBURG, WV 25401	10
23 HOSPITAL DR, PETERSBURG, WV 26847	10
23 WABASH AVE, PHILIPPI, WV 26416	10
230 HEAVNER AVE, ELKINS, WV 26241	10
231 CAPITOL ST, CHARLESTON, WV 25301	10
2310 KANAWHA BLVD E, CHARLESTON, WV 25311	100
2311 OHIO AVE, PARKERSBURG, WV 26101	50
23236 GEORGE WASHINGTON HWY, AURORA, WV 26705	5
235 BARRETT ST, GRAFTON, WV 26354	10
239 COURT AVE, WESTON, WV 26452	10
239 WILLOW SPRING DR, CHARLES TOWN, WV 25414	10
24 RULAND RD, KEARNEYSVILLE, WV 25430	10
2403 FAIRLAWN AVE, DUNBAR, WV 25064	20
2403 FAIRLAWN AVE, DUNBAR, WV 25064	50
242 MAIN ST, CASS, WV 24927	10
245 POINT MOUNTAIN RD, VALLEY HEAD, WV 26294	5
2460 MURPHYS RUN RD, BRIDGEPORT, WV 26330	100
248 DUNHAM CUT RD, BELINGTON, WV 26250	5
24940 NORTHWESTERN PIKE, ROMNEY, WV 26757	10
24948 NORTHWESTERN PIKE, ROMNEY, WV 26757	10
24954 NORTHWESTERN PIKE, ROMNEY, WV 26757	10
25 BRUSH COUNTRY RD, MARLINTON, WV 24954	5
25 RED OAKS SHOPPING CTR ,RONCEVERTE, WV 24970	3
2507 9TH AVE, PARKERSBURG, WV 26101	10
255 DEPOT ST, WESTON, WV 26452	10
257 N STATE ROUTE 2, NEW MARTINSVILLE, WV 26155	10
2619 PENNSYLVANIA AVE, WEIRTON, WV 26062	10
26452 EAST LYNN RD, WAYNE, WV 25570	20
26452 EAST LYNN RD, WAYNE, WV 25570	50
269 AIKENS CTR, MARTINSBURG, WV 25404	202
269 CHARLESTON RD, SPENCER, WV 25276	5
2699 PARK AVE, HUNTINGTON, WV 25704	100
270 MYLAN PARK LN, MORGANTOWN, WV 26501	50
2700 CHARLES AVE, DUNBAR, WV 25064	10
2800 WASHINGTON ST W, CHARLESTON, WV 25387	5
2807 JACKSON AVE, POINT PLEASANT, WV 25550	10
2807 JACKSON AVE, PT PLEASANT, WV 25550	10
281 TUNNEL HILL RD, SALEM, WV 26425	5
284 FACTORY ST, CLARKSBURG, WV 26301	10
2850 5TH AVE, HUNTINGTON, WV 25702	10
286 BLUE PRINCE RD, BLUEFIELD, WV 24701	10
2880 N PLEASANTS HWY, SAINT MARYS, WV 26170	100
2935 COMMERCE ST, WELLSBURG, WV 26070	5
295 SKIDMORE LN, SUTTON, WV 26601	10
2959 US ROUTE 52, HANOVER, WV 26839	5

Street Address	Speed in MBPS
299 CONFEDERATE RD, FRANKLIN, WV 26807	10
300 CAPITOL ST, CHARLESTON, WV 25301	10
300 LAKEVIEW CTR, PARKERSBURG, WV 26101	100
300 TECHNOLOGY DR, SOUTH CHARLESTON, WV 25309	5
301 AMBROSE LN, PRINCETON, WV 24739	5
301 EAGLE MOUNTAIN RD, CHARLESTON, WV 25311	10
304 SCOTT AVE, MORGANTOWN, WV 26508	10
3100 16TH STREET RD, HUNTINGTON, WV 25701	10
312 3RD AVE, HINTON, WV 25951	10
313 ANTHONY CENTER RD, WHITE SULPHUR SPRINGS,	50
3134 AMMA RD, AMMA, WV 25005	5
314 FAYETTE PIKE, MONTGOMERY, WV 25136	100
315 N OHIO AVE, CLARKSBURG, WV 26301	3
316 HOWARD AVE, MULLENS, WV 25882	10
316 MAPLEWOOD AVE, LEWISBURG, WV 24901	50
32 RANDOLPH AVE, ELKINS, WV 26241	10
320 ADAMS ST, FAIRMONT, WV 26554	10
320 SUMMERS ST, HINTON, WV 25951	10
321 MARKET ST, SPENCER, WV 25276	10
322 70TH ST SE, CHARLESTON, WV 25304	3
3225 ROBERT C BYRD DR, BECKLEY, WV 25801	10
32353 VETERANS MEMORIAL HWY, TERRA ALTA, WV	5
324 4TH AVE, SOUTH CHARLESTON, WV 25303	100
326 CENTRAL AVE, WAYNE, WV 25570	5
3266 WINFIELD RD, WINFIELD, WV 25213	10
3293 JEFFERSON ST N, LEWISBURG, WV 24901	10
33 MOUNTAINHEART LN, MATHENY, WV 24860	10
33 SOUTHFORK PLAZA DR, BUCKHANNON, WV 26201	10
330 HARPER PARK DR, BECKLEY, WV 25801	20
330 RED OAKS SHOPPING CTR, RONCEVERTE, WV 24970	20
34 AUCTION LN, BUCKHANNON, WV 26201	20
34 STATE HL, CAPON BRIDGE, WV 26743	5
3405 WINFIELD RD, WINFIELD, WV 25213	10
350 CAPITOL ST, CHARLESTON, WV 25301	300
3549 MAIN ST, WEIRTON, WV 26062	10
355 DOLAN DR, AUGUSTA, WV 26704	20
3554 TEAYS VALLEY RD, HURRICANE, WV 25526	10
357 WALNUT ST, HAMLIN, WV 25523	10
357 WALNUT ST, HAMLIN, WV 25523	10
36 ALLENS FORK RD, SISSONVILLE, WV 25320	5
360 OLD ROUTE 73, BRUCETON MILLS, WV 26525	5
367 GUS R DOUGLASS LN, CHARLESTON, WV 25312	20
3708 SUTTON LN, SUTTON, WV 26601	50
3772 TEAYS VALLEY RD, HURRICANE, WV 25526	5
378 MAIN ST, GRANTSVILLE, WV 26147	10
38 GRAPEVINE RD, MARTINSBURG, WV 25405	50
38 SEVERNA PKWY MARTINSBURG, WV 25403	10
3870 NATIONAL RD, TRIADELPHIA, WV 26059	10
397 MID ATLANTIC PKWY, MARTINSBURG, WV 25404	50
40 14TH ST, WHEELING, WV 26003	10
40 COMMERCE DR, WESTOVER, WV 26501	50
400 5TH ST, PARKERSBURG, WV 26101	20
400 ABBEY RD, BELINGTON, WV 26250	50

Street Address	Speed in MBPS
400 TELETECH DR, MOUNDSVILLE, WV 26041	50
401 2ND ST, PARKERSBURG, WV 26101	10
401 GUFFEY ST, FAIRMONT, WV 26554	10
404 MAIN ST, POINT PLEASANT, WV 25550	10
405 CAPITOL ST, CHARLESTON, WV 25301	10
407 NEVILLE ST, BECKLEY, WV 25801	50
408 ALEXANDER ST, CEDAR GROVE, WV 25039	10
408 EB SAUNDERS WAY, CLARKSBURG, WV 26301	10
408 LEON SULLIVAN WAY, CHARLESTON, WV 25301	20
409 VIRGINIA ST E, CHARLESTON, WV 25301	100
409 WOOD MOUNTAIN RD, GLEN JEAN, WV 25846	10
410 S MAIN ST, MOOREFIELD, WV 26836	10
416 ADAMS ST, FAIRMONT, WV 26554	100
4188 WASHINGTON ST W, CHARLESTON, WV 25313	10
4190 WASHINGTON ST W, CHARLESTON, WV 25313	100
428 MAIN ST, LOGAN, WV 25601	10
4285 CEDAR LAKES DR, RIPLEY, WV 25271	10
430 S 2ND AVE, PADEN CITY, WV 26159	10
431 RUNNING RIGHT WAY, JULIAN, WV 25529	100
4319 DENMAR RD, HILLSBORO, WV 24946	50
433 MID ATLANTIC PKWY, MARTINSBURG, WV 25404	100
4476 TRIPLETT RIDGE RD, CLAY, WV 25043	50
4496 CEDAR LAKES DR, RIPLEY, WV 25271	10
45 18TH ST, WHEELING, WV 26003	10
450 S 1ST AVE, PADEN CITY, WV 26159	10
452 MAIN ST, CLAY, WV 25043	10
453 VAN VOORHIS RD, MORGANTOWN, WV 26505	50
454 MCDOWELL ST, WELCH, WV 24801	50
454 MCDOWELL ST, WELCH, WV 24801	100
467 MAIN ST, MADISON, WV 25130	10
47 SCHOOL ST, PHILIPPI, WV 26416	300
4701 MACCORKLE AVE SE, CHARLESTON, WV 25304	10
4720 BRENDA LN, CHARLESTON, WV 25312	100
4752 CHIMNEY DR, CHARLESTON, WV 25302	10
4757 POTOMAC HIGHLANDS TRL, GREEN BANK, WV	50
489 MID ATLANTIC PKWY, MARTINSBURG, WV 25404	10
49 HAWKS NEST PARK RD, ANSTED, WV 25812	10
49 MATTALIANO DR, PHILIPPI, WV 26416	10
493 MUD LICK RD, BUCKHANNON, WV 26201	10
4947 ELK GARDEN HWY, ELK GARDEN, WV 26717	5
4994 ELK RIVER RD S, ELKVIEW, WV 25071	10
4994 ELK RIVER RD S, ELKVIEW, WV 25071	50
50 COURT ST, WELCH, WV 24801	10
500 QUARRIER ST, CHARLESTON, WV 25301	10
500 SUMMERS ST, CHARLESTON, WV 25301	1000
500 TELETECH DR, MOUNDSVILLE, WV 26041	10
5000 GREENBAG RD, MORGANTOWN, WV 26501	10
502 EAGLE MOUNTAIN RD, CHARLESTON, WV 25311	10
505 CAPITOL ST, CHARLESTON, WV 25301	10
512 WATER ST, BARBOURSVILLE, WV 25504	10
515 CENTRAL AVE, CHARLESTON, WV 25302	10
5187 US ROUTE 60, HUNTINGTON, WV 25705	10
5205 HUSKY HWY, MANNINGTON, WV 26582	5

Street Address	Speed in MBPS
5206 GAULEY TPKE ,HEATERS, WV 26627	5
53 KIESS DR, PETERSBURG, WV 26847	10
532 PENNSYLVANIA AVE, FAIRMONT, WV 26554	10
535 NORTH ST, UNION, WV 24983	10
537 ENTERPRISE DR, GASSAWAY, WV 26624	10
540 N JEFFERSON ST, LEWISBURG, WV 24901	10
541 HARLEY O STAGGERS DR, KEYSER, WV 26726	10
549 MALL RD, OAK HILL, WV 25901	10
550 INDUSTRIAL DR, OAK HILL, WV 25901	10
56 DOH DR, ROMNEY, WV 26757	10
56 PICKENS GRADE RD ,HACKER VALLEY, WV 26222	5
5707 MACCORKLE AVE SE, CHARLESTON, WV 25304	300
5900 GUYAN RIVER RD, BARBOURSVILLE, WV 25504	10
60 MANFRED HOLLAND WAY ,DUNBAR, WV 25064	20
60 PENNSYLVANIA ST, WEST UNION, WV 26456	10
600 7TH ST, MOUNDSVILLE, WV 26041	1000
600 CHURCH ST S, RIPLEY, WV 25271	10
605 CHERRY ST, SAINT MARYS, WV 26170	10
60B MOOREFIELD INDUSTRIAL PARK ,MOOREFIELD, WV	20
611 7TH AVE, HUNTINGTON, WV 25701	10
619 VIRGINIA ST W, CHARLESTON, WV 25302	100
62 REGAL CT, BERKELEY SPRINGS, WV 25411	10
6200 US ROUTE 60 E, BARBOURSVILLE, WV 25504	5
624 DEPOT ST, PARKERSBURG, WV 26101	100
627 LUBECK AVE, PARKERSBURG, WV 26101	10
6402 WEBSTER RD, COWEN, WV 26206	5
641 N STATE ROUTE 2, NEW MARTINSVILLE, WV 26155	5
67 N TORNADO WAY, KEYSER, WV 26726	10
677 RIPLEY RD, SPENCER, WV 25276	10
69 16TH ST, WHEELING, WV 26003	20
7 INDUSTRIAL BLVD, INDUSTRIAL, WV 26426	50
7 PLAYERS CLUB DR, CHARLESTON, WV 25311	100
701 22ND ST, POINT PLEASANT, WV 25550	10
703 7TH AVE, HUNTINGTON, WV 25701	20
707 PROFESSIONAL PARK DR, SUMMERSVILLE, WV	50
71 WAYNE ST, FORT GAY, WV 25514	10
712 N MAIN ST, MOOREFIELD, WV 26836	10
714 WELLS ST, SISTERSVILLE, WV 26175	10
731 ELLENBORO RD, HARRISVILLE, WV 26362	5
738 WARD RD, ELKINS, WV 26241	10
738 WARD RD, ELKINS, WV 26241	10
750 5TH AVE, HUNTINGTON, WV 25701	10
7619 S CALHOUN HWY, MILLSTONE, WV 25261	5
765 JEFFERSON ST S, LEWISBURG, WV 24901	10
768 BRUSHY FORK RD, BUCKHANNON, WV 26201	10
795 VIRGINIA AVE, WELCH, WV 24801	50
80 N MAIN ST, WEBSTER SPRINGS, WV 26288	10
800 NEW RIVER TOWN CTR, BECKLEY, WV 25801	10
801 MADISON AVE, HUNTINGTON, WV 25704	100
8051 BLOOMERY PIKE, SLANESVILLE, WV 25444	3
808 B ST, SAINT ALBANS, WV 25177	10
812 QUARRIER ST, CHARLESTON, WV 25301	100
8174 OLD LOGAN RD, CHAPMANVILLE, WV 25508	10

Street Address	Speed in MBPS
818 CACAPON LODGE DR, BERKELEY SPGS, WV 25411	10
819 3RD AVE, MARLINTON, WV 24954	10
82 EMERGENCY DR, NEW CUMBERLAND, WV 26047	10
82 FFA DR, RIPLEY, WV 25271	50
8209 COURT AVE, HAMLIN, WV 25523	10
83 BRUSHY FORK RD, BUCKHANNON, WV 26201	100
830 NORTHSIDE DR, SUMMERSVILLE, WV 26651	10
830 VIRGINIA AVE, WELCH, WV 24801	10
836 LUNICE CREEK HWY, PETERSBURG, WV 26847	10
837 CHESTNUT RIDGE RD, MORGANTOWN, WV 26505	1000
8388 MARSHALL HWY, RAYSAL, WV 24879	3
840 VIRGINIA AVE, WELCH, WV 24801	10
843 SHELTER RD, PRINCETON, WV 24739	20
848 NORTHSIDE DR, SUMMERSVILLE, WV 26651	10
85 INDUSTRIAL DR, GRANTSVILLE, WV 26147	20
851 N STREETCAR WAY, MOUNT CLARE, WV 26408	5
852 NORTHSIDE DR, SUMMERSVILLE, WV 26651	10
8581 UNION HWY, MOUNT STORM, WV 26739	5
875 SWEET SPRINGS VLY RD, UNION, WV 24983	5
878 E MAIN ST, MILTON, WV 25541	20
88 SENIOR SQ, ELIZABETH, WV 26143	10
888 BURNSVILLE RD, BURNSVILLE, WV 26335	5
89 RICHARD D MINNICH DR, SUTTON, WV 26601	100
89 RICHARD D MINNICH DR, SUTTON, WV 26601	1000
900 EMMETT ROUSCH DR, MARTINSBURG, WV 25401	20
900 PENNSYLVANIA AVE, CHARLESTON, WV 25302	300
901 8TH ST, MOUNDSVILLE, WV 26041	10
901 SHELTER RD, PRINCETON, WV 24739	10
904 OLD FRAME RD, ELKVIEW, WV 25071	5
907 MISSION DR, PARKERSBURG, WV 26101	20
908 BULLITT ST, CHARLESTON, WV 25301	100
91 ARNOLD RD, WESTON, WV 26452	10
92 MCDOWELL ST, WELCH, WV 24801	10
9209 SENECA TRL, PARSONS, WV 26287	10
9288 COAL RIVER RD, SETH, WV 25181	5
9346 SENECA TRL, PARSONS, WV 26287	20
936 SHARPE HOSPITAL RD, WESTON, WV 26452	100
937 US HIGHWAY 19 S, WESTON, WV 26452	10
9390 RIVER RD, MULLENS, WV 25882	5
94 GRAPEVINE RD, MARTINSBURG, WV 25405	10
94 MAIN ST, CLAY, WV 25043	20
9407 SENECA TRL, MILL CREEK, WV 26280	5
95 GOSHEN RD, MORGANTOWN, WV 26508	5
956 YATES AVE, GRAFTON, WV 26354	3
980 ALTMAN AVE, PARKERSBURG, WV 26104	100

SEGRA

RFP Addendum #1 and Acknowledgement

Department of Administration
Purchasing Division
2019 Washington Street East
Post Office Box 50130
Charleston, WV 25305-0130

State of West Virginia
Centralized Request for Proposals
Info Technology

Folder: 1034853

Doc Description: Addendum #1 - Statewide Contract for Data Transport Services

Proc Type: Statewide MA (Open End)

Reason for Modification:

Addendum #1 is issued to change the bid opening date, attach vendor Q&A's, attach the Pre-Bid Sign-I..... See Page 2 for complete info

Date Issued	Solicitation Closes	Solicitation No	Version
2022-06-02	2022-06-16 13:30	CRFP 0212 SWC2200000001	2

BID RECEIVING LOCATION

BID CLERK
DEPARTMENT OF ADMINISTRATION
PURCHASING DIVISION
2019 WASHINGTON ST E
CHARLESTON WV 25305
US

VENDOR

Vendor Customer Code:

Vendor Name : Lumos Networks, LLC dba Segra

Address : 1200

Street : Greenbrier St

City : Charleston

State : WV **Country :** USA **Zip :** 25311

Principal Contact : Greg Florence

Vendor Contact Phone: 304-414-0411 **Extension:** NA

FOR INFORMATION CONTACT THE BUYER
Jessica L Hovanec
304-558-2314
jessica.l.hovanec@wv.gov

Vendor Signature X **FEIN#** 84-1452950 **DATE** 6/10/22

All offers subject to all terms and conditions contained in this solicitation

Reason for Modification:
Addendum #1 is issued to change the bid opening date, attach vendor Q&A's, attach the Pre-Bid Sign-In Sheet, and to attach a revised pricing page.

ADDITIONAL INFORMATION

Addendum #1 is issued to change the bid opening date, attach vendor Q&A's, attach the Pre-Bid Sign-In Sheet, and to attach a revised pricing page.

Bid Opening date changes from 06/09/2022 to 06/16/2022. Bid Opening time remains the same at 1:30 PM ET.

The West Virginia Purchasing Division is soliciting responses on behalf of the West Virginia Office of Technology (WVOT) to obtain Wide Area Network (WAN) services that will be utilized by the WVOT and other Statewide agencies, per the specifications and terms and conditions as attached hereto.

Mandatory Pre-Bid Meeting to be held on May 18, 2022 at 1:30 PM in the Executive Room at Building 7, WV Capitol Complex State Training Center, 1900 Kanawha Blvd E, Charleston, WV 25305

****ONLINE SUBMISSIONS FOR THIS REQUEST FOR PROPOSAL (RFP) ARE PROHIBITED****

****ADDITIONALLY, the Vendor should clearly separate and identify the cost proposal from the technical proposal in a separately sealed envelope.

INVOICE TO	SHIP TO
ALL STATE AGENCIES VARIOUS LOCATIONS AS INDICATED BY ORDER No City WV 99999 US	STATE OF WEST VIRGINIA VARIOUS LOCATIONS AS INDICATED BY ORDER No City WV 99999 US

Line	Comm Ln Desc	Qty	Unit of Measure	Unit Price	Total Price
1	Telecom/Data Transport Services - See Pricing Page	1.00000	EA		

Comm Code	Manufacturer	Specification	Model #
81161700			

Extended Description:
Telecom/Data Transport Services - See Pricing Page

SCHEDULE OF EVENTS

Line	Event	Event Date
1	Mandatory Pre-Bid Meeting on May 18, 2022 at 1:30 PM EDT	2022-05-18
2	Technical Questions due by May 25, 2022 at 10:00 AM EDT	2022-05-25

ADDITIONAL TERMS AND CONDITIONS

See attached document(s) for additional Terms and Conditions

SOLICITATION NUMBER: CRFP SWC2200000001
Addendum Number: 1

The purpose of this addendum is to modify the solicitation identified as CRFP SWC2200000001 ("Solicitation") to reflect the change(s) identified and described below.

Applicable Addendum Category:

[X] Modify bid opening date and time

[X] Modify specifications of product or service being sought

[X] Attachment of vendor questions and responses

[X] Attachment of pre-bid sign-in sheet

[ ] Correction of error

[ ] Other

Description of Modification to Solicitation:

1) To change the bid opening date from June 9, 2022 to June 16, 2022. Bid opening time of 1:30 PM ET remains the same.

2) To attach a revised Exhibit A - Pricing Page

3) To attach the Vendor Questions and Answers

4) To attach the Mandatory Pre-Bid Sign-In Sheet

Additional Documentation: Documentation related to this Addendum (if any) has been included herewith as Attachment A and is specifically incorporated herein by reference.

Terms and Conditions:

1. All provisions of the Solicitation and other addenda not modified herein shall remain in full force and effect.

2. Vendor should acknowledge receipt of all addenda issued for this Solicitation by completing an Addendum Acknowledgment, a copy of which is included herewith. Failure to acknowledge addenda may result in bid disqualification. The addendum acknowledgement should be submitted with the bid to expedite document processing.

ADDENDUM ACKNOWLEDGEMENT FORM
SOLICITATION NO.: CRFP SWC2200000001

Instructions: Please acknowledge receipt of all addenda issued with this solicitation by completing this addendum acknowledgment form. Check the box next to each addendum received and sign below. Failure to acknowledge addenda may result in bid disqualification.

Acknowledgment: I hereby acknowledge receipt of the following addenda and have made the necessary revisions to my proposal, plans and/or specification, etc.

Addendum Numbers Received:
(Check the box next to each addendum received)

[X]	Addendum No. 1	[ ]	Addendum No. 6
[ ]	Addendum No. 2	[ ]	Addendum No. 7
[ ]	Addendum No. 3	[ ]	Addendum No. 8
[ ]	Addendum No. 4	[ ]	Addendum No. 9
[ ]	Addendum No. 5	[ ]	Addendum No. 10

I understand that failure to confirm the receipt of addenda may be cause for rejection of this bid. I further understand that that any verbal representation made or assumed to be made during any oral discussion held between Vendor's representatives and any state personnel is not binding. Only the information issued in writing and added to the specifications by an official addendum is binding.

Lumos Networks, LLC d/b/a Segra
Company

Authorized Signature

6/10/2022
Date

NOTE: This addendum acknowledgement should be submitted with the bid to expedite document processing.

CRFP SWC2200000001, Addendum #1
Vendor Questions & Answers

Q1: 4.1.1.1 - Qualification and Experience Information. How will the State reach out to obtain references? Via email or phone call?
A1: The State may contact a reference by either method.

Q2: 4.1.1.1 - Qualification and Experience Information. Can you provide the name, telephone number and email address of the State personnel reaching out to references to ensure that customer reference is informed?
A 2: We are not at liberty to disclose that information at this time.

Q3: 4.3.1.1.1.2. The State desires that the Vendor provide Ethernet WAN services that utilize SD-WAN overlay services as defined in the Metro Ethernet Forum (MEF) 3.0 standards. https://www.mef.net/service-standards/overlay-services/sdwan/. Please describe your company's ability to meet this goal. Can the State fully define their SD-WAN requirements?
A3: Please provide your company's proposed SD-WAN solution. The state is interested in obtaining the most robust, reliable, secure and cost effective SD-WAN solution available.

Q4: 4.3.1.1.1.2. The State desires that the Vendor provide Ethernet WAN services that utilize SD-WAN overlay services as defined in the Metro Ethernet Forum (MEF) 3.0 standards. https://www.mef.net/service-standards/overlay-services/sdwan/. Please describe your company's ability to meet this goal. Does the State of WV want costing information included for SD-WAN at this time, or does the State of WV just want to know how the vendor would implement SD-WAN as an overlay service?
A4: The State does want SD-WAN pricing at this time and to understand how the vendor would implement SD-WAN as an overlay service.

Q5: If the State does want pricing included, will SD WAN be included at every site?
A5: The State may or may not install SD-WAN service at every site

Q6: If not at every site, can an additional line item be added to Exhibit A Pricing Page for SD-WAN sites?
A6: The State has revised the pricing sheet.

a. Vendors are now required to provide Ethernet WAN Service and SD-WAN enabled Ethernet WAN Service pricing as separate line items

Q7: Does the State of WV intend to install and manage the SD-WAN equipment, or is it to be installed and managed by the vendor?
A7: The SD-WAN equipment is to be installed and managed by the Vendor as part of their service

Q8: Also, does the State of WV have a preferred equipment vendor for SD-WAN hardware?
A8: The State does not have a preferred equipment vendor for SD-WAN hardware.

Q9: Is there a specific SD-WAN feature or capability that the state is interested in, for example: Application Aware Routing or Single pane-of-glass?
A9: The State does not have a specific SD-WAN feature or capability that it is interested in at this time.

Q10: 4.3.1.2.2. The State desires all sites listed in Appendix A be migrated to vendor Ethernet WAN service within 365 calendar days from contract effective date. The State reserves the right to reprioritize this list as necessary. Please describe your company's plan to accomplish these migrations. Please describe your company's ability to migrate all sites listed in Appendix A within 365 calendar days from contract effective date. Exhibit A is the Pricing Page. Is 4.3.1.2.2 intended to reference Exhibit B: Site List?
A10: No, Appendix A and Exhibit A are two different documents.

Q11: 4.3.1.4. Part 4: Security for WAN and DIA Services Is the State open to considering future security initiatives, such as Governance Risk and Compliance, Threat and Vulnerability, and SOC Services? If so, would the state provide details in the Q&A and provide line items in the Exhibit A pricing page?
A11: No

Q12: 4.3.1.4.1 The Vendor should support customer evaluation of security incidents and compliance verification evaluations, as deemed necessary by the customer. Can the State define the type of security incidents?
A12: Please refer to the following document for State definitions of security incidents.

a. Cyber Incident: http://www.wvlegislature.gov/wvcode/code.cfm?chap=5A&art=6C

Q13: Does the State want Endpoint Detection and Response (EDR) or Managed Detection and Response (MDR)? Is the State looking for a Secure Service Edge (SSE) platform to protect cloud data? Is the State looking for a deception solution to protect all company data? If the answer to any of these questions is yes, will the State provide details in the Q&A and provide a line item to Exhibit A pricing page?
A13: The State does not require EDR, MDR or SSE services as part of this contract except for Managed Internet Services found in section 4.3.2.3.22.2.

Q14: 4.3.1.4.1 The Vendor should support customer evaluations of security incident and compliance verification evaluation, as deemed necessary by the customer. What manner of support is the State looking for? Can you provide examples?
A14: Please refer to Section 30 of the General Terms and Conditions published with the RFP.

Q15: 4.3.2.1.1.1. The Vendor must provide Ethernet WAN services that will terminate into existing State network equipment. Can the State of WV provide a list of their existing network equipment that the vendor must connect to?
A15: The State will not provide a list. All WVOT managed network equipment is IEEE 802.3 standard routers and switches.

Q16: 4.3.2.1.1.6 The proposed WAN services must support the transport of existing applications and services currently being utilized by the State of West Virginia. The Vendor proposed solution must allow existing or future 3rd party applications and services (example: Google Cloud, AWS, Azure) to be accessed or to function in a robust, secure, and reliable manner from the vendors core network. Does the State of WV want costing information included for the secure connection to existing/future cloud service providers at this time, or does the State of WV just want to know how the vendor would provide these services?
A16: The State does not want costing information at this time, rather to ensure that secure connections to cloud hosted services can be provided if requested/required.

Q17: If the State does want pricing included, will this service be required at every site? If not at every site, can an additional line item be added to the Exhibit A Pricing Page?
A17: The State expects the vendor to detail their capabilities to securely connect to cloud hosted services.

Q18: Also, what is the expected total aggregate data usage expected for the secure data connections?
A18: The State does not know the expected total aggregate data usage.

Q19: 4.3.2.1.2.1. Vendor must provide dedicated DIA services purchased from the State demarcation point to the Internet backbone. Will the State be providing internet services for all State agencies?
A19: The State offers WAN and DIA as options for all agencies and at all locations.

Q20: 4.3.2.1.2.1. Vendor must provide dedicated DIA services purchased from the State demarcation point to the Internet backbone. Will the State be establishing a new Internet Hub separate from WVNET?
A20: The State does not plan to establish a new Internet Hub at this time. The State offers WAN and DIA as options for all agencies and at all locations.

Q21: 4.3.2.1.2.1. Vendor must provide dedicated DIA services purchased from the State demarcation point to the Internet backbone. Will the State have a main internet hub location for connectivity to the internet? If so, which site or sites will be designated as such?
A21: The State currently leverages WV-Net as their primary Internet provider. The State offers WAN and DIA as options for all agencies and at all locations, the DIA services will route traffic directly to the vendor provided Internet service without traversing the WAN.

Q22: 4.3.2.1.2.2.2. Denial of Service: Vendor must respond to Denial of Service attacks reported by State within 15 minutes of State opening a trouble ticket. Is the State requesting a DDOS security solution, and if so, will the State of WV add a line item to Exhibit A pricing page?
A22: No. However, the State expects that the service provider has an inherent DDOS response capabilities included as part of their Managed Internet Service offer.

Q23: 4.3.2.1.4.1. Vendor will be responsible for coordination of the installation and ongoing management of the 4G/5G wireless service. Is it the States desire to be able to install and manage the 4G/5G equipment similar to the Leased Router? Or, as a bundled service similar to Managed Internet? If not bundled, can the State provide a line item to Exhibit A pricing page?
A23: The State expects the vendor to install and maintain the 4G/5G equipment and service.
Q24: 4.3.2.3.3.8 Itemized Cost for Individual Billing Components and 4.3.2.3.3.10 Itemized Cost for Any Surcharges and Total Cost Exhibit A Pricing Page 'Description of Service' elements imply a bundled rate, which conflicts with the itemized requirements in sections 4.3.2.3.3.8 and 4.3.2.3.3.10. How does the State want to care for the individual billing components, including surcharges? Can the State clarify and revise Exhibit A Pricing Page if necessary.
A24: Rate on the Pricing Page will be a monthly rate. The invoice received from the Vendor must include the details requested.

Q25: 4.3.2.3.19.1.1. For each day beyond the forty-five (45) day installation intervals defined or agreed to above, where the new service is not installed within the installation timelines, liquidated damages of $500 per day will be assessed at the State's discretion. Will the State consider including a "Force Majeure" standard prior to considering any Liquidated Damages provision in the contract?
A25: Liquidated Damages will be assessed at the discretion of the State. The State cannot prematurely commit to assessing or not assessing the Liquidated Damages.

Q26: 4.3.2.3.22.2. Managed Internet Service - Does the State of WV plan to install and manage the router for the Managed Internet Service the same as indicated on the Leased Router?
A26: The Vendor is responsible for installation and management of the router in the Managed Internet Service

Q27: 4.3.2.4.2. The Vendor will be responsible for resolving all security vulnerabilities that may affect equipment or transmission services provided to the customer. Can the State fully define or explain what is included in all security vulnerabilities?
A27: As defined by OWASP, a vulnerability is a hole or a weakness in the application, which can be a design flaw or an implementation bug, that allows an attacker to cause harm to the stakeholders of an application.

Q28: Are you asking for a vulnerability assessment? If so, can you add a line item to Exhibit A pricing page. And, what outcomes are you looking for?
A28: The state is not looking for a vulnerability assessment

Q29: And, is this pertaining to the vendor's network and equipment, not the leased router that the State plans to manage?
A29: This pertains to all vulnerabilities residing on vendor managed systems, infrastructure, or equipment. This does not include the state-managed/leased router.

Q30: EXHIBIT B - List of Sites For address at 469 AIKENS CTR, MARTINSBURG, WV 25404, should the speed be listed as 20Mbps?
A30: Yes

Q31: Instructions to Vendors: Bid Opening - Can the State provide a 30 day extension from when answers to questions are released to vendors?
A31: The State is extending the bid response deadline to June 16th, 2022. 1:30 PM EST

Q32: 4.3.2.1.2.3 Will the government accept non-contiguous IP blocks smaller than a /24?
A32: Yes

Q33: 4.3.2.1.2.4 In the event that more than one circuit is required at a site to achieve a bandwidth requirement, does the state of West Virginia require diversity for all circuits at that site? If so, what level of diversity is required?
A33: No

Q34: 4.3.2.3.19.1.1 For installation intervals that may exceed the forty-five day requirement, would a emporary 4G/5G solution be acceptable?
A34: Yes, if it meets the bandwidth requirement of the service ordered and approved by the State in advance of installation.

Q35: 4.3.2.3.19.1 The telecommunications industry standard for fiber/ethernet circuit installation is 90-120 days. A 45-day interval will inadvertently favor the incumbent provider. Will the State of West Virginia consider changing the installation timeline to 90-120 days?
A35: No

Q36: 4.3.2.3.19.1.1 Will the State of West Virginia consider revising "liquidated damages of $500 per day will be assessed at the State's discretion" to "liquidated damages of $500 per day, not to exceed the monthly recurring charge of the circuit will be assessed at the State's discretion"? Given the aggressive installation timeline, it is possible the penalty for missing the delivery would exceed the actual cost of the service being ordered.
A36: No

Q37: 4.1 and Exhibit B: Site List In 4.1 the State indicates that there are approximately 1000 WAN circuits and services installed statewide but in Exhibit B there is address information for only 467 locations. Can the State provide the location information for the remaining sites or address the discrepancy?
A37: The list provided in Exhibit B are the circuits managed by WVOT. Many additional agencies across the state leverage the legacy WAN contract. Other state agencies may choose to utilize the new contract in the future.

Q38: 4.3.2.3.19.1 Will the State clarify if the 45 day requirement is based on calendar days or business days?
A38: Calendar

Q39: Section 3 Given the current supply chain shortage caused by COVID-19 and other forces majeure, such as geo-political and economic influences, would the state consider adding the following Force Majeure Clause to the General Terms and Conditions:

> FORCE MAJEURE. Neither party will be responsible to the other for any delay, failure in performance, loss or damage due to fire, explosion, power blackout, earthquake, volcanic action, cable cuts by third parties, flood, weather elements, strike, embargo, labor disputes, civil or military authority, war, acts of God, acts or omissions of carriers or suppliers, software bugs, viruses and the like, acts of regulatory or governmental agencies, or other causes beyond their reasonable control, except for the obligation to pay amounts due under this Agreement.

A39: Contract terms and conditions negotiations will commence when appropriate. Should any Vendor desire their terms to be incorporated, it must note so in its response.

Q40: Section 4.3.2.1.4 - Can unlimited data and no throttling be waived?
A40: No

Q41: What throughput is expected in 4G/5G
A41: The State recognizes that speed will vary based on location and whether it's 4/G or 5/G.

Q42: What is the current expenditure per site? is there a budget?
A42: No

Q43: Is the state requesting pricing options for Leased router and purchased router or just leased?
A43: Leased

Q44: Are all existing edge routers expected to be replaced?
A44: No

Q45: Pricing requested by the state appears to ask for a price per speed requirement. However, pricing per site varies per speed required. Because pricing varies per location can a tier pricing scheme be provided?
A45: No

Q46: Only paragraph 4.3.2.1.2.2.1 has availability SLA of 99.999% for DIA. Is this SLA expected on any other service such as Ethernet/4G/5G?
A46: The 99.999% SLA is applicable to DIA and Ethernet WAN services.

Q47: Only paragraph 4.3.2.1.2.2.4 has packet delivery SLA of 99.5% for DIA. Is this SLA expected on any other service such as Ethernet/4G/5G?
A47: The 99.5% packet delivery SLA is applicable to DIA and Ethernet WAN services.

Q48: Are other services such as Cable/Fiber/Microwave/Satellite acceptable considering that SDWAN solutions can help achieve high level SLA's with broadband services?
A48: The State has not defined nor required any specific WAN transport solution except for 4G/5G.

Q49: We would like to request an extension of the due date. We request that the due date be extended to 3 weeks after all questions have been answered.
A49: The State is extending the bid response deadline to June 16th 2022. 1:30 PM EST

Q50: Given transition takes up to 12 months from the date of award, can the base period be increased to 4 years instead of 3?
A50: No

Q51: Please provide an example for each of the provisions underlined in #2 below of what the state is intending with this clause?

> 36. INDEMNIFICATION: The Vendor agrees to indemnify, defend, and hold harmless the State and the Agency, their officers, and employees from and against: (1) Any claims or losses for services rendered by any subcontractor, person, or firm performing or supplying services, materials, or supplies in connection with the performance of the Contract; (2) Any claims or losses resulting to any person or entity injured or damaged by the Vendor, its officers, employees, or subcontractors by the publication, translation, reproduction, delivery, performance, use, or disposition of any data used under the Contract in a manner not authorized by the Contract, or by Federal or State statutes or regulations; and (3) Any failure of the Vendor, its officers, employees, or subcontractors to observe State and Federal laws including, but not limited to, labor and wage and hour laws.

A51: Term 36. INDEMNIFICATION, is withdrawn from this Solicitation.

Q52: Section 4.3, paragraph two states "Vendor should describe its approach and methodology to providing their services by addressing the mandatory requirements as well as the goals and objectives identified below." Can vendors write to the goals and objectives when responding to the mandatory requirements or is the State of West Virginia expecting vendors to provide point-by-point responses to 4.3.2 Mandatory Requirements and 4.3.1 Goals and Objectives?
A52: Please refer to Vendor Proposal, Section 5.

Q53: Would the State of WV entertain a 2 week extension to respond to this RFP?
A53: The State is extending the bid response deadline to June 16th 2022. 1:30 PM EST

Q54: What percentage of your network is served with broadband today?
A54: Unclear what the term "broadband" means in this question. The State OT manages approximately 250 ocations with DIA services today, and approximately 476 locations with dedicated WAN circuits.

Q55: What percentage is served with 4G/5G today?
A55: The State OT currently manages two locations with 4G/5G service.

Q56: Since fiber services are usually symmetrical, same bandwidth upstream & downstream, and broadband services are typically asymmetrical, different bandwidth upstream and downstream, how do you want providers to reflect that difference on the pricing sheet for dedicated internet access?
A56: Bandwidth speeds for DIA service may be asymmetrical, however, download speed must match the required speeds as detailed in RFP and on the pricing sheet.
Q57: Do you foresee the vendor completing demarc extensions on the Capitol campus (1900 Kanawha Blvd., E), or will the Office of Technology be using their own fiber/copper for these connections?
A57: Vendor is responsible for Dmarc extensions

Q58: In Exhibit B – List of Sites, can you please confirm the current connection speed for the following location? It looks like it should be either 200M or 20M (202M appears to be a type-o). **269 Aikens Ctr, Martinsburg, WV 25404**
A58: The correct speed is 20M

Q59: In Section 3: General Terms and Conditions, Section 8 Insurance – As it relates to Cyber Liability Insurance, the typical standard coverage is $1,000,000 per occurrence. Is the State of WV willing to accept $1,000,000 per occurrence in the area of Cyber Liability Insurance?
A59: No

Q60: In pricing Exhibit A: All the Description of Services or the fields are correct for Dedicated Internet Access (DIA); however, there are several fields *(pricing fields)* that are missing for the various components that make up the topology of WAN services. Specifically, the various components of SD-WAN as it relates to software revisions, throughput licenses, hardware prices, etc. Will the State consider adding these fields to the Exhibit A – Pricing Page?
A60: The proposed price should include all costs associated with providing the Ethernet WAN services.

Q61: Section 3, General Terms and Conditions, Paragraph 11. The section indicates "Vendor shall pay liquidated damages in the amount specified below **or** as described in the specifications". The State has chosen to mark both boxes thus creating two potential events of liquidated damages. The first event being under Box 1 as specified and the second being under Box 2 as contained in the Specifications (section 4.3.2.3.19.1.1). Each individual event has a liquidated damages amount of $500 per day. Both events can collectively result in total liquidated damages of $1,000 per day. Is it the intent of the State to have two liquidated damages events subjecting the vendor to the potential that both events shall apply?
A61: No, Liquidated Damages will be assessed at $500 per day. Circumstances that would warrant Liquidated Damages were outlined in the specifications.

Q62: With regard to Box 1, the first liquidated damages event, what is the definition of "Installation Deadlines" date?
A62: Installation deadline is the 45-day period the Vendor has to install services following five calendar days from the time the State submits an order.

Q63: Which party establishes the Installation Deadline date for a service?
A63: Installation deadline is the 45-day period the Vendor has to install services following five calendar days from the time the State submits an order.

Q64: Must the State and Vendor mutually agree upon the established Installation Deadline date?
A64: Installation deadline is the 45-day period the Vendor has to install services following five calendar days from the time the State submits an order.

Q65: Can the established Installation Deadline date be changed by the Vendor upon 2 days advanced notice to the State?
A65: No

Q66: Are there any events that the State would consider an acceptable reason for an Installation Deadline date being missed, such as, the result of an act of God (a flood), the result of workforce impacts from a pandemic, the result of supply chain shortages, the result of actions taken or failed to be taken by the State, the result of the Vendor not being granted timely access to the facility to complete the installation work?
A62: Circumstances will be evaluated on an individual basis

Q67: Will the State agree to provide notice to the Vendor advising when a liquidated damages event has been incurred as a result of a missed service Installation Deadline date and afford the vendor with a thirty (30) day period of time from such notice date to cure such event without incurring any liquidated damages charges for such event?
A67: No

Q68: In Section 4.3.2 Mandatory Requirements, 4.3.2.3 Part 3: Service and Support for WAN and DIA and 4G/5G Services, Section 4.3.2.3.19.1 states the installation timeline is 45 days where no "special construction" is required. "Special Construction" is a defined term in the agreement, however the State does not appear to utilize the defined term in this section (special construction, as opposed to Special Construction). Is it the State's intent to apply the meaning of the defined term Special Construction in this section?
A68: Yes

Q69: Are the 45 days established in this liquidated damages section measured in business days or calendar days?
A69: Calendar

Q70: Industry standard timeframes extended to businesses across the country as well as those located within the State of WV to install an ethernet fiber internet connection and/or configure and establish SD WAN services is approximately 90-120 business days where no Special Construction is required. Can the State please advise why it requires an installation timeline which is well less than half of the timeframe delivered by the general industry to all other customers?
A70: The State requires installation in 45 calendar days to ensure timely transition and functionality.

Q71: Is the State aware of any unique telecommunication infrastructure, telecommunication facilities, technical resources or field personnel that exist within its offices and facilities that would afford the Vendor the ability to complete an installation timeline in such an expedited manner for these services?
A71: Each site is unique; however, the aggressive deadline is required to ensure a timely transition and functionality.

Q72: Is the State willing to consider changing the installation timeline to follow normal industry standards of 90-120 business days?
A72: No

Q73: With the measurement of a timeline interval, such as an installation timeline, a start date has to be established to allow for the measurement of the period of time. What is the start date for the installation timeline of a service for the purpose of measuring the related period of time interval? How is the start date established and determined for a specific service installation?
A73: The 45 day period will begin five calendar days after the vendor receives TCR from the State for service.

Q74: Given that the liquidated damages contained in Section 4.3.2.3.19.1.1 are at the State's discretion, will the State agree to provide notice to the Vendor advising when it intends to exercise its discretion to charge liquidated damages as a result of a failed installation timeline for a service and afford the vendor with a thirty (30) day period of time from such notice date to cure such event without incurring any liquidated damages charges for such event?
A74: No

Q75: Under Section 4.3.1.2 Part 2: Vendor Ethernet WAN Services Migration Plan, sub section 4.3.1.2.2, the State indicates it desires all sites be migrated over to the new services being provided by the Vendor within 365 days from the contract effective. If this migration plan interval is the intent and desire of the State, would the two liquidated damages events identified in Question 1 above only begin to apply and be incurred by the Vendor after 365 days from the contract effective date?
A75: No, Liquidated Damages could be applied for any installation within the contract period.

Q76: Can the State please provide clarity as to how the three different timelines and their related dates, (1) the Missed Installation Deadline date in Section 11, (2) the installation timeline interval established in Section 4.3.2.3.19.1.1 and (3) the 365 calendar days migration plan timeline in Section 4.3.1.2.2, are to be managed and viewed collectively?
A76: All services are to be migrated within 365 calendar days of contract award. A site is expected to be installed within 45 calendar days of the State's order. Each day after 45 calendar days, liquidated damages may be assessed.

Q77: If the 365 calendar days migration plan timeline is successfully achieved, will that effectively and completely relieve the Vendor of any liquidated damages that may otherwise be incurred as a result of an installation deadline date or installation timeline interval which occurs prior to the end of the 365 calendar days migration plan timeline?
A77: No - Liquidated Damages can be assessed for any site installation throughout the life of the contract.

Q78: Will the State agree to begin the 365 calendar days migration plan timeline upon the establishment and completion of the Operations Plan (section 4.3.1.2.1) agreed upon by the State and the Vendor, which is desired to occur within 60 calendar days of the contract effective date?
A78: No

Q79: In the RFP, its stated that refurbished equipment will not be accepted. With the current shortages of microchips in the marketplace we are seeing growing delays in procuring new equipment. Will the State of WV accept certified refurbished equipment as a bridge or replacement equipment?
A79: No

Q80: In the RFP, its stated that refurbished equipment will not be accepted. With the current shortages of microchips in the marketplace we are seeing growing delays in procuring new equipment. Will the State of WV accept refurbished equipment with quicker SLA terms of replacement equipment?
A80: The requirement will remain unchanged.

Q81: In the RFP, its stated that circuits must be delivered in 45 days. Per industry standards, Dedicated Ethernet and Fiber can take 60-90 days, however Broadband takes 30-45 days to deliver. Can the state explain this time frame and if there are instances where this time frame can be extended without penalty.
A81: The State seeks services to be installed within 45 days where no special construction is necessary.

Q82: Please explain the number of sites where service is to be delivered. In the RFP, its mentioned that there are 1000+ but in the spreadsheet at the end of the RFP there are less than 500. Will all sites require equipment? Will we utilize existing equipment?
A82: Please see previous response regarding the discrepancy. The State is unsure how the Vendor is defining 'equipment' to answer this question accurately.

Q83: Please explain the preferred access for the WAN service. MPLS, DIA, Broadband, Wireless 5G/4G or a combination?
A83: The State has no preference on access type as long as the service meets the requirements defined in the RFP.

Q84: How does the State expect to utilize SDWAN for these services?
A84: SDWAN may be used for redundancy purposes and to direct specific subsets of traffic directly to the cloud rather than backhauling to a central location.

Q85: From our understanding of the RFP it seems that SD-WAN is a desired option. For our design we would like to offer the State of West Virginia an option of either a Managed Router or SD-WAN device. Is it alright to append the price sheet to allow for the two options for each speed defined for the State to consider?
A85: The Vendor must not append the price sheet. Doing so shall result in disqualification. The Vendor should provide the State with a solution that meets the State's goals outlined in the RFP.

Q86: Will this contract be available to other governmental bodies such as county & municipal governments?
A86: Other governmental bodies may choose to utilize the contract.

Q87: How do we reflect special construction charges for sites included in the RFP list, or other sites not included, that choose to utilize this contract, since there is no special construction column on the pricing sheet?
A87: Special construction pricing shall be determined on an as-needed basis and procured in the appropriate manner. The State reserves the right to accept or reject proposed special construction for any site when deemed unnecessary.

Q88: Can you elaborate on specifically what the vendor will need to manage/maintain in the current WAN infrastructure?
A88: The winning Vendor will not manage current WAN infrastructure.

Q89: You reference approximately 1000 WAN circuits and services statewide under existing contracts. This does not match the circuit quantities in the price list. Can you elaborate on what makes up the difference?
A89: The listing provided shows those sites for which the WVOT is responsible. Other entities have chosen to use the contract; however, the WVOT has no visibility into those sites. The discrepancy is those who have utilized the contract outside of the purview of the WVOT (i.e., educational entities, local governments, etc.).

EXHIBIT A - PRICING PAGE

The quantities indicated below (Column B) are the best estimate of network inventory near the time of release.
If the inventory changed after data capture or was missed during the data capture, it does not change the evaluation.
The evaluation will be based on the quantities represented in this section. Vendors must provide costs for each Service, including $0 if applicable.
If there were not any current installations of a circuit type being requested under this RFP, it was represented with a quantity of 1 for evaluation purposes.
If a current circuit type was not being requested under this RFP, it was not included in this evaluation,
but was left in the inventory for vendor reference regarding a potential installation site.
Column D is calculated by multiplying twelve (12) months by Column B and Column C.
Column F is calculated by multiplying Column B and Column E to show the total cost for Non-Recurring.
Column G is calculated by adding Column D and Column F to show the total cost for bothAnnual and Non-recurring costs.

A	B	C	D	E	F	G
Description of Service	Qty	Monthly Recurring Cost (MRC) - Vendor Response	Annual Cost - - Calculated (12 * B * C)	Non-Recurring Cost (NRC) - Vendor Response	Total NRC - - Calculated (B * E)	Total Cost - - - - Calculated (D + F)
Ethernet WAN Service 5Mbps	40					
Ethernet WAN Service 10Mbps	200					
Ethernet WAN Service 25Mbps	40					
Ethernet WAN Service 50Mbps	40					
Ethernet WAN Service 100Mbps	50					
Ethernet WAN Service 200Mbps	1					
Ethernet WAN Service 300Mbps	5					
Ethernet WAN Service 500Mbps	1					
Ethernet WAN Service 1Gbps	5					
Ethernet WAN Service 2Gbps	1					
Ethernet WAN Service 3Gbps	1					
Ethernet WAN Service 5Gbps	1					
Ethernet WAN Service 7Gbps	1					
Ethernet WAN Service 10Gbps	1					
Ethernet WAN Service 20Gbps	1					
Ethernet WAN Service 40Gbps	1					
SD-WAN enabled Ethernet WAN Service 5Mbps	5					
SD-WAN enabled Ethernet WAN Service 10Mbps	5					
SD-WAN enabled Ethernet WAN Service 25Mbps	5					
SD-WAN enabled Ethernet WAN Service 50Mbps	5					
SD-WAN enabled Ethernet WAN Service 100Mbps	5					
SD-WAN enabled Ethernet WAN Service 200Mbps	5					
SD-WAN enabled Ethernet WAN Service 300Mbps	5					
SD-WAN enabled Ethernet WAN Service 500Mbps	5					
SD-WAN enabled Ethernet WAN Service 1Gbps	5					
SD-WAN enabled Ethernet WAN Service 2Gbps	1					
SD-WAN enabled Ethernet WAN Service 3Gbps	1					
SD-WAN enabled Ethernet WAN Service 5Gbps	1					
SD-WAN enabled Ethernet WAN Service 7Gbps	1					
SD-WAN enabled Ethernet WAN Service 10Gbps	1					
SD-WAN enabled Ethernet WAN Service 20Gbps	1					
SD-WAN enabled Ethernet WAN Service 40Gbps	1					
Dedicated Internet Access 50Mbps	1					
Dedicated Internet Access 100Mbps	1					
Dedicated Internet Access 500Mbps	1					
Dedicated Internet Access 1Gbps	1					
Dedicated Internet Access 2Gbps	1					
Dedicated Internet Access 5Gbps	1					

Dedicated Internet Access 10Gbps	1					
Dedicated Internet Access 25Gbps	1					
Dedicated Internet Access 40Gbps	1					
4G/5G Wireless Service *(Unlimited Data, no data throttling)*	1					
Leased Router (5mbps Service)	1					
Leased Router (10mbps Service)	1					
Leased Router (25mbps Service)	1					
Leased Router (50mbps Service)	1					
Leased Router (100mbps Service)	1					
Leased Router (200mbps Service)	1					
Leased Router (300mbps Service)	1					
Leased Router (500mbps Service)	1					
Leased Router (1Gbps Service)	1					
Leased Router (2Gbps Service)	1					
Leased Router (3Gbps Service)	1					
Leased Router (5Gbps Service)	1					
Leased Router (7Gbps Service)	1					
Leased Router (10Gbps Service)	1					
Leased Router (20Gbps Service)	1					
Leased Router (40Gbps Service)	1					
Managed Internet Service (50Mbps)	1					
Managed Internet Service (100Mbps)	1					
Managed Internet Service (500Mbps)	1					
Managed Internet Service (1Gbps)	1					
Managed Internet Service (2Gbps)	1					
Managed Internet Service (5Gbps)	1					
Managed Internet Service (10Gbps)	1					
Managed Internet Service (40Gbps)	1					
Total Annual Costs and Non-Recurring Costs						

Miscellaneous Costs and information

	Provided by		Hourly Rate	Estimate of Hours	Total Cost
	Vendor (Y or N)	Subcontractor (Y or N)			
Extension of Circuit demarcation				100	

	Cost per Circuit Expedited	Estimate of Requests	Total Cost
Expedite Charge		100	

Overall Cost Summary

Total Annual Costs and Non-Recurring Costs	
Extension of Circuit demarcation	
Expedite Charge	
Total Cost for Evaluation	

Pre-Bid Sign-In Sheet

Solicitation Number: CRFP SWC22*01
Date of Pre-Bid Meeting: 05/18/2022
Location of Prebid Meeting: Executive Room, Bldg 7

Please Note:
Vendors must sign-in on this sheet to verify attendance at the Pre-Bid meeting.
Failure to legibly sign in may be grounds for declaring a vendor ineligible to bid.
For further verification, please also provide a business card if possible.

Firm Represented:*	Rep Name (Printed):	Firm Address:	Telephone #:	Fax #:	Email:
Verizon	Sandy Hawkins	4700 MacCorkle Ave SE Chas WV 25304	304 807-0207	304 356-3590 877 294-8612	sandra.k.hawkins@verizon.com
Verizon	Kevin Walker	4700 MACCORKLE AVE SE CHAS WV 25304	304 533-7227	304 356-3590	andrew.walker@verizon.com
MetTel	James Gwiazda	1090 Vermont Ave NW washington DC 20005	202-657-1977		jgwiazda@mettel.net
Frontier	Chad Stepp	1500 MacCorkle Ave SE Chas, WV 25396	304 410-5659		chad.stepp@ftr.com
Frontier	Rex Foster	1500 MacCorkle Ave Chas, WV 25396	304-834 0272		rex.foster@ftr.com
BCN	Julian Jacquez	130 whispering woods Charleston, WV 25304	304-612-3877		JJacquez@BCNTele.com

***One Vendor Per Representative** - No one individual is permitted to represent more than one vendor at the pre-bid meeting. Any individual that does attempt to represent two or more vendors will be required to select one vendor to which the individual's attendance will be attributed. The vendors not selected will be deemed to have not attended the pre-bid meeting unless another individual attended on their behalf.*

Pre-Bid Sign-In Sheet

Solicitation Number: CRFP SWC22*01
Date of Pre-Bid Meeting: 05/18/2022
Location of Prebid Meeting: Executive Room, Bldg 7

Please Note:
Vendors must sign-in on this sheet to verify attendance at the Pre-Bid meeting.
Failure to legibly sign in may be grounds for declaring a vendor ineligible to bid.
For further verification, please also provide a business card if possible.

Firm Represented:*	Rep Name (Printed):	Firm Address:	Telephone #:	Fax #:	Email:
SEGRA	ERIC JARRETT	1200 GREENBRIER ST CHAS WV	304-352-1166		eric.jarrett@segrawv.com
SEGRA	QASC FLORENCE	1200 GREENBRIER ST CHAS WV	304-414-0411		GREG.FLORENCE@SEGRA.COM
Zscaler	Chris Schmidt	1069 Elderberry Loop Delaware, OH 43015	(917) 856-5114		CSchmidt@zscaler.com
Segra	Randy Jones	1200 Greenbrier St Chas WV	304-720-2991		randy.jones@segra.com
BCN	Michael Ginsburg	130 Whispering Woods Charleston, WV	908-367 5969		Mginsburg@bcntele.com
Method1	Kent McMillion	328 Skyline Drive Charleston, WV 25302	304-720-6460		

***One Vendor Per Representative** - No one individual is permitted to represent more than one vendor at the pre-bid meeting. Any individual that does attempt to represent two or more vendors will be required to select one vendor to which the individual's attendance will be attributed. The vendors not selected will be deemed to have not attended the pre-bid meeting unless another individual attended on their behalf.*

Pre-Bid Sign-In Sheet

Solicitation Number: CRFP SWC22*01
Date of Pre-Bid Meeting: 05/18/2022
Location of Prebid Meeting: Executive Room, Bldg 7

Please Note:
Vendors must sign-in on this sheet to verify attendance at the Pre-Bid meeting.
Failure to legibly sign in may be grounds for declaring a vendor ineligible to bid.
For further verification, please also provide a business card if possible.

Firm Represented:*	Rep Name (Printed):	Firm Address:	Telephone #:	Fax #:	Email:
Advantage Touch Tone	Jonathan Knight	950 Kanawha, Charleston WV 25301	304-342-0726		JKnight@advantage.tech
Hughes Network Systems	Amir Dehdashty	11717 Exploration Ln Germantown, MD	202-251-6401		amir.dehdashty@hughes.com

***One Vendor Per Representative** - No one individual is permitted to represent more than one vendor at the pre-bid meeting. Any individual that does attempt to represent two or more vendors will be required to select one vendor to which the individual's attendance will be attributed. The vendors not selected will be deemed to have not attended the pre-bid meeting unless another individual attended on their behalf.*

SEGRA

Disclosure of Interested Parties to Contracts

West Virginia Ethics Commission

Disclosure of Interested Parties to Contracts

Pursuant to W. Va. *Code* § 6D-1-2, a state agency may not enter into a contract, or a series of related contracts, that has/have an actual or estimated value of $1 million or more until the business entity submits to the contracting state agency a Disclosure of Interested Parties to the applicable contract. In addition, the business entity awarded a contract is obligated to submit a supplemental Disclosure of Interested Parties reflecting any new or differing interested parties to the contract within 30 days following the completion or termination of the applicable contract.

For purposes of complying with these requirements, the following definitions apply:

"Business entity" means any entity recognized by law through which business is conducted, including a sole proprietorship, partnership or corporation, but does not include publicly traded companies listed on a national or international stock exchange.

"Interested party" or *"Interested parties"* means:

(1) A business entity performing work or service pursuant to, or in furtherance of, the applicable contract, including specifically sub-contractors;
(2) the person(s) who have an ownership interest equal to or greater than 25% in the business entity performing work or service pursuant to, or in furtherance of, the applicable contract. (This subdivision does not apply to a publicly traded company); and
(3) the person or business entity, if any, that served as a compensated broker or intermediary to actively facilitate the applicable contract or negotiated the terms of the applicable contract with the state agency. (This subdivision does not apply to persons or business entities performing legal services related to the negotiation or drafting of the applicable contract.)

"State agency" means a board, commission, office, department or other agency in the executive, judicial or legislative branch of state government, including publicly funded institutions of higher education: Provided, that for purposes of W. Va. Code § 6D-1-2, the West Virginia Investment Management Board shall not be deemed a state agency nor subject to the requirements of that provision.

The contracting business entity must complete this form and submit it to the contracting state agency prior to contract award and to complete another form within 30 days of contract completion or termination.

This form was created by the State of West Virginia Ethics Commission, 210 Brooks Street, Suite 300, Charleston, WV 25301-1804. Telephone: (304)558-0664; fax: (304)558-2169; e-mail: ethics@wv.gov; website: ethics.wv.gov.

West Virginia Ethics Commission

Disclosure of Interested Parties to Contracts

(Required by *W. Va. Code* § 6D-1-2)

Name of Contracting Business Entity: Lumos Networks, LLC dba SEGRA **Address:** 1200 Greenbrier St Charleston, WV 25311

Name of Authorized Agent: GREG FLORENCE **Address:** 1200 GREENBRIER ST, CHAS, WV 25311

Contract Number: _____ **Contract Description:** STATEWIDE CONTRACT FOR DATA TRANSPORT SVC

Governmental agency awarding contract: WEST VIRGINIA PURCHASING DIVISION ON BEHALF OF WV OFFICE OF TECHNOLOGY

☐ **Check here if this is a Supplemental Disclosure**

List the Names of Interested Parties to the contract which are known or reasonably anticipated by the contracting business entity for each category below *(attach additional pages if necessary)*:

1. **Subcontractors or other entities performing work or service under the Contract**
   ☐ Check here if none, otherwise list entity/individual names below.

2. **Any person or entity who owns 25% or more of contracting entity (not applicable to publicly traded entities)**
   ☐ Check here if none, otherwise list entity/individual names below.

3. **Any person or entity that facilitated, or negotiated the terms of, the applicable contract (excluding legal services related to the negotiation or drafting of the applicable contract)**
   ☐ Check here if none, otherwise list entity/individual names below.

Signature: _____ Date Signed: 6/6/22

Notary Verification

State of West Virginia, County of Kanawha:

I, _____, the authorized agent of the contracting business entity listed above, being duly sworn, acknowledge that the Disclosure herein is being made under oath and under the penalty of perjury.

Taken, sworn to and subscribed before me this 6th day of June, 2022

_____
Notary Public's Signature

To be completed by State Agency:

Date Received by State Agency: _____

Date submitted to Ethics Commission: _____

Governmental agency submitting Disclosure: _____

OFFICIAL SEAL
STATE OF WEST VIRGINIA
NOTARY PUBLIC
STEVEN HAMULA
208 Majestic Drive, Cross Lanes, WV 25313
My Commission Expires November 14, 2028

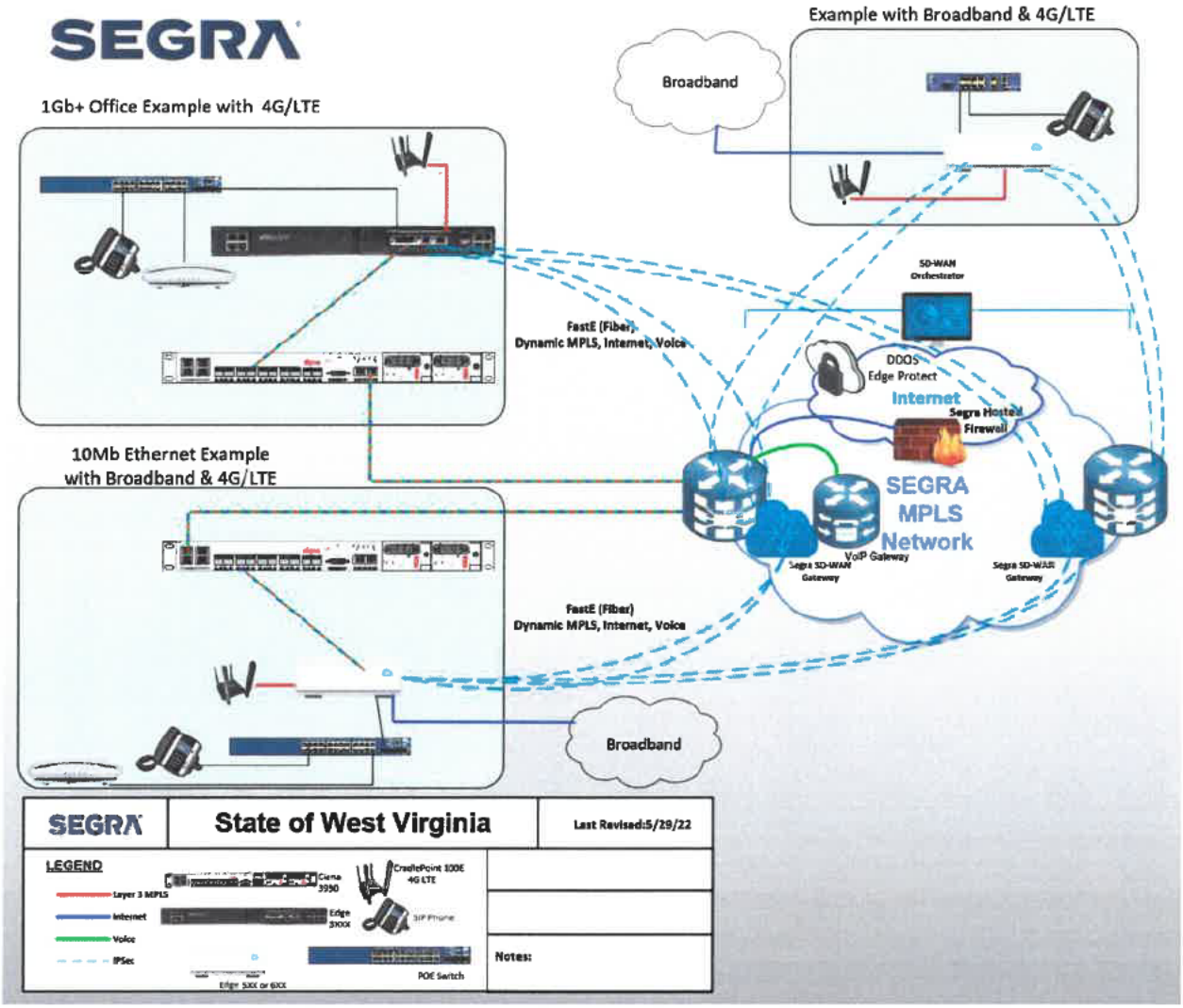
SEGRA

Segra's SD-WAN Solution Exhibit

The Segra SD-WAN solution is based on the VeloCloud product set and has three main components:

- VCO (VeloCloud Orchestration), which provides session set up, tear down of secure tunnels, and a portal for each instance, as well as performance, monitoring, and analytics;
- VCG (VeloCloud Gateways), for connectivity into the Segra MPLS network; and
- VCE (VeloCloud Edge Device), which is deployed by Segra technicians at the customer location and can act as a WAN aggregate and router.

State of West Virginia Network Design, Traffic Overview



Our design allows for a co-managed SD-WAN solution, with a multitude of transport mediums (MPLS, Ethernet DIA, 4G/5G LTE, Broadband, TDM) to interface directly with State agencies to deploy and professionally install VCEs (VeloCloud Edge). The VCE is the VeloCloud SD-WAN data plane component that is deployed at an end user's location. The VCEs at the various agencies can be viewed and managed by Segra as well as the State of West Virginia technical team. All VCE management is performed via the VeloCloud Orchestrator (VCO) in the customer portal. The local edge (VCE) can also allow for visibility (local) and, if desired, can be managed by someone (local) to the specific agency.

Due to the compute complexities of SD-WAN and amount of compute/processing needed to provide the service, the limitation of SD-WAN can scale to 5Gb. Beyond 5Gb, Segra would be deploying a FortiNet as a comparable Cisco managed router. This allows these select non-SD-WAN enabled circuits to be tied in seamlessly to the network. This limitation is more of a technology threshold, not solely a VeloCloud ceiling threshold. Please see the list of anticipated routing equipment below. This equipment is in addition to the Ciena (or equivalent) Fiber NID that would be deployed for a fiber-based circuit delivery at a customer site.

Anticipated Equipment	Description	Throughput for Sites (or Other)	Office Size
VeloCloud Edge 510N	Managed Router w/ SD-WAN	Up to 100M	Small
VeloCloud Edge 510N	Managed Router w/ SD-WAN	100M to 200M	Medium
VeloCloud Edge 620N	Managed Router w/ SD-WAN	200M to 350M	Medium
VeloCloud Edge 620N	Managed Router w/ SD-WAN	350M to 500M	Large
VeloCloud Edge 3400 or 3800	Managed Router w/ SD-WAN	1000M to 5000M	Large
FortiNet 1XXX (Managed Router Only)	Managed Router	5000M+	Large+
Cradlepoint E100	4G/LTE Router	4G/Wireless Router	All (dual SIM, option of AT&T or Verizon as Wireless Carrier)

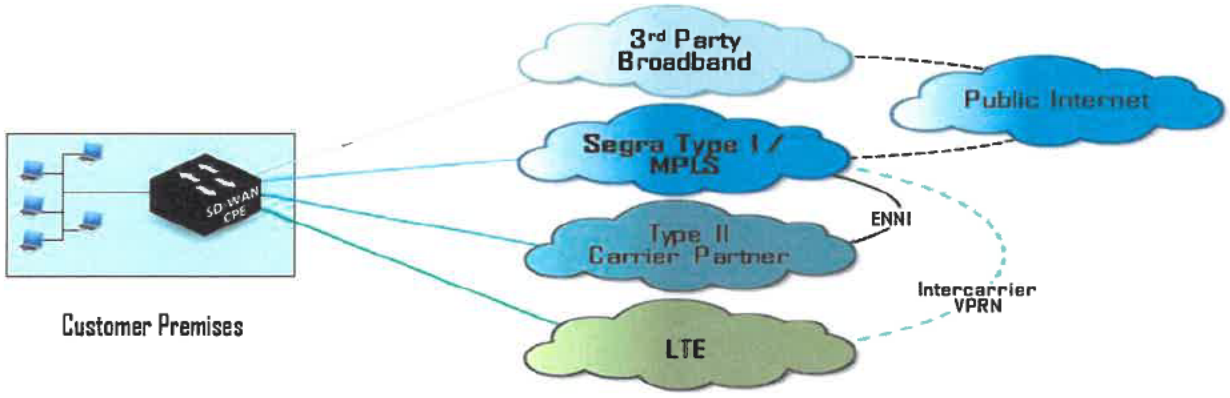
The proposed SD-WAN solution allows for agnostic transport mediums to securely connect to Segra's MPLS network. It is also enabled by WAN redundancy, provisioning ease, fast deployment, and flexible traffic assignment based on application, as well as a portal for viewing bandwidth consumption analytics at a granular and historical level.

The SD-WAN design provides customers with a highly available solution by bonding primary service/access to secondary and back-up WAN options. This approach will allow the State of West Virginia to customize the WAN applications and policies by site via an online portal.

The following elements of the solution will allow personnel who may not be well-versed in networking technologies to create, apply, and change configuration parameters:

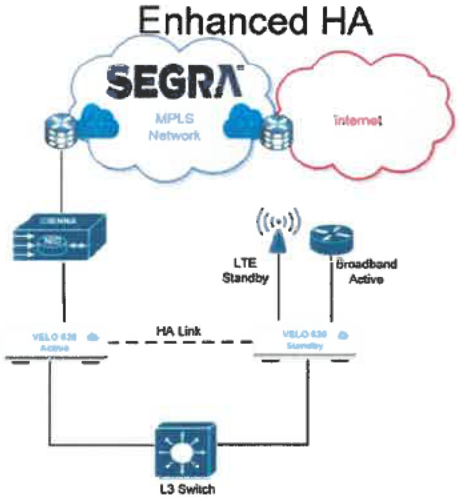
- The solution is preconfigured (zero touch) prior to deployment and installed by Segra technicians, minimizing the technical expertise needed for the State of West Virginia and its local agency or office contacts. This also helps to limit any on-site interaction during COVID.
- The SD-WAN portal used to manage configuration parameters will be supported by a database of the State of West Virginia's WAN policies and analytics. Granted State of West Virginia personnel can easily access this information.

- The portal can be accessed locally or remotely, allowing the State of West Virginia to have personnel with the knowledge necessary for a configuration update and the ability to perform a task regardless of the personnel's location.
- The Segra team will train selected State of West Virginia personnel and associated Administrators to use the portal and manage policies within it. This training will be recorded for future playback and reference. We will also provide ongoing support and any additional training, as needed.
- State of West Virginia Administrators for the SD-WAN solution will be able to create portal logins with role-based access.
- Portal views for troubleshooting and visibility of Segra hosted SIP, Hosted Voice, and Unified Communications become increasingly easier to manage (Quality of Service) and monitor (Jitter, Packet Loss, Latency) if Segra is the provider of WAN services.



Enhanced Failover/Redundancy:

- One or more of MPLS, DIA, LTE, 3rd Party Broadband access methods available at each device.
- Based on configuration, can be active/active or active/standby.
- Sub-second Failover. VoIP calls are maintained.
- High Availability (HA) configurations with redundant Edges are available.
    - Available by doubling the equipment/router selection.



The SD-WAN design provides customers with a highly available solution by bonding the primary service to secondary and back-up WAN options (broadband, Private Fiber, Public Fiber, LTE). This approach will allow the State of West Virginia to customize the WAN applications and policies by site, via an online portal.

Compliance with the State of West Virginia's Outlined Specifications

Segra's solution meets the State of West Virginia's requirements for an SD-WAN service that also acts as a managed router service as shown below:

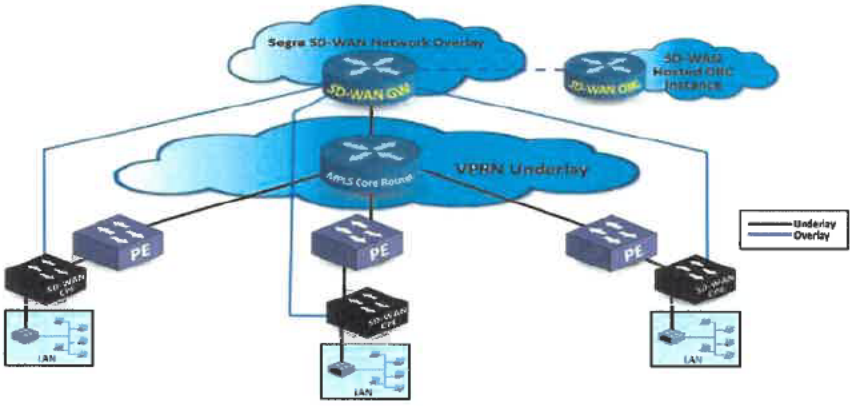
State of West Virginia Specification		Compliance
Router replacement	Lightweight replacement for traditional WAN routers that is agnostic to WAN transport	✓ VCE appliance
	Office component must physically terminate a carrier service	✓ VCE appliance
Process simplicity	Configuration parameters are application-centric and/or business-centric, and can be created/applied/changed by personnel who are not well-versed in networking technologies	✓ Solution configuration/installation by Segra ✓ VCO, user friendly WAN portal ✓ VCO knowledge base of West Virginia WAN policies and analytics ✓ Local or remote access to the portal ✓ On-site and web-based SD-WAN administrator training ✓ Portal user permissions based on role/knowledge
	The level of expertise required to configure the office is similar to that required to set up a basic home wireless network with consumer-grade equipment	✓ Same as above
	Rapid zero-touch configuration for new offices	✓ Zero-touch VCE appliance
Increased availability and performance	Allows traffic to be distributed across multiple WAN connections in an efficient and dynamic fashion, based on business and/or application policies	✓ Dynamic Multi Path Optimization (DMPO) ✓ Forward Error Correction (FEC)
	Redundancy and failover throughout the nodes, with evaluation of behavior in the event of link failure, brownout, or brownout The network core should be fully redundant with the State of West Virginia being automatically connected to the next closest point-of-presence (PoP) in the event of an outage	✓ DMPO Fully redundant core network and transport Non-stop routing Non-stop services IP Fast ReRoute (FRR) Resilient switch fabric Optional redundant management ✓ Modular and distributed software ✓ Optional redundant power supply ✓ Separate control and management planes

State of West Virginia Specification		Compliance
	Network load balancing to support multiple connections with varying use of those connections. Provides support for load balancing schemes offered (active/active), tunnel bonding, and failover times between connections	✓ DMPO
	Path selection to monitor the characteristics of the various paths to between two locations, selecting the optimum path for a given application	✓ DMPO
	Traffic management that restricts access and shapes traffic to the WAN connection, particularly when bandwidth is limited. Describe Quality of Service (QoS) between the State of West Virginia premises and the provider edge, type of traffic shaping, and rate limiting	Traffic classes with predefined QoS policies Application mapping to traffic classes ✓ Out-of-the-box mapping for 6,000 applications Intelligent enforcement based on network access conditions
	Management of and visibility into steering traffic by accurately classifying traffic	✓ Multi-source inbound QoS to measure bandwidth usage and proactively regulate traffic and bandwidth distribution based on traffic quantity and priority ✓ Link steering classes
Secure VPNs	Service chaining of other network services and devices, such as WAN optimization controllers, firewalls, Secure Web Gateways (SWGs)	✓ Secure overlay, independent of underlying transport components ✓ Device authentication ✓ Automatic security configuration/mgmt
	Office component can support automated creation of secure VPNs with a minimum of 128-bit encryption (with future support for 256-bit encryption)	✓ AES-128 (Advanced Encryption Standard) ✓ AES-256
Security	Compliance with all IRS Publication 1075 requirements pertaining to the safeguarding of Federal Tax Information	✓ Compliant

SD-WAN Edges (CPE) are zero-touch, enterprise-class appliances that provide secure, optimized connectivity to private, public and hybrid applications, as well as physical and virtualized compute services. Real-time applications, such as voice and video flows, can benefit from Forward Error Correction (FEC) during periods of packet loss. DMPO (Dynamic Multi Path Optimization) automatically enables FEC on single or multiple links.

With multiple links, DMPO will select up to two best links at any given time for FEC. Duplicated packets are discarded, and out of order packets are re-ordered at the receiving end before being delivered to the final destination. DMPO enables jitter buffer for the real-time applications when the WAN links experience jitter or latency. Each SD-WAN implementation is a combination of two logical networks (overlay indicating SD-WAN services, underlay indicating traditional MPLS Ethernet Layer 3/VPRN services), shown below:

Overlay	The SD-WAN network and its associated premium features. Rides on top of the underlay	Purchased by customer as an SD-WAN service, separate and distinct from Underlay service(s).
Underlay	The base connectivity method(s) established at each customer site	Purchased by customer as one or more of VPRN, DIA, LTE, or 3rd Party Broadband; separate and distinct from SD-WAN service

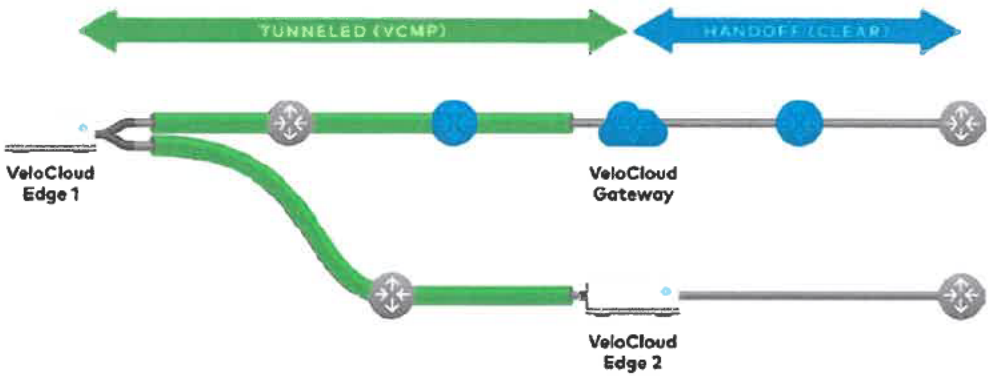


In the proposed solution, the DMPO tunnels are established between VCE (VeloCloud Edge) and VCG (VeloCloud Gateway), or between VCE and VCE. The VeloCloud Management Protocol (VCMP) header is added to the packet before leaving the VCE, which adds an overhead of 59 bytes.

Once the traffic reaches the VCG or the VCE on the receiving end, all tunnel headers (VCMP, IPSec) are removed, and the original user data are passed to the next hop router, which would be an L3 switch/router in an enterprise scenario, or a Provider Edge (PE) in a service-provider scenario. Edge endpoints monitor gateway availability, as well as path performance metrics, and immediately switch to alternate gateways independently of the controller.

Segra's SD-WAN delivers holistic application "Quality of Experience" (QoE), with local prioritization and bandwidth allocation, as well as steering between links and remediation of link quality issues. Granular application recognition, simple business prioritization policies, and continuous monitoring of available link capacity and quality drive the solution's DMPO.

Application flows can be shifted on a per-packet basis, mid-session, between different links, or split across links. This ability, combined with on-demand remediation including error correction and jitter buffering, enables the use of broadband Internet as an integral part of an enterprise-grade WAN. Priority or network sensitive traffic, such as VoIP, video conferencing, etc., no longer need to have, or be limited to, private/MPLS circuits to meet SLA objectives.



The solution's DMPO performs continuous uni-directional measurements of performance metrics - loss, latency, and jitter -- of every packet, on every tunnel, between any two DMPO endpoints, VCE or VCG. Per-packet steering allows independent decisions in both uplink and downlink directions without introducing any asymmetric routing. DMPO uses both passive and active monitoring approaches.

When user traffic is present, the DMPO tunnel header contains additional performance metrics including sequence number and timestamp, thus enabling the DMPO endpoints to identify lost and out-of-order packets, and calculate jitter and latency in each direction. The DMPO endpoints communicate the performance metrics of the path between each other every 100 ms.

When there is no user traffic, an active probe is sent every 100 ms, and after 5 minutes of no high priority user traffic, the probe frequency is reduced to 500 ms. This comprehensive measurement enables the DMPO to react very quickly to the change in the underlying WAN condition, resulting in the ability to deliver sub-second protection against brownout and blackout in the WAN.

We provide 24/7/365 proactive monitoring via Segra managed CNOC/NOC. Service availability is monitored using dry contact alarms, SNMP traps, syslog, Ethernet CFM, and Netcool, which receives all the monitoring and alarming information. Operations staff monitor Netcool 24x7x365 and initiate the incident response process when alarms indicate an incident has occurred. Policies and procedures are in place to monitor and upgrade network segments at predefined utilization thresholds.

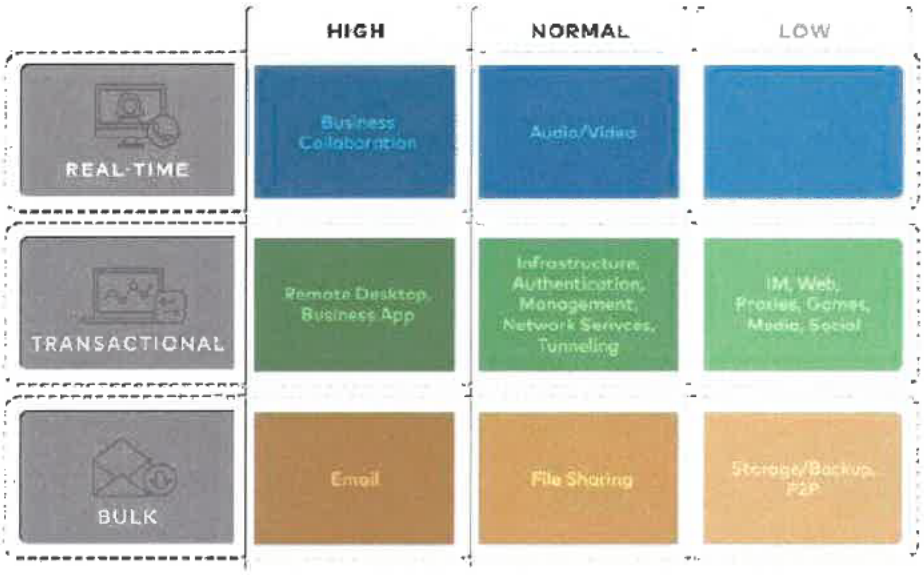
Security control effectiveness is tested and measured using a combination of quarterly vulnerability assessments, annual penetration tests, and formal security and risk assessments when there are major changes to the environment. Third-party assessments of varying types are conducted annually. Security test results are communicated to senior management in quarterly security update meetings. Vulnerability scans are reported monthly to senior management and relevant staff via an email report.

The Business Policy contains the out-of-the-box Smart Defaults functionality that maps more than 6,000 applications to Traffic Classes. Customers can immediately use application-aware QoS without having to define policy. Each Traffic Class is assigned a default weight in the scheduler. These parameters can be changed in the Business Policy. Below are the default values for the 3x3 matrix with nine (9) Traffic Classes. If the State of West Virginia were to identify an application not recognized by the application library, a request can be made to Segra for the application, whether an

'in house' application or public. Segra will work with VeloCloud to have it built in/recognized by the VeloCloud SD-WAN solution.

A Traffic Class is defined with a combination of Priority (High, Normal, or Low) and Service Class (RealTime, Transactional, or Bulk), resulting in a 3x3 matrix with nine (9) Traffic Classes. Application/ Category and scheduler weight can be mapped to these Traffic Classes. All applications within a Traffic Class will be applied with the aggregate QoS treatment, including scheduling and policing.

All applications in a given Traffic Class will have a guaranteed minimum aggregate bandwidth during congestion based on scheduler weight (or percentage of bandwidth). When there is no congestion, the applications are allowed to burst up to the maximum aggregated bandwidth. A policer can be applied to cap the bandwidth for all the applications in a given Traffic Class.



Example: The customer has a 90 Mbps Internet link and a 10 Mbps MPLS circuit on the edge, and the aggregate bandwidth is 100 Mbps. Based on the default weight and Traffic Class mapping above, all applications that map to Business Collaboration will have a guaranteed bandwidth of 35 Mbps, and all applications that map to Email will have a guaranteed bandwidth of 15 Mbps. Business policies can be defined for an entire category (e.g., Business Collaboration), applications (e.g., Skype for Business), and more granular sub-applications (e.g., Skype File Transfer, Skype Audio, Skype Video).

Default Weight and Traffic Class Mapping

For a private link that has a CoS (Class of Service) agreement with an MPLS provider, the provider will guarantee a different SLA for each CoS on the MPLS link. DMPO can treat each CoS as a different link and make granular application-aware decisions for private links with CoS agreements. A policer can be defined for an MPLS CoS underlay to ensure service provider committed bandwidth SLAs are being honored by the customer.

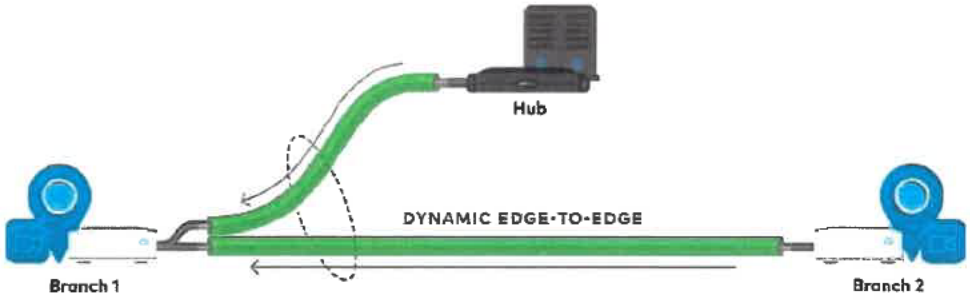
Example: A customer office edge has a 10 Mbps MPLS link, and the service provider offers an SLA that guarantees 40% of the bandwidth for CoS1 (DSCP=EF, CS5), which is real-time traffic, and the remaining 60% of the bandwidth for the rest of the traffic. The service provider will police their PE with an aggregate rate of 10 Mbps and also police the rate for CoS1 traffic so it does not exceed (DSCP=EF, CS5) 4 Mbps.

If the CoS1 traffic on the MPLS underlay exceeds 4 Mbps, packets will be dropped by the service provider, thus impacting quality of service. A 4 Mbps policer for CoS1 on the customer Edge ensures traffic in that class never exceeds 4 Mbps. The rest of the traffic can burst up to the link speed if no congestion exists and is guaranteed a minimum bandwidth during times of congestion.

In legacy WAN networks, service providers and enterprises have the ability to allocate bandwidth or police traffic based on CoS offered by the service provider. With SD-WAN, there is a need to apply a similar concept to the WAN overlay that may include one or more transports from multiple service providers. IT administrators may want to police high priority Business Collaboration traffic on the aggregated overlay tunnel to ensure a service provider offered SLA is honored or proactively police non-critical applications for security or QoS compliance reasons. To accommodate these use cases, policing can be defined for a Traffic Class (i.e., Service Class and Priority).

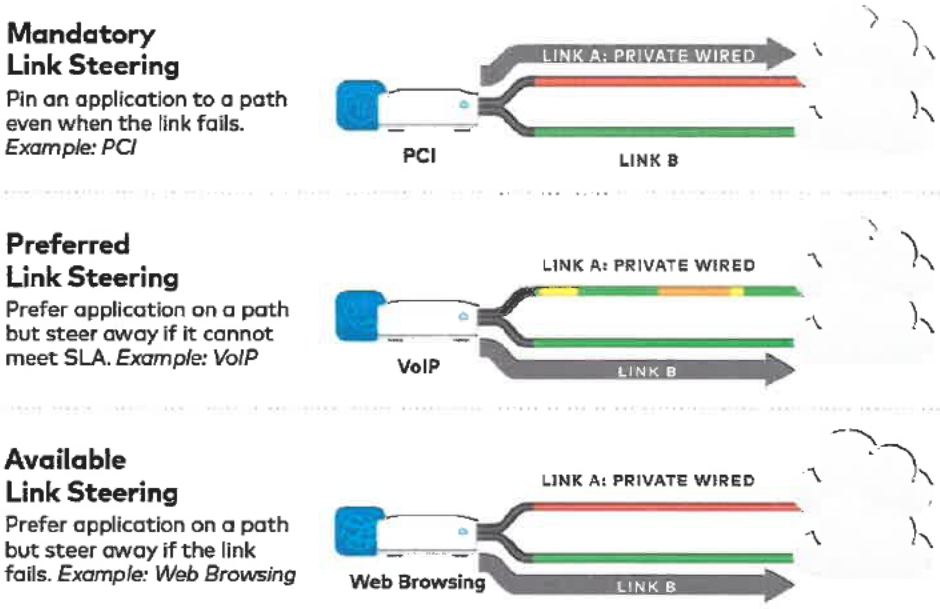
The SD-WAN solution enables multi-source inbound QoS, which proactively measures the bandwidth usage with multiple remote peers, and will begin to regulate the traffic before congestion. Additionally, available bandwidth will be distributed fairly between direct internet traffic and all

remote peers based on the quantity and priority of traffic that each remote device has to transmit, as illustrated below.



Dynamic Edge-to-Edge

Example: Consider a customer with the hub and spoke topology with the dynamic office-to-office functionality enabled. If an important video call is initiated from Office 1 to Office 2, these offices can talk over a dynamically established overlay tunnel. The challenge with the traditional WAN technologies is that the hub is unaware of the high priority video call between the two offices. This might result in the hub sending low priority traffic towards Office 1 and causing quality issues for the important video sections. With SD-WAN multi-source inbound QoS enabled, Office 1 will proactively inform the hub to slow down the low priority traffic.



Link Steering

SD-WAN provides a secure overlay that is independent of the underlying transport components. SD-WAN devices are authenticated before they participate in the overlay. Any combination of circuits can support secure, encrypted transmission, and the separated control plane enables automated configuration and key management across the multitude of offices. Additionally, a

network designer can include segmentation as an overlay that is both independent and consistent across the various underlying components.

Encryption is standard IPsec with AES128 and optionally AES256 encryption and supports interoperable IPSec connections to non-VeloCloud VPN devices including Cisco ISR, Cisco ASA, Palo Alto Networks, as well as Amazon VPC and others. An additional proprietary header between VeloCloud tunnel endpoints provides the "Dynamic Multi-Path Optimization" for per-packet application steering and on-demand remediation, while maintaining application sessions. However, for encrypted traffic, this can be entirely within standard IPsec transport.

Training

Segra can train State of West Virginia selected personnel on the SD-WAN and MPLS services before, during, and after service implementation. Training options are available on-site or remotely via live web conference. Training will ensure that the State of West Virginia and related Agencies staff have the information necessary to operate the services effectively and confidently. Segra also offers instructional web tutorials that are already built and available, as shown in the screenshot below.[1] If needed, training can also be provided before and after service activation.

SD-WAN Training Tutorial Screenshot

The training will explain how to use the portal to view current site status, circuit status, and the analytics associated with the service. The session will also include instruction on using the portal to manage SD-WAN sites, which will address application management, alerts management, and other related topics.

[1] https://www.segra.com/wp-content/themes/fs-theme/psupport-html-videos/Segra_SD-WAN_Tutorial_02-022021/story_html5.html

Testing and Acceptance after Site Turn-Up

Segra will assume that access to the State of West Virginia and related Agency facilities for verification testing will require, at a minimum, the following information:

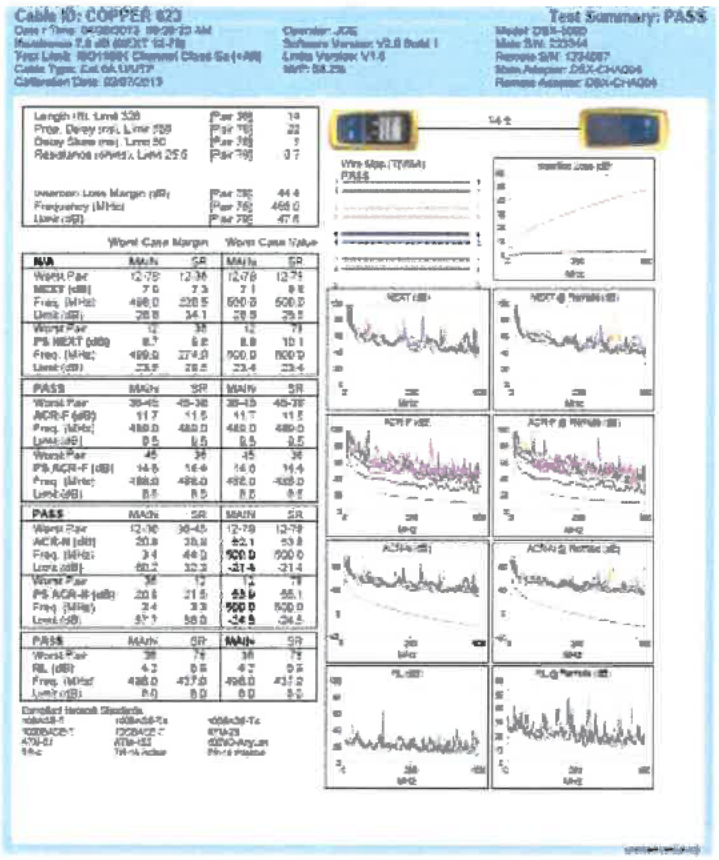
- State of West Virginia facility location (physical address),
- Procedures for physical access to the State of West Virginia facility (including point of contact for access),
- A list of Segra personnel requiring access,
- The dates when access is required,
- Test cases to be performed at the State of West Virginia facility, and
- Equipment required at the facility to complete the verification testing.

Managed Network Service (MNS) Testing Criteria

General Testing Criteria	
Criteria	**Description**
Verification & Acceptance Testing Approach	Segra will perform verification and acceptance testing specific to KPIs, AQLs, and SLAs for each service.
Development of Test Plan	Each service will have a verification test plan that demonstrates compliance with KPIs per the TS-02 Test Scenario example.
Test Methodology	The MNS verification test plan is for specific service orders (actual locations and order numbers TBD subsequent to award).
Parameters to be Measured	Segra will demonstrate that awarded services are delivered based on KPIs and SLAs defined in Performance Metrics for services managed for this TO.
Measurement Procedure	Measurement procedure(s) will be implemented in accordance with steps in the service test methodology process for this service and TO requirements.
Acceptance (Pass/Fail) Criteria	Demonstration that service works properly according to KPIs and AQLs as defined in Performance Metrics.
Fallback Approach	If a test fails in any service verification test, appropriate service-specific remediation will take place, followed by re-testing.
Testing Conditions	
Criteria	**Description**
Observation	Service testing will be available for the State of West Virginia observation upon notice to Segra.
Test Equipment	Segra will provide test equipment, hardware, software, and analysis tools.

MNS Test Cases	
Criteria	**Description**
MNS Test Cases	Test as defined per service; trouble ticket report data.
Test Data, Results, and Deliverables	
Criteria	**Description**
Test Data Sets	Monthly availability data in Excel, PowerPoint, and/or PDF formats.
Test Results and Acceptance	Trouble ticket report data.
Full TVP	Provide for State of West Virginia approval after TO award.
Testing Report	Provided within 3 days of service installation and testing.

Cable and Wiring Service (CWS) Sample Test

Cable and Wiring Service Sample Test	
Test Case	Full/Complete Cable Testing (Certified).
Test Parameters	Near End Cross Talk (NEXT), Attenuation, Attenuation-to-Crosstalk Ratio, Loop. Resistance, Impedance, and Capacitance.
Test Examples	
Equipment Used	Fluke DTX-1800.

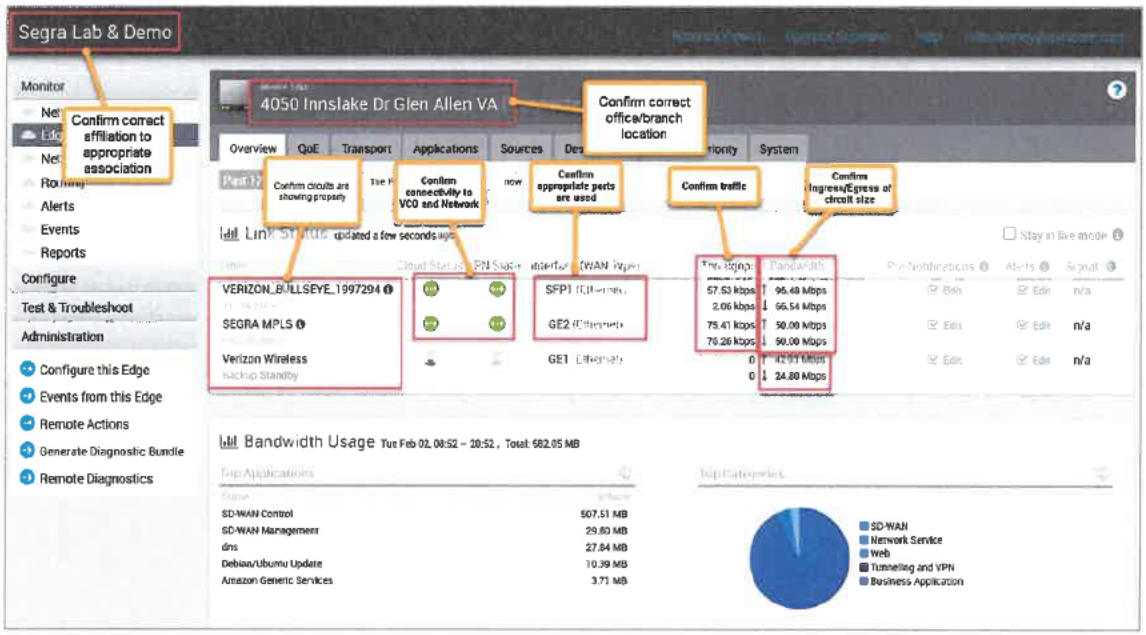
SD-WAN Sample Test

SD-WAN Sample Test	
Test Case	Segra circuit test and turn up.
Test Parameters	Port Setup/Status, Throughput, RTD Streams.
Test Examples	**Port Setup** Port: 1G Copper Port 1 Port Selection: 10/100/1000Base-T Auto Negotiation: On Advertisement: Default-ALL Flow Control: Both On MDIX: Auto Transmit clock offset: Disabled **Port Status** Line Rate (bps): 1GE Link Status: Link UP Link Speed: 1000T Link Mode: Full **Throughput Measurement Setup** Delay Measurement Mode: Round Trip Delay Histogram: Enable Sampling Period: 1sec Threshold (Max RTD allowed): 100.00us **Throughput Measurement Results** **Global Result** **Aggregate Result** ST: 2021-01-27 10:52:30 / ET: 00/00:05:27 TX / RX Line Rate (bps): 1.000G / 1.000G Utilization (%): 50.000% / 50.000% Utilization (bps): 500.000M / 500.000M Framed Rate (bps): 493.464M / 493.469M Data Rate (bps): 487.582M / 487.586M **Stream #1 Results** **Summary Result** ST: 2021-01-27 10:52:30 / ET: 00/00:05:27 TX / RX Utilization (%): 50.000% / 50.000% Utilization (bps): 500.000M / 500.000M Framed Rate (bps): 493.464M / 493.468M Data Rate (bps): 487.582M / 487.586M # of Bytes: 20009447900 / 20009447900 Total Frames: 13251290 / 13251290 Bad Frames: 0 / 0
Equipment Used	VeEX TX300.

The VCE device will need an internet connection to pull its configuration and have management from the VCO (Orchestrator). The Segra technician will need to have a working LTE device, or the customer will need to have a working DHCP internet connection to bring the VCE devices online. If there is no path or direct connection to the internet, the VCE devices will not come online and receive their configuration.

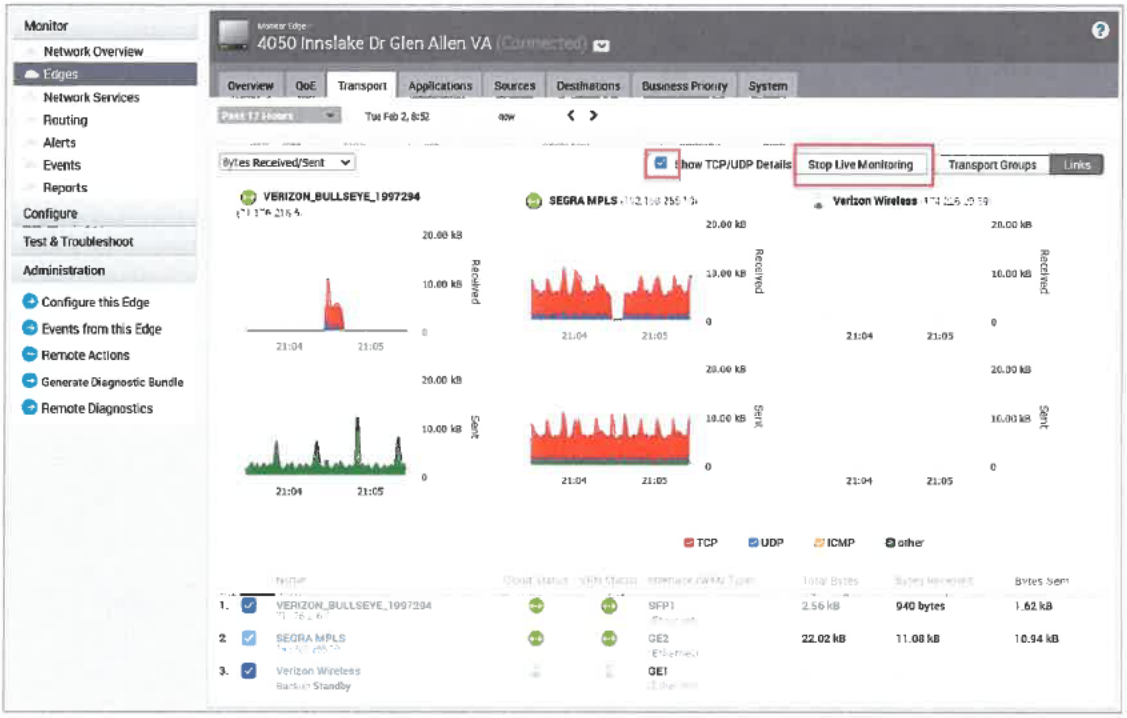
Our team pre-provisions the VCE in office and tests prior to deployment. The Segra technician validates that the unit has been powered up and connected appropriately to circuit(s)/transport medium(s). The bootstrap powering up of the unit generally takes 5 to 10 minutes.

Once the device is deployed and installed by the technician on an active connection(s), the portal available from the VCO allows validation of proper functionality. The VCE transport functionality appears and shows circuit ingress and egress throughput available as well real-time traffic. The technician locally, as well as the Segra IP Engineer, engages on an open conference bridge and validates that the unit is performing and has been installed per specifications both physically as well as confirmed from the VCO activity.



VCO/Portal Example

After confirming information under the 'Overview' tab on the portal is accurate and responding appropriately, the Segra IP Engineer then transitions to the 'Transport' tab. Under this tab, the IP Engineer selects 'Live Mode' and checks the button of 'Show TCP/UDP Details' and checks over a period of 15 minutes to ensure active circuits are responding appropriately. Circuits such as 4G/5G LTE are by default set up in 'Standby Mode' as not to generate unnecessary keep alive traffic.



VCO/Portal Transport Example

After the 15-minute review, the on-site technician should then test failover (if selected for the site) by unplugging WAN uplink cables and ensure it fails over appropriately to the redundant/failover circuit. Once this is confirmed, the turn-up of service is deemed a success and complete. The technician will acquire sign off from State of West Virginia personnel prior to leaving.

Fallback Approach

If a test fails in any service verification test, Segra will make appropriate service-specific remediation and re-test. If a service order requires re-testing, Segra may modify the service-specific verification test plan to precisely address the State of West Virginia's concerns. Upon completion of the re-testing, we will re-issue the Service Order Completion Number (SOCN, Segra often refers to as "service birthdate") and provide the State with an updated service-specific verification test report. From our understanding, the State of West Virginia refers to this as certificate of acceptance date (COA).

If a service order requires re-testing and/or is rejected by the State of West Virginia, Segra may modify the service-specific verification test plan to precisely address the State's reasons for rejection. Segra will use trouble ticket processes to inform the State of progress. Upon successful completion of the re-testing, we will issue a new SOCN and provide the State with an updated verification test report.

Acceptance Reporting

When service-specific verification testing is completed and the test results demonstrate compliance with the associated KPIs and acceptance criteria, Segra will provide the State of West Virginia with the appropriate verification test report. We will deliver a SOCN within one (1) day of delivery of the test report.

Once the SOCN is delivered, the State of West Virginia will have three (3) business days to review the verification test results. Segra will not begin billing for services if the State of West Virginia rejects the services within 30 days of receipt of the SOCN.

New Services Verification Tests

Segra will submit updates to this verification plan for any new services that are added due to contract modifications. This report specifies the delineation of times between trouble tickets being opened and closed over billing periods for the service. TTRs (Time to Repair), as specified in TO (Time of Outage) service performance metrics, are not part of verification testing at turn up, but are measured as performance KPIs for compliance to specified AQLs (Acceptable Quality Limit).

Verification Test Report

After Segra collects all verification test data, we will record the results for each test case and provide the table to the relevant personnel at the State of West Virginia or corresponding agency.

SEGRA

Segra's Service Level Agreement (SLA)

SEGRA®

EXHIBIT C
MASTER SERVICE AGREEMENT
DATA & VOICE SERVICE LEVEL AGREEMENT

General. This Data & Voice Service Level Agreement (SLA) describes target network performance and service level metrics for end user data and voice services via Ethernet or TDM provided by Segra.

1. **Access Circuit Network Availability.**

1.1 "Network Availability" is the percentage of total minutes during a calendar month that the Services are available to the Customer. Network Availability is calculated as follows:

$$\text{Network Availability \%} = \frac{[(\text{Total Minutes in the Month}) - (\text{Sum of Total Outage Minutes})] \times 100}{\text{Total Minutes in the Calendar Month}}$$

The Services shall be deemed to be "unavailable" whenever an outage is recorded on a Segra trouble ticket classified as "major" or "critical" by Segra Network Operations Center which results in Customer not having the ability to transmit or receive packets by means of the Services, and "Total Outage Minutes" shall be deemed to be the length of time during which the Services are unavailable to the Customer, as reflected on such trouble tickets. "Total outage minutes" shall not include any outages (i) occurring during scheduled maintenance activities; (ii) attributable to any act or omission of Customer; (iii) attributable to Customer's applications, equipment or facilities; (iv) resulting from reasons of Force Majeure or other causes beyond the reasonable control of Segra or (iv) lasting ten minutes or less.

1.2 The objective for Network Availability is 99.999%. For any month in which the objective is not met, Customer will receive a credit, which may be applied towards Customer's subsequent monthly invoice(s), up to and not exceeding the monthly recurring charges for the affected Services [i.e., the portion(s) of the Services directly made unavailable as a result of the outage(s) in question] for each cumulative hour or portion thereof during which such Services are unavailable to the Customer (subject to the limitations set forth herein.) Unavailability and credits will be prorated and paid in 15-minute increments.

2. **Access Circuit Mean Time to Repair**

2.1 Mean Time to Repair (MTTR) is the average time required to repair service to an operational condition if service(s) are not active or Customer is experiencing consistent service degradation. The MTTR objective is four (4) hours depending on for outages due to electronic equipment failure and fiber optic facilities failure and ten (10) hours for outages due to fiber cuts.

2.2 If the MTTR is not met, Customer may request a credit, to be applied towards Customer's subsequent monthly invoice(s), up to and not exceeding the monthly recurring charges for each hour over the four-hour MTTR [i.e., the portion(s) of the Services directly made unavailable as a result of the outage(s) in question] per violation. For any month in which the objective is not met, customer may receive a credit for each location.

2.3 **Exclusion:** MTTR statistics will not include any time lost waiting on repair-related information from customer or access to customer premises.

3. **Circuit Latency**

3.1 "Average Latency" is the monthly average round-trip latency from a core network node to any other designated core network node on the Segra network, determined by measuring round-trip network responses over such portions of the network.

3.2 The objective for Average Latency is to not be greater than 8 milliseconds inside a Metropolitan Area. The objective for Average Latency is to not be greater than 30 milliseconds between Metropolitan markets. For any month in which the objective is not met, Customer will receive a credit, which may be applied towards Customer's monthly invoice, equal to 1/30 of the monthly recurring charges for the Services.

Latency = **Sum of the roundtrip delay measurements for an On-Net Service**
Total # of measurements for an On-Net Service

Metro Area Market 8ms Latency	WAN 30ms Latency	National 90ms Latency
Round trip where both sites A and Z are within the same Metro Area Market	Round trip between any 2 Metro Area Markets within the same WAN	Round trip between any two WANs
• Atlanta, GA • Asheville, NC • Charlotte, NC • Fayetteville, NC • Greensboro, NC • Raleigh, NC • Wilmington, NC • Pittsburgh, PA • Charleston, SC • Columbia, SC • Florence, SC • Greenville, SC • Myrtle Beach, SC • Ashburn, VA • Charlottesville, VA • Hampton Roads, VA Harrisonburg, VA • Richmond, VA • Roanoke, VA • Waynesboro, VA • Charleston, WV • Morganton, WV	WAN defined by State Borders • Georgia • Kentucky • North Carolina • Maryland • Ohio • Pennsylvania • South Carolina • Virginia • West Virginia	

4. Circuit Jitter

4.1 "Average Jitter" is the monthly average variation in the time between packets arriving, as measured at designated portions of the Segra network, determined by measuring Jitter over such portions of the network during a calendar month.

4.2 The objective for Average Jitter is to not be greater than 2 milliseconds. For any month in which the objective is not met, customer will receive a credit of 1 days value monthly recurring charge specified in the agreement for each occurrence which the parameters are not met, which may be applied towards Customer's monthly invoice, up to and not exceeding the monthly recurring charges for the Services.

5. Packet Loss

5.1 "Packet Loss" or "Frame Loss Ratio" is defined as the percentage of frames that are not successfully received compared to the total frames that are sent in a calendar month, except where any packet or frame loss is the result of an Excluded Disruption. The percentage calculation is based on frames that are transmitted from a network origination point and received at a network destination point (Segra network hub to Segra network hub). Packet Loss / Frame Loss Ratio is calculated as follows:

Packet Loss / Frame Loss (%) = 100 (%) – Frames Received (%)

5.2 The Packet Delivery Service Level for Segra SIP solution is less than 0.25% (on average) of total IP packets dropped per month. The Packet Delivery Service Level will be measured by Segra between four (4) Segra North American Gateways, and is defined as the percentage of IP packets dropped between such Gateways.

Cumulative Unavailability per event (in hours: minutes: seconds)	Service Level Credit
0:00:01 – 00:30:00	No Credit
00:31:01– 01:30:00	1 day
01:30:01– or more	3 days

6. **Missed Service Standard**

6.1 Missed Service Standard is measured as three trouble tickets or missed service standards within a calendar month.

6.2 In the event that the objective for Missed Service Standard is exceeded then the affected site will be eligible for an additional 10% credit of the monthly recurring charge.

7. **Service Credits**

7.1 In order to receive any of the service credits described in this SLA, Customer must notify Segra within ninety days from the time Customer becomes eligible to receive a service credit. Failure to comply with this requirement will forfeit Customer's right to receive a service credit.

7.2 Reports are prepared and credits for documented occurrences are issued within 60 business days of receipt of Customer notice.

SEGRA

Segra's Escalation Contacts and Contact Information

Ready to maximize your potential?

Communications is the lifeline of all businesses and organizations today. We're here to help you manage your challenges and capitalize on your opportunities.

Segra's Escalation Contacts and Contact Information

Customer Service is a key element to all successful companies. Segra is no exception. As we continue to grow, Segra's ability to differentiate its products and services by our customer service is absolutely critical. It is with this focus that we created Segra's Customer Solution Center (CSC).

The CSC is Segra 's tier one customer support group responsible for handling and triaging all incoming requests. The solution center is intended to be the irst stop to solve our customer's issues with just one call. The CSC is supported by the CNOC, NOC and Billing operations to handle all troubles that require escalation or tier two support.

Our CSC is here to actively listen to your needs and/or concerns whether it concern the management of your voice services, billing inquiries or troubles. Please give us the opportunity to serve you.

CUSTOMER SOLUTIONS CENTER ESCALATION LIST

TECHNICAL/ CUSTOMER	1st Level	TCSC Technician On-Duty (M-F 8A-5P EST)	833.467.3472 customercare@segra.com
	2nd Level	Cheryl Morlan Technical CSC Manager	800.294.9910 cheryl.morlan@segra.com
	3rd Level	Nicole Smart Sr. Director, Customer Service	800.294.3928 nicole.smart@segra.com
BILLING	1st Level	BCSC Specialist On-Duty (M-F 8A-5P EST)	833.467.3472 billingsupport@segra.com
	2nd Level	Teresa Bright Manager, BCSC	800.264.3820 teresa.bright@segra.com
	3rd Level	Nicole Smart Sr. Director, Customer Service	800.294.3928 nicole.smart@segra.com

SERVICE DELIVERY ESCALATION LIST

1st Level	Assigned Project Manager	
2nd Level	Manager Project Management	servicedeliveryescalations@segra.com
3rd Level	Cheryl Thibodeaux Director, Project Management	O: 803.995.8555 C: 803.587.0646 cheryl.thibodeaux@segra.com

ENTERPRISE REPAIR ESCALATION LIST (CNOC)

MONDAY - FRIDAY		
1st Level	On-Duty Technical Support Analyst	1.833.467.3472 (option 2)
2nd Level	On-Duty (7 a.m.- 12 a.m.) Enterprise Repair Escalations Manager	800.304.1498
3rd Level	Andrea Redfern Sr. Manager, Voice	800.304.0320 andrea.redfern@segra.com
3rd Level	Scott Dunham Sr. Manager, Elite CNOC	844.733.4318 scott.dunham@segra.com
4th Level	Fred Christian Sr. Director, Enterprise Repair	888.696.0408 fred.christian@segra.com

SATURDAY - SUNDAY		
1st Level	On-Duty Technical Support Analyst	1.833.467.3472 (option 2)
2nd Level	On-Duty Enterprise Repair Escalation Manager	800.304.1498
3rd Level	Fred Christian Sr. Director, Enterprise Repair	888.696.0408 fred.christian@segra.com

SEGRA

Segra's Drug and Alcohol Use Policy

Segra Policy Manual

Drug and Alcohol Use

Effective Date: January 18, 2021

PURPOSE: To establish procedures that will help ensure that Segra remains a drug-free workplace. Substance abuse, while at work or otherwise, seriously endangers the safety of the individual user, as well as potentially other employees and the general public, and creates a variety of workplace problems, including increased injuries on the job, increased absenteeism, increased health-care benefit costs, increased theft, decreased morale, decreased productivity, and a decline in the quality of products and services provided by Segra.

POLICY: Segra is firmly committed to the health and safety of our employees and to maintaining a drug-free workplace. The Company considers the influence of alcohol and drugs in the workplace to be detrimental to our employees and to our continued growth and future success. Employees are advised of the Drug and Alcohol Use policy (included in the Employee Handbook), dangers of drug abuse, penalties associated with convictions of drug abuse violations, and the availability of counseling and rehabilitation.

PROCEDURE:

1. Prohibited Activities include, but are not limited to:
   - Illegal involvement with drugs on Company time or Company property or at any time or place during the workday or at any time in a Company vehicle will result in disciplinary action up to and including discharge;
   - Illegal off-duty involvement with drugs will result in disciplinary action up to and including discharge;
   - The term "illegal involvement" means illegal possession, use, manufacture, dispensation, distribution, purchase, or being under the influence of any controlled substance or violation of any applicable federal or State Criminal drug statute;
   - Employees who use alcoholic beverages on the job or report or return to work under the influence of alcohol will be subject to disciplinary action up to and including termination;
   - Employees' offices and desks, Company vehicles, privately-owned vehicles, personal property on Company premises, and work sites are subject to search with reasonable cause for illegal drugs or other evidence of violations of this policy.
2. Notifications/Enforcement:
   - All employees will be expected to adhere to the Company's policy on drugs and alcohol;
   - All employees must notify the Company of any criminal drug statute conviction within five days of such conviction;
   - All employees will be expected to report violations of the Company Drug and Alcohol Policy or other actions that threaten harm to the Company or to their fellow employees. Employees are expected to use good judgment and common sense in exercising this responsibility.
3. Drug/Alcohol Testing: Reasonable Cause Testing:

- Current employees will be tested at the direction of management where "reasonable grounds" exist to suspect that an employee has illegally used drugs or has used alcohol in violation of Company policy. An example of "reasonable grounds" could include, but would not be limited to, an investigation of a serious on-the-job accident where the cause is questionable. Impaired ability to perform the required job is another example of "reasonable grounds." Observations of behavior supporting reasonable grounds for drug or alcohol testing will be documented using the "Reasonable Grounds Behavior Observations form (attached).
- An employee who is observed by a supervisor to be impaired in the performance of his/her work may be removed from duty and subject to disciplinary action. An employee who is suspected of being under the influence of alcohol or drugs may be requested to undergo a urinalysis test, breath alcohol test, or saliva alcohol test to identify the presence of drugs or alcohol. Employees who refuse testing will be subject to disciplinary action up to and including discharge.
- Persons taking legally prescribed drugs will have the opportunity to disclose this use prior to testing. Appropriate action will be taken concerning employees whose job performance is impaired by the influence of legal drugs in accordance with their medical prescription.
- A reasonable suspicion to justify drug or alcohol testing may be based on the employee being involved in an incident or otherwise acting in such a manner that suggests the employee is working under the influence of alcohol or illicit substances.

4. Pre-employment Drug Screening: All offers of employment are made contingent on a successful drug-screening process. Any applicant whose test results are positive or who refuses to give consent/submit to testing will be regarded as having failed to complete the application process and will not be given further consideration for employment.

5. Compliance with Drug/Alcohol Screening requirements to work on customer premises: In some instances, Segra employees may perform labor or provide services on the premises of a non-Segra entity. To the extent that such entity maintains its own drug/alcohol testing policy or program, Segra employees may be obligated to subject themselves to, and comply with that policy as a condition of continued employment with Segra. Compliance with the policies of other entities may include, but are not limited to, pre-site access testing, annual testing, random testing, reasonable suspicion testing, or post-accident testing.

6. Post-Accident Drug/Alcohol Screening: All workplace accidents, including vehicular accidents will require the employee to comply with drug/alcohol screening. Exceptions can be approved by Human Resources and/or Safety and Risk Manager.

7. Drug Testing Under U.S. Department of Transportation and Department of Defense Regulations: In addition to the testing occasions set forth above, employees who are required to maintain a Commercial Drivers License (CDL) are subject to random testing, periodic testing, post-accident/incident testing, and return-to-duty/follow-up testing under Department of Transportation Federal Motor Carrier regulations. At least 25% of these employees will be randomly tested on an annual basis. Any employee subject to testing under these provisions whose test results are positive will be removed from duty and will be subject to disciplinary action up to and including termination.

8. Testing Procedures: All drug and alcohol testing will be performed by an independent and highly reputable laboratory or health-care provider. All positive test results will be subject to confirmation testing.

9. Drug-Free Awareness Education includes, but is not limited to:

- Review of Employee Handbook with every new employee to include training on Company's Drug and Alcohol Use Policy, the dangers of illegal drugs in the workplace, and penalties imposed for violations of the policy;
- Training for management and supervisory employees regarding drug and alcohol abuse in the workplace, including training on identifying factors that may be indicative of drug/alcohol abuse;
- Information regarding drug counseling and rehabilitation programs, inclusive of referral to the Company's Employee Assistance Program.

Attachment

Reasonable Grounds Behavior Observations

Employee Name: _____ Date Observed: _____

Time Observed: From: _____ AM PM TO: _____ AM PM

Location: _____

Behavior Witnessed: (check all that apply)

1. Speech Patterns
   - Normal ☐ Slurs ☐
   - Unintelligible ☐ Quiet ☐
   - Confused ☐ Whispers ☐
2. Driving
   - Normal ☐ Near Collision ☐
   - Erratic ☐ Citations ☐
   - Multiple Accidents ☐ Missed Deliveries ☐
3. Movement/Balance
   - Normal ☐ Falls ☐ Unsteady ☐
   - Sways ☐ Holds to Balance ☐ Unable to maintain normal movement/balance ☐
   - Staggers ☐ Tremors ☐
4. Walking/Turning
   - Normal ☐ Falls ☐ Impaired ☐
   - Sways ☐ Stumbles ☐ Erratic ☐
   - Arms Raised (Balance) ☐ Reaches for support ☐
5. Awareness
   - Normal ☐ Stupor ☐ Lacks Coordination ☐
   - Confused ☐ Paranoid ☐ Impaired ☐
   - Sleepy ☐ Fearful ☐ Unresponsive ☐
6. Work Patterns
   - Normal ☐ Angry ☐ Disappears ☐ Refuses Direction ☐
   - Late for Work ☐ Tired ☐ Unresponsive ☐ Decrease Productivity ☐
   - Repeated Errors ☐ Dirty/Disheveled ☐ Failure to Report ☐ Overly Defensive ☐
7. Odor — Alcohol ☐ Marijuana ☐ Other _____

Comments: (Please detail reasons/causes for documenting observations)

Witness: _____

Signature: _____ Date: _____

SEGRA

Access Control Policy

Policies and Documentation

Document No.: **SEC200-09-01**

Title: **Access Control Policy**

SEGRA SM

Initial Author/Creator:	Edward Fahner	Original Date of Issue:	3/07/2022
Dir. IT Security Services:	Paul Southerington	Approval Date:	3/10/2022
Security Architect:	Edward Fahner	Approval Date:	3/10/2022
Chief Information Officer:	Rose Chambers	Approval Date:	3/22/2022
Chief Operating Officer:	Dan Watts	Approval Date:	4/22/2022
Chief Technology Officer:	Scott Wallhermfechtel	Approval Date:	5/04/2022
Chief Legal Officer:	Robin Dunson	Approval Date:	5/05/2022

REVISION HISTORY

Revision No.	Description	Revision Date	Author
00	Initial release.	8/15/2018	Edward Fahner
01	Updated legal company name	1/25/2021	Edward Fahner

TABLE OF CONTENTS

1. PURPOSE

This policy states access control principles set forth by the operating companies of MTN Infrastructure TopCo, Inc. (the Company) to protect information assets under the care of the Company.

2. SCOPE

This policy applies to all security policies, standards and procedures created, maintained and distributed for use by the Company or on the Company's behalf. All systems, data and infrastructure belonging to or entrusted to the Company, test, development, production or otherwise, is in scope. Any "unknown" system is in scope until demonstrated otherwise.

This does not apply to network access provided as a service. It does apply to devices, software and systems providing those services.

More granular policies, standards and procedures falling under this policy may have a more limited scope. For example, less general policies may apply only to the 5e switch or only to the Corporate IT Network, and may be maintained by different organizations.

3. DEFINITIONS

Policy - A high-level statement of company goals and objectives accompanied by a reference to relevant standards that provide more detailed direction for compliance.

Standards - Mandatory activities, actions, rules or regulations designed to provide policies with support structure and specific direction that they require to be meaningful and effective.

Procedures - The step-by-step process required for the implementation of the requirements set by standards.

Information Asset - Any data in any form, belonging to the Company or entrusted to the Company, and the equipment used to transmit, manage, process or store said data. This includes, but is not limited to, corporate, customer and third party data.

System - In the context of this policy; Any information processing device or software containing or transporting Information Assets, or any device providing network access or services. This could be any computer, server, software, database, network router, switch, transport equipment, etc.

Credentials - A common implementation is a username and password combination; however, credentials could be implemented using a wide variety of other technologies, examples of which are cryptographic certificates, token authenticators, passwords without a username and one time pads.

4. ACCESS CONTROL POLICY

4.1. Access to information assets and systems must be granted to, and only to, authorized persons or systems based on business and security requirements.

4.2. The privileges of all users, systems and programs must be restricted based on legitimate business need.

4.3. All multi-user systems containing non-public information assets must employ user identification systems to control access to said non-public information.

4.4. All Company system and network privileges must be promptly terminated at the time that a worker ceases to provide services to the Company.

4.5. In the event that an authorized user of Company systems changes their primary job function, it is the responsibility of the user's new manager or sponsor to notify the appropriate systems administrators of the person's new system access needs to remain complaint with 4.1.

4.6. Credentials

4.6.1. Every user or system must have unique credentials for access to Company multi-user systems and computers.

4.6.2. Shared, generic or group credentials may only be used if absolutely necessary and if specifically authorized by management.

4.6.3. Passwords must not be weak or trivial.

4.6.4. All individual and shared user login passwords must be changed periodically.

4.6.5. Systems that store password information must follow industry-standard best practices for hashing and encryption whenever possible.

4.6.6. Passwords must not be written down and left in a place where unauthorized persons might discover them.

4.6.7. All vendor-supplied default passwords must be changed before any computer or communications system is used for Company business.

4.6.8. Remote access to Company systems from public or non-Company networks must use multi-factor authentication.

4.6.9. Management must establish override facilities to be used in those exceptional circumstances where controls must be compromised to maintain on-going business operations. The ability to use override facilities must be severely restricted, and these facilities must be used only when absolutely necessary.

4.6.10. If a multi-user system employs fixed passwords as its primary access control mechanism, all passwords on that system must be changed immediately after evidence of system compromise has been discovered, and all users must change their fixed passwords on other machines, if the passwords on the compromised machine are also used on these other machines.

4.6.11. Where possible, authentication credentials must not be visibly displayed when entered.

4.7. Record Keeping and Audit

4.7.1. All requests for additional privileges on Company multi-user systems or networks must be submitted on a completed system access request form.

4.7.2. So that their privileges may be expediently revoked on short notice, current access control records reflecting all systems on which users have credentials must be maintained.

4.7.3. All override facility usage must be logged.

4.7.4. Whether successful or not, all attempts to log in to Company production information systems must be logged.

4.7.5. The identity of every user who accesses private information resident on Company information systems must be logged.

4.7.6. All user ID approvals, creation, deletion, and privilege change activity performed must be logged.

4.7.7. Operations staff or information security staff must review records reflecting security relevant events on all production multi-user machines in a periodic and timely manner.

4.7.8. Systems administrators must ensure that access granted to their system remains appropriate through the use of periodic reviews.

4.8. Responsibilities

4.8.1. Managers are responsible for assuring their team members follow this policy for the technologies and processes they design or implement.

4.8.2. The Information Security team is responsible for maintaining this policy.

5. NIST ALIGNMENTS

- NIST CSF 1.1 PR.AC-1 Identities and credentials are issued, managed, revoked, and audited
- NIST CSF 1.1 PR.AC-3 Remote access is managed
- NIST CSF 1.1 PR.AC-4 Access permissions and authorizations are managed, incorporating least privilege and separation of duties
- NIST CSF 1.1 PR.AC-6 Identities are proofed and bound to credentials, and asserted in interactions when appropriate
- NIST CSF 1.1 PR.PT-1 Audit/log records are determined, documented, implemented, and reviewed in accordance with policy
- NIST SP 800-53 Rev. 4 AC-1 Access Control Policy and Procedures
- NIST SP 800-53 Rev. 4 AC-2 Account Management
- NIST SP 800-53 Rev. 4 AC-3 Access Enforcement
- NIST SP 800-53 Rev. 4 IA Identification and Authentication
- NIST SP 800-53 Rev. 4 AU Audit and Accountability

6. RECORD OF FEEDBACK

September 6, 2018 - Morgan Brown, Director OSP - email, No Comment

September 6, 2018 - Jennifer Benson, Purchasing Supervisor - email, No Comment

September 6, 2018 - Anthony Ratliff, Manager Network Planning OSP - email, No Comment

September 6, 2018 - Corinne P. Cox, Sr. Director, IT - email, No Comment

September 7, 2018 - Greg Guerra, Chief Operating Officer - email, No Comment

September 7, 2018 - John Lewis, VP IT Operations - email, requested a definition of "override facility", otherwise no comments.

September 7, 2018 - Josh Wolff, SVP/GM Datacenters - email, No Comment

September 7, 2018 - Scott Wallhermfechtel - email, requested 4.1 include authorized systems, policy modified to include this

September 7, 2018 - Scott Snyder, Director Network Planning - email, No Comment

September 7, 2018 - Brian Ramsey, Director of Voice Operations - email, No Comment

September 10, 2018 - Dave Binford, Director Network Engineering - email, No Comment

September 10, 2018 - Zoey Fahner, NOC Engineer III - email, No Comment

September 10, 2018 - Doug James, Network Engineer - email, No Comment

September 10, 2018 - Mary McDermott, SVP General Counsel & Secretary - email, request to include NIST alignment and references, added the NIST alignments

September 10, 2018 - Bill Sabo, Director Program Management - email, No Comment

September 13, 2018 - Paul Southerington, Manager IT Assurance - email, No Comment

September 13, 2018 - Anthony Ratliff, Manager Network Planning OSP - email, No Comment

September 13, 2018 - Josh Wolff, SVP/GM Datacenters - email, No Comment

September 13, 2018 - Mike Wallace, IT Security Manager - email, No Comment

September 13, 2018 - Justin Okonski, Network Engineer - email, No Comment

September 13, 2018 - Corey Fisher, NOC Manager - email, No Comment

September 13, 2018 - Victor Vandevander, NOC Engineer III - email, No Comment

September 13, 2018 - Bradley Frye, Director Network Engineering & Planning - email, No Comment

September 13, 2018 - Mike Fridley, SR MGR Engineering - email, No Comment

6.1. Historic Approvals

Current approvals are at the top of this document.

September 17, 2018 - Paul Southerington, Manager IT Assurance

September 17, 2018 - Edward Fahner, Security Architect

September 17, 2018 - BC Bridger, VP Information Technology

September 18, 2018 - Tom Ferry, CTO & SVP of Engineering

September 21, 2018 - F. Gregory Guerra, Chief Operating Officer

September 21, 2018 - Diego Anderson SVP / GM RSB

September 21, 2018 - Ethan Joshua Wolff, SVP / GM Lumos Data Centers

September 24, 2018 - Johan G. Broekhuysen, Chief Financial Officer

September 24, 2018 - Mary McDermott, General Counsel

January 25, 2021 – Edward Fahner, Security Architect

January 26, 2021 – Paul Southerington, Dir. IT Security Services

February 1, 2021 – Bruce T. Dyke, Chief Information Officer

February 2, 2021 – Jason W Campbell, Chief Operating Officer

March 16, 2021 – Peter Zarrella, Chief Financial Officer

March 16, 2021 – Mary McDermott, General Counsel

SEGRA

Physical and Environmental Security Policy

Initial Author/Creator:	Edward Fahner	Original Date of Issue:	3/07/2022
Dir. IT Security Services:	Paul Southerington	Approval Date:	3/10/2022
Security Architect:	Edward Fahner	Approval Date:	3/10/2022
Chief Information Officer:	Rose Chambers	Approval Date:	3/22/2022
Chief Operating Officer:	Dan Watts	Approval Date:	4/22/2022
Chief Technology Officer:	Scott Wallhermfechtel	Approval Date:	5/04/2022
Chief Legal Officer:	Robin Dunson	Approval Date:	5/05/2022

REVISION HISTORY

Revision No.	Description:	Revision Date:	Author
00	Initial release.	9/17/2018	Edward Fahner
01	Updated legal company name	1/25/2021	Edward Fahner
02	Removed no longer applicable DOJ visitor log requirement	03/07/2022	Edward Fahner
		Click here to enter a date.	
		Click here to enter a date.	

TABLE OF CONTENTS

1. PURPOSE

The purpose of the Physical Security Policy is to outline the responsibilities and expectations for the physical security of information assets managed by the operating companies of MTN Infrastructure TopCo, Inc. (the Company). The controls described in this policy and other policies in the SEC series of documents are collectively known as Company Security Program, which is designed to reflect the Company's business objectives, prevent the unauthorized use of or access to our information systems and maintain the confidentiality, integrity and availability of information assets.

2. SCOPE

This policy applies to all Company entities, employees, contractors and third-party partners, visitors as well as all office spaces, equipment areas, equipment and systems used by or supporting the Company.

This policy does not apply to physical spaces sold to customers in the form of a colocation product. The security requirements for customer colocation spaces dictated and enumerated by product requirements.

This policy does not apply to customer managed facilities or equipment where the Company has placed equipment for the sole purpose of providing service to said facility.

3. Physical and Environmental Security Policy

3.1 Information assets must be housed securely and protected against identified risks.

3.2 Physical Security Perimeter

3.2.1 Security Perimeters must be defined and used to protect areas that contain ether sensitive or critical information and information processing facilities.

3.2.2 Clearly defined security areas (such as "equipment room", "office space", or "data center") must be separated by physical perimeter barriers (walls, cages, etc.) with controlled entry/exit points.

3.2.3 Perimeters must be physically sound, with no gaps in the perimeter or areas where a break-in could easily occur.

3.2.4 Doors to security areas must be access controlled and must not be left unlocked or open.

3.2.5 Door access systems must be interlocked to the fire alarm system such that doors unlock or open according to the minimum requirements of the local fire code.

3.2.6 Emergency services personnel must be able to gain access to any area in an emergency, for instance using key-cards held securely by facilities or site security.

3.3 Physical Entry Controls

3.3.1 Secure areas must be protected by appropriate entry controls to ensure that only authorized personnel are allowed access.

3.3.2 Personnel must be screened according to the Company's documented screening process in order to be granted access to equipment areas.

3.3.3 Non-screened personnel must be escorted by screened personnel at all times while in equipment areas.

3.3.4 Visitors must only be granted access for specific, authorized business purposes.

3.3.5 All access to secure areas must be logged.

3.3.6 Access logs must be periodically reviewed.

3.3.7 Access rights to secure areas must be regularly reviewed and updated.

3.4 Delivery and Loading Areas

3.4.1 Incoming material must be registered in accordance with asset management procedures on entry to the site.

3.4.2 Incoming material must be inspected for evidence of tampering or damage en route. If such tampering is discovered it must be immediately reported to facilities management.

3.5 Equipment Siting and Protection

3.5.1 No eating, drinking or smoking is permitted in proximity to information processing equipment.

3.5.2 Automatic temperature and humidity controls must be used where needed to prevent fluctuations harmful to information systems.

3.5.3 Environmental conditions such as temperature or humidity must be monitored for conditions which could adversely affect the operation of information processing equipment.

3.5.4 Manufacturer's instructions for protecting equipment against environmental hazards must be observed at all times, e.g. protection against exposure to extreme temperatures.

3.6 Supporting Utilities

3.6.1 Equipment should be protected from power failures and other disruptions caused by failures in supporting utilities (e.g. electricity, HVAC, water, gas).

3.6.2 Supporting utilities must be appraised regularly for their capacity to meet business growth.

3.6.3 Supporting utilities must be inspected and tested regularly to ensure their proper function.

3.6.4 Utilities supporting information processing equipment must be alarmed to detect malfunctions.

3.6.5 Emergency lighting and communications must be provided.

3.7 Data Loss Prevention

3.7.1 Equipment and media taken off premises must not be left unattended in public places.

3.7.2 Storage media, systems or network devices containing confidential data (e.g. customer network configurations, names of customers, financial information) must be destroyed, erased, or have all confidential data overwritten using techniques to make the original information non-retrievable before equipment disposal or re-use.

3.8 Responsibilities

3.8.1 Users detecting violations of this policy must immediately report the violation to their direct manager, who must verify the nature of the violation and report it to Company management, as appropriate. A determination must be made by appropriate management as to the extent of risk that any non-compliance condition presents and what remediation activities are required.

3.8.2 Users who deliberately violate information security policies will be subject to disciplinary action up to and including termination of employment or association with the Company.

3.8.3 This policy is owned jointly by Facilities and the Company's Cyber Security organizations, who are responsible for the content, review and upkeep of the related documentation. The policy must be reviewed periodically (at least annually), or after any major changes to Company business practices or processing environment(s), to ensure that the contents remain appropriate. New revisions of the policy must be documented and published.

4. NIST ALIGNMENTS

This policy aligns with the following NIST controls

- 800-53 r4 PE-2 Physical Access Authorizations
- 800-53 r4 PE-3 Physical Access Control
- 800-53 r4 PE-11 Emergency Power
- 800-53 r4 PE-12 Emergency Lighting
- 800-53 r4 PE-14 Temperature And Humidity Controls
- 800-53 r4 MP-6 Media Sanitization
- CSF PR.AC-2 Physical access to assets is managed and protected
- CSF PR.IP-5 Policy and regulations regarding the physical operating environment for organizational assets are met
- CSF PR.IP-6 Data is destroyed according to policy

5. Record of Feedback

)18/9/27 - Zoey Fahner, NOC Engineer III - email, No comment
2018/9/27 - Nathan Wall, Senior Engineer - email, No comment
2018/9/27 - Morgan Brown, Director OSP - email, No comment
2018/9/27 - Jack Wade, Director OSP Engineering - email, No comment
2018/9/27 - Josh Wolf, SVP/GM Datacenters - email, No comment
2018/9/27 - Victor Vandevander, NOC Engineer III - email, No comment
2018/9/27 - Justin Okonski, Network Engineer - email, No comment
2018/9/27 - Marcos Correa, NOC Manager - email, No comment
2018/9/27 - Bill Sabo, Program Management - email, No comment
2018/9/27 - Syed Qtub Ahmed, Senior Engineer - No comment
2018/9/27 - Brian Ramsey, Director of Voice Operations - No comment
2018/9/28 - Scott Wallhermfechtel, VP Network Operations - email, No comment
2018/9/28 - Johan Broekhuysen, CFO - email, no changes requested
2018/9/30 - Jennifer Benson, Purchasing Supervisor - email, No comment
2018/9/30 - Corinne Cox, Sr. Director IT - email, No comment

5.1 Historic Approvals

Current approvals are at the top of this document.

October 17, 2018 - Paul Southerington, Manager IT Assurance
October 16, 2018 - Edward Fahner, Security Architect
October 18, 2018 - Tom Ferry, CTO & SVP of Engineering
:tober 23, 2018 - F. Gregory Guerra, Chief Operating Officer
Jctober 19, 2018 - Diego Anderson SVP / GM RSB
October 19, 2018 - Ethan Joshua Wolff, SVP / GM Lumos Data Centers
November 12, 2018 - Johan G. Broekhuysen, Chief Financial Officer
November 1, 2018 - Mary McDermott, General Counsel

SEGRA

Network Communications Policy

Policies and Documentation

Document No.: **SEC200-13-01**

Title: **Network Communications Policy**

Initial Author/Creator:	Edward Fahner	Original Date of Issue:	3/07/2022
Dir. IT Security Services:	Paul Southerington	Approval Date:	3/10/2022
Security Architect:	Edward Fahner	Approval Date:	3/10/2022
Chief Information Officer:	Rose Chambers	Approval Date:	3/22/2022
Chief Operating Officer:	Dan Watts	Approval Date:	4/22/2022
Chief Technology Officer:	Scott Wallhermfechtel	Approval Date:	5/04/2022
Chief Legal Officer:	Robin Dunson	Approval Date:	5/05/2022

REVISION HISTORY

Revision No.	Description:	Revision Date:	Author
00	Initial release.	11/12/2018	Edward Fahner
01	Updated legal company name.	1/25/2021	Edward Fahner
		Click here to enter a date.	
		Click here to enter a date.	
		Click here to enter a date.	

TABLE OF CONTENTS

1. Purpose

This policy documents a set of rules, advised by security architecture, mandated by Senior Management, in order to protect information assets under the care of the operating companies of MTN Infrastructure TopCo, Inc. (the Company). This document should be viewed as a mandate from the signers for the business to implement the described policy controls.

2. Scope

This policy applies to all security policies, standards and procedures created, maintained and distributed for use by the Company or on the Company's behalf. All systems, data and infrastructure belonging to or entrusted to the Company, test, development, production or otherwise, is in scope. Any "unknown" system is in scope until demonstrated otherwise.

This does not apply to network access provided as a service. It does apply to devices, software and systems providing those services.

More granular policies, standards and procedures falling under this policy may have a more limited scope. For example, less general policies may apply only to the 5e switch or only to the Corporate IT Network, and may be maintained by different organizations.

3. Definitions

Confidential - Confidential information is any information, proprietary to the business of the Company and details of which are generally not known or made available to the public, that if disclosed, could cause an adverse impact to the Company or its Affiliates, employees, stockholders, business partners or customers. Adverse impact includes financial loss, gains to competitors, embarrassment, loss of confidence or loss of standing in the community.

Demilitarized Zone - A demilitarized zone (DMZ) is a logical network inserted as a neutral zone between public and private networks. A DMZ is filtered such that a public network may communicate with the DMZ in a limited fashion, a private network and the DMZ may communicate in a limited fashion, and the public network may not communicate directly with the private network.

Firewall - A firewall includes stateless packet filters, stateful packet filters and/or application layer filters running on any device.

Logical Network - An abstract network where a network signaling protocol is shared. In common practice this is an IP routing domain or ethernet broadcast domain, segmented from other logical networks using a security gateway such as an air gap, firewall or similar. A single logical network can span multiple organizations and physical topologies. Multiple logical networks can exist on the same physical topology.

Private Network - A logical network that is intended to be accessible only by identified and specifically permitted parties. A private network can transport or tunnel a public network without becoming a public network. A private network that interacts with a public network can unintentionally become a public network.

Public Network - A logical network accessible via network protocols to an unidentified or not specifically permitted third party. A public network is not trusted. From the perspective of the Company, network access provided as a service is public.

System - Any information processing device or software containing or transporting Information assets, or any device providing network access or services. This could be any computer, server, software, database, network router, switch, transport equipment, etc.

4. Network Communications Policy

4.1 Systems and networks must be segregated into separate physical or logical networks according to trust levels and information security risk.

4.2 Placement of a specific system onto a specific logical network segment must likewise be based on risk and trust levels.

4.3 Logical network boundaries must employ control mechanisms that enforce segregation. Examples include but are not limited to

- firewalls
- physical isolation
- tunneling

4.4 Company systems must not be on a public network unless providing a service to unknown third parties on said public network.

4.5 Systems that require communications with both public and private networks must be protected by firewalls and be located within a demilitarized zone (DMZ).

4.6 Systems on a private network communicating with systems in a DMZ must be protected from the DMZ network by one or more firewalls.

4.7 All networks crossing national boundaries must be broken into separately defined logical network domains.

4.8 Wireless networks must always be treated as unique logical network segments.

4.9 Company managed logical network segments, their boundaries and the controls enacted between them must be centrally documented.

4.10 Control mechanisms between logical network boundaries must be periodically reviewed, and the results of such review must be documented.

4.11 Security mechanisms, service levels and management requirements of all network services should be identified and included in network services agreements, whether these services are provided in-house or purchased.

4.12 Operational responsibility for network boundary enforcement should be separated from application/server operations.

4.13 Confidential Company data passing over public networks or any network with risk of being made public must be encrypted.

4.14 Controls must be in place to prevent the attachment of unauthorized devices to Company managed networks.

4.15 Responsibilities

4.15.1 Managers are responsible for assuring their team follows this policy for the technologies and processes they design or implement.

4.15.2 The Information Security team is responsible for maintaining this policy.

5. REFERENCES

This document is based on

ISO/IEC 27001:2013: Information Technology - Security Techniques - Information Security Management Systems - Requirements. International Organization for Standardization, Geneva, Switzerland.

ISO/IEC 27002:2013: Information Technology - Security Techniques - Code of practice for information security controls. International Organization for Standardization, Geneva, Switzerland.

6. NIST ALIGNMENTS

- NIST CSF 1.1 PR.AC-3, PR.AC-5, PR.DS-2, PR.PT-4, ID.AM-3
- NIST SP 800-53 Rev. 4 CA-3, SC-7, SC-8
- NIST SP 800-53 Rev. 4 AC-4, AC-17, AC-18

7. Record of Feedback

2018/11/12 Alesia Truxell, Sr Mgr Project Management, email - update document with new approval list
2018/11/12 Greg Guerra, COO, email - No comment
2018/11/12 Mike Fridley, Senior Manager of Design, email - No comment
2018/11/12 Andrew Marcovsky,Senior Product Manager, email - No comment
2018/11/12 Jack Wade, Director OSP Engineering, email - No comment
2018/11/12 John Douglas, VP IT, email - update document with new approval list
2018/11/12 Dan Watts, VP Product Management and Business Development, email - No comment
2018/11/12 Brian Dempsey, Senior Network Engineer, email - No comment
2018/11/12 Zoey Fahner, NOC Engineer III, email - No comment
2018/11/12 Bill Sabo, Director Program Management, email - update document with new approval list
2018/11/12 Ryan Barber, NOC Engineer II, email - No comment
2018/11/12 Nathan Wall, Senior Engineer, email - No comment
2018/11/12 Derek Jennings, Senior Network Engineer, email - No comment
2018/11/13 Victor Vandevander, NOC Engineering III, email - No comment
2018/11/13 Mary McDermott, SVP General Counsel / HR, email - No comment
2018/11/13 Justin Okonsky, Network Engineer, email- No comment
2018/11/14 Denise Yurish, Sr Director Supply Chain and Facilities, email - No comment
2018/11/14 Jed Kennedy, Sr Director Network Strategy, email - No comment

8. Historic Approvals

Current approvals are at the top of this document.

December 11, 2018 - Paul Southerington, Manager IT Assurance
December 11, 2018 - Edward Fahner, Security Architect
December 12, 2018 - Tom Ferry, CTO & SVP of Engineering
December 18, 2018 - F. Gregory Guerra, Chief Operating Officer
December 17, 2018 - Diego Anderson SVP / GM RSB
December 17, 2018 - Ethan Joshua Wolff, SVP / GM Lumos Data Centers
December 20, 2018 - Johan G. Broekhuysen, Chief Financial Officer
December 20, 2018 - Mary McDermott, General Counsel
January 25, 2021 – Edward Fahner, Security Architect
January 26, 2021 – Paul Southerington, Dir. IT Security Services
February 1, 2021 – Bruce T. Dyke, Chief Information Officer
February 2, 2021 – Jason W Campbell, Chief Operating Officer
March 16, 2021 – Peter Zarrella, Chief Financial Officer
March 16, 2021 – Mary McDermott, General Counsel

SEGRA

Supplier Relationships Security Policy

Policies and Documentation

Document No.: **SEC200-15-06**

Title: **Supplier Relationships Security Policy**

SEGRA SM

Initial Author/Creator:	Edward Fahner	Original Date of Issue:	3/07/2022
Dir. IT Security Services:	Paul Southerington	Approval Date:	3/10/2022
Security Architect:	Edward Fahner	Approval Date:	3/10/2022
Chief Information Officer:	Rose Chambers	Approval Date:	3/22/2022
Chief Operating Officer:	Dan Watts	Approval Date:	4/22/2022
Chief Technology Officer:	Scott Wallhermfechtel	Approval Date:	5/04/2022
Chief Legal Officer:	Robin Dunson	Approval Date:	5/05/2022

Revision History

Revision No.	Description:	Revision Date:	Author
00	Initial release.	10/20/2017	Edward Fahner
03	Added statement indicating outsourcers subject to other documents, added nist alignments	1/16/2018	Edward Fahner
04	Added policy items requiring management and regulatory review	3/12/2018	Edward Fahner
05	Updating for joint company using verbiage from Mike Wallace's Spirit policy	1/9/2019	Edward Fahner
06	Updated legal company name, changed "CTO" to "business owner VP" in 4.6 to reflect current titles and responsibilities	1/25/2021	Edward Fahner
07	Removed DOJ/USG approval, changed "principal equipment" to "information infrastructure"	03/07/2022	Edward Fahner

TABLE OF CONTENTS

1. PURPOSE

To ensure protection of the organization's assets that are accessible by suppliers and to maintain an agreed level of information security and service delivery from suppliers.

2. SCOPE

This policy applies to all policies, standards and procedures created, maintained and distributed by the employees and partners of the operating companies of MTN Infrastructure TopCo, Inc. (the Company). All systems, data and infrastructure belonging to or entrusted to the Company is in scope. Any "unknown" system is in scope until demonstrated otherwise.

More granular policies, standards and procedures falling under this policy may have a more limited scope. For example, less general policies may apply only to a specific business unit or set of systems, and may be maintained by different organizations within the Company.

3. DEFINITIONS

adverse impact - Adverse impact includes financial loss, gains to competitors, embarrassment, loss of confidence or loss of standing in the community for/to the Company, its affiliates, employees, stockholders, business partners or customers.

confidential - Confidential information is any information, proprietary to the business of the Company and details of which are generally not known or made available to the public, that if disclosed, could cause an adverse impact.

contractor - In context of this policy, a **contractor** is an individual hired as a contingent worker.

information Infrastructure - includes but is not limited to HVAC, power, fire supression, network, live or active fiber optic cable or wiring, servers, Segra PCs/laptops, routers, switches, virtual machines, cloud services, systems, software, batteries, CPEs, DSLAMs, MUXs, DACs

outsourcer - A person or organization which provides goods or services by contract from outside the Company; an external supplier of goods or services; a vendor; a business service provider who assumes responsibility for performing a specific business process of the Company.

risk management team (Company team) - An informal organization consisting of Information Security, Legal, Finance, business leaders and any relevant subject area experts.

sensitive - For this policy, **sensitive** is something that could potentially be leveraged to cause an adverse impact to the Company through misuse, mistake or malice. Confidential information is sensitive. A fuse panel that could power off important equipment is sensitive.

U.S. Records - Customer billing records, subscriber information, and any other material information used, processed, or maintained in the ordinary course of business relating to the services offered by the Company in the U.S., including the content of of communications recorded by the Company. U.S. Records includes information subject to disclosure to a U.S. Federal or state government entity under the procedures specified in Section 2703(c) and (d) and Section 2709 of Title 18 of the U.S. Code. US Records are a sensitive information asset and are confidential.

4. POLICY

4.1 Individual contractors hired as contingent workers must be vetted as per the Company's Human Resource policies.

4.2 A process to identify new third-party relationships will be in place.

4.3 Risk based due diligence must be performed on prospective third parties before contracts are signed, including reviews of:

- Third party company's reputation and history
- Quality of services provided to other customers
- Number and competence of staff and managers
- Financial stability of the company and commercial record
- Quality assurance and security management standards currently followed by the company (ex. Certified compliance with ISO9000 or ISO/IEC 27001)
- Ownership by a foreign entity or non-US based operations
- Results of a risk assessment

4.4 Business owners, with help from the risk management team as needed, will conduct and present the results of a risk assessment to management prior the signing of an outsourcing contract.

4.4.1 The risk assessment must include

- Nature of logical and physical access to the Company's information assets and facilities
- Sensitivity, volume and value of information assets involved
- Commercial risks such as the possibility of the outsourcer's business failing completely, or of them failing to meet agreed service levels or providing services to the Company's competitors where that might create a conflict of interest
- Mitigating security and commercial controls known to be employed by the Company and/or the outsourcer

4.5 If the outsourcer is to be given any sensitive access or information assets, a formal contract between the Company and the outsourcer must exist to protect both parties.

4.5.1 The contract shall clearly define the type of access granted or information exchanged and the purpose for doing so.

4.5.2 If information being exchanged is confidential a binding confidentiality agreement shall be in place between the Company and the outsourcer.

4.5.3 Contracts must acknowledge that the outsourcer is responsible for the security of Company confidential data that it possesses, stores or transmits.

4.5.4 All contracts shall be submitted the Company's legal counsel for review.

4.5.5 Depending on the risk assessment, contract should;

- Restrict "offshore" access, storage or subcontracting
- Acknowledged that the third party is responsible for the security of the Company's confidential data that it possesses, stores or transmits.
- Require the return or destruction of data upon contract termination
- Require notification to Company of security events or incidents affecting Company data
- Agree to participate in the Company's change management controls
- Agree that the Company may monitor the service provided by outsourcer, audit the outsourcer's compliance with the contract, review and validate outsourcer's security controls, or employee a mutually agreed independent third party auditor for this purpose

4.6 New outsourcers involved in providing, installing, operating, managing or maintaining Information Infrastructure must be reported to and approved by the business owner VP and Chief Legal Officer.

4.7 If parts of the Company's information infrastructure are hosted at third party locations, the third party operator shall ensure the Company's assets are physically and/or logically isolated from other systems depending on the nature of the service provided.

4.8 The Company will periodically audit third party facilities or services to ensure they are in compliance with the Company's security policies and to ensure all contractually agreed requirements are being met.

4.9 The Company shall ensure that all sensitive information assets given to the outsourcer are retrieved or destroyed on or before the termination of the outsource contract.

4.10 Outsourcers are subject to all Company security policies and procedures when interacting with the Company's information assets or visiting Company facilities.

4.11 Responsibilities

4.11.1 Management is responsible for designating owners of business process that are outsourced, overseeing the outsourcing activities and ensuring this policy is followed.

4.11.2 Designated owners of outsourced business processes are responsible for assessing and managing the commercial and security risks associated with outsourcing, working with Information Security, Legal and other functions as necessary.

4.11.3 Information Security, in conjunction with Legal and Risk Management is responsible for assisting outsourced business process owners to analyze the associated risks and develop appropriate process and controls.

4.11.4 Information Security is responsible for maintaining this policy.

4.11.5 Internal Audit is authorized by management to assess compliance with all corporate policies at any time.

5. REFERENCES

This document is based on;

ISO/IEC 27001:2013: Information Technology - Security Techniques - Information Security Management Systems - Requirements. International Organization for Standardization, Geneva, Switzerland.

ISO/IEC 27002:2013: Information Technology - Security Techniques - Code of practice for information security controls. International Organization for Standardization, Geneva, Switzerland.

Aaron d'Souza and Gary Hinson 2008. ISO 27001 Security Information Security Policy on Outsourcing. Generic sample policy published at www.ISO27001security.org

Spirit Communications Policy Manual - Mike Wallace

6. NIST ALIGNMENTS

- 800-53r4 PS-7 Third Party Personnel Security
- 800-53r4 SA-9 External Information System Services
- 800-53r4 SA-12 Supply Chain Protection
- NIST CSF 1.1 ID.SC Supply Chain Risk Management

7. Record of Feedback

- 2017/10/20 Sherri Yowell, Director of Human Resources - face to face, agreed for vendor security policy to reference the HR policy for contingent workers, HR contingent worker policy updated to include necessary vetting
- 2017/10/20 Johan Broekhuysen, CFO - email, request to add language concerning nation of origin to 4.2 evaluation criteria, requested operational reporting with requirements, otherwise OK
- 2017/10/22 Paul Southerington, Manager IT Assurance Services - email, request to add encryption as a recommended contractual control, requested edits to "physical and logically isolated" where it's impossible (cloud), requested clarity in audit clause (edited for clarity)
- 2017/10/23 Jay Martin, Sr. Director Product Management - email, no changes, forwarded to others for comment
- 2017/10/23 John Lewis, VP Information Technology - email, requested definitions, implementation discussion/recommendations
- 2017/10/23 William Sabo, Director Program Management - email, no changes requested, forwarded to others for comment
- 2017/10/23 Brian Ramsey, Director of Voice Operations - email, OK with policy as is
- 2017/10/23 David Anderson, Senior Architect - email, no changes requested
- 2017/10/23 Scott Wallhermfechtel, VP Network Engineering and Operations - email, concerns about definition and usage of "sensitive", concerns around the monitor and audit clauses, both of which were edited for clarity, implementation discussion/recommendations
- 2017/10/23 Sherri Yowell, Director of Human Resources - email, looks good as is
- 2017/10/23 Janet Cole, Manager of Contingent Staffing - email, verified incorporation into contractor processes, no changes requested
- 2017/10/23 Josh Wolff SVP/GM Data Centers - email, aggregated responses from team including Chris Allgauer, Director of Technical Operations and Rolando Stinson, Director of Data Center Operations. Questions about scoping for when a contract/risk assessment is required, changes made for clarity. Concerns about required physical segregation with certain types of services where that's impossible (cloud), edited to accommodate.
- 2017/10/23 Bret Phillips, Director Internal Audit - email, no changes
- 2017/10/25 Jack Wade, Director OSP Engineering - email, no changes
- 2017/10/25 Morgan Brown, Director OSP - email, no changes
- 2017/10/25 Michael Cardoso, Director Network Operations - email, no changes
- 2017/10/25 Paul Southerington, Edward Fahner - formal approval
- 2017/10/26 David Lee Smith, John Lewis, Scott Wallhermfechtel, Joshua Wolff, Diego Anderson, Tom Ferry - formal approval
- 2018/1/15 Mary McDermott, SVP General Counsel - meeting, request for a control indicating outsourcer's are subject to Company's other policies such as the facilities security plan
- 2018/3/05 Mary McDermott, SVP General Counsel - formal approval
- 2018/3/12 Johan Broekhuysen, CFO - email, request addition of approval controls to meet regulatory requirements
- **2019/01/09 - Major revision** - revising for new company
- 2019/01/15 - Mary McDermott, SVP General Counsel - requested meeting with her staff to review
- 2019/01/15 - Scott Wallhermfechtel, VP Network Operations - email, changes to company branding
- 2019/01/15 - Johan Broekhuysen, CFO - email, no changes
- 2019/01/18 - Sherri Yowell (Director HR), Jen Marshall (Regulatory Manager), Mary McDermott (SVP GC) - meeting, no changes
- 2019/01/22 - Michael Fuqua, VP IT - email, changes to branding in this policy, improvements to supporting process

7.1 Historical Approvals

Current approvals are at the top of this document.

January 29, 2019 - Paul Southerington, Manager IT Assurance
January 29, 2019 - Edward Fahner, Security Architect
January 29, 2019 - Michael R. Fuqua, VP Information Technology
January 29, 2019 - Tom Ferry, CTO & SVP of Engineering
January 31, 2019 - F. Gregory Guerra, Chief Operating Officer
January 29, 2019 - Diego Anderson SVP / GM RSB
January 29, 2019 - Johan G. Broekhuysen, Chief Financial Officer
January 29, 2019 - Mary McDermott, General Counsel
January 25, 2021 – Edward Fahner, Security Architect
January 26, 2021 – Paul Southerington, Dir. IT Security Services
February 1, 2021 – Bruce T. Dyke, Chief Information Officer
February 2, 2021 – Jason W Campbell, Chief Operating Officer
March 16, 2021 – Peter Zarrella, Chief Financial Officer
March 16, 2021 – Mary McDermott, General Counsel

SEGRA

Information Systems Acceptable Use Standard

Document No.: SEC201-06-04-210126

Title: **Acceptable Use Standard**

Initial Author/Creator:	Edward Fahner	Original Date of Issue:	3/8/2021
Dir. IT Security Services:	Paul Southerington	Approval Date:	3/10/2022
Security Architect:	Edward Fahner	Approval Date:	3/10/2022
Chief Information Officer:	Rose Chambers	Approval Date:	3/22/2022

Revision History

Revision No.	Description:	Revision Date:	Author
00	Initial release.	2/7/2019	Edward Fahner
03		2/12/2019	Edward Fahner
04	Updated legal company name	1/26/2021	Edward Fahner
05	Accepted edits by Fuqua; replaced usage of "corporate" with "Company", inserted "Company" where ownership may be unclear	2/26/2021	Edward Fahner
		Click here to enter a date.	

TABLE OF CONTENTS

1. Purpose

is standard outlines the acceptable use of information systems at the operating companies of MTN Infrastructure TopCo, Inc. (Company) in order to protect both the employee and the company. Inappropriate use exposes the Company to additional risks including financial loss, loss of reputation, loss of service, privacy breach of customer or employee confidentiality, corruption of data and legal issues.

Effective security is a team effort involving the participation and support of every Company employee and affiliate who deals with information and/or information systems of the Company. It is the responsibility as condition of employment of every Company employee who uses Company systems, computers and networks to know these guidelines, and to conduct their activities accordingly.

2. Scope

This standard applies to all permanent or temporary users of Company internal-use information resources and systems, regardless of whether users are directly employed by the Company or a third party.

This standard applies to all equipment owned or leased by the Company, to all equipment attached to Company internal networks including the management areas of the service providing networks, usage of externally hosted ("cloud ") services, and any internal use of Company product offerings.

This standard does not otherwise apply to Company products or customers using those products, regardless of their relationship with the Company.

3. Definitions

PNI – Customer Proprietary Network Information, as defined by the FCC. Includes information about customers, their call records, and the services provided to them.
Extranet – External networks of partners or customers connected to our intranet
Executive Officer - A member of executive management that reports directly to the CEO
Internet – Sites and networks external to the Company Intranet. This includes networks and systems managed by the Company that are publicly reachable from third party networks.
Intranet – The Company internal networks that are intended to be accessible only by identified and specifically permitted parties, mostly consisting of Company employees and contractors.
Malware – Any software program or component that is malicious in nature, including viruses, spyware, worms, and security exploits
Spam – Unauthorized and/or unsolicited electronic mass mailings
Information Resource – Internet/Intranet/Extranet-related systems, including but not limited to computer equipment, software, operating systems, network equipment, servers, storage media, network accounts providing electronic mail, WWW browsing, and other network access.

4. Acceptable Use Standard

Information resources will be used in a Company approved, ethical, and lawful manner which avoids loss or damage to Company operations, image, or financial interests. Use of information resources must comply with official policies and procedures on acceptable use as described below; with all other Company policies; and with all local, state and federal law and regulations.

Under no circumstances is an employee of Company ever authorized to engage in any activity that violates local, state, federal, or international law or regulations.

4.1 General Use and Ownership

4.1.1 Personal use

Occasional personal use of systems is permitted provided it does not interfere with the performance of the employee's Company duties; does not create additional costs, risks or burden to the company; and does not violate any law, regulation, or Company corporate policy.

Individual Company departments may provide guidelines concerning personal use of information resources, with the understanding that departmental guidelines do not supersede Company policy, and those departmental guidelines must adhere to Company policy and standards. In the absence of such Company departmental policies, or if there is any uncertainty, employees should consult their manager and or Company Information Security Department.

4.1.2 Account responsibility

Each employee is responsible for all activity performed with his/her Company accounts.

If a Company account or Company PC is suspected lost or stolen the employee is responsible for reporting it to their manager and Company Information Security.

4.1.3 Public Image

Employees should avoid making statements that misrepresent or defame the Company on internet forums or social media sites, whether connected via corporate networks or personal systems.

Employees must follow any established Company policies regarding communications or social media.

4.1.4 Content responsibility

Each Employee is responsible for all content placed on Company systems or transmitted over Company networks.

4.2 Security and Proprietary Information

4.2.1 Confidential information

Employees should take all necessary steps to prevent unauthorized access to Company confidential information and follow the guidelines of the Company HR Confidentiality/Proprietary Information policy.

4.2.2 Password responsibility

All users are responsible for the security of login account information, including passwords and other forms of credentials to Company systems, equipment and networks. Users must keep credentials secure and not share account information. Users should report any request for their password(s) or account information to both their manager and Company Information Security.

Passwords must be changed periodically. Passwords must be created and managed in accordance with Company published policy (see publication "SEC200-09-00-180910 Access Control Policy" on Sharepoint) and any relevant password standards or guidelines. When in doubt employees may also reference the IT standard "IT-09-100 Password Standard" on Sharepoint or contact their manager for guidance.

4.2.3 Account Sharing

Revealing account credentials or allowing others (including but not limited to family members and co-workers) to use an employee's account are expressly forbidden. Exceptions must be approved by a Company Executive Officer and/or Company Information Security.

4.2.4 Unattended Systems

All Company devices should be configured to lock access after a period of inactivity. This period may vary by Company departments, but the maximum idle time should not exceed 30 minutes (10 minutes preferred) for any Company department area.

PC, laptops and other tablet-oriented devices should use password-protected screensavers; mobile devices should use a minimum six-digit pin, biometric (preferred) and/or pattern unlock feature.

4.2.5 Portable Computers and Mobile Devices

Because information contained on portable computers, phones, tablets, and any other mobile devices is especially vulnerable, special care should be exercised in accordance with published Company Security document titled "Mobile Security Guidelines" (published on Company Sharepoint site).

4.2.6 Malware Protection

PCs and laptops connecting to Company information resources must run up-to-date antivirus/anti-malware software as approved by Company Information Security Department. Continuous or real-time scanning capabilities should be enabled. Company IT provided systems have this protection installed by default and the user is not allowed to disable it.

4.2.7 E-mail Attachments

Employees must use extreme caution when opening attachments or clicking links in emails received from unknown or suspicious senders, as these messages may contain viruses or other forms of malware.

Suspicious emails should be reported to Company Information Security using the "Phish Alert" button in the company email software, or by forwarding the complete email to phish@segra.com.

4.3 Unacceptable Use

The following activities are expressly prohibited. The lists below are not exhaustive, but attempt to provide a framework for activities which fall into the category of unacceptable Company use. If a user is unsure if an activity is prohibited, they should contact their manager or Company Information Security.

Employees may be exempted from these restrictions if their legitimate Company job responsibilities specifically require such activity (e.g., systems administration staff may have a need to disable the network access of a host if that host is disrupting production services).

Unacceptable Company System and Network Activities:

4.3.1 Copyright / Property Rights Infringement

- Acquisition, use, or distribution of software for which the end user or the Company does not have an appropriate license.
- Unauthorized use or distribution of other copyrighted material
- Distribution or acquisition of unauthorized video, music, images, or other media.
- Any other violation of the rights of any person or organization protected by copyright, trade secret, patent, or other intellectual property rights.

4.3.2 Sharing of Confidential Information

- Revealing information about, or lists of, Company employees, customers, locations, services, revenue or CPNI to parties outside the Company without appropriate management approval.
- CPNI may not be revealed to third parties without approval from Company Information Security or Legal & Regulatory Affairs.

Providing confidential or proprietary material to parties outside the Company without appropriate management and/or Legal approval (e.g., marketing data, financial information, information on networks or equipment).

4.3.3 Circumventing Security

- Attempting to bypass web content filters for non-business purposes.
- Attempting to bypass any host or network security control for systems you are not responsible for.
- Accessing an internal network via a remote access service or device without the approval of corporate management.
- Attaching a remote access or wireless device to an internal network in order to bypass VPN or log-in requirements.

4.3.4 Network Monitoring/Scanning

- Executing any form of network monitoring which will intercept data not intended for the employee's host, unless performed as part of the employee's normal job function.
- Use of programs, web sites, or utilities that exploit weaknesses in security, that circumvent established authorization procedures and systems, or that bypass security and monitoring controls.
- Port scanning systems or networks you are not responsible for is prohibited unless authorized by the system owner or Information Security.
- Blocking or disabling authorized discovery or vulnerability scanning.

4.3.5 Security Breaches or Disruptions

Knowingly introducing malicious software ("malware") into the network.

- Accessing data for which the employee is not an intended recipient (excluding lawful requests or authorized network troubleshooting activities).
- Logging into a server or system for which the employee is not authorized.
- Injecting malicious traffic into a production network, including flooding, spoofing, or forged routing information.
- Connecting unauthorized network devices such as wireless access points.
- Denial of Service – any act with the intent to disable or interfere with normal production network or system operation.

4.3.6 Inappropriate use of Company Information Resources

- Using company information resources to promote or maintain a personal or private business.
- Using company information resources or facilities (such as electricity) to mine crypto currencies.
- Using company information resources to participate in non-work related distributed computing projects.
- Attaching any unauthorized device to any Company network for any purpose not explicitly approved by management.

Una]cceptable Company Communications Activities:

4.3.7 Junk Mail - Sending unsolicited email messages to individuals who did not specifically request such material, including the sending of "junk" email or email spam.

4.3.8 Soliciting - Soliciting others for commercial ventures, religious or political causes, outside organizations, or other non-business matters. Company approved fund-raising drives for selected charitable organizations are an exception.

4.3.9 Forgery - Falsification of email or network header information outside of a test environment for non-debugging purposes

4.3.10 Chain mail - Creating or forwarding chain letters, "Ponzi" or other "pyramid" schemes of any type.

4.3.11 Fraudulent Offers - Making fraudulent offers of products, items, or services.

4.3.12 Harassment - Using Company information resources in violation of the Sexual and Other Unlawful Harassment Policy or hostile workplace laws in the user's local jurisdiction.

4.4 Monitoring and Privacy

4.4.1 No Expectation of Privacy

While the Company desires to provide a reasonable level of privacy, all data created on corporate systems remains the property of the Company.

Users should have no expectation of privacy or confidentiality of information stored on any network device belonging to the Company or transmitted across Company networks.

4.4.2 Message Privacy

All messages created, sent, or retrieved using Company systems or across Company networks are the property of the Company and may be regarded as public information. The Company reserves the right to access the contents of any such messages if the company believes, in its sole judgment, that it has a business need to do so.

4.4.3 Right to Monitor

The Company owns and reserves the right to monitor all uses of its information resources and will monitor network traffic to identify unauthorized attempts to access, upload or change information or otherwise cause damage.

4.4.4 Use Constitutes Permission

Any use of information resources residing on or connected to any Company Intranet constitutes permission to monitor that use.

4.4.5 Disclosure

All Company communications, including text, images, and web traffic history, may be disclosed to law enforcement or other third parties without consent or notification of the sender or the receiver.

4.4.6 Authorized Monitoring

System administrators and other employees with unrestricted access to data, email, and similar services must receive Company management approval prior to decrypting or reading the communications or data, including email, of other employees.

5. NIST ALIGNMENTS

This policy aligns with the following NIST controls

- 800-53 r4 PL-4 Rules of Behavior

Security Incident Response

Document No.: SEC201-07-04

Title: **Security Incident Response**

Initial Author/Creator:	Edward Fahner	Original Date of Issue:	5/5/2021
Director IT Security Services:	Paul Southerington	Approval Date:	12/2/2021
Security Architect:	Edward Fahner	Approval Date:	11/9/2021
Chief Information Officer:	Bruce Dyke	Approval Date:	11/9/2021

Revision History

Revision No.	Description:	Revision Date:	Author
00	Initial release	10/23/2011	John Lewis
01	Updated for Segra.	5/15/2019	Edward Fahner
02	Minor restructuring, clarifications, modifications to reporting	5/24/2019	Paul Southerington
03	Added Department of Defense obligations	8/13/2020	Edward Fahner
04	Removed references to DoD, DoJ and LOA	11/09/2021	Edward Fahner

TABLE OF CONTENTS

1. Purpose

This document defines how to respond to a security incident.

2. Scope

This standard applies to all users and systems of Company systems and networks.

3. References

All references are available on Sharepoint or Confluence, using search.

- ***SLSCC-11 CPNI Security Breach Policy*** - Sharepoint
- ***Media Analyst and Investor Communications Policy*** - Sharepoint
- ***NOC Process and Procedures*** - Confluence
- ***SLSCC-09 Fraud - Tips, Guidelines and Disputes*** - Sharepoint

4. Definitions

Security Incident - A security incident is any event that threatens the confidentiality, integrity, or availability of Company information assets, information systems, or networks. This includes:

- Any unexpected or unauthorized change, disclosure, or interruption to Company information resources that could be damaging to our customers, employees, operations, or reputation.
- Any violation of Company security policies or acceptable use policies.

Security Incident Severity - The severity of a security incident from the perspective of the Information Security team. Incidents that are low severity to the Information Security team may be high severity to an operational team. As an example, a fiber cut may be an Low-severity security incident, while still being a significant operational incident.

High Severity	**Defining Criteria:** ● Significant privacy, financial, public relations, or regulatory risk ● Targeted malicious intent, or high impact non-targeted malice ● Significant impact on operations **Examples:** ● Compromise of any communication infrastructure ● Compromise of administrative or privileged account (root, Administrator, etc.) ● Loss or compromise of information confidentiality (data theft, CPNI/PII leak) ● Successful remote access by an attacker
Medium Severity	**Defining Criteria:** ● Small risk of financial, regulatory, or public-relations impact ● Automated malicious acts or non-malicious but harmful acts ● Minimal impact to day-to-day operations **Examples:** ● Malware or Virus on PC ● Unauthorized deployment of or changes to hardware, software, or configurations ● Security policy violations, compliance violations (SOC2, contractual, etc) ● Possible account compromise (fell for a phishing email, etc.)
Low Severity	**Defining Criteria:** ● Little to no financial, regulatory, or public-relations impact ● Impact is strictly limited to availability

	• Fully mitigated malicious acts • Routine **Examples:** • Non-malicious equipment failure, fiber damage, etc. • Unsuccessful or low-impact DDoS • An attack blocked by a firewall • Unsuccessful logins • Facility or environmental alarms • Telephone/Toll Fraud • Theft of encrypted device (laptops, mobile devices)

5. STANDARD

5.1 High Severity Security Incidents

5.1.1 High Severity Security Incidents must be reported to Information Security Immediately (see appendix to this standard for contact information).

5.1.2 If Information Security is unreachable, escalate following the organization chart as documented on Segra SharePoint

5.1.3 If an attack is ongoing, and Segra services or data are being actively compromised, operational staff may (and should) take action to terminate the activity, being mindful to preserve any forensic evidence to the best of their ability.

5.1.4 Information Security is responsible for forensic analysis, determining and documenting impact.

5.1.5 Information Security is responsible for escalations to Legal & Regulatory, system owners or other management if needed.

5.1.6 Information Security will provide further mitigation and ongoing prevention options.

5.1.7 Information Security will discuss significant events in quarterly executive meetings and monthly email reports.

5.1.8 Breaches of CPNI must follow the ***SLSCC-11 CPNI Security Breach Policy***.

5.1.9 Communications with media, analysts or investors must follow the ***Media Analyst and Investor Communications Policy***.

5.2 Medium Severity Security Incidents

5.2.1 Medium Severity Security Incidents must be reported to Information Security within 1 business day.

5.2.2 Operations should take action to mitigate the incident, preserving any forensic evidence to the best of their ability.

5.2.3 Information Security will include medium severity incidents in quarterly and monthly reporting cycles.

5.3 Low Severity Security Incidents

5.3.1 Incidents impacting availability are managed according to ***NOC Process and Procedures***.

5.3.2 Incidents impacting physical facilities and network infrastructure are managed according to ***NOC Process and Procedures***.

5.3.3 Telephone/Toll fraud incidents are managed according to the document ***SLSCC-09 Fraud - Tips, Guidelines and Disputes***.

5.3.4 It is not necessary to report Low Severity Security Incidents to Information Security.

5.3.5 Information Security will examine logs and operational reports at least monthly to keep informed of Low Severity events.

5.4 Preserving Forensic Evidence - Post Event

5.4.1 Don't delete anything, especially logs.

5.4.2 Isolate the system from the network, preferably by physically disconnecting or disabling connectivity.

5.4.3 Back up all system and application logs and buffers, and take screen shots or photos of errors or informative information that may not persist post-repair.

5.4.4 Unless advised otherwise by Information Security, do not reboot or power off systems unless strictly necessary.

5.4.5 First responders should avoid further investigation once the impact of the incident is stopped, unless otherwise directed by Information Security.

5.5 Cyber Threat Intelligence Sharing

5.5.1 Fully anonymized incident data may be shared with 3rd parties for the purpose participating in and receiving threat intelligence data.

5.5.2 Any Incident data may be shared with law enforcement and US intelligence agencies.

5.5.3 Compliance violations will be shared with the appropriate compliance authority or auditors as required.

6. RESPONSIBILITIES

6.1.1 The owner of this standard is the Information Security team.

6.1.2 Information Security is responsible for verifying that security incidents are reported and follow this standard.

6.1.3 Information Security is responsible for evaluating lesson's learned from incidents and proposing improvements to Company's control environment to better handle or avoid future incidents.

6.1.4 All employees are responsible for reporting immediately to Information Security and to their immediate supervisor any instances where this standard cannot be or was not followed.

7. Appendix – Contacting Information Security

ate of last revision: 5/17/2021

7.1.1 This contact information will be maintained outside of the formal standard and may be updated as needed.

7.1.2 Redacted versions of this document may omit this section.

7.1.3 Notification Procedures and escalation contacts are as shown below.

	High	Medium	Low
Notification Within	**Immediate**	1 business day	As needed
Notification Method	Follow call tree below. If no immediate answer, leave voicemail. If no response within 1 hour, proceed to next contact.	• email [redacted] • Begin the subject line with: [HIGH, MEDIUM or LOW] SECURITY INCIDENT	

	Contact Title	Contact Name	Contact Number
1	**Director, Information Security**	Paul Southerington	[redacted]
2	**Security Architect**	Edward Fahner	[redacted]
3	**VP, Information Technology**	Mike Fuqua	[redacted]
4	**Incident Response Retainer**	[redacted]	[redacted]

In the event that internal staff are unavailable, the Incident Response Retainer is a third party service which can be activated by any Segra C-level executive.

8. NIST ALIGNMENTS

This policy aligns with the following NIST controls

- 800-53 r4 IR-1 through 8, Incident Response
- CSF PR.IP-7 and 9, DE.AE, RS

Security Risk Management

Initial Author/Creator:	Edward Fahner	Original Date of Issue:	1/25/2021
Dir. IT Security Services:	Paul Southerington	Approval Date:	3/10/2022
Security Architect:	Edward Fahner	Approval Date:	3/10/2022
Chief Information Officer:	Rose Chambers	Approval Date:	3/22/2022

REVISION HISTORY

Revision No.	Description:	Revision Date:	Author
00	Initial release.	3/4/2019	Edward Fahner
01	Reapproval – no changes	1/25/2021	Edward Fahner
		Click here to enter a date.	
		Click here to enter a date.	
		Click here to enter a date.	

TABLE OF CONTENTS

1. PURPOSE

ıe purpose of the Company's Security Risk Management Standard is to document:

- how the Company identifies security risks that could cause loss of confidentiality, integrity, and/or availability
- how to identify risk owners
- criteria for assessing consequences and likelihood of a risk
- calculations for quantifying risk
- criteria for accepting risks

The goal of these practices documented here is to ensure our information security program will achieve its intended outcome, to prevent or reduce undesired effects and to formalize a method of continual improvement the Company's security posture.

2. SCOPE

This standard describes activities performed by information security workers, operational support, and management.

The techniques in this standard will be applied to all planning, design, implementation, and usage of all security controls, activities, and technologies affecting Company information assets. The policy applies to all classes of protected information in all departments.

3. Risk Assessment and Treatment

.1 Risk identification

3.1.1 Risks will be identified by both periodic and ongoing review of;

- Information Assets - through documentation, scanning, consulting asset owners or manual auditing processes
- Threats - by reviewing incidents, external threat catalogs and the knowledge of asset owners and users
- Existing controls - documentation, asset configurations and staff interviews
- Vulnerabilities - scanning tools, security testing, interviews, physical inspection, research
- Consequences - past incidents, analysis of operational, business, legal and technical impacts by the appropriate subject area experts

3.1.2 Risk will be ranked on a scale of 1 to 10 based on impact and likelihood, with 10 being the highest risk. The risk score will be calculated using one of;

- OWASP Risk Rating Methodology - This is the authoritative method.
- Simple method #1 - Impact 1 through 5, Likelihood 1 through 5, (Likelihood x Impact) x (10/25) = Risk - This method may be used to quickly score risks or convert from other systems.

Risks calculated using the simple method need to be recalculated using the OWASP method if there is any contention or question about the scoring.

3.1.3 Factors for scoring "Impact" include;

- Asset value
- Scale and quantity of data
- Sensitivity of data
- Ownership of data
- Is data disclosed, corrupted or lost?
- Service loss or degradation
- Traceability of the threat actor and opportunities for remediation
- Fiscal damages
- Reputation damages, including loss of accounts or sales
- Disclosure of PII, CPNI, or other sensitive/classified data
- Regulatory or Legal repercussions
- Impacts to customers

3.1.4 Factors for scoring "Likelihood" include:

- Skill required to exploit, and how common is that skill
- Skill of the hypothetical threat actor
- Motivation to exploit
- Resources required to exploit
- Size of the threat actor group
- Breadth of exposure
- Ease of discovery
- Ease of exploitation
- How well known the vulnerability is
- Likelihood of a successful exploit being detected

3.1.5 The Information Security Team is responsible for identifying, tracking and scoring risks, and reporting on them to management

3.1.6 Risks are owned by the operational, engineering or management teams responsible for the asset at risk. When ownership is ambiguous, ownership will be decided on and assigned by senior management.

3.2 Risk Treatment

3.2.1 The Information Security Team will solicit risk owners and senior management to make decisions on identified risks.

3.2.2 Management may decide how to treat the risk from available options:

- Mitigate - The risk will be reduced by altering controls, such as implementing new policy or technology
- Retain - Knowingly and objectively accept the risk, providing that the risk meets the risk acceptance criteria
    - Risks with a score lower than three (out of ten) may be accepted without question.
    - Accepting a risk with a score higher than four requires permission from senior management. All participating senior management must be informed of the risk and the decision. The reasoning behind the acceptance must be documented.
- Avoid - The activity or condition that introduces the risk will be avoided
- Share or Transfer - Share or offload the risk onto an external party

3.2.3 Risk treatment options will be evaluated for resources required and the amount of risk removed.

3.2.4 The Information Security Team will recommend mitigations to asset owners, track the acceptance and progress of those mitigations, and reporting on these activities to senior management.

3.2.5 The Information Security Team is responsible for identifying the effectiveness of (in terms of risk reduction) available risk mitigations.

3.2.6 Security resource allocations should be prioritized based on return-on-investment, where the mitigation cost is the investment, and the amount of risk reduction is the return. Higher risks will receive priority over lower risks. Higher ROI will receive priority over lower ROI.

3.3 Periodic Review and Approval

3.3.1 This standard is owned by the Company Information Security team, which is responsible for the content, review and upkeep of the related documentation. The standard must be reviewed periodically (at least annually), or after any major changes to Company business practices or processing environment(s), to ensure that the contents remain appropriate. New revisions of the standard must be documented and published.

4. NIST ALIGNMENTS

For reference, this policy aligns with the following NIST controls;

- 19.1 Risk Assessment and Treatment - NIST CSF ID.RM-1, NIST SP 800-53 PM-9
- 19.1.1 Risk Identification - NIST CSF ID.CA-4, ID.RA-5, NIST SP 800-53 RA-3
- 19.1.2 Risk Treatment - NIST CSF ID.RA-6, NIST SP 800-53 PM-4
- 19.1.2.2 NIST CSF ID.RM-2, NIST SP 800-53 Rev. 4 PM-9

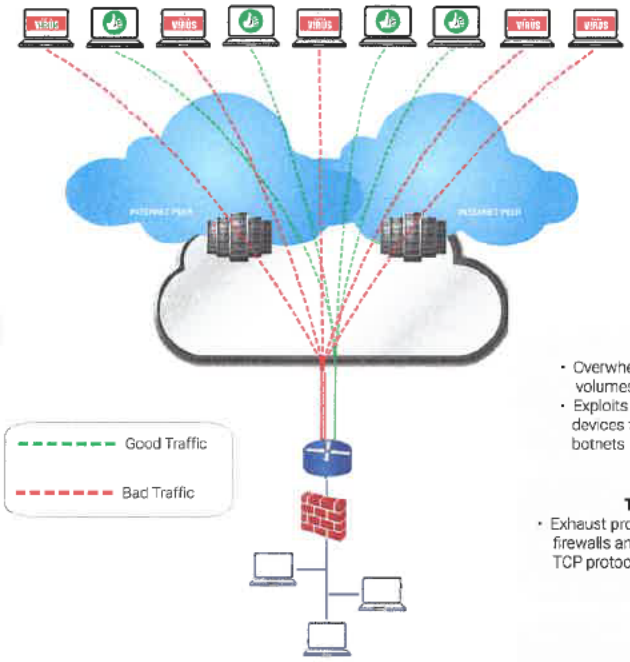
SEGRA

Segra's Product and Services Information

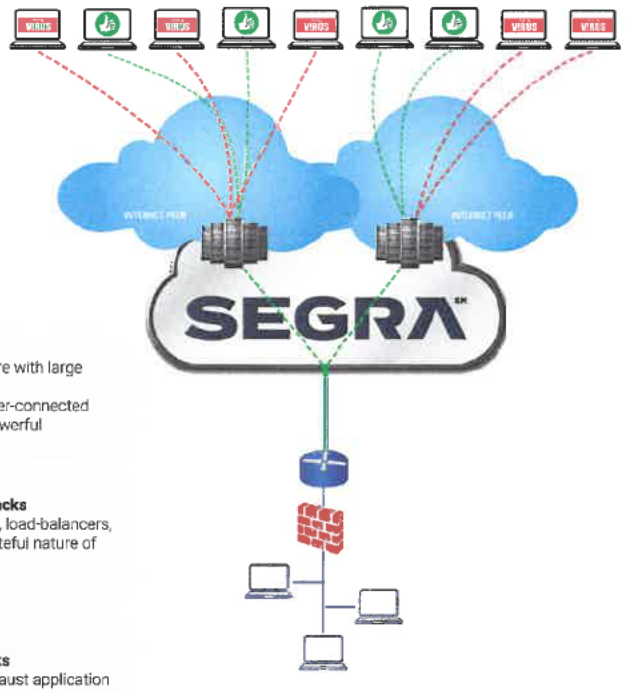
DDoS Edge Protect

Distributed Denial of Service (DDoS) attacks can strike at any time with potentially devastating effects to your network. At a minimum, these assaults compromise your user/customers' experience and can often shut down networks completely, resulting in lost productivity, revenue and costly bandwidth charges. With these attacks becoming a regular threat to the online business community, it pays to be prepared. Segra's DDoS Protection Service employs a multi-layered approach to DDoS defense to ensure your organization is safeguarded from both complex, stealthy DDoS attacks, and the very large attacks that can quickly saturate Internet connectivity.

ATTACK IN PROGRESS



ATTACK MITIGATED



Volumetric Attacks
- Overwhelms a targets infrastructure with large volumes of traffic (bps/pps)
- Exploits easily accessible and better-connected devices that create increasingly powerful botnets

TCP State-Exhaustion Attacks
- Exhaust protocol resources in servers, load-balancers, firewalls and routers by exploiting stateful nature of TCP protocol

Application Layer Attacks
- 'Low & slow' attacks that stealthily exhaust application resources as opposed to flooding a targets network

DDoS ATTACKS DENIED AT INTERNET PEERING POINTS

- Network Traffic analyzed constant by Segra's SOC
- Automated attack alert email
- DDoS Protection for entire subnets
- Scrubbing service available, yet not needed

SPECIFICATIONS

- Types of Attacks Addressed - Volumetric, reflective and resource-exhaustion
- Availability - Only available in conjunction with Segra DIA service

DDoS Edge Protect

DDoS protection appliances are located at high-volume entry points on the Segra core network where attacks are most likely to occur, such as public transit connections. The appliances automatically inspect all traffic as soon as it arrives at an entry point, immediately discarding malicious packets while sending legitimate packets to their destination. During this process, other network services continue to operate without interruption, even latency-sensitive applications like voice and video.

FAST

The protection capability is purpose-built for speed and low latency, so attacks are detected and mitigated immediately without impacting network performance.

EFFECTIVE

The protection is comprehensive, identifying both existing and newly discovered attack types, and preventing direct attacks as well as their side effects.

RISK REDUCTION

The fast, effective protection included in the Segra DIA service significantly minimizes the risk of DDoS attacks from the public Internet.

REAL-TIME FILTERING

Inspection, detection and scrubbing occur as soon as traffic arrives at the Segra network.

AUTOMATIC PROCESSING

All filtering functions are performed automatically, without the requirement for regular human intervention and/or delay.

IN-LINE OPERATION

Traffic stays on the Segra network during filtering instead of being physically and/or logically diverted for processing, minimizing latency.

COMPREHENSIVE PROTECTION ANALYTICS

Inherent analytics detect a variety of attack types and are updated continually with the latest intelligence on DDoS threats.

CORE FUNCTIONALITY

DDoS protection is required as a standard, core function of the Segra DIA service. Taking this approach protects the entire Segra network path from DDoS attacks, and in turn, the entire Segra DIA customer base. The approach also complements any local DDoS solution a customer may implement since a local solution cannot protect the Segra network path.

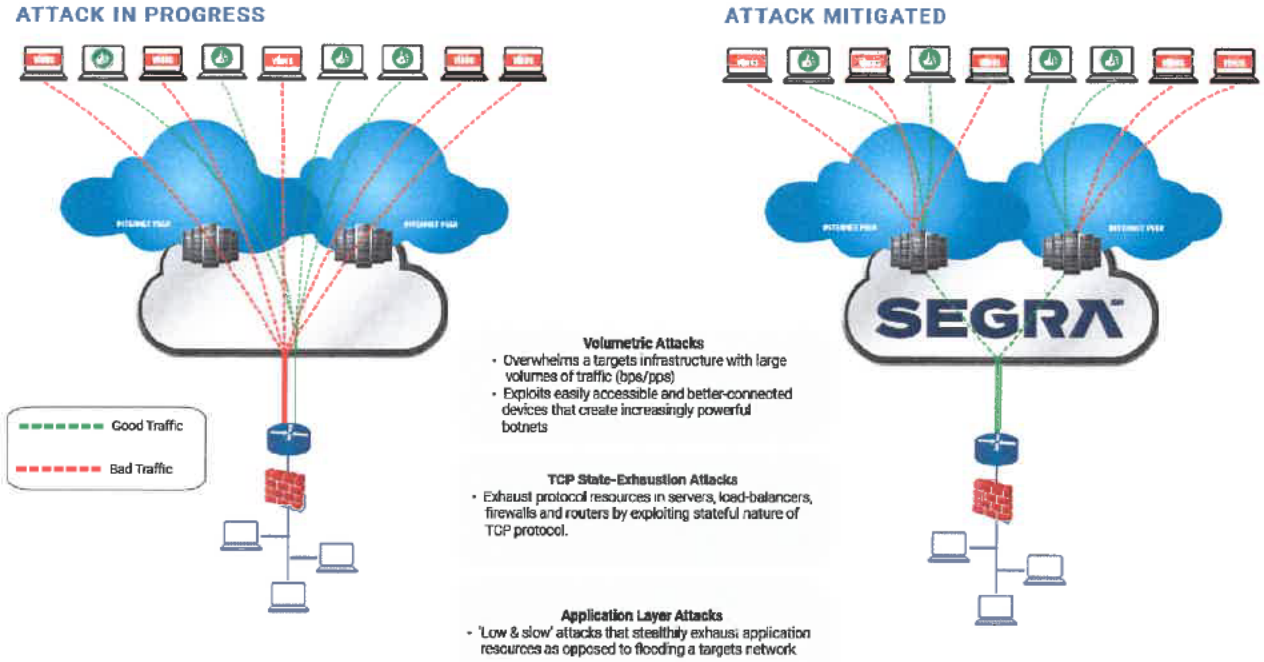
SCALABILITY

The DDoS protection appliances are designed and located to easily keep pace with growth in the Segra footprint and the customer networks we serve. Any site a customer adds to the Segra network is automatically protected from DDoS attacks without configuration changes.

Segra DDoS Edge Protect

Segra's DDoS Protection Service employs a multi-layered approach to DDoS defense to ensure your organization is safeguarded from both complex, stealthy DDoS attacks, and the very large attacks that can quickly saturate Internet connectivity. Segra's DDoS Edge Protect provides automatic DDoS Detection and Mitigation without the delays inherent in other services that re-route the affected traffic to a scrubbing facility. Short-duration, sub-saturating DDoS attacks are particularly dangerous to the network, and these attacks are much more common than before.

Even if a scrubbing center solution is activated—usually 30 minutes after the attack has been initiated—the damage has already been done. The best way to defend against these low-level, sub-saturating attacks is to use a real-time, inline DDoS mitigation solution that automatically and immediately detects and blocks such attacks. Segra utilizes pre-scripted BGP announcements for very large volumetric attacks that could potentially disrupt our Public or Private peering points. If this type of event occurs Segra will promptly reroute impacted traffic to a Scrubbing center which then "scrubs" the rerouted traffic by dropping the suspected DDoS attack traffic and passing the valid traffic to the customer's access router. Segra will resume the normal routing of impacted traffic once it reasonably determines the DDoS attack has subsided.



DDoS - Volumetric Attacks

A volumetric attacks goal is to flood a target with as much traffic as possible to prevent it from operating normally. To be successful, the volumetric DDoS attack only needs to take up enough of the targets Internet Connection capacity to affect legitimate operations; a really successful attack will be able to affect most or all of the target's clients. Some common examples of a volumetric attack are Internet Control Message Protocol (ICMP)/User Datagram Protocol (UDP) packet floods, Spoofed packet floods and malformed packet floods.

With these DDoS styles of attacks continuing to get easier and with the amount of residential bandwidth continuing to grow at a fast rate, botnets will continue to become more and more powerful with fewer exploited individual bots. Any company that does business on the Internet or has connectivity via the Internet needs to take these types of attacks seriously. This means that more and more organizations need to have a DDoS solution in mind as they continue to build out their networks and security systems.
When using a DDoS protection service, all or most of the traffic going to and from a target network is routed through the protection services networking equipment. This service "scrubs" all of the potential threat DDoS traffic and forwards all valid traffic to the target's network.

DDoS attacks result in:

- Service outages
- Costly downtime
- Lost productivity
- Brand damage
- Negative customer impact

Traditional security solutions like firewalls and IPS devices are ineffective against advanced cyber threats. In fact, they are frequently targets themselves. Customers are actively being targeted and are receiving ransom request from off-shore attackers.

Facts about Volumetric DDoS Attacks

- DDoS Attacks are occurring at an alarming frequency. They are designed to inflict a complete outage, degrade service, or make way for more malicious threats.
- Malicious traffic carrying DDoS threats flow freely over service providers networks. Even more worrying is that most customers end up paying their providers for the bandwidth that delivers potentially dangerous Internet content.

What makes up a Volumetric Attack?

- TCP Flood Attacks
- HTTP GET/POST Floods
- UDP Flood Attacks
- UDP Fragmentation Attacks
- ICMP Floods

What is Segra Doing to Protect Customers?

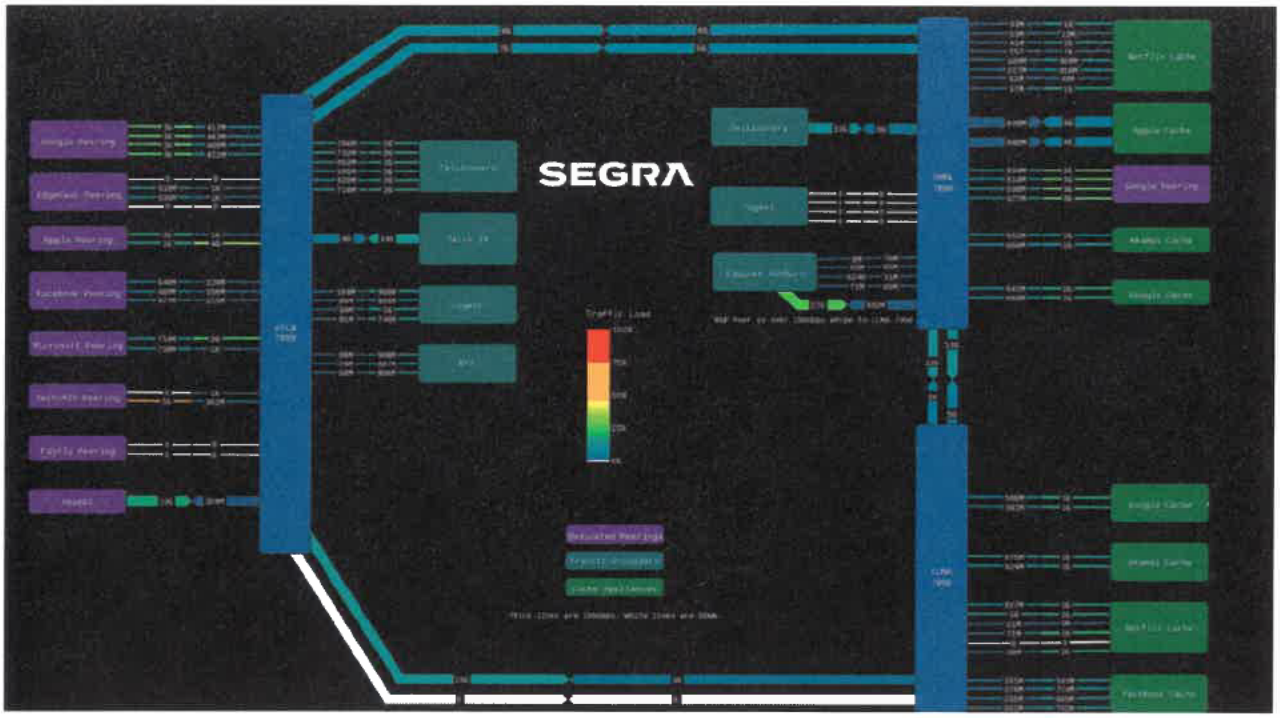
Segra has seen the increase in this malicious traffic. To combat this threat, Segra has enabled a DDoS defense to our customers called DDoS Edge Protect. All of our customers are protected against Volumetric DDoS attacks while many of our competitors deliver raw, unsecure Internet traffic. Our offering affords customers peace of mind in knowing these threats will be blocked at the edge of your network. We protect at all thirty-four internet entry points into our Core Network utilizing hardware from industry DDoS leader Corero. Threats will be stopped before they can cause outages and service degradation. DDoS Edge Protects where firewalls cannot since the protection occurs prior to reaching the customers network at the internet peer source, offering our customers trouble free protection.

Segra Internet, DDoS Protected

Segra's IP backbone consists of multiple 100 Gigabit transport circuits with full redundancy and multiple transit points to other national Tier 1 Internet providers. Segra has connectivity to the following upstream internet service providers: Telia (Tier 1), Cogent (Tier 2), NTT (Tier 1), Lumen (Tier1)

CDN'S		Transit Peers (DIA)		Direct Peers		
Google Cache	Facebook	TiNet	Level 3	Microsoft	Fastly	
Akamai		Cogent	NTT	Amazon (AWS)	Apple	
NetFlix		TeliaSonera		Facebook	Google	Edgecast

Below is a 'weather map' snapshot of Segra IP Transit, outlining Peering Partners (turquois colored, upstream providers) as well dedicated OnNet caching servers (green colored), IX Exchanges (turquois as well, IP internet exchanges with multiple collective providers and tech companies) and direct peering (purple color). The thicker links indicating 100Gb circuits, all thinner links are 10Gb circuits.



Backbone

Our IP Network Core is powered by Nokia 7950 XRS-20 Routers. The 7950 XRS-20 is a 16 Terabit per second core router that can deliver 80 100GE interfaces in a single rack (5x more than the current norm). It can be upgraded to 7950 XRS-40 and/or multi-chassis configurations as demand requires, and is designed to accommodate up to 2 terabits per slot.

Segra has deployed the Nokia 7950 XRS routing platform at three core locations where our Public and Private Peering connections are routed. These strategic locations are Columbia, South Carolina, Atlanta, Georgia and Charlotte, North Carolina. The 7950 XRS-20 are interconnected with 100 Gigabit per second (100G) links over diverse and redundant connections.

100 gigabit per second (100G) links serve as the foundation of our IP transport backbone network. As these links speeds evolve to 400 Gb and Terabit speeds, Our 7950 XRS Core routing platform is already in place to accelerate the deployment of next generation high-speed connections.

Segra utilizes fully meshed Nokia 7750 SR-12e as distribution routers to reach our customers. The Nokia 7750 SR series delivers high-performance routing and an extensive range of IP applications. The 7750 SR scales system capacity to 9.6 Terabits per second and is equipped with high-density Gigabit Ethernet (GE), 10GE, 40GE and 100GE interfaces.

Segra has deployed Nokia 7750 SR12-e routers in Columbia, Greenville, Florence, Charleston, Charlotte, North Carolina and Atlanta, Georgia. These routers are interconnected with multiple 10 Gigabit Ethernet links that are diverse and redundant over Segra's owned DWDM fiber backbone throughout the Carolinas.

Public Peering

Segra utilizes a strategy of maintaining Public Peering Points and Private IP Transit connections with multiple Tier 1 providers. Current Internet Exchange point aggregates thousands of peering sessions onto the shared fabric, Public Peering points are Atlanta IX, Ashburn, Virginia, and Los Angeles, California. Each Public and Private Peer supports dual-stack IPv4 and IPv6.

The Public Peering Point located in Ashburn, Virginia is a Global Internet Exchange facility that utilizes IP peering via an Ethernet switching fabric. These interconnections are designed on a centralized Ethernet Switching fabric and the necessary supporting infrastructure to support multiple 100 Gbps connections.

The Public Peering Point in Atlanta is located at the AtlantaIX exchange facility. This Internet Exchange is a neutral, high performance Internet peering fabric for participants. The AtlantaIX public peering point is designed on a centralized Ethernet Switching fabric and the necessary supporting infrastructure to support multiple 100 Gbps connections.

The Public Peering point in Los Angeles located at the CoreSite-Any2 LA1 International Internet eXchange point. This Public Peering is located at one of the most interconnected buildings on Earth, – One Wilshire at 624 S. Grand – with interconnections to Telehouse's LAIIX, located at 626 Wilshire Blvd. These interconnections are designed on a centralized Ethernet Switching fabric and the necessary supporting infrastructure to support multiples of 100 Gbps connections.

These Strategic Public Peering Points give Segra and our customers a nationwide presence to the internet with enhanced end-to-end network performance, speed, and reliability.

Private IP Transit Peering

Segra also maintains Private IP Transit connections with other Tier 1 Global Internet providers to augment our public peers and provide additional global reach for our customers.

Segra runs BGP (IPV4 & IPV6) with these IP Transit providers to optimize routing entering and leaving the Segra autonomous systems (AS). All providers allow Segra to manipulate traffic in their Autonomous Systems, which gives a lot of power and traffic manageability to Segra.

Each Private IP Transit connection consists of multiple 10 Gigabit peering connections and terminate into our Core 7950 XRS IP routers. These connections are located in Atlanta, Georgia and Charlotte, North Carolina.

This Public and Private Peering strategy has provided our customers with the utmost in networking performance and reliability.

Caching Services

Segra hosts large Akamai caching environments/content distribution networks located in Columbia, South Carolina and Charlotte, North Carolina. These content caching servers are used to improve performance for high bandwidth intensive content applications such as streaming video and operating system updates. When content is requested from companies like NetFlix, Microsoft, Apple, Facebook, Twitter, and Google the information is not necessarily returned from that company's web site or Data Center. Instead, the information is returned from the Akamai web cache or Google content distribution server located at the Segra POP(s) listed above.

Segra utilizes the Corero SmartWall Threat Defense System (TDS) as the core of our managed security service offering DDoS Edge Protect. Spirit's DDoS Edge protect is a managed security service that eliminates cyber threats in real-time. It provides comprehensive DDoS protection capable of mitigating a wide range of DDoS attacks all while maintaining full connectivity to avoid disrupting the delivery of legitimate traffic. It does this by implementing wire speed scrubbing, preventing the need to redirect traffic offsite through a scrubbing center allowing for an increased uptime.
It is designed to handle large network-based DDoS attacks or floods, reflective amplified spoof attacks, as well as application layer attacks that are typically too low to be detected by out of band solutions. This DDoS Edge Protect product protects where firewalls cannot since the protection occurs prior to reaching the customer's network at the Internet peer source.

Segra's DDoS Edge Protect provides automatic DDoS Detection and Mitigation without the delays inherent in other services that re-route the affected traffic to a scrubbing facility. Short duration, sub-saturating DDoS attacks are particularly dangerous to the network, and these attacks are much more common than before. Even if a scrubbing center solution is activated—usually 30 minutes after the attack has been initiated—the damage has already been done. The best way to defend against these low-level, sub-saturating attacks is to use a real-time, inline DDoS mitigation solution that automatically and immediately detects and blocks such attacks. Segra also partners with Arbor Networks and utilizes pre-scripted BGP announcements for very large volumetric attacks that could potentially disrupt our Public or Private peering points. If this type of event occurs Segra will promptly reroute impacted traffic to a Scrubbing center which then "scrubs" the rerouted traffic by dropping the suspected DDoS attack traffic and passing the valid traffic to the customer's access router. Segra will resume the normal routing of impacted traffic once it reasonably determines the DDoS attack has subsided.

Segra also currently has the Infrastructure in place to allow us to actively monitor all threats and DDoS attacks in real time. The Spirit Security Operations Center (SOC) brings together the people, technology and process to identify threats in real-time and take immediate action. In partnership with our Network Operations Center, our network is monitored 24x7x365.

This team is responsible for the following:

a) Identifying real-time threats
b) Triaging and mitigating through automation and manual investigation and remediation
c) Ensuring that all traffic is scrubbed against the latest threat intelligence
d) Provides access to real-time security analytics, access to qualified cyber-security professionals and automated management of threats that can be addressed in line to ensure that they never reach a customer's facility

In the event of a DDoS attack, Segra Communications will:

a) Issue Alert(s) to the Segra Security Operations Center about the IP threat(s) via email or text notification.
b) Issue alert to the UGU Technical Point of Contact via phone call, email or text notification as directed by the UGU technical point of contact.

DDOS Management Service services are composed of:

(1) Mitigation

Provide UGU with redirection capabilities in the event of a DDoS attack upon detection, and Spirit Communications has read, understands and will comply.
During the first two (2) weeks following the Service Activation Date, Spirit will analyze and examine customer traffic flow data and any patterns within such data in order to baseline customer traffic patterns to assist in determining when a DDoS Attack is occurring.
Spirit currently offers a DDoS Edge Protect Solution which does not currently require a redirection of traffic to mitigate an attack. Through the use of Spirit's Corero SmartWall Threat Defense System (TDS) we are able to mitigate DDoS attacks at up-to 10 Gbps in real-time utilizing Corero's Wire Speed Scrubbing. This is done by using the Spirit DDoG Edge Protect appliances built in DDoS Signature and Pattern matching algorithms, and is able to do so while reducing the total number of False Positives of a standard DDoS Solution.

(2) Scrubbing

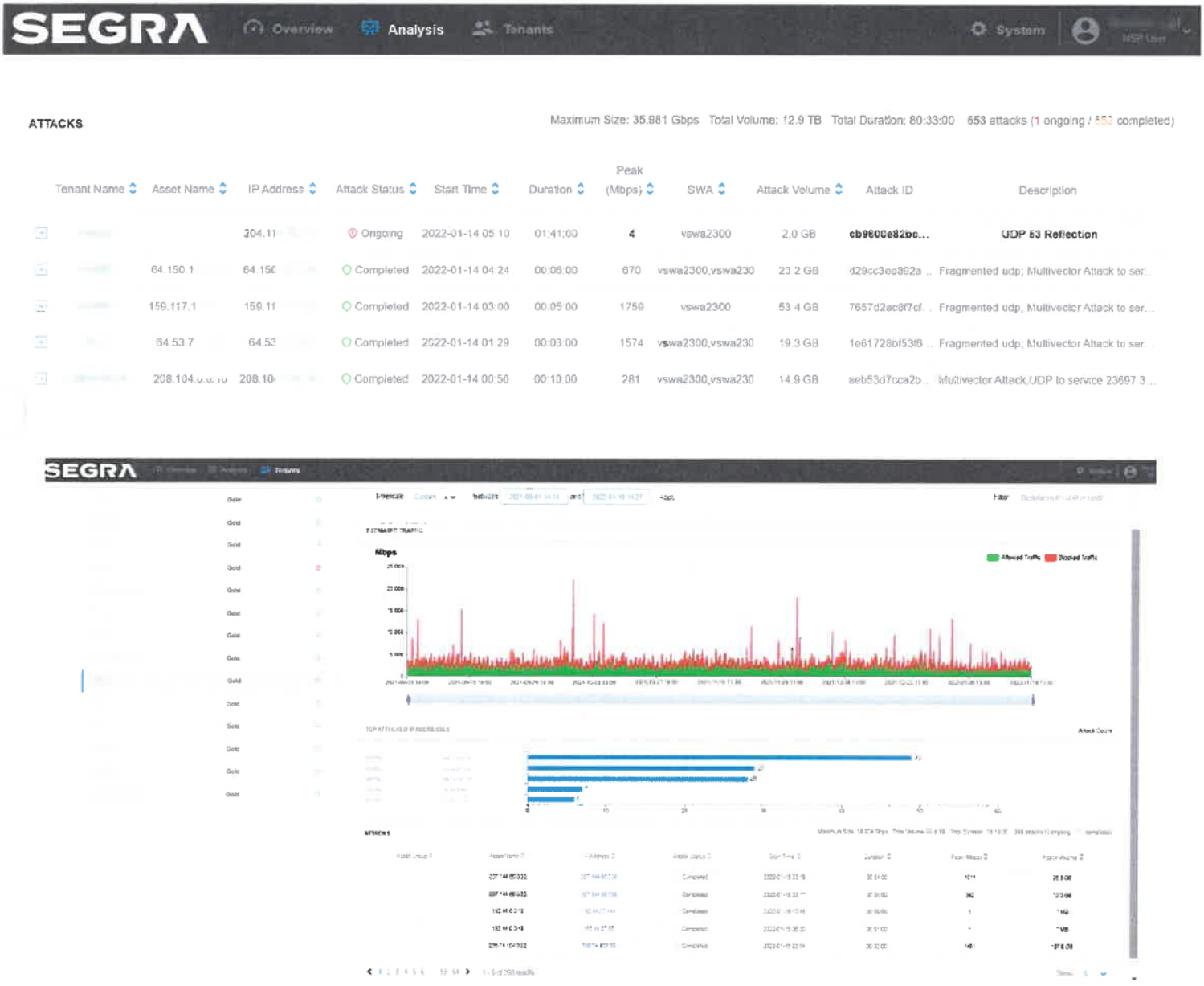
Should the need arise for protection in excess of 100 Gbps at multiple internet peering points and a redirect is required, Segra is also partnered with Arbor Networks and utilizes pre-scripted BGP announcements for very large volumetric attacks that could potentially disrupt our Public or Private peering points. If this type of event occurs Segra will promptly reroute impacted traffic to a Scrubbing center which then "scrubs" the rerouted traffic by dropping the suspected DDoS attack traffic and passing the valid traffic to the customer's access router. Segra will resume the normal routing of impacted traffic once it reasonably determines the DDoS attack has subsided.

Segra's DDoS Edge Protect solution does not require a redirection of traffic to mitigate an attack. Through the use of Segra's Corero SmartWall Threat Defense System (TDS) we are able to mitigate DDoS attacks 100 Gbps+ in real-time utilizing Corero's Wire Speed Scrubbing. This is done by using the Segra DDoS Edge Protect appliances built in DDoS Signature and Pattern matching algorithms, and is able to do so while reducing the total number of False Positives of a standard DDoS Solution.

(3) Segra SOC DDoS Visibility

Segra's web application portal enables Segra SOC to monitor attacks and provides historical attack insight.

Example below highlights a recent snapshot of portal that outlines recent mitigated attacks (Attack ID & Description), where the attack was mitigated (SWA). Patches are globally identified and applied thru the global network of Corero identification and mitigation.



Segra DDoS Edge Protect, Attack Coverage

Category of DDoS Attack Type	Spirit Protect, DDoS Attack Coverage
Volumetric DDoS Attacks	TCP Flood Attacks HTTP GET/POST Floods UDP Flood Attacks UDP Fragmentation Attacks ICMP Floods
Reflective DDoS Attacks	NTP Monlist Response Amplification SSDP/UPnP Responses SNMP Inbound Responses Chargen Responses Smurf Attack Fraggle Attack DNS DNS Amplification
Resource Exhaustion DDoS Attacks	Malformed and Truncated Packets (e.g. UDP Bombs) IP Fragmentation/Segmentation AETs Invalid TCP Segment IDs Bad checksums and illegal flags in TCP/UDP frames Invalid TCP/UDP port numbers Use of reserved IP addresses Slow HTTP requests (from tools like Slowloris, RUDY, Slowread)
Other DDoS Attacks	Command and Control Operations Tunnel Inspection (GRE, MPLS etc.) GRE, MPLS etc. NTP Monlist Requests Whitelisting Known malicious IP Addresses (botnets, scanners, anonymization services, phishing sites, spammers) Customized Protection with IP Reputation and Geolocation Policies Blacklisting of IP Addresses Port address range filters (provides protection for generic TCP/UDP port based attacks) Smart-Rule – Heuristics based engine leverages heuristics and behavioral analysis to track and rate limit L1-L4 attacks

Dedicated Internet Access

High-speed connectivity to the Internet is a must-have for your IT systems and your presence with customers. Don't slow your business down with Internet access that's shared across many users and likely to be congested, unpredictable and not secure. Segra DIA provides a dedicated, secure, reliable connection to the Internet that has guaranteed bandwidth to help ensure that your business is always online, at the speed you need.

Your site is connected to the Segra Internet POP by a local access loop. The bandwidth on the loop is dedicated, not shared across many users, which preserves your Internet connection speed since there is no competition for the bandwidth.

INCREASE PRODUCTIVITY

Increase productivity by providing the reliable, high-performance Internet access employees and systems need to operate every day.

SCALABILITY

Offers scalability by supporting a range of access speeds, so you can grow your Internet bandwidth as your online business needs increase.

FEATURES

- Dedicated Access - Your bandwidth connection to the Internet is not shared, giving you reliably fast access to the web.
- Synchronous Upload and Download Speeds – With Segra DIA, Internet upload and download speeds are the same, enabling the consistent access performance needed for online transactions to complete quickly.
- Bandwidth Scalability – DIA bandwidth can be increased to up to 5G speeds, so there is plenty of room to increase bandwidth as your Internet access needs grow.
- Multi-Service Support – The DIA connection can support other network services, providing a single network for your telecommunication needs. If the connection includes Segra IP Voice services, QoS prioritizes bandwidth for the voice traffic. In addition, interoffice traffic can be separated from Internet traffic for security purposes.
- Multi-Site Support – DIA can connect multiple sites to bring current and future locations online.
- Carrier-Class Service Level Agreement (SLA)

SPECIFICATIONS

- Speeds – 3 Mbps to 8 Gbps
- Ports – 10/100 Mbps, 1 Gbps, 10 Gbps
- Access - Type 1/on-net or Type 2/off-net access
- Availability - Across the entire Segra network

Ethernet WAN

Segra Ethernet WAN provides the configuration flexibility to join sites, the bandwidth scalability to feed applications, the access to reach the Internet and private VPNs at business speeds, and the service resiliency to keep your network running. Segra Ethernet WAN is ideal for enterprises that need to connect sites with a versatile, scalable, carrier-class network fabric. Our premium fiber network reaches major markets throughout the Mid-Atlantic and Southeast, as well as outlying areas in the region not typically served by other providers.

SWITCHED

Ethernet WAN switched is a Layer 2 service so it is transparent to your existing network, which simplifies administration and preserves control. In addition, your staff can make IP routing changes to your network without coordinating with Segra. Essentially, Segra Ethernet WAN connects your sites without any impact to your existing IP routing; your locations operate as if they were simply connected by an Ethernet cable.

ROUTED

Ethernet WAN routed is a Layer 3 service, it uses routing to send data between your organization's sites. The information is routed from your organization's LAN from one location to another, via the Segra WAN. Segra is responsible for the IP routing necessary to move the data across the WAN, freeing your IT team from this work.

FLEXIBILE AND SCALABLE

Ethernet WAN service supports multiple topologies and a range of speeds to connect sites in the manner that best suits your application needs.

COST-EFFICIENCY

With Ethernet WAN, you pay only for the bandwidth you need, and you can increase bandwidth without expensive equipment upgrades.

RESILIENCY

Ethernet WAN includes resiliency mechanisms to ensure traffic delivery, as well as end-to-end Quality of Service (QoS) options for traffic prioritization across the Segra WAN.

	Switched	Routed
TOPOLOGIES	MEF Certified Designs	Fully Meshed
QoS	Multiple end-to-end options	Multiple end-to-end options
ACCESS	Type 1 (on-net) and type 2 (off-net)	Type 1 (on-net) and type 2 (off-net)
PORTS	1 Gbps, 10 Gbps	1 Gbps, 10 Gbps
SPEEDS	20 Mbps to 10 Gbps	20 Mbps to 10 Gbps
SLAs	Carrier-class for service availability	Carrier-class for service availability

SD-WAN

Segra's fully managed SD-WAN (Software-Defined Wide Area Networking) solution simplifies branch office networking by providing security, fail-over, application prioritization, and diverse connectivity options. Segra's SD-WAN offering serves as an augment to our MPLS service and allows our customers to bond primary, secondary, and tertiary local broadband, Internet, and wireless connections in order to create a highly available, cost effective, integrated network.

SIMPLE SECURE NETWORK

This turnkey solution allows you to quickly deploy a simplified network design that includes security, orchestration, monitoring, and centralized troubleshooting tools.

DELIVER SITE AGILITY

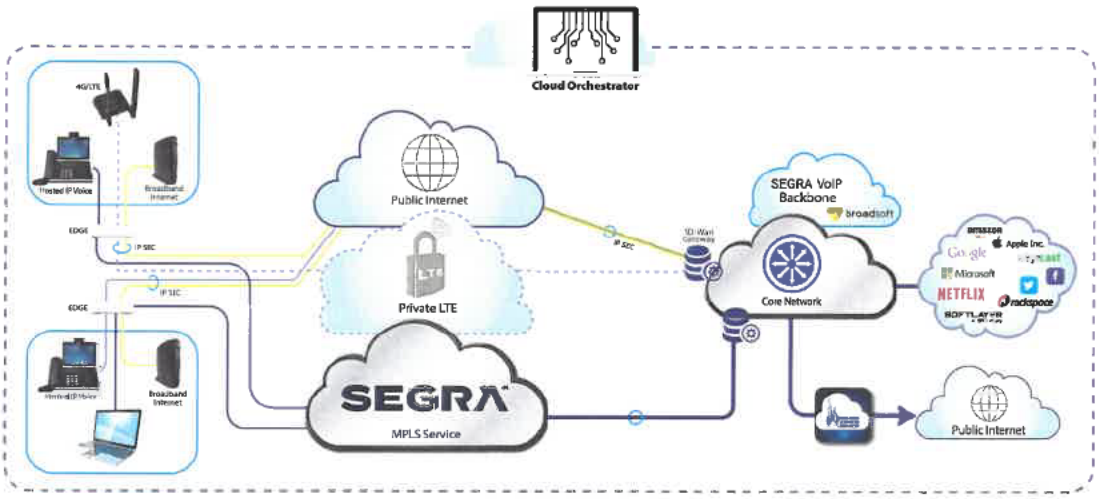
Using Segra's SD-WAN, local Internet Service Providers (ISPs) easily coexist and inter-operate with your Segra MPLS network. You will be able to manage each branch via one centralized online application to ensure that your network is performing optimally.

OPTIMIZE APPLICATION PERFORMANCE

With Segra's SD-WAN, you can optimize application performance over dedicated, hybrid, or Internet links with direct, secure, access to enterprise and cloud applications. SD-WAN brings consolidated monitoring and visibility to all WAN links and all service providers. Via the centralized web interface, you can allocate your available bandwidth to best fit the applications that are crucial to your business.

REDUCE COST

Segra SD-WAN delivers robust and secure enterprise-grade WAN at your branch office(s) regardless of connection type or carrier. Installing Segra's turnkey SD-WAN solution saves on expensive hardware installations and helps to control costs associated with various ISPs serving your branch office(s).



SD-WAN

At each location, a Segra SD-WAN Edge device is installed and WAN delivery devices are connected. This device then allows you to view the location's ISP connections via one single pane of glass in the Segra SD-WAN portal. The Cloud Orchestrator coordinates and monitors all traffic being passed between your site, the Segra managed gateways, MPLS network, and Data Centers. The orchestrator ensures that your policies and procedures are being correctly applied across your network. SD-WAN Gateways act as the controller of the policies for your MPLS based traffic routed over the Internet. The gateways set your traffic and application priority based on your business needs and available network resources.

APPLICATION 1

One design enables MPLS connectivity for locations where there are currently no Segra provided circuits. Segra's SD-WAN technology secures Internet from any ISP and safely connects back to the Segra MPLS network. This equips you with the ability to manage various aspects of your organization's network, using a single source, regardless of provider.

APPLICATION 2

Another design provides customers with a highly available solution by bonding Segra's primary service to secondary and backup WAN options (broadband, bonded T1's, LTE, Ethernet over Copper). This design also allows you to customize your location's applications and policies, via our online portal, ensuring that you have the ability to manage your bandwidth resources.

MPLS

Segra's MPLS solution is a dedicated connection that uses the Segra private network to ensure maximum access to your vital services. It is ideal for critical business communications with voice, data and Internet connectivity.

Segra's MPLS solution provides fast downloads and uploads, more reliability, scalability and security than DSL or Cable modems. Speeds using Ethernet are constant and provide greater broadband connectivity for transferring data and access to websites important to you company's operations.

MPLS is also great for connecting multiple locations. This solution allows you to create point-to-point and multi-point to multi-point connections and tie all locations together over the secure MPLS network.

NETWORK REACH
Your Data is safe and secure on our expansive super-regional fiber network.

TRUSTED
Segra is a long term provider for many state and local services agencies throughout our entire footprint.

QUALITY OF SERVICE
Quality of service (QoS) assured by our industry-leading Service Level Agreements that fit your business needs.

SECURE
Your data never touches the public Internet. It remains on Segra's private, fiber network ensuring data security and privacy.
(VPRN and VPLS enabled)

LOCAL SUPPORT
Our local Network Operations Center (NOC) provides proactive network monitoring and management 24/7/365.

SCALABLE
Highly scalable, cost-effective connectivity that can grow with your business.

FLEXIBLE
Secure, reliable, flexible solutions that are responsive to your business needs – anywhere, anytime.

RELIABLE
Our fully redundant network core assures your data is available on-demand and gets to its destination - always.

PERFORMANCE
Our MPLS network ties together all your locations - enabling a converged private network for voice, data, and video - to deliver increased performance and stability.

VPRN Service

With VPRN, you can link your locations with carrier-class Ethernet and carrier-managed WAN routing. Your business is growing and so is your network, but your IT resources aren't. You need a WAN that will expand efficiently without taxing your IT team. Segra VPRN does both. It provides the flexible, scalable network you need and offloads the burden of complicated WAN routing from your IT staff. You get exceptional Ethernet service with expertly managed WAN routing – perfect for a growing business with limited IT resources.

Because VPRN is a Layer 3 service, it uses routing to send data between a customer's sites. The information is routed from the customer's LAN at one location, over the Segra WAN, to the customer's LAN at another location. Segra is responsible for the IP routing necessary to move the data across the WAN, freeing your IT team from this work.

IT RESOURCE EFFICIENCY

Segra manages the IP WAN routing associated with VPRN, allowing you to use your IT resources for other projects.

HIGH PERFORMANCE

VPRN operates over Segra's fiber optic Ethernet network to provide the high-performance, scalable, resilient WAN service you expect.

SCALABILITY

You can easily add sites to their VPRN service without taking on the related IP WAN routing work.

COST EFFICIENCY

VPRN supports a range of bandwidth options so customers can choose the speed that best fits their application and budget requirements.

FEATURES

- Topologies – Fully meshed
- Access – Type 1 (on-net) and Type 2 (off-net)
- Ports – 10 Mbps, 100 Mbps, 1Gbps, and 10 Gbps
- Speeds – Speed from 2Mbps to 10Gbps
- QoS – Multiple end-to-end QoS options
- SLAs – Carrier-class for service availability

Segra's FCC Form 498

File electronically at https://forms.universalservice.org/portal/login

FCC Form 498 OMB 3060-0824

Service Provider And Billed Entity Identification Number and General Contact Information Form

Estimated Average Burden Hours Per Response: .75 hour

FCC Form 498 is used to collect contact and remittance information for service providers and billed entities that receive support from the Federal universal service support programs. For greater flexibility, this form allows service providers to use the same general contact information for all their contacts and the same remittance data collected for each of the four programs or multiple contact and remittance information. Please report any changes to this information on a revised FCC Form 498 to prevent any delays in notification and the timeliness of disbursements. Persons willfully making false statements on this form can be punished by fine or forfeiture, under the Communications Act, 47 U.S.C. Secs. 502, 503(b), or fine or imprisonment under Title 18 of the United States Code, 18 U.S.C. Sec. 1001.

Please read instructions, located at: https://www.usac.org/service-providers/resources/forms, before beginning this application.

Provider Type

Please check one box below *See Instruction Section III.A*

☑ Service Provider ☐ School/Library or other Billed Entity

Submission Type

Please check one box below *See Instruction Section III.A*

☐ Original Application for FCC Form 498 ID ☑ Revision to existing FCC Form 498 on file with USAC

☐ Request for FCC Form 498 ID Merger/Consolidation ☐ Request for FCC Form 498 ID Deactivation

See Instruction Section III.A

Service Provider and Billed Entity Identification Number (FCC Form 498 ID) 1 4 3 0 2 4 8 4 8
(To be inserted by USAC for first time applications. **Required for subsequent revisions.**)

499 Filer ID ☐☐☐☐☐☐
(Required if your company is required to file the FCC Form 499)

Block 1: Organization Information [All Fields REQUIRED]

See Instruction Section III.B

1 Lumos Networks LLC
Company or Billed Entity Name

2 DBA Segra; FKA FiberNet, LLC
Name Entity or Company is Doing Business As (DBA) or Formerly Known As (FKA)

3 LUMOS NETWORKS CORP
Holding Company Name (*For Service Providers*)

4 8 0 0 6 9 7 2 7 4
Federal EIN, or TAX ID Number of Holding Company

5 ☐ Check this Box if the Company is part of or maintains affiliate companies and complete page 2.

6 One Lumos Plaza
Street Address

7
Address Line 2

8 Waynesboro 9 VA 10 22980
City State Zip Code + 4

Block 2: General Contact Information [All Fields REQUIRED]

See Instruction Section III.C

11 First: Anthony Middle Initial: Last: Stroman 12 E-rate/AR
General Contact (Company Preparer Name) Title

13 (803) 726-4074
Phone Number Ext.

14 One Lumos Plaza
Street Address

15
Address Line 2

16 Waynesboro 17 VA 18 22980
City State Zip Code + 4

19 Anthony.stroman@segra.com
E-mail Address

Block 3: Federal EIN, DUNS and FCC Registration Number [All Fields REQUIRED]

See Instruction Section III.D

20 8 4 1 4 5 2 9 5 0
Enter Federal Employer Identification Number
(Federal EIN or Tax ID Number)

21 ☐ Corporation ☐ Partnership ☑ Other
(Check applicable corporate structure.)

22 1 9 6 8 8 6 5 9 2
Enter Dunn and Bradstreet Number (DUNS)

23 0 0 0 3 7 7 1 0 1 1
FCC Registration Number (CORES ID)

This is a Supplemental Page for Companies with Affiliate Relationships

Block 4: Affiliate Company Information

See Instruction Section III.E

Please list all companies with which this FCC Form 498 ID is affiliated. The term "affiliate" means a person that (directly or indirectly) owns or controls, is owned or controlled by, or is under common ownership or control with, another person. For purposes of this paragraph, the term "own" means to own an equity interest (or the equivalent thereof) of more than 10 percent.

Affiliate FCC Form 498 ID Number	Affiliate Company Name

(Attach additional copies of this page if necessary)

This page is for High Cost Program participants only.

For more information about the High Cost Program, please refer to: https://www.usac.org/high-cost/

Block 5: High Cost Support Financial Institution and Remittance Information [ALL Fields REQUIRED]

See Instruction Section III.F

☐ ***Check this box to discontinue use of this FCC Form 498 ID for High Cost Support.***

Financial institution information is required. Electronic payment of universal service support payments is mandated by the Debt Collection Improvement Act of 1996, Pub. Law 104-134, 110 Stat. 1321-358.

☐ Check this box if this information is the same as the General Contact information (Block 2) and complete lines 29-31.

24 Lumos Networks LLC
Remittance Company Name, if different from Company Name

25 First: Amy Middle Initial: E Last: Gruber 26 Manager
Remittance Contact Name - Statements will be sent to Remittance Contact's attention Title

27 (540) 946-3510 Ext 28 amy.gruber@segra.com
Phone Number E-mail Address for receipt of remittance advice

29 BB&T
Remittance Financial Institution for ACH or locked box transfer of funds (required)

30 [redacted] 31 [redacted]
Financial Institution Account Number for ACH (required) ACH Financial Institution Transit Number - must be nine digits (required)

Block 6: Organization Contact for High Cost Support

See Instruction Section III.G

☐ Check this box if this information is the same as the General Contact information (Block 2) and continue on to Block 7.

32 First: Amy Middle Initial: E Last: Gruber 33 Manager
Contact Name for High Cost Program Title
(Must be a company employee or designated representative)

34 One Lumos Plaza
Contact Address or PO Box for High Cost Program

35
Address Line 2

36 Waynesboro 37 VA 38 22980
City State Zip Code + 4

39 (540) 946-3510 Ext 40 amy.gruber@segra.com
Phone Number E-mail Address of High Cost Program Contact

This page is for Lifeline Program participants only.

For more information about Lifeline Support, please refer to: https://www.usac.org/lifeline/

Block 7: Lifeline Support Financial Institution and Remittance Information [All Fields REQUIRED]

See Instruction Section III.H

☐ ***Check this box to discontinue use of this FCC Form 498 ID for Lifeline Support.***

Financial institution information is required. Electronic payment of universal service support payments is mandated by the Debt Collection Improvement Act of 1996, Pub. Law 104-134, 110 Stat. 1321-358.

☐ Check this box if this information is the same as the General Contact information (Block 2) and complete lines 46-48.

41 Lumos Networks LLC
Remittance Company Name, if different from Company Name

42 First: Jen Middle Initial: Last: Marshall 43 Regulatory
Remittance Contact Name - Statements will be sent to Remittance Contact's attention Title

44 (540) 946-6805 Ext 45 marshallj@lumosnet.com
Phone Number E-mail Address for receipt of remittance advice

46 BB&T
Remittance Financial Institution for ACH or electronic transfer of funds (required)

47 [redacted] 4[redacted]
Financial Institution Account Number for ACH (required) ACH Financial Institution transit Number - must be nine digits (required)

Block 8: Organization Contact for Lifeline Support

See Instruction Section III.I

☐ Check this box if this information is the same as the General Contact information (Block 2) and continue on to Block 9.

49 First: Jen Middle Initial: Last: Marshall 50 Regulatory
Contact address for Lifeline Program Title
(Must be a organization employee or designated representative)

51 One Lumos Plaza
Contact Address for Lifeline Program

52
Address Line 2

53 Waynesboro 54 VA 55 22980
City State Zip Code + 4

56 (540) 946-6805 Ext 57 marshallj@lumosnet.com
Phone Number E-mail Address of Lifeline Program Contact

This is a Supplemental Page for Participants in the High Cost and Lifeline Programs.

Block 9: High Cost and Lifeline Study Area/FCC Form 498 ID Association

See Instruction Section III.J

This information will be used to associate the Study Area Codes (SAC) to this FCC Form 498 ID for the purposes of High Cost and Lifeline Support.

☑ Check this box if there is no change to the SAC data on file.

☐ Check this box if you are changing your organization's SAC data currently on file with USAC.

Study Area Code (SAC)	SAC Company Name	Study Area Type	
179008		☐ Incumbent	☑ Competitive
189004		☐ Incumbent	☑ Competitive
209002		☐ Incumbent	☑ Competitive
		☐ Incumbent	☐ Competitive
		☐ Incumbent	☐ Competitive
		☐ Incumbent	☐ Competitive
		☐ Incumbent	☐ Competitive
		☐ Incumbent	☐ Competitive
		☐ Incumbent	☐ Competitive
		☐ Incumbent	☐ Competitive
		☐ Incumbent	☐ Competitive
		☐ Incumbent	☐ Competitive
		☐ Incumbent	☐ Competitive
		☐ Incumbent	☐ Competitive
		☐ Incumbent	☐ Competitive
		☐ Incumbent	☐ Competitive
		☐ Incumbent	☐ Competitive
		☐ Incumbent	☐ Competitive
		☐ Incumbent	☐ Competitive
		☐ Incumbent	☐ Competitive
		☐ Incumbent	☐ Competitive
		☐ Incumbent	☐ Competitive

(Attach additional copies of this page if necessary)

This page is for Rural Health Care Program participants only.

For more information about Rural Health Care Support, please refer to: https://www.usac.org/rural-health-care/

Block 10: Rural Health Care Support Financial Institution and Remittance Information [ALL Fields REQUIRED]

☐ ***Check this box to discontinue use of this FCC Form 498 ID for Rural Health Care Support.***

Financial institution information is required. Electronic payment of universal service support payments is mandated by the Debt Collection Improvement Act of 1996, Pub. Law 104-134, 110 Stat. 1321-358. ***See Instruction Section III.K***

☐ Check this box if this information is the same as the General Contact information (Block 2) and complete lines 63-65.

58 Lumos Networks dba Segra
Remittance Company Name, if different from Company Name

59 First: Anthony Middle Initial: E Last: Strohman 60 Accts Rece
Remittance Contact Name - Statements will be sent to Remittance Contact's attention Title

61 (803) 726-4074 62 Anthony.Stroman@segra.com
Phone Number Ext E-mail Address for receipt of remittance advice

63 BB&T
Remittance Financial Institution for ACH or locked box transfer of funds (required)

64 [redacted] 65 [redacted]
Financial Institution Account Number for ACH (required) ACH Financial Institution transit Number - must be nine digits (required)

Block 11: Organization Contact for Rural Health Care Support

See Instruction Section III.L

☐ Check this box if this information is the same as the General Contact information (Block 2) and continue on to Block 12.

66 First: Anthony Middle Initial: Last: Strohman 67 Accts Rece
Contact Name for Rural Health Care Program Title
(Must be a company employee or designated representative)

68 1500 Hampton St
Contact Address for Rural Health Care Program

69
Address Line 2

70 Columbia 71 SC 72 29201
City State Zip Code + 4

73 (803) 726-4074 74 Anthony.Stroman@segra.com
Phone Number Ext E-mail Address of Rural Health Care Program Contact

This page is for Schools and Libraries Program participants only.

For more information about the Schools and Libraries Program, please refer to: https://www.usac.org/e-rate/

Block 12: Schools and Libraries Support Financial Institution and Remittance Information [ALL Fields REQUIRED]

☐ ***Check this box discontinue use of this FCC Form 498 ID for Schools and Libraries Support.***

Financial institution information is required. Electronic payment of universal service support payments is mandated by the Debt Collection Improvement Act of 1996, Pub. Law 104-134, 110 Stat. 1321-358. ***See Instruction Section III.M***

☐ Check this box if this information is the same as the General Contact information (Block 2) and complete lines 80-82.

75 Lumos Networks dba Segra
Remittance Company Name, if different from Company or Billed Entity Name

76 First: Anthony Middle Initial: Last: Strohman 77 Accts Rece
Remittance Contact Name - Statements will be sent to Remittance Contact's attention Title

78 (803) 726-4074 Ext 79 Anthony.Stroman@segra.com
Phone Number E-mail Address for receipt of remittance advice

80 BB&T
Remittance Financial Institution for ACH or locked box transfer of funds (required)

81 [redacted] 82 [redacted]
Financial Institution Account Number for ACH (required) ACH Financial Institution Transit Number - must be nine digits (required)

Block 13: Organization Contact for Schools and Libraries Support

See Instruction Section III.N

☐ Check this box if this information is the same as the General Contact information (Block 2) and continue on to Block 14.

83 First: Anthony Middle Initial: Last: Strohman 84 Accts Receivable
Contact Name for Schools and Libraries Program Title
(Must be a company, or entity employee or designated representative)

85 1500 Hampton St
Contact Address for Schools and Libraries Program

86
Address Line 2

87 Columbia 88 SC 89 29201
City State Zip Code + 4

90 (803) 726-4074 Ext 91 Anthony.Stroman@segra.com
Phone Number E-mail Address of Schools and Libraries Program Contact

Disbursement Offsets and Healthcare Connect Certification

Block 15: Offsetting Disbursement Payments Against Federal Universal Service Contribution Obligations For High Cost Participants

See Instruction Section III.P

The following information pertains only to telecommunications companies participating in the High Cost Program. A telecommunications company may choose to offset its payment against its Federal universal service contribution. A telecommunications company must have an FCC Form 499 Filer ID number in order to offset its High Cost Program payments against its Federal universal service contribution. In order to obtain an FCC Form 499 Filer ID number, visit https://www.usac.org/service-providers/resources/forms and select FCC Form 499. You do not need an FCC Form 499 Filer ID in order to be issued a FCC Form 498 ID.

92 ☐ Yes, I want my High Cost Program disbursement payments to be offset against my Federal universal service contribution obligations. This box must be checked in order to receive offsets. The Default is "No."

Block 16: Offsetting Disbursement Payments Against Federal Universal Service Contribution Obligations For Lifeline Participants

See Instruction Section III.Q

The following information pertains only to telecommunications companies participating in the Lifeline Program. A telecommunications company may choose to offset its payment against its Federal universal service contribution. A telecommunications company must have an FCC Form 499 Filer ID number in order to offset its Lifeline Program payments against its Federal universal service contribution. In order to obtain an FCC Form 499 Filer ID number, visit https://www.usac.org/service-providers/resources/forms and select FCC Form 499. You do not need an FCC Form 499 Filer ID in order to be issued a FCC Form 498 ID.

93 ☐ Yes, I want my Lifeline Program disbursement payments to be offset against my Federal universal service contribution obligations. This box must be checked in order to receive offsets. The Default is "No."

Block 17: Offsetting Disbursement Payments Against Federal Universal Service Contribution Obligations For Rural Healthcare Participants

See Instruction Section III.R

The following information pertains only to telecommunications companies participating in the Rural Health Care Program. In accordance with FCC rule section 54.679 regarding Rural Health Care payments, a telecommunications company may choose to offset its payment against its Federal universal service contribution. A telecommunications company must have an FCC Form 499 Filer ID number in order to offset its Rural Health Care Program payments against its Federal universal service contribution. In order to obtain an FCC Form 499 Filer ID number, visit https://www.usac.org/service-providers/resources/forms and select FCC Form 499. You do not need an FCC Form 499 Filer ID in order to be issued a FCC Form 498 ID.

94 ☐ Yes, I want my Rural Health Care Program disbursement payments to be offset against my Federal universal service contribution obligations. This box must be checked in order to receive offsets. The Default is "No."

Block 18: Certification to Assist Health Care Providers

See Instruction Section III.S

In accordance with FCC rule section 54.640(b), service providers participating in the Healthcare Connect Fund Program must certify, as a condition of receiving support, that they will provide to health care providers, on a timely basis, all information and documents regarding supported equipment, facilities, or services that are necessary for the health care provider to submit required forms or respond to FCC or USAC inquiries. USAC may withhold disbursements to the service provider if the service provider, after written notice from USAC, fails to comply with this requirement.

95 ☑ I certify, as a condition of receiving support under the Healthcare Connect Fund Program, that the above-named service provider will provide to health care providers, on a timely basis, all information and documents regarding the supported equipment, facility(ies), or service(s) that are necessary for the health care provider to submit required forms or respond to FCC or USAC inquiries.

Block 19: Offsetting Disbursement Payments Against Federal Universal Service Contribution Obligations For Schools and Libraries Participants

See Instruction Section III.T

The following information pertains only to telecommunications companies participating in the Schools and Libraries Program. In accordance with FCC rule section 54.515 regarding Schools and Libraries Program payments, a telecommunications company may choose to offset its Schools and Libraries Program payment against its Federal

96 ☐ Yes, I want my Schools and Libraries Program disbursement payments to be offset against my Federal universal service contribution obligations. This box must be checked in order to receive offsets. The Default is "No."

Service Identification

Block 20: Principal Communications Types [REQUIRED Field]

See Instruction Section III.U

Select up to 5 boxes that best describe the reporting entity. Enter numbers starting with "1" to show the order of importance -- see instructions.

	Audio Bridging Provider		Interconnected VoIP
	Coaxial Cable		Paging and Messaging
	Non-Interconnected VoIP		SMR (Dispatch)
	Private Service Provider		Shared-Tenant Service Provider
	Toll Reseller		Cellular/PCS/SMR
	Incumbent LEC Operator		Interexchange Carrier
	Service Provider Satellite		Payphone Service Provider
	Service Provider Wireless		Local Reseller
	Data		Internet Service Provider
1	CAP/CLEC		Non-Traditional Provider (NTP)
	Network / Infrastructure		School/Library or other Billed Entity Recipient

Data Act Business Types

Block 21: Data Act Business Types [REQUIRED Field]

See Instruction Section III.V

Select up to 3 boxes that best describe the reporting entity. Enter numbers starting with "1" to show the order of importance – see instructions.

	State Government
	County Government
	City or Township Government
	Special District Government
	Regional Organization
	U.S. Territory or Possession
	Independent School District
	Public/State Controlled Institution of Higher Education
	Indian/Native American Tribal Government(Federally-Recognized)
	Indian/Native American Tribal Government (Other than Federally-Recognized)
	Indian /Native American Tribal Designated Organization
	Public/Indian Housing Authority
	Nonprofit with 501C3 IRS Status (Other than an Institution of Higher Education
	Nonprofit without 501C3 IRS Status (Other than an Institution of Higher Education
	Private Institution of Higher Education
	Individual
1	For-profit Organization (Other than Small Business)
	Small Business
	Hispanic-serving Institution
	Historically Black College or University (HBCU)
	Tribally Contolled College or University (TCCU)
	Alaska Native and Native Hawaiian Serving Institution
	Non-domestic (non-U.S.) Entity
	Other

Officer Certification

Block 22: Officer Certification [All Fields REQUIRED]

See Instruction Section III.W

I certify that I am an officer of the above-named service provider, that I am authorized to submit this FCC Form 498 data on behalf of the above named

Persons willfully making false statements on this form can be punished by fine or forfeiture, under the Communications Act, as amended, 47 U.S.C. Secs. 220(e), 502, 503(b), or fine or imprisonment under Title 18 of the United States Code, 18 U.S.C. Sec. 1001.

Officer Information		Check this box if this information is the same as the General Contact information (Block 2)

Signature of the Officer Date

First: Middle Initial: Last: Title

Printed Name

E-mail Address of Company Officer

Notice: The Federal Communications Commission (the Commission) has designated the Universal Service Administrative Company (USAC) as administrator of Federal universal service. One of the functions of USAC is to provide a mechanism for the billing, collection, and disbursement of funds for the various Federal universal service programs. In an effort to implement these requirements and obligations, the Commission has adopted this collection of information. Pursuant to the Commission rules, 47 C.F.R. §§ 54.301, 54.303, 54.307, 54.309, 54.311, 54.407, 54.413, 54.515, 54.611, 54.702, 54.802, and 54.902, USAC must obtain information relating to service provider name and address, telephone number, Federal employee identification number, contact names and telephone numbers, and billing and collection information. Each service provider receiving Federal universal service support from the High Cost, Lifeline, Rural Health Care, or Schools and Libraries Programs, should complete the FCC Form 498. USAC will use this information in administering the billing, collections, and disbursement operations of the Federal universal service programs.

Reminder: You are not required to respond to a collection of information sponsored by the Federal government, and the government may not conduct or sponsor this collection, unless it displays a currently valid Office of Management and Budget (OMB) control number. This collection has been assigned an OMB control number of 3060-0824.

The Commission is authorized under the Communications Act of 1934, as amended, to collect the information we request in this form. We will use the information you provide for the Federal universal service billing, collections, and disbursement purposes. If we believe there may be a violation or a potential violation of a state or Federal statute, or of a Commission regulation, rule, or order, your form may be referred to the Federal, state, or local agency responsible for investigating, prosecuting, enforcing, or implementing the statute, rule, regulation, or order. In certain cases, the information in your application may be disclosed to the Department of Justice, a court, or adjudicative body when (a) the Commission; or (b) any employee of the Commission; or (c) the United States Government is a party of a proceeding before the body or has an interest in the proceeding. In addition, consistent with the Communications Act of 1934, FCC regulations and orders, the Freedom of Information Act, 5 U.S.C. § 552, or other applicable law, information provided in or submitted with this form or in response to subsequent inquiries may be disclosed to the public.

If you owe a past due debt to the Federal government, the information you provide may also be disclosed to the Department of the Treasury Financial Management Service, other Federal agencies, and/or your employer to offset your salary, IRS tax refund, or other payments to collect that debt. The Commission may also provide the information to these agencies through the matching of computer records where authorized.

If you do not provide the information we request on the form, the Commission may delay processing of your application, or may return your application without action.

This Notice is required by the Paperwork Reduction Act of 1995, Pub. L. No. 104-13, 44 U.S.C. 3501 et seq. We have estimated that each response to this collection of information will take, on average, 1 hour. Our estimate includes the time to read the instructions, look through existing records, gather and maintain the required data, and actually complete and review the form for response. If you have any comments on this estimate, or how we can improve the collections and reduce the burden it causes you, please write to the Federal Communications Commission, AMD-PERM, Washington D.C. 20554, Paperwork Reduction Project (3060-0824). We will also accept your comments via Internet if you send them to PRA@fcc.gov. Please DO NOT SEND COMPLETED DATA COLLECTION FORMS TO THIS ADDRESS.

To submit this form: **Access the USAC E-File System here: http://usac.org/about/tools/e-file.aspx/**

For support: **USAC Customer Operations, Forms Processing**
700 12th Street, N.W., Suite 900
Washington, DC 20005
(888) 641-8722
CustomerSupport@usac.org

Questions? **See the FCC Form 498 Instructions found at https://www.usac.org/service-providers/resources/forms**

Use this form for:

- New application for a FCC Form 498 ID (FKA SPIN/Service Provider Identification Number)
- Revision to existing 498 data currently on file with USAC
- Merger or Consolidation of FCC Form 498 ID (Additional documentation is required, please see page 2 of the instructions)
- Deactivation of an FCC Form 498 ID (Please see page 2 of the instructions)

Segra's FCC Form 473

FCC Form 473

Do not write in this space.

Approval by OMB
OMB Control No. 3060 – 0856
Estimated time per response: 1.0 hours

Please read instructions before completing.

Universal Service for Schools and Libraries
Service Provider Annual Certification Form

(To be completed by Service Provider)

Block 1: Service Provider Information

1. Service Provider Name
Lumos Networks LLC

2. Service Provider Identification Number (SPIN)	**3. Funding Year:**
143024848	July 1, 2022 through June 30, 2023

4. Contact Name
Anthony Stroman

5. Complete Mailing Address of Contact Person
Street Address, P.O. Box or Route Number
1500 Hampton St

Columbia	SC	29201
City	**State**	**Zip Code**

6. Telephone Number with Area Code	**7. Fax Number with Area Code**
803-726-4074	803-726-4175

8. Email Address
anthony.stroman@segra.com

Block 2: Certification

I declare under penalty of perjury that the foregoing is true and correct: I am authorized to submit this Service Provider Annual Certification Form on behalf of the above-named Service Provider, which has been assigned the above-referenced Service Provider Identification Number, and that based on information known to me or provided to me by employees responsible for the data being submitted, I hereby certify that the data set forth in this Form has been examined and reviewed and is true, accurate and complete. I acknowledge that any false statement on this Form or on the Service Provider Invoice Form (FCC Form 474) can be punished by fine or forfeiture under the Communications Act, 47 U.S.C. § 502, 503 (b), or fine or imprisonment under Title 18 of the United States Code, 18 U.S.C. § 1001, and that any such false statement could subject this Service Provider to liability under the False Claims Act.

9. I certify that the Service Provider Invoice Forms (FCC Form 474) that are submitted by this Service Provider contain requests for universal service support for services which have been billed to the Service Provider's customers on behalf of schools, libraries, and consortia of those entities, as deemed eligible for universal service support by the fund administrator.

10. I certify that the Service Provider Invoice Forms (FCC Form 474) that are submitted by this Service Provider are based on bills or invoices issued by the Service Provider to the Service Provider's customers on behalf of schools, libraries, and consortia of those entities as deemed eligible for universal service support by the fund administrator, and exclude any charges previously invoiced to the fund administrator for which the fund administrator has not yet issued a reimbursement decision.

11. I certify that the bills or invoices issued by this Service Provider to the Billed Entity are for equipment and services eligible for universal service support by the Administrator, and exclude any charges previously invoiced to the Administrator by the Service Provider.

12. I certify that any requests for reimbursement that are sought under a Service Provider Invoice Form (FCC Form 474) for discounts for products or services that contain both eligible and ineligible components are properly allocated as required by the Commission's rules at 47 C.F.R. § 54.504(e).

13. I certify that the invoices that are submitted by this Service Provider to the Billed Entity for reimbursement pursuant to Billed Entity Applicant Reimbursement Forms (FCC Form 472) are accurate and represent payments from the Billed Entity to the Service Provider for equipment and services provided pursuant to E-rate program rules.

Service Provider Name Lumos Networks LLC
SPIN 143024848
Contact Name Anthony Stroman
Contact Telephone Number 803-726-4074

Block 2: Certification (Continued)

14. I certify that this Service Provider makes available to customers, upon their request, separate prices for distinct services to assist Billed Entity Applicants in identifying the portions of their bills that represent the costs of services provided to eligible entities for eligible purposes.

15. I certify that no non-discount portion of the costs for eligible services will be waived, paid, or promised to be paid by this Service Provider. I acknowledge that the provision by any service provider of a supported service, or of free services or products unrelated to the supported service or product constitutes a rebate of the non-discount portion of the supported services as stated in 47 C.F.R. § 54.523.

16. I certify that no kickbacks, as defined in 41 U.S.C. § 8701, were paid by this Service Provider to anyone in connection with the schools and libraries universal support program.

17. I certify that this Service Provider is in compliance with the Commission's rule and orders regarding gifts and this Service Provider has not directly or indirectly offered or provided any gifts, gratuities, favors, entertainment, loans, or any other thing of value to any eligible schools, libraries, or consortium that includes eligible schools or libraries, except as permitted by the Commission's rule at 47 C.F.R. § 54.503(d).

18. I certify that if the fund administrator, as necessary, requests additional supporting information, this Service Provider will make all documents requested available to the Fund Administrator as required by 47 C.F.R. § 54.516(b). I certify that this Service Provider will retain for at least 10 years (or whatever retention period is required by the rules in effect at the time of this certification), after the latter of the last day of the applicable funding year or the service delivery deadline for the funding requests, (1) any and all records that I rely upon to complete this form and each Service Provider Invoice Form (FCC Form 474) that is submitted by this Service Provider during the present funding year, (2) any and all records issued by this Service Provider to the Billed Entity for reimbursement pursuant to Billed Entity Applicant Reimbursement Forms (FCC Form 472), and (3) all documents necessary to demonstrate compliance with the statutory or regulatory requirements for the schools and libraries universal service support program as required by 47 C.F.R. § 54.516(a)(2) I acknowledge that this Service Provider may be audited pursuant to 47 C.F.R. § 54.516(c), and that the Service Provider must provide such records as required by 47 C.F.R. § 54.516(b)

19. I certify that the prices in any offer that this Service Provider makes pursuant to the schools and libraries universal service support program have been arrived at independently, without, for the purpose of restricting competition, any consultation, communication, or agreement with any other offeror or competitor relating to (i) those prices, (ii) the intention to submit an offer, or (iii) the methods or factors used to calculate the prices offered.

20. I certify that the prices in any offer that this Service Provider makes pursuant to the schools and libraries universal service support program will not be knowingly disclosed by this Service Provider, directly or indirectly, to any other offeror or competitor before bid opening (in the case of a sealed bid solicitation) or contract award (in the case of a negotiated solicitation) unless otherwise required by law.

21. I certify that no attempt will be made by this Service Provider to induce any other concern to submit or not to submit an offer for the purpose of restricting competition.

22. I certify that this Service Provider is not suspended or debarred from participating in Federal programs.

23. I certify that, in addition to the foregoing, this Service Provider is in compliance with the rules and orders governing the schools and libraries universal service support program, and acknowledges that failure to be in compliance and remain in compliance with those rules and orders may result in the denial of discount funding and/or cancellation of funding commitments. I acknowledge that failure to comply with the rules and orders governing the schools and libraries universal service support program could result in civil or criminal prosecution by law enforcement authorities.

24. I certify that no universal service support has been or will be used to purchase, obtain, maintain, improve, modify, or otherwise support any equipment or services produced or provided by any company designated by the Federal Communications Commission as posing a national security threat to the integrity of communications networks or the communications supply chain since the effective date of the designations.

25. I certify that no Federal subsidy made available through a program administered by the Commission that provides funds to be used for the capital expenditures necessary for the provision of advanced communications services has been or will be used to purchase, rent, lease, or otherwise obtain, any covered communications equipment or service, or maintain any covered

communications equipment or service previously purchased, rented, leased, or otherwise obtained, as required by 47 C.F.R. § 54.10.

26. Signature of authorized person	27. Date
Signed electronically by Anthony Stroman	5/31/2022
28. Printed name of authorized person	
Anthony Stroman	

29. Title or position of authorized person
E-Rate/RHCP Coordinator

Address of authorized person
1500 Hampton St, Columbia SC 29201

31. Telephone number of authorized person
803-726-4074

FCC NOTICE FOR INDIVIDUALS REQUIRED BY THE PRIVACY ACT AND THE PAPERWORK REDUCTION ACT

Part 54 of the Commission's Rules authorizes the FCC to collect the information on this form. Failure to provide all requested information will delay the processing of the application or result in the application being returned without action. Information requested by this form will be available for public inspection. Your response is required to obtain the requested authorization.

The public reporting for this collection of information is estimated to be 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the required data, and completing and reviewing the collection of information. If you have any comments on this burden estimate, or how we can improve the collection and reduce the burden it causes you, please write to the Federal Communications Commission, AMD-PERM, Paperwork Reduction Act Project (3060-0856), Washington, DC 20554. We will also accept your comments regarding the Paperwork Reduction Act aspects of this collection via the Internet if you send them to PRA@fcc.gov. PLEASE DO NOT SEND YOUR RESPONSE TO THIS FORM TO THIS ADDRESS.

Remember – You are not required to respond to a collection of information sponsored by the Federal government, and the government may not conduct or sponsor this collection, unless it displays a currently valid OMB control number or if we fail to provide you with this notice. This collection has been assigned an OMB control number of 3060-0856.

THE FOREGOING NOTICE IS REQUIRED BY THE PRIVACY ACT OF 1974, PUBLIC LAW 93-579, DECEMBER 31, 1974, 5 U.S.C. 552a(e)(3) AND THE PAPERWORK REDUCTION ACT OF 1995, PUBLIC LAW 104-13, OCTOBER 1, 1995, 44 U.S.C. SECTION 3507.

Segra's Detailed Work Breakdown Structure

Detailed Work Breakdown Structure with Intermediate & Major Milestones

The preliminary Work Breakdown Structure (WBS) is provided as this attachment. Upon award, the PM team will align this with the final project schedule.

Timeline to Completion at High Level

- Turn up for fiber serviced sites <45 days
- Estimated installation window is 90 to 120 calendar days from receipt of contract/award, which can be adjusted/expedited per customer request
- SD-WAN deployment is 4 to 6 weeks

The Segra Project Coordinator will work closely with the State of West Virginia to create the SDP (Service Design Package) to define project deliverables, specify solution delivery processes, and gain formal approval for the SD-WAN project. Please refer to the **SD-WAN Workbook**, included in our response on page 296.

The Project Coordinator/Project Manager will involve other members of our joint service implementation teams as needed during the development of the SDP. Please see the **List of All Significant Activities, Major Milestones, and Deliverables** below.

Once the SDP is established, Segra will begin the following process to provide the SD-WAN solution to the State of West Virginia. The information below provides a high-level overview of the process, and major milestones are noted with an asterisk (*).

Intermediate and Major Milestones

Step	Phase	Activities
1	Assessment of Site-by-Site Requirements and Solution Design	✓ Segra Engineers will work with the State to determine the configuration parameters for the State of West Virginia's SD-WAN policies on a site by-site basis.
2	Order Entry	✓ The Order Entry group will work with the Segra account team for the State of West Virginia to confirm the accuracy of all order information.
3	Project Review	✓ The Engineering team will review node needs and bandwidth utilization for the proposed fiber routes. Any network enhancements/augmentations will be identified at this time and shared with the State of West Virginia as possible dependencies.
4	Site Walks	✓ The Project Manager, Operations, and Outside Plant teams will schedule and make site visits to gather as much information as possible about the fiber route and customer premise needs. Also in this phase, the teams will identify any contingencies or dependencies that may alter or affect the overall Project Plan timelines.
5	Discovery Calls	✓ The Segra Project Coordinator/Project Manager will initiate a sequence of internal and external discovery calls. The internal discovery call will bring together the Segra teams involved in the

Step	Phase	Activities
		project to clarify and confirm the State of West Virginia's requirements and corresponding implementation parameters. ✓ The external discovery call will be the Project Manager's first official contact with the State of West Virginia to discuss all phases of the installation. The Project Manager will also convey timelines, contacts, and contingencies to the customer, as well as escalation processes.
6	Make Ready*	✓ In this phase (normally the longest), Outside Plant Engineering will have all fiber route easements, pole-attachment agreements, and local government zoning restrictions/policies resolved. ✓ At this point, a job package will be built and released to the Outside Plant Construction group. ✓ For information about the make-ready activities for the customer site, please refer to **Segra's Remediation Guide** and **Segra Environmental-Electronic Requirements for Fiber Projects**, included in our response on pages 309 and 307, respectively.
7	Construction*	✓ The Outside Plant group will execute the fiber build to the State of West Virginia location. The Outside Plant group will also work with the State of West Virginia to get entrance conduits and internal fiber routes/conduit in place to reach the predetermined demarcation point.
8	Equipment Installation*	✓ The Operations group will work with the State of West Virginia to get the needed Ethernet/DWDM equipment installed and powered up at the predetermined demarcation point (phases 6, 7, and 8 are worked in parallel).
9	Network Routing	✓ The Network Engineering group will map the State of West Virginia circuit through our network, in preparation for equipment turn-up and customer handoff.
10	Node Insertion and Splicing*	✓ The Outside Plant and Operations groups will schedule, internally and externally, the window for the maintenance work necessary to splice and insert the equipment into the designated fiber ring and verify that the ring integrity is re-established.
11	Testing*	✓ The Operations group will work with our Data Maintenance Engineers to activate any customer-facing ports for testing purposes. ✓ The Operations group will run any required tests or predetermined testing parameters from the customer. If required by the State of West Virginia, circuit testing birth certificates can be provided. ✓ Please refer to the **Managed Network Service (MNS) Testing Criteria**, under **Segra's SD-WAN Solution Exhibit**, included in our response on page 180.
12	Cutover Scheduling	✓ The Project Manager schedules a time with the State of West Virginia to cut over to the Segra network.

Step	Phase	Activities
13	Network Cutover*	✓ The Operations group works with the State of West Virginia and the Data Maintenance Engineering group to groom traffic/services over to the Segra network.
14	Administrator Training	✓ Prior to the training sessions, Segra will work with the State of West Virginia to create the necessary login credentials and permission levels for the users to be trained. ✓ On the cutover day for the first State of West Virginia location to be activated, Segra team members will provide on-site training for the State of West Virginia's SD-WAN administrators. ✓ This training will be recorded for future reference and playback, and additional live training options will be available for the other State of West Virginia sites as they come online with the SD-WAN service. ✓ Please refer to the **Training** section, under **Segra's SD-WAN Solution Exhibit**, included in our response on page 179.
15	Support	✓ The Segra Network Operations Center (NOC), Customer Network Operations Center (CNOC), and Customer Support Center (CSC) will begin supporting the State of West Virginia upon cutover with 24/7/365 support.
16	Close Out	✓ The Project Manager reviews the implementation status with the customer to identify any additional needs the customer may have and address them. ✓ If there are no open issues, the Project Manager will close out the project and send completion literature to the State of West Virginia, notifying them that all Segra-related implementation items have been delivered and the services will be placed into billing.

List of All Significant Activities, Major Milestones, and Deliverables

Significant Activities and Major Milestones

At a high level, the project will follow the steps listed below:

- Understand the State of West Virginia current Network/Environment
- Prepare Implementation Team for the State of West Virginia
- Customer/State of West Virginia Kick-off call (review initial orders and provide contacts/roles)
- Segra Personnel (Sales Engineer) to work with the State of West Virginia personnel on SD-WAN and, if needed, corresponding MPLS Workbook population (please refer to the **MPLS Workbook**, included in our response on page 299 and the **SD-WAN Workbook**, included in our response on page 296)
- Create Users and Roles for Access
- Create Security Access Rules for the State of West Virginia Access to GUI
- Document Existing State of West Virginia Network and Outline Transition Plan
- Gather SD-WAN configuration details for each location (please refer to the **SD-WAN Workbook**, included in our response on page 296)

- Prepare the State of West Virginia Environment
- Configuration of Edge Devices per the SD-WAN Workbook (please refer to the **SD-WAN Workbook**, included in our response on page 296)
- Verify all Devices are Being Monitored (test failover and NOC monitoring)
- Resolve any noticed troubles or routing adjustments needed
- Review Events for Accuracy
- Set Up Notification Policy and Optional Weekly Reports
- Incident Review - Verify notifications and reports are being generated and delivered
- Training of key personnel on the SD-WAN portal, engagement with support, review of maintenance and escalation procedures
- Acceptance Testing
- Project Review/Complete

	Week 1-2	Week 3-4	Week 5	Week 6
Call #1 Kickoff	1 Hour			
Call #2 Gateway/Orchestrator setup	1.5 Hours			
Call #3 Device configuration for initial Edge Devices	1 Hours			
Configures remaining devices		10-40 Hours		
Schedule optional 1 hour troubleshooting calls		1 Hour		
Once all devices reporting in, schedule incident review 1 week out		0 Hours		
Call #4 Incident Review and Tuning / customer training			1 Hours	
Turn on reports and notifications			0 Hours	
Project Review/Complete				Complete

General Deployment Guidelines and Times

Segra Team Internal Kick-off

- Get Segra technical POC information and complete Work Order and Discovery Worksheet
- List the requirements needed to implement/set up at the State of West Virginia site (protocols, accounts, rules, population of corresponding needed workbooks)
- Overview of the SD-WAN platform
- Customer information: number of locations and corresponding circuits, local and technical contacts
- Document existing network and outline transition from current MPLS network to future MPLS/SD-WAN network with consideration of minimal impact on Agency Office(s) and users as well as maintaining communications between offices
- List proposed installation dates for each location for circuit delivery and availability
- Gather any additional helpful information that we should know about the State of West Virginia

State of West Virginia Kick-Off Call

- Introduction and Roles
- Agenda Overview
- Brief description of installation process
- Overview of data we need to gather pre-installation
- Discuss customer schedule and time restraints
- Set a proposed install date
- Agree upon action items

Gateway Orchestrator Configuration

- Completed by Segra in accordance with conversations and population of SD-WAN workbook
- Set up of corresponding logins
- Acceptance Testing - Review with the State of West Virginia corresponding personnel, validate configured appropriately prior to Edge device configurations

Review and Tuning

- Review current configuration and performance
- Ensure it meets the State of West Virginia's expectations
- Adjust appropriately if needed, assure NOC/CNOC/CSC/Elite NOC are up to date on any changes made

Reporting/Alerting

- Ensure that NOC(s) are receiving appropriate alarms
- Ensure local and technical contacts are up to date for specific location(s)

Project Review/Complete

- Ensure that corresponding sites as they relate to the requests from the order are fulfilled, functioning properly, and as desired by the State of West Virginia personnel
- Order deemed as complete and set up for appropriate agreed upon billing

Deliverables

The Segra PM will work closely with the State of West Virginia during the planning phase to confirm layout/content requirements for each deliverable and confirm recipients (e.g., email distribution lists). Segra will typically submit deliverables electronically. The reports can include detailed items, such as labor hours expended, materials used, and issues encountered. These reports provide vital status on whether a job is completing ahead of or behind schedule, as well as what factors may be affecting it.

SEGRA

SD-WAN Workbook

Customer Information

SEGRA

Account Information

Customer Name:		Sales Rep:	
Quote # :		Sales Support Rep:	
OPP-ID:		Sales Engineer:	
Existing Customer Account #:		Technical Contact:	
Revised By:		Revised Date:	

Authorized Velo Contacts

Name:		Name:	
Cell:		Cell:	
Work:		Work:	
Email:		Email:	
Alerts?		Alerts?	

Customer Private IP and VLAN Information

LAN Name/Location	IP Subnet	Subnet Mask	DNS	DHCP Pool	VLANs

Comments:

SD-WAN Service Workbook

Site Information

Site Address	

Service Types

MPLS Connection Type	Select	SD-WAN High Availability?	Select
SD-WAN Make/Model		Are there Non-VeloCloud SD-WAN devices?	No

WAN Connectivity

Number of Access Loops: *(How many WAN connections are there into the VeloCloud Edge?)*

WAN Accesses	Provider	Type	IP Address	Subnet Mask	Gateway IP Address
WAN Access 1	Select	Select			
WAN Access 2	Select	Select			
WAN Access 3	Select	Select			
WAN Access 4	Select	Select			
WAN Access Comments:					

Customer Layer 3 Device on LAN

Will there be a Layer-3 (Routing Device) on the LAN-Side of the Velocloud Edge?	

Layer 3 Device Notice

Please note that in the event of a customer router on the LAN-side of the VeloCloud Edge device, that SEGRA will hand-off a /30 to peer with that router. Subnets within the MPLS network will be statically-routed to that router. In this case, most of the SD-WAN functionality (Analytics, performance, etc.) are lost. This is not recommended by SEGRA. SEGRA recommends that the VeloCloud device handle all Layer 3 functionality.

Layer 3 Device Comments:	

Applications

Please Identify Business-Critical Applications (add additional rows, if necessary).

Application Name	
Application Description	
Application IP Address	
Application DNS Name	
Any other Unique Identifier (TCP Port, etc.)	

VPN

Will customer be utilizing Segra Hosted or Managed Firewall Service?	Select
Will this location participate in Site-to-Site VPN(s)?	Select
Will this site need to connect to a Data Center VPN?	Select

Make/Model of Firewall/VPN Concentrator	Make	
	Model	
Source NAT Address		(e.g. 165.166.9.254/X)
Subnets at Data Center		(e.g. 165.166.9.254/X)
		(e.g. 165.166.9.254/X)
		(e.g. 165.166.9.254/X)

Additional VPN Notes

INTERNET / FIREWALL / NAT

How do users access the internet from this site?	Select
Are we replacing a firewall at this location?	Select

If the answer to the above is yes, please include any inbound NAT rules, below:

SEGRA

MPLS Workbook

Customer Information

SEGRA

Account Information			
Customer Name:		Sales Rep:	
Quote # :		Sales Support Rep:	
OPP-ID:		Sales Engineer:	
Existing Customer Account #:		Technical Contact:	
Revised By:		Revised Date:	

									VPNN (L3) ONLY									
Site #	Site Name	Site Address	City	State	Service Type	Bandwidth (MB/LTE)	MPLS Type	QOS	CPE Management	Router Model	Routing Protocol	Router Network	Prefix	LAN Name/Location	IP Subnet	Subnet Mask	DNS	DHCP Pool	VLANs
	ex. Main Site				Select		Select	Select	Select	Select	Static	192.168.251.0/24 (Segra Default)	/30						
	ex. Remote OR Main Site Hand off #2																		

Additional Notes:

Quality of Service Templates

	Std	CoS-Basic		CoS-Premium				Custom CoS-Premium	
Class	DE001	BA001	BA002	PR001	PR002	PR003	PR004	PR005	PR006
Real-Time	N/A	N/A	N/A	25%	50%	30%	0%	70%	35%
Interactive	N/A	N/A	N/A	25%	5%	20%	50%	5%	35%
Priority Business	N/A	50%	75%	25%	25%	25%	25%	15%	20%
Best Effort[1]	100%	Default	Default	Default	Default	Default	Default	Default	Default

Best Effort (BE) is the default class and is not configured with policies. In order to ensure BE traffic does not get starved out by Priority Business class traffic, 10% of overall bandwidth is reserved for the BE class. Both BE and Priority Business can burst to utilize all available bandwidth when available.

Priority Business Burst and Best Effort Burst can compete for available bandwidth and are allocated the available bandwidth based on a weighted ratio. For example, with template PR001, the burst traffic is allocated at a 25:10 ratio between Priority Business and BE

Segra's Sample Bill

SUB-ACCOUNT SAMPLE INVOICE

SEGRA

Voice. Data. Internet.

PO Box 631140
Cincinnati, OH 45263-1140

Invoice Information

Invoice Date:	06/01/22
Account Number:	########
Invoice Number:	9999999
Due Date:	06/26/22
Total Amount Due:	**$0.97**
Amount Enclosed:	$_____

Please put your account number on your check and make payable to Segra

Segra
PO Box 631140
Cincinnati, OH 45263-1140

West Virginia Office of Technology
ATTN: Jessica L Hovanec
ALL STATE AGENCIES
VARIOUS LOCATIONS AS INDICATED BY ORDER

########################## ############

Please detach and return above portion with your payment

Invoice Information

Invoice Date:	06/01/22
Account Number:	########
Invoice Number:	999999
Due Date:	06/26/22
Total Due:	**$0.97**

Summary of Charges

Previous Balance:	0.00
Total Payments Received Through 06/01/22:	0.00
Balance Forward:	0.00
Total Voice Services:	0.20
State Tax:	0.01
State Universal Service Charge:	0.01
State Relay Fund:	0.25
E911 Tax:	0.50
Total Current Charges:	0.97
Total Amount Due by 06/26/22	0.97

Important Messages

This is a Sample Invoice to explain how Sub-Accounting will appear. Sub-Accounting is used when a customer needs to separate charges to multiple divisions.

Some examples are:

A Retail Establishment has several stores.
In this case, each store would be a different sub-account

B. A large office suite customer has different tenants in its building.
Each tenant would have a different sub-account.

C. Company needs to separate expenses by department (i.e. Accounting, HR, Sales and Outreach)
There are several sub-accounts:
Accounting
HR
Sales
Outreach

For more information regarding your account, please call us at 833.GO.SEGRA or email customercare@segra.com

SEGRA

Account Name Test Enterprise Account | **Account Number** ####### | **Invoice Number:** 9999999

Summary of Charges Through 06/31/22

NRC	Equip	Bundled	Voice	Data	Internet	Usage	Fees	Taxes	Totals
Account Level Charges									
0.00	0.00	0.00					0.00	0.00	0.00
Sub Account # 1									
0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
EQUIP.teteetette Test Enterprise Account									
0.00	0.00	0.00	0.00	0.00	0.00				0.00
ETHR.2000594..SPC te									
0.00	0.00			0.00	0.00				0.00
ETHR.2000753..SPC Te									
0.00	0.00			0.00	0.00				0.00
G11G11 Test Enterpris									
0.00	0.00			0.00	0.00				0.00
INTOFF.1000010 Test I									
0.00	0.00			0.00	0.00				0.00
TDM.4001322..SPC Test Enterprise Account									
0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	.00	0.00
TDM.4001706..SPC Test Enterprise Account									
0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	.00	0.00
8037244118 Mass Name Change									
0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.	0.00
803-726-7747 Mass Name Change									
0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.0	0.00
991-991-9923 Test Enterprise Account									
0.00	0.00	0.00	0.20	0.00	0.00	0.00	0.00	0.02	0.22
996-669-6321 Test Enterprise Account									
0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.75	0.75
ETHR.2002639..SPC Test Enterprise Account									
0.00	0.00			.00	0.00	0.00	0.00	0.00	0.00
ETHR.9994105..SPC Test E									
0.00	0.00			.00	0.00	0.00	0.00	0.00	0.00
ETHR.9999584..SPC Test E									
0.00	0.00			.00	0.00	0.00	0.00	0.00	0.00
TDM.4002316..SPC Test En									
0.00	0.00			.00	0.00	0.00	0.00	0.00	0.00
TDM.9992193..SPC Test Enterprise Account									
0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
TDM.YoYo999..SPC Test Enterprise Account									
0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	.00
Total									
0.00	0.00	0.00	0.20	0.00	0.00	0.00	0.00	0.77	0.97

MASTER SUMMARY PAGE

On the Master Summary page . sub-accounts will be indented to show services that fall under the sub-account.

The Master Summary page will appear on page 3 of any invoice. This shows all services rendered and the total will match the total from page 1 of the invoice. In this case it is $0.97

ITEMS that are not in a sub-account (at the account level).

SUB-ACCOUNT SUMMARY PAGE -

Each Sub-Account will have a separate summary page so charges can be viewed at a glance. Directly following these pages are the standard details for each of the services rendered in a sub-account per FCC standards.

	NRC	Equip	Bundled	Voice	Data	Internet	Usage	Fees	Taxes	Totals
Mass Name Change	0.00	0.00	0.00				0.00	0.00	0.00	0.00
EQUIP..te...otte Test Enterprise Accou...	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
ETHR 2000594..SPC test Ent...	0.00	0.00				0.00			0.00	0.00
ETHR 2000753..SPC Test Enterp	0.00	0.00				0.00			0.00	0.00
G11G11 Test Enterprise Accou	0.00	0.00				0.00			0.00	0.00
INTOF F.1000010 Test Enterpris	0.00	0.00				0.00	0.00		0.00	0.00
TDM.4001322..SPC Test Enterpr	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
TDM.4001706..SPC Test Enterprise Account	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
Total	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00

The sub-account name appears 1st

Services rendered under the Sub-Account will appear in numerical order first, then alphabetically (i.e Phone Number 555-555-5555 would appear before your circuit ID . These services will appear in the same order on the following pages.

Per line totals and the Sub-Account total appear in the last column

Monthly Charges - Continued

Mass Name Change
Mass Name Change Grand Total $0.00

. ETHR.2000594..SPC (A) Ent
Data Services
Access Bandwidth 03/01->03/31 Bandwidth 10 Mbps 0.00
Bandwidth/Private Line 03/01->03/31 Ethernet Bandwidth 0.00
Total Data Services $0.00

ETHR.2000594..SPC test Ent Grand Total $0.00

. ETHR.2000753..SPC Test Enterprise Account (B)
Data Services
Access Bandwidth 03/01->03/31 Bandwidth 20 Mbps
Bandwidth/Private Line 03/01->03/31 Ethernet Bandwidth 0.00
Total Data Services $0.00

ETHR.2000753..SPC Test Enterprise Account Grand Total $0.00

G11G11 Test Enterprise Account
Voice Services (C)
Voice Mail BW Anywhere
Features 03/01->03/31 Repeat Calling 0.00
Total Voice Services $0.00

Data Services (C)
Bandwidth/Private Line 03/01->03/31 Monthly Bandwidth Access 0.00
Total Data Services $0.00

G11G11 Test Enterprise Account Grand Total $0.00

. INTOFF.1000010 Test Enterprise Account
Internet Services
Internet Bandwidth 03/01->03/31 30 Mbs Download Speed 0.00
Internet Bandwidth 03/01->03/31 5 Mbs Upload Speed 0.00
Internet Bandwidth 03/01->03/31 Broadband Internet
Internet Bandwidth 03/01->03/31 Download Speed Group 0.00
Web Services 03/01->03/31 Upload Speed Group 0.00
Total Internet Services (D) $0.00

INTOFF.1000010 Test Enterprise Account Grand Total $0.00

. TDM.4001322..SPC Test Enterprise Account
Data Services
Access Bandwidth 03/01->03/31 DS1 0.00
Data Bandwidth 03/01->03/31 1 Gbps Data
Data Bandwidth 03/01->03/31 Data 0.00
Data Bandwidth 03/01->03/31 Data Bandwidth 0.00
Data Bandwidth 03/01->03/31 MPLS VPLS Service Interstate 0.00
Total Data Services $0.00

TDM.4001322..SPC Test Enterprise Account Grand Total (E) $0.00

. TDM.4001706..SPC Test Enterprise Account
Data Services
Access Bandwidth 03/01->03/31 DS1 0.00
Total Data Services $0.00

TDM.4001706..SPC Test Enterprise Account Grand Total $0.00

Mass Name Change Grand Total **$0.00**

SERVICE DETAIL PAGES

Details from the Summary page appear here. Items that are important :

A. **Service ID: Phone Number or Circuit ID. Appears here as: ETHR.2000594..SPC.**

B. **Service Name: Individual Line Name. Possibilities include Mary Smith or Reception Phone # 1, etc. Example: Test Enterprise Account**

C. **Category Header: From the summary page, these headers categorize the type of charge. Examples here: Voice/Data Service**

D. **Category Total: Total from categorized services. Example: Internet Services total**

E. **Service Grand Total: Also on far right column of Summary Page. Example: TDM.4001322..SPC Grand Total**

SEGRA

Segra Environmental-Electronic Requirements for Fiber Projects

SEGRA

SITE INSTALLATION REQUIREMENTS

- ✓ Commercial power requirements are for an outlet with dedicated 20 amp service w/isolated ground, 105-125 VAC, 60 Hz. *Outlet type will be* L520R (Twist Lock).
- ✓ #6 Stranded or solid, insulated copper ground to an approved ground source.
- ✓ Wall and floor space for installation of the equipment. Typical equipment installation options will be either a free standing floor cabinet or a wall mounted cabinet.

➢ General Space Requirement Guidelines:

- Cabinet = 4'w x 4d' x 6'h area free from obstructions.
- Wall Mount = 4'w x 6'h area with ¾" plywood.
  - Both options will require a 2'w x 2'h wall space with 3/4" plywood to be used for service distribution.
- Water lines, steam pipes, and cutoff valves within the immediate area of the equipment should be avoided.
- The immediate area around the equipment must be free of dirt and dust.
- Controlled environmental space with a temperature range of 45°**F** to 80°**F**, with relative humidity of 30%-55%.

➢ Access and Location Consideration:

- Building common space, equipment or existing telephone room, or area dedicated for telecommunication services.
- Entry with 24x7 unescorted access.
  - ☐ Yes, there is 24 hour unescorted access.
  - ☐ No, there is not 24 hour access. Please add contact information below

Name	
Contact Number	

➢ Fiber installation requirements - Customer's responsibility:

- A minimum of one and one-quarter inch (1.25") EMT conduit or plenum rated inner-duct from the fiber demarcation point inside the building to the exterior point of entry.
- On the outside of the building (Segra's connection point), a (minimum size) of 2" mogul LB or a 2" Smart LB, or an 18" x 18" x 10" pull box will need to be installed.
- All 90 degree bends must be "long radius". A pull box (24" x 6" deep must be installed after three (3) 90 degree.

X _____
Site Representative

_____
Site Representative Title

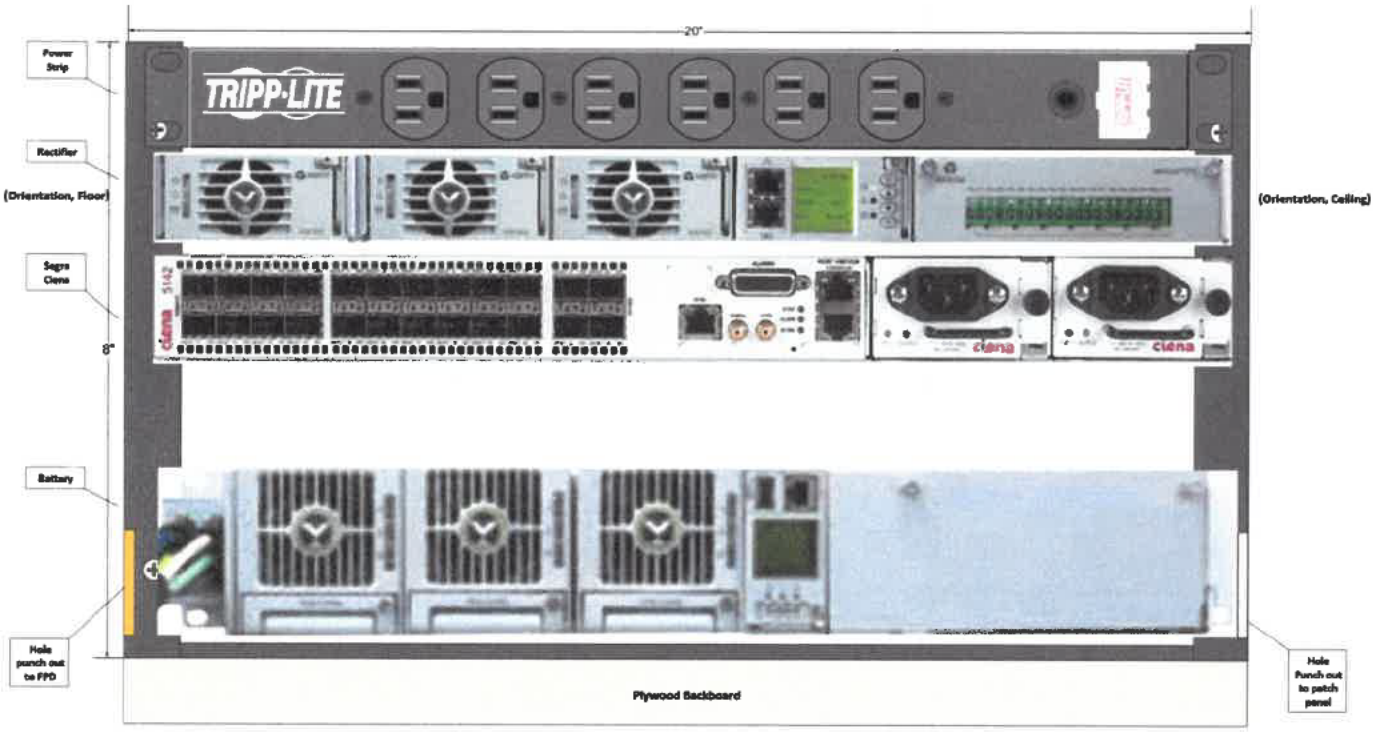
SEGRA

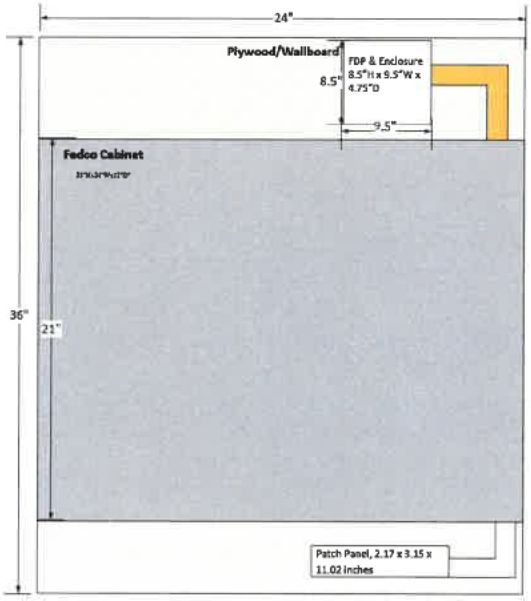
Segra's Remediation Guide

SEGRA

Segra Installation Model B (Ring)

- OCC 1RU FDP (RTC1U-3APB)
- Ciena 5142
- Rectifier
- Power Strip
- Minimum clear 2'x3' space, ¾" plywood wallboard
- Requires L520R within 5 feet
- Batteries (eight hours)





Segra Installation Model B Example (Ring)

Completed installed cabinet (door closed)

- FEDCO 21"Hx24"Wx12"D
- 180 degree full access cabinet
- Standard 19" vertical equipment mounting
- Includes PN CES-LVP-21x24x12-U-0, CES-LPV-GNDBAR5X1 , CES-LPV-MTGBKT (hardware, ground bar...)

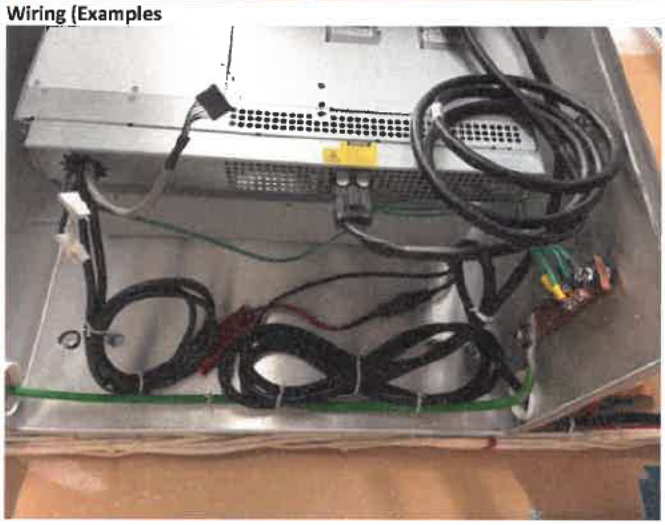
Completed installed cabinet (door open)

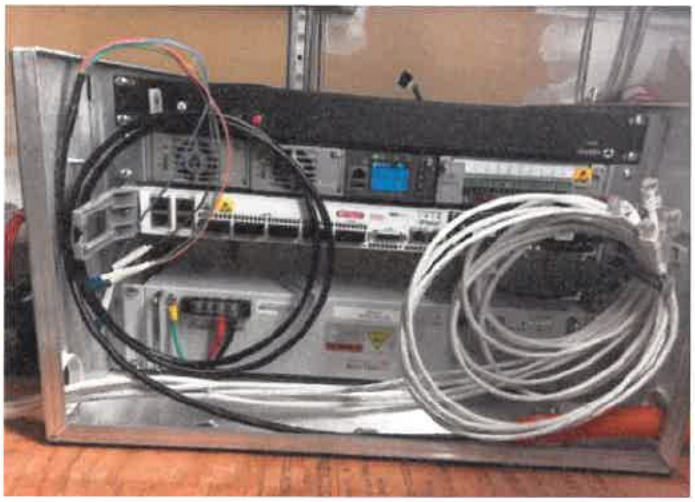
Installed equipment (switch and rectifier)

Installed equipment (Batteries)

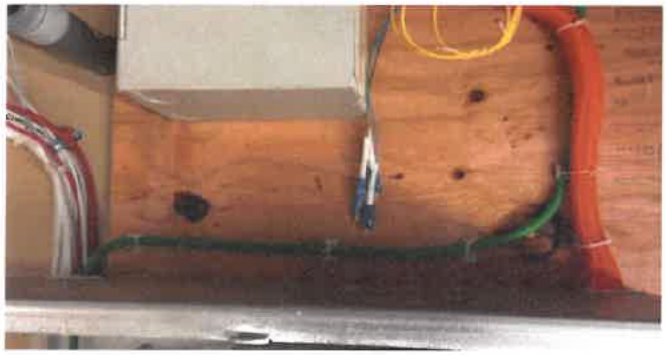
Installed equipment (Patch Panel customer DMARC)

Wiring (Examples





Grounding (equipment side)



Ground wire routing

Ground source

- Relay racks/cabinets must be grounded by placing an exposed #6 or larger grounding wire to the building's ground source.

Ground wire will be attached to the closest ground rod (earth ground) or building bus bar available and run to the Network Terminating Equipment location in the room.

L5-20R Twist lock

- 125 Volts
- 15 Amps

Power needs to be within 5' of placement of cabinet

SEGRA

2022 Pentest Results Summary

Executive Summary

Introduction and Scope

Optiv Security Inc. (Optiv) and Lumos Networks Inc. d/b/a SEGRA (SEGRA) collaboratively performed an Operational Technology Penetration Test consisting of logical network security testing techniques. The assessment was designed to evaluate the overall security posture associated with SEGRA logical network security controls intended to prevent unauthorized access and abuse of SEGRA information and assets.

Optiv conducted the Operational Technology Penetration Test as a full-disclosure/non-evasive engagement between April 11 and April 15, 2022. As is customary for this engagement type, Optiv readily leveraged information provided by SEGRA while not attempting to evade SEGRA's detective and preventive measures.

Findings Measurement and Rating

Throughout the duration of the test, Optiv discovered the following overall finding severities across all assessment activities performed during the Operational Technology Penetration Test.

Also shown is a general rating for each assessment category performed throughout this engagement. The rating definitions can be referenced in Appendix V.

Assessment Component	High	Med	Low	Info	Rating
OT Penetration Test	4	4	0	0	**Average**

For detailed guidance on how to improve the security posture of SEGRA's network environment, please reference the Assessment and Component Overview contained in the following section of this report.

SEGRA

Segra's Systems and Organization Controls (SOC 2) Type II Report

MTN Infrastructure TopCo, Inc., dba SEGRA

Systems and Organization Controls (SOC 2) Type II Report

Report on MTN Infrastructure TopCo, Inc., dba SEGRA's Description of its Ethernet, Wavelength and Dedicated Internet Access System and on the Suitability of the Design of its Controls to Meet the Service Commitments and System Requirements Relevant to the Security and Availability Trust Services Criteria

Throughout the Period July 1, 2020 to June 30, 2021
with Report of Independent Auditors

Report on MTN Infrastructure TopCo, Inc., dba SEGRA's Description of its Ethernet, Wavelength and Dedicated Internet Access System and on the Suitability of the Design of its Controls to Meet the Service Commitments and System Requirements Relevant to the Security and Availability Trust Services Criteria

Throughout the Period July 1, 2020 to June 30, 2021

Contents

Section 1 – Independent Service Auditors' Report

BAUKNIGHT PIETRAS & STORMER, P.A.
Tax | Assurance | Consulting

1501 Main Street
Suite 600
PO Box 1330
Columbia, SC 29202
T 803-771-8943
F 803-771-8958

Independent Service Auditors' Report

To the Board of Directors
MTN Infrastructure TopCo, Inc., dba SEGRA

Scope

We have examined MTN Infrastructure TopCo, Inc., dba SEGRA's ("SEGRA"), accompanying description of its ethernet and internet access system titled "Ethernet, Wavelength and Dedicated Internet Access System" throughout the period July 1, 2020 to June 30, 2021 ("description") based on the criteria for a description of a service organization's system set forth in DC 200, *2018 Description Criteria for a Description of a Service Organization's System in a SOC 2® Report* (AICPA, *Description Criteria*) ("description criteria") and the suitability of the design and operating effectiveness of controls stated in the description throughout the period July 1, 2020 to June 30, 2021, to provide reasonable assurance that SEGRA's service commitments and system requirements were achieved based on the trust services criteria relevant to security and availability ("applicable trust services criteria") set forth in TSP 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* ("AICPA, *Trust Services Criteria"*).

The description indicates that complementary user entity controls that are suitably designed are necessary, along with controls at SEGRA, to achieve SEGRA's service commitments and system requirements based on the applicable trust services criteria. The description presents SEGRA's controls, the applicable trust services criteria, and the complementary user entity controls assumed in the design of SEGRA's controls. Our examination did not include such complementary user entity controls and we have not evaluated the suitability of the design or operating effectiveness of such controls.

Service Organization's Responsibilities

SEGRA is responsible for its service commitments and system requirements and for designing, implementing, and operating effective controls within the system to provide reasonable assurance that SEGRA's service commitments and system requirements were achieved. SEGRA has provided the accompanying assertion titled "Assertion of Executive Management of MTN Infrastructure TopCo, Inc., dba SEGRA" ("assertion") about the description and the suitability of the design and operating effectiveness of controls stated therein.

SEGRA is also responsible for preparing the description and assertion, including the completeness, accuracy, and method of presentation of the description and assertion; providing the services covered by the description; selecting the applicable trust services criteria and stating the related controls in the description; and identifying the risks that threaten the achievement of the service organization's service commitments and system requirements.

Board of Directors
MTN Infrastructure TopCo, Inc.

Service Auditor's Responsibilities

Our responsibility is to express an opinion on the description and on the suitability of design and operating effectiveness of controls stated in the description based on our examination. Our examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants. Those standards require that we plan and perform our examination to obtain reasonable assurance about whether, in all material respects, the description is presented in accordance with the description criteria and the controls stated therein were suitably designed to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

An examination of a description of a service organization's system and the suitability of the design and operating effectiveness of controls involves the following:

- Obtaining an understanding of the system and the service organization's service commitments and system requirements.
- Assessing the risks that the description is not presented in accordance with the description criteria and that controls were not suitably designed.
- Performing procedures to obtain evidence about whether the description is presented in accordance with the description criteria.
- Performing procedures to obtain evidence about whether controls stated in the description were suitably designed to provide reasonable assurance that the service organization achieved its service commitments and system requirements based on the applicable trust services criteria.
- Testing the operating effectiveness of controls stated in the description to provide reasonable assurance that the service organization achieved its service commitments and system requirements based on the applicable trust services criteria.
- Evaluating the overall presentation of the description.

Our examination also included performing such other procedures as we considered necessary in the circumstances.

Board of Directors
MTN Infrastructure TopCo, Inc.

Inherent Limitations
The description is prepared to meet the common needs of a broad range of report users and may not, therefore, include every aspect of the system that individual report users may consider important to meet their informational needs. There are inherent limitations in any system of internal control, including the possibility of human error and the circumvention of controls. Because of their nature, controls may not always operate effectively to provide reasonable assurance that the service organization's service commitments and system requirements are achieved based on the applicable trust services criteria. Also, the projection to the future of any conclusions about the suitability of the design or operating effectiveness of controls is subject to the risk that controls may become inadequate because of changes in conditions or that the degree of compliance with the policies or procedures may deteriorate.

Description of Tests of Controls
The specific controls we tested and the nature, timing, and results of those tests are listed in Section 4.

Opinion
In our opinion, in all material respects,

a. the description presents SEGRA's ethernet and internet access system that was designed and implemented throughout the period July 1, 2020 to June 30, 2021 in accordance with the description criteria.

b. the controls stated in the description were suitably designed throughout the period July 1, 2020 to June 30, 2021 to provide reasonable assurance that SEGRA's service commitments and system requirements would be achieved based on the applicable trust services criteria, if its controls operated effectively throughout that period and if the user entities applied the complementary user entity controls assumed in the design of SEGRA's controls throughout that period.

c. the controls stated in the description operated effectively throughout the period July 1, 2020 to June 30, 2021 to provide reasonable assurance that SEGRA's service commitments and system requirements were achieved based on the applicable trust services criteria if the user entities applied the complementary controls assumed in the design of SEGRA's controls throughout that period.

Board of Directors
MTN Infrastructure TopCo, Inc.

Restricted Use
This report, including the description of tests of controls and the results thereof in Section 4, is intended solely for the information and use of SEGRA, user entities of SEGRA's ethernet and internet access system throughout the period July 1, 2020 to June 30, 2021, business partners of SEGRA subject to risks arising from interactions with the ethernet and internet access system, practitioners providing services to such user entities and business partners; prospective user entities and business partners; and regulators who have sufficient knowledge and understanding of the following:

- The nature of the service provided by the service organization.
- How the service organization's system interacts with user entities, business partners, and other parties.
- Internal control and its limitations.
- Complementary user entity controls and how those controls interact with the controls at the service organization to achieve the service organization's service commitments and system requirements.
- User entity responsibilities and how they may affect the user entity's ability to effectively use the service organization's services.
- The applicable trust services criteria.
- The risks that may threaten the achievement of the service organization's service commitments and system requirements and how controls address those risks.

This report is not intended to be, and should not be, used by anyone other than the specified parties.

July 24, 2021

Section 2 – Assertion of Executive Management of MTN Infrastructure TopCo, Inc., dba SEGRA

SEGRA

11215 N Community House Rd
Ste 1000
Charlotte, N.C 28277
segra.com

Assertion of Executive Management of MTN Infrastructure TopCo, Inc., dba SEGRA

We have prepared the accompanying description of MTN Infrastructure TopCo, Inc., dba SEGRA's ("SEGRA") ethernet and internet access system titled "Ethernet, Wavelength and Dedicated Internet Access System" throughout the period July 1, 2020 to June 30, 2021 ("description") based on the criteria for a description of a service organization's system set forth in DC 200, *2018 Description Criteria for a Description of a Service Organization's System in a SOC 2® Report* (AICPA, *Description Criteria*) ("description criteria"). The description is intended to provide report users with information about the system that may be useful when assessing the risks arising from interactions with SEGRA's system, particularly information about system controls that SEGRA has designed, implemented, and operated to provide reasonable assurance that its service commitments and system requirements were achieved based on the trust services criteria relevant to security and availability ("applicable trust services criteria") set forth in TSP 100, 2017 *Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* ("AICPA, Trust Services Criteria").

The description indicates that complementary user entity controls that are suitably designed are necessary, along with controls at SEGRA, to achieve SEGRA's service commitments and system requirements based on the applicable trust services criteria. The description presents SEGRA's controls, the applicable trust services criteria, and the complementary user entity controls assumed in the design of SEGRA's controls.

We confirm, to the best of our knowledge and belief, that:

1) The description presents SEGRA's ethernet and internet access system titled, "Ethernet, Wavelength and Dedicated Internet Access System" that was designed and implemented throughout the period July 1, 2020 to June 30, 2021 in accordance with the description criteria.
2) The controls stated in the description were suitably designed throughout the period July 1, 2020 to June 30, 2021 to provide reasonable assurance that SEGRA's service commitments and system requirements would be achieved based on the applicable trust services criteria, if its controls operated effectively throughout that period, and if user entities applied the complementary controls assumed in the design of SEGRA's controls throughout that period.
3) The controls stated in the description operated effectively throughout the period July 1, 2020 to June 30, 2021 to provide reasonable assurance that SEGRA's service commitments and system requirements were achieved based on the applicable trust services criteria if complementary user entity controls assumed in the design of SEGRA's controls operated effectively throughout that period.

Jason Campbell, Chief Operating Officer

7/24/2021
Date

Section 3 – Description of MTN Infrastructure TopCo, Inc., dba SEGRA's Ethernet, Wavelength and Dedicated Internet Access System

MTN Infrastructure TopCo, Inc., dba SEGRA
Section 3 – Description of MTN Infrastructure TopCo, Inc., dba SEGRA's Ethernet, Wavelength and Dedicated Internet Access System

This is a System and Organization Controls ("SOC") 2, Type II report and includes a description of MTN Infrastructure TopCo, Inc., dba SEGRA's ("SEGRA"), Ethernet, Wavelength and Dedicated Internet Access System, and the controls in place to provide reasonable assurance that SEGRA's service commitments and system requirements were achieved based on the trust services criteria relevant to the security and availability criteria set forth in TSP section 100, (2017) *Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* ("AICPA, *Technical Practice Aids*") ("applicable trust services criteria"), throughout the period July 1, 2020 to June 30, 2021, which may be relevant to users of the Ethernet, Wavelength and Dedicated Internet Access System. It does not encompass all aspects of the services provided or procedures followed for other activities performed by SEGRA.

Due to the various COVID-19 related state requirements, SEGRA modified certain processes and procedures during a portion of the examination period and subsequent to the examination through the date of this report to enhance the safety of SEGRA employees and its customers. These changes had no impact on the description or controls of SEGRA's ethernet and internet access system.

3.1 Company Overview and Background

SEGRA provides Ethernet Wide Area Network ("WAN"), Wavelength ("Wave") and Dedicated Internet Access ("DIA"). These services are primarily provided along the east coast between Pennsylvania and Georgia using a network of approximately 30,000 fiber route miles and over a million total fiber strand miles. The business has over 10,400 on-net fiber locations comprised of approximately 4,500 on-net enterprise and more than 7,200 unique contracted fiber to the cell site ("FTTC") locations.

SEGRA primarily serves medium and large businesses, including government, healthcare, education, communications carriers and cell phone providers.

SEGRA was formed in 2018 as a merger between Lumos Networks Corp. and Spirit Communications. In November 2017, EQT Partners, a Swedish private equity group, purchased a majority stake in Lumos Networks Corp. In April 2018, EQT Partners purchased a majority stake in Spirit Communications. The two telecommunication companies were merged under MTN Infrastructure TopCo, Inc. and the SEGRA brand name.

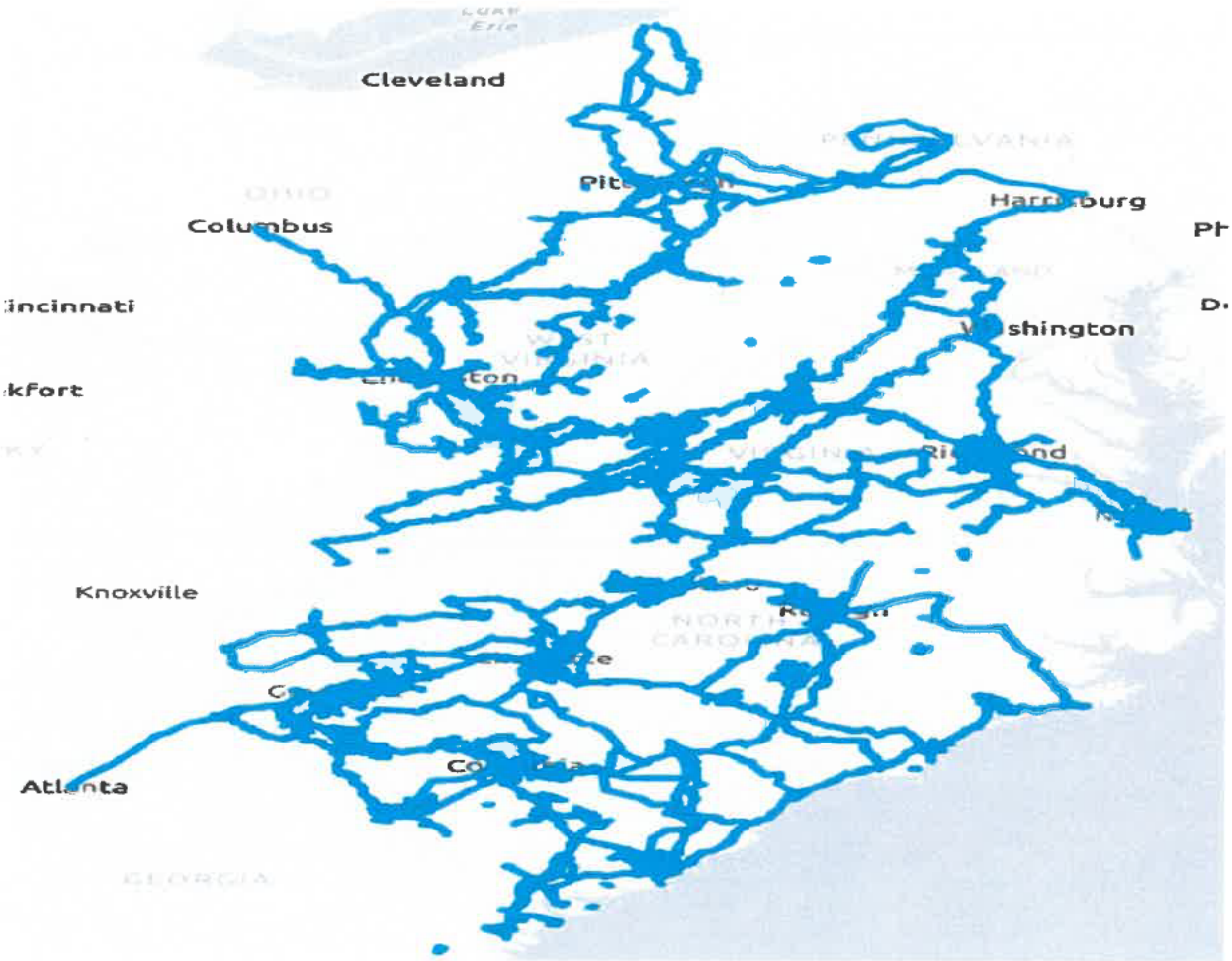
Today, SEGRA provides fiber services to 44 markets in 10 states. SEGRA is headquartered in Charlotte, North Carolina, with 23 major office locations and employs more than 900 employees.

MTN Infrastructure TopCo, Inc., dba SEGRA
Section 3 – Description of MTN Infrastructure TopCo, Inc., dba SEGRA's Ethernet, Wavelength and Dedicated Internet Access System

Scope and Boundaries

This description addresses SEGRA's DIA, Wave and Ethernet WAN services provided by the SEGRA on-net fiber network within the markets of Virginia, West Virginia, Pennsylvania, Maryland, Ohio, North Carolina, South Carolina, Georgia, Tennessee and Kentucky. If a customer of SEGRA has not purchased certain services, the portions of the description that cover those services will not be relevant to those customers. The controls described in this report may not apply to services other than those described. For that reason, it is recommended that customers confirm the services they have purchased with their SEGRA account executive.

In May 2020, SEGRA acquired North State Telecommunications Corporation ("North State") and as of June 30, 2021, no integration is planned. As such, this description does not include customers of or fiber paths previously managed by North State. The map below represents the full area serviced by SEGRA and the in-scope area with regards to this report during the period, with the exception of the North State fiber routes discussed above.



Incidents and Changes

Throughout the period July 1, 2020 to June 30, 2021, SEGRA identified one security incident with a cloud vendor. SEGRA's Software-as-a-Service risk tracking and incident response platform was compromised by an unknown third party. SEGRA moved the functionality in-house and canceled service with the cloud vendor. No known impact resulted from the compromise. SEGRA did not identify any additional security incidents during the period.

Throughout the period July 1, 2020 to June 30, 2021, SEGRA did not identify any significant system changes that impact the users of this report.

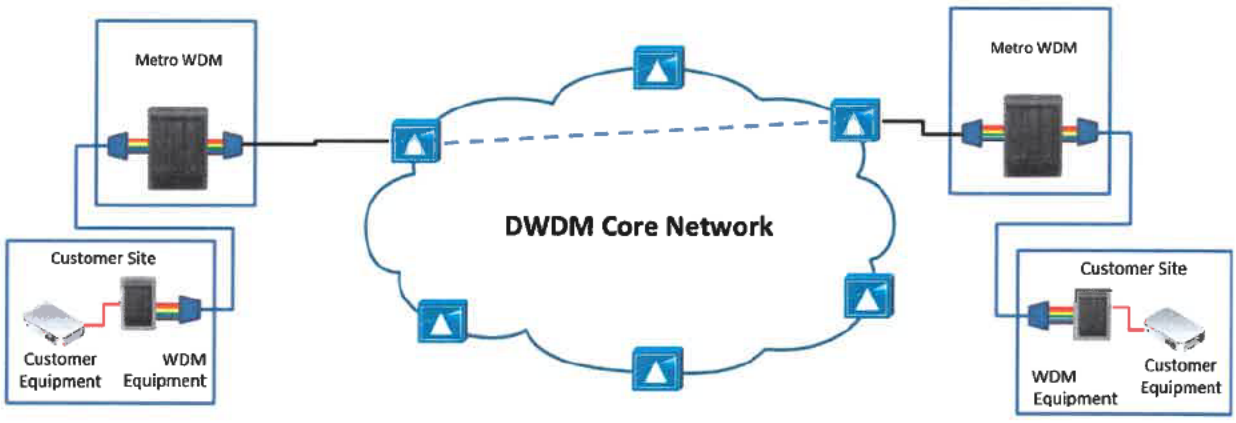
MTN Infrastructure TopCo, Inc., dba SEGRA
Section 3 – Description of MTN Infrastructure TopCo, Inc., dba SEGRA's Ethernet, Wavelength and Dedicated Internet Access System

Services Provided

Service Type	Specific Type	Features Available
Wave	• 1 gbit/s • 10 gbit/s • 100 gbit/s	
Ethernet WAN Switched	• E-Line • E-LAN • E-Access • Varying speeds	• Service Level Agreement • Diverse building entry • Redundant customer premise equipment • Geo-diverse customer premise equipment termination • Link aggregation control protocol
Ethernet WAN Routed	• Full-Mesh Topology	• Service Level Agreement • Diverse building entry • Redundant customer premise equipment • Geo-diverse customer premise equipment termination
DIA	• Varying speeds	• Border gateway protocol • Distributed denial of service mitigation

Wave Services

Wave services is a dedicated, linear routed, unprotected, point-to-point fiber-based data transport solution with a two fiber Network Interface at both ends. The Wave services utilize dense wavelength division multiplexing ("DWDM") across SEGRA's fiber optic network, and support multi-protocol connectivity.



MTN Infrastructure TopCo, Inc., dba SEGRA
Section 3 – Description of MTN Infrastructure TopCo, Inc., dba SEGRA's Ethernet, Wavelength and Dedicated Internet Access System

Ethernet WAN Switched

SEGRA's Ethernet WAN Switched is a wide area data networking service, delivered at Layer 2, which allows for the networking of multiple customer locations such that they may operate as a single logical entity. Ethernet services are provided using the SEGRA Carrier Ethernet Network, consisting primarily of Cisco, Nokia, and Ciena packet switches, the SEGRA DWDM fiber optic transport network and the SEGRA fiber network.

Ethernet WAN Routed

SEGRA Ethernet WAN Routed is a routed data service that connects two or more locations in an any-to-any multipoint configuration. Layer 3 services are provided using the Cisco and Nokia IP routers, the SEGRA multiprotocol label switching ("MPLS") Network, the SEGRA DWDM fiber optic transport network, and the SEGRA fiber network.

Dedicated Internet Access

SEGRA DIA provides a secure, reliable connection to the public internet delivering guaranteed bandwidth over dedicated Ethernet access. DIA is provided using SEGRA's Carrier Ethernet Network and Cisco or Nokia equipment configured as internet protocol ("IP") routers.

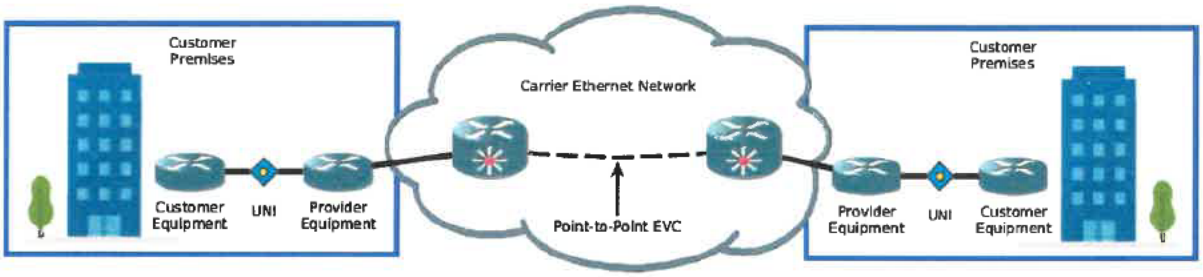
BGP ("Border Gateway Protocol") is available as an optional feature for DIA redundancy. When a customer's network connects to multiple upstream circuits or providers, the customer can use BGP to announce their network address space to all available connections for fail-over or shortest path routing.

SEGRA DIA uses in-line filtering appliances to provide proactive distributed denial of service ("DDoS") mitigation for DIA customers.

E-Line

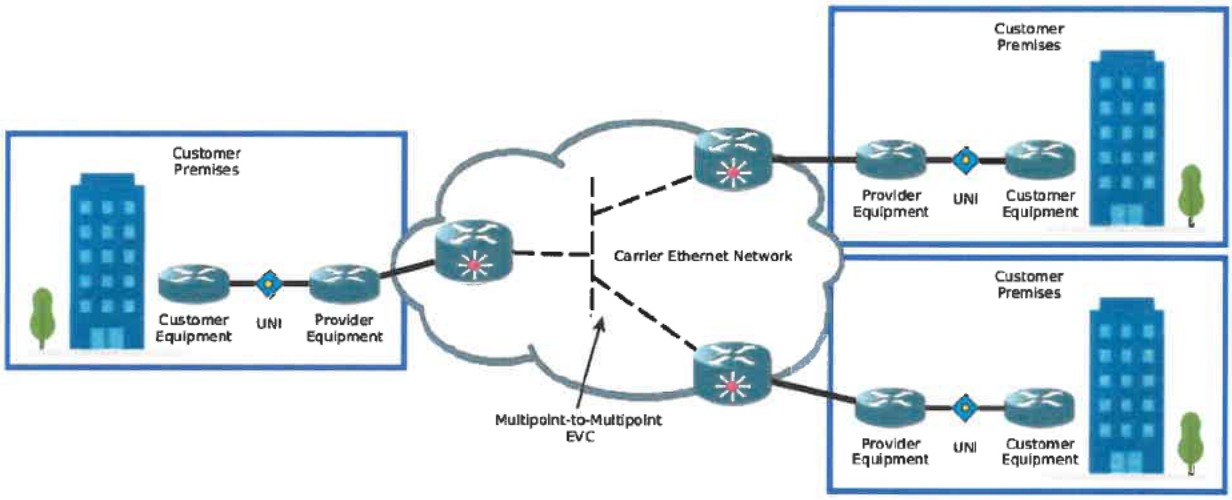
E-Line is the most basic carrier ethernet topology. E-Line is a Layer 2 service that connects two sites in a point-to-point configuration. E-Line often serves as a more flexible, reliable, and economical alternative to traditional time-division multiplexing point-to-point private lines.

The hand-off point at each site is an ethernet port or UNI on a piece of SEGRA provided customer premises equipment ("CPE"), also known as Provider Equipment ("PE"). The two UNIs are associated via a point-to-point ethernet virtual connection ("EVC") path.



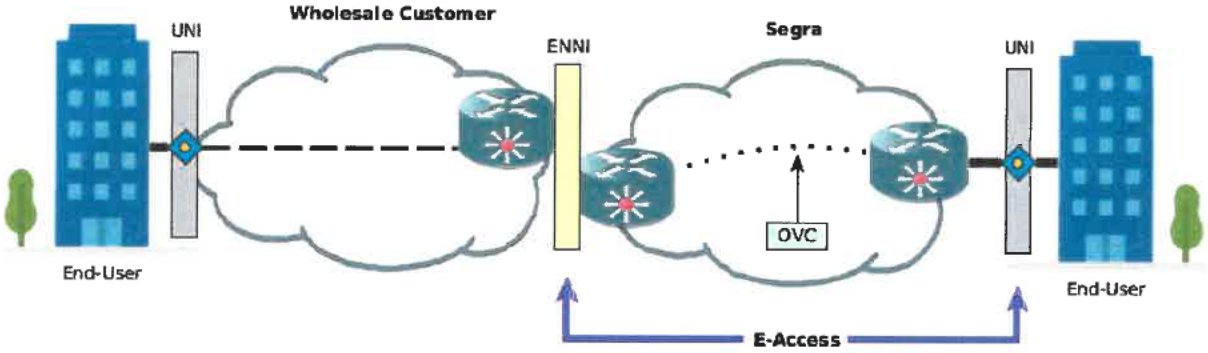
E-LAN

E-LAN is an Ethernet service that connects two or more locations in an any-to-any multipoint configuration. All endpoints may forward frames freely between one another. From the customer's view, the E-LAN service appears and behaves as an ethernet local area network between sites. E-LAN may have many UNIs.



E-Access

E-Access is an Ethernet service for wholesale applications that enables carriers to reach end-users outside their native service area with last-mile Ethernet access via the SEGRA network. E-Access is implemented in a one-to-many hub configuration, with multiple ethernet access links aggregated at a single external network-to-network interface ("ENNI") that serves as the demarcation and traffic exchange point between carriers. Operator Virtual Connections (OVCs, a type of EVC) associate these ENNIs and UNIs.



MTN Infrastructure TopCo, Inc., dba SEGRA
Section 3 – Description of MTN Infrastructure TopCo, Inc., dba SEGRA's Ethernet, Wavelength and Dedicated Internet Access System

Service Commitments and System Requirements

The performance of SEGRA's Ethernet services is governed by service level agreements ("SLA"). Measurements include mean frame delay (latency), inter-frame delay variation (jitter), and frame loss ratio (frame loss). Additionally, the SEGRA SLA includes and measures availability and mean time to repair ("MTTR").

Availability is the percentage of minutes in a calendar month during which SEGRA's Ethernet Service is available to exchange data between SEGRA served customer end points. It is computed as follows:

$$\frac{\text{Total Minutes in Calendar Month - Total Minutes of Non-Availability}}{\text{Total Minutes in Calendar Month}}$$

Total minutes in calendar month is determined by multiplying 24 hours by the number of days in the month multiplied by 60 minutes.

Total minutes of non-availability means the total of all minutes of network non-availability for a specific Ethernet service in a calendar month. If the optimal power backup feature is not part of the provided service configuration, any time period of service interruption resulting from a power outage affecting customer premise equipment provided by SEGRA is considered available time and is not included as minutes of non-availability in the network availability calculation.

The customer's Ethernet Service is considered available until the date and time SEGRA receives notification of service unavailability subject to validation by SEGRA from the customer.

Ethernet service can be ordered in protected or unprotected configurations:

Category	Unprotected	Protected
Availability Objective	99.99%	99.999%
Mean One-Way Frame Delay (Latency)	≤10ms (one-way)	≤10ms (one-way)
Frame Loss Ratio (frame loss)	≤0.0001%	≤0.0001%
Inter-Frame Delay Variation (jitter)	≤3ms	≤3ms
(MTTR)	4 Hours	2 Hours

MTTR is a performance objective only and outage credits will not apply if the objective is not met.

If the services suffer a service outage meaning the service is not available for use of any kind, the customer will be entitled to a credit based on their Monthly Recurring Cost ("MRC") as outlined in the following table:

Aggregate Length of Service Outage	Credit: Unprotected	Credit: Protected
≥1 minute and <2 hours	No Credit	10% of the MRC for the disrupted service.
≥2 hours and <4 hours	10% of the MRC for the disrupted service.	25% of the MRC for the disrupted service.
≥4 hours and <8 hours	20% of the MRC for the disrupted service.	50% of the MRC for the disrupted service.
≥8 hours and <12 hours	35% of the MRC for the disrupted service.	75% of the MRC for the disrupted service.
≥12 hours	50% of the MRC for the disrupted service.	100% of the MRC for the disrupted service.

If the Ethernet services suffer from degradation and fail to meet the guarantees set forth, the customer will be entitled to credits per the table below.

Length of Service Degradation	Credit
<15 minutes	No credit
≥15 minutes and <1 hour	2% of the MRC for the degraded service
≥1 hour	5% of the MRC of the degraded service for each full hour of service degradation, up to a maximum of 25% of the MRC for any thirty-day period.

The maximum credit for all service interruptions occurring during any thirty-day period shall not exceed the monthly service charges due to SEGRA from the customer during said thirty-day period.

SLA performance is measured from user-network interface to user-network interface ("UNI"), the physical ethernet port defined as the demarcation point between SEGRA equipment ("PE", Provider Equipment) and Customer managed equipment ("CE", Customer Equipment), for all prescribed measurements.

3.2 System Components

Infrastructure

SEGRA's optical infrastructure consists of approximately 30,000 route miles of single mode fiber optic cable and wavelength-division multiplexing ("WDM"), coarse wavelength-division multiplexing and DWDM optical transport equipment from industry leaders such as BTI, Cisco and Ciena.

The optical infrastructure directly supports the Wave product, and indirectly by way of dependencies, all Ethernet, and DIA services.

SEGRA's ethernet infrastructure consists of the supporting optical network, with carrier grade MPLS routers and ethernet switches from Cisco, Nokia, and Ciena, built into redundant topologies such as partial mesh and ring configurations.

The ethernet infrastructure directly supports the Ethernet products, and indirectly by way of dependencies, Ethernet WAN Routed and DIA services.

The Ethernet WAN Routed and DIA infrastructure consists of the supporting optical and ethernet networks, and carrier grade IP routers from Cisco and Nokia located in key markets.

DDoS mitigation appliances are placed at every point a DIA router peers with a transit provider that provides full internet routing tables to SEGRA. The DDoS mitigation appliances are always on and protect the SEGRA infrastructure and DIA customers from DDoS attacks.

The internal management network provides day-to-day administrative connectivity for managing the primary infrastructure. This network leverages the same products sold to customers, along with additional firewall and virtual private network ("VPN") functionality, to provide private, isolated, industrial control networks.

The out-of-band network provides administrative access for non-routine maintenance or failures. This network doesn't rely on any of the electronics used for the primary services and isn't impacted by equipment failures.

Additional infrastructure includes the supporting equipment spaces, buildings, power, heating, ventilation, and air conditioning ("HVAC"), desktop computers, VPNs, and firewall devices used for internal operations of the system.

Software

The primary infrastructure runs software specifically written for the device it runs on by the device's manufacturer. For example, Cisco routers run the Cisco IOS-XR software. The primary infrastructure is not a general computing platform and only runs the manufacturer provided software.

SEGRA uses a work-flow and documentation system to manage process and work orders. This system allows management to define, delegate and track individual steps in a business process throughout the entire process. This system is maintained by the Information Technology department of SEGRA ("IT").

SEGRA uses two primary forms of VPN accessing the primary infrastructure. Both forms of VPN require multi-factor authentication. The VPN is designed to be redundant and diverse in order to provide access to the primary infrastructure, even if the supporting infrastructure is malfunctioning. Remote access to the primary infrastructure is only granted to authorized personnel.

The primary infrastructure authenticates users with centralized authentication software. This software provides a single place to manage administrative user accounts, integrate with Human Resources, log authentication requests and enforce access policy.

The ticket system tracks customer issues, outages, incidents and repairs. The ticket system is operated by the Network Operations Center ("NOC") and maintained by IT.

Inventory control software keeps track of physical assets, their locations and hardware configurations. A second inventory system keeps track of logical configurations and IP addressing. Change control software is used to formally approve and track changes to the infrastructure according to the change control policy.

A monitoring system is used to receive simple network monitoring protocol ("SNMP") alarms, log messages and actively poll infrastructure for their status. The monitoring system categorizes the information it receives and displays alarms that may indicate an actionable incident to NOC workstations and a large TV monitor on the NOC wall. The monitoring system is responded to according to the detailed written incident response procedures.

Performance and capacity monitoring software is used to measure infrastructure utilization and performance. This is used as part of internal capacity management procedures, to determine when to build new infrastructure and for managing SLA guarantees and credits for customers. The performance monitoring software measures service utilization, availability, latency, and packet loss.

MTN Infrastructure TopCo, Inc., dba SEGRA
Section 3 – Description of MTN Infrastructure TopCo, Inc., dba SEGRA's Ethernet, Wavelength and Dedicated Internet Access System

People

SEGRA has a staff of approximately 900 employees organized in the following relevant functional areas:

- *President, Chief Operations Officer*. Performs product planning, engineering, IT and day-to-day functions required for deploying and maintaining the services and primary infrastructure.

    - The NOC teams monitor the infrastructure for incidents, responds to, and drives the repair of anything that breaks. The NOC teams manage incidents and are responsible for following incident handling procedures, escalation procedures and communication with customers and stakeholders. The NOC teams provide multiple tiers of engineering staff to facilitate trouble shooting and changes.
    - Field Operations manages the electronic infrastructure necessary to provide the customer services. Field Operations technicians are dispatched by the NOC staff in response to an incident or change.
    - Network Engineering and Planning tracks capacity and infrastructure needs, initiates new projects to expand or optimize the networks, develops and tests new equipment or configurations, and produces configuration templates and design guides for use by other teams.
    - Network Delivery manages fiber optic design, construction and repair.
    - Customer Service provides project management and field technicians new service turn-ups.
    - The Customer Solutions Center provides technical and billing support to customers.
    - Product Management & Business Development performs market analysis, designs new products to sell and provides sales support.
    - IT provides SEGRA's internal IT networks, servers, desktop PC's, and software development.
    - Information Security is responsible for SEGRA's cyber security and cyber risk management programs.

- *Legal & Human Resources* provides legal, compliance, regulatory, contract review and human resources.

- *Finance* provides supply chain, inventory management, internal audit, billing, collections, tax, accounting, financial reporting, financial planning and analysis and similar.

- *Sales* builds relationships with customers to help them meet or exceed their data communications needs using SEGRA's products.

Data

SEGRA transmits customer data and content reliably and accurately from one location to another without modification. Data is transmitted to the system by customer equipment, transported to another location, and transmitted back to another customer device exactly as it was originally received without modification. SEGRA does not otherwise manage customer data or content.

The point-to-point Ethernet WAN products E-LINE and E-Access measure the performance of data delivery and offer SLAs with service credits based on availability, latency, jitter, and packet loss. Reporting is available for the SLA components from the service monitoring software. SLA components and reporting on those components are customizable and can be tailored to meet the needs of the customer and the network topology the customer requires.

Processes and Procedures

Management has developed and communicated procedures to restrict logical access to the communications infrastructure. Changes to these are performed as needed and policies are authorized by senior management. These procedures cover key security life cycle areas such as assessment of business impact resulting from proposed security controls, selection, documentation and implementation of security controls, self-assessments of the performance of controls, authorization, removal or changes to system access, management of access roles and membership, maintenance and support of the system, incident response, change control, capacity management, and baseline configurations. Security policies are reviewed annually and bench-marked against the International Organization for Standardization's 27000 series for information security management systems and the United States Department of Commerce's National Institute of Standards and Technology's Cybersecurity Framework.

3.3 Description of Controls Relevant to the Security Trust Services Criteria

Control Environment

Ethics and Integrity

SEGRA publishes its core values on its internal website. The core values include attributes such as putting the customer first, honesty and integrity. There is an internal program to recognize employees who demonstrate the core values. Annual employee appraisals include aspects of the core values as a measurable performance factor. To clarify what ethical behavior entails, the SEGRA board of directors maintains a code of business conduct and ethics. There are whistle blower hotlines available for employees to anonymously report ethics violations to senior leadership or the board of directors.

Organizational Structure and Assignment of Authority and Responsibility

Management has put an organizational structure in place that defines operating units and reporting lines of each respective area. This framework empowers the organization to design, direct and control the operation by segregating personnel and business functions into divisions as dictated by work obligations. Organizational charts are in place to communicate key areas of authority, responsibility, and appropriate lines of reporting to personnel. These charts are available to personnel via the Company's intranet.

Human Resources Policies and Practices

Policies and procedures have been written and implemented to help guarantee quality employees are hired. The SEGRA Human Resource policies and practices related to hiring, orientation, training, evaluating, counseling, promoting, compensation, and remedial actions are clearly written and communicated where appropriate. Standards for hiring qualified individuals, with requisite educational background, prior work experience, past accomplishments, and evidence of integrity and ethical behavior illustrate SEGRA's commitment to competent and trustworthy employees. Training policies and practices are designed to inform employees of their roles and responsibilities within the company and define employee expectations and behavior. Raises and promotions are based on employee performance against expectations.

Formal hiring procedures are in place and performed by the Human Resource Department including background checks, credit checks for financial positions, and drug tests.

Performance evaluations are conducted by Human Resources at least annually as outlined in the Human Resources policies and procedures document.

Established policies and procedures provide management with an action plan for disciplinary measures and have been communicated to managers.

Commitment to Competence

Management has designed job position requirements and descriptions that include required skills, knowledge, and experience levels. Tuition reimbursement and employee training programs are in place. Documented hiring practices require prospective employees to interview with department members who can accurately assess the applicant's skill set using a combination of resume, portfolio, and interview questions.

Communication and Information

SEGRA performs assessments at least annually to identify the information and information processes required and expected to support the internal control and the achievement of SEGRA's service commitments and system requirements. SEGRA's most valuable and sensitive digital data and mission-critical systems are identified during the assessment, including internal and external sources of data.

SEGRA has established information security policies and processes to communicate to employees their responsibilities concerning processing and controls. These policies and processes are available to all employees on the Company's internal network.

SEGRA has established whistle blower hot-lines for reporting ethics or policy violations to management or the board of directors.

The formal written change management, incident response and disaster recovery procedures provide communication trees and instruction for communicating and escalating changes, routine incidents or non-routine disasters, both inside the company and externally. This assures that significant events are communicated properly and in a timely manner.

A media and investor communications policy defines who may communicate what outside the company to the media, analysts or investors.

Risk Assessment

SEGRA uses a documented risk management practice to continuously search for and evaluate risks using a formula balancing likelihood and impact. Responsible persons in the risk management activities are identified. The executive team is informed of risks over a defined threshold.

The information security team assesses security risks on an ongoing basis. This is done through regular management meetings with executive and director level staff, IT and operational personnel, reviewing and acting on security events, performing quarterly vulnerability assessments, annual penetration tests, and conducting formal security and risk assessment activities when major changes to the environment take place.

Changes in security threats and risks are reviewed by the Company's General Counsel and Secretary, CIO, COO, VP of Engineering and Operations, SVP General Manager and if needed, the CFO and VP of IT (collectively referred to as "senior management") at least quarterly.

A strategic security plan is developed and communicated by the security architect in conjunction with management and operational staff. Policy changes are approved by the Cyber Security Committee.

Monitoring

Service availability is monitored using dry contact alarms, SNMP traps, syslog, ethernet CFM, and Netcool, which receives all the monitoring and alarming information. Operations staff monitor Netcool 24x7, 365 and initiate the incident response process when alarms indicate an incident has occurred.

Policies and procedures are in place to monitor and upgrade network segments at predefined utilization thresholds.

Security control effectiveness is tested and measured using a combination of quarterly vulnerability assessments, annual penetration tests, and formal security and risk assessments when there are major changes to the environment. Third party assessments of varying types are conducted annually.

Security test results are communicated to senior management in quarterly security update meetings. Vulnerability scans are reported monthly to senior management and relevant staff via an email report.

Control Activities

In order to ensure management's directives are carried out as expected, policies and procedures are developed to support SEGRA control activities and are available to all employees. Control activities occur at all levels and in all functions. These policies and procedures align with the controls to help ensure all necessary actions are taken to address risks to SEGRA's goals and objectives. They include activities such as approvals, verifications, authorizations, and security of assets that belong to SEGRA.

Logical and Physical Access Controls

SEGRA access authentication and authorization is governed by an Access Control Policy. Controls are in place to assure authentication and authorization follow industry best practices. Controls are implemented based on risk assessment findings.

Access controls include granting access only to authorized personnel according to business need. Access requests are logged, require approval, and current access privileges are reviewed quarterly. Every internal user must use unique credentials and passwords must meet complexity requirements. Shared and generic credentials must not be used except as an emergency override in the event of an authentication systems failure. Accounts are revoked by IT when Human Resources sends a notice of termination. Access to infrastructure must be logged.

Policies and procedures are in place for controlling physical access into office and equipment facilities. Access to SEGRA facilities housing equipment is controlled by an electronic key card badge system. Badges into equipment areas are restricted to authorized operational personnel. Access attempts are logged and traceable to individual cardholders.

Badge access is granted and revoked by the Facilities Team. Badge access requests are documented via a trouble ticket system, and approved by the director of the individual requesting the access. Cards are issued to new hires based on a new hire notification form sent from Human Resources. Cards are disabled when an employee departs the company on the date and time specified by a Human Resource departures form. Human Resources or the manager will retrieve the card from the separating individual.

A visitor log is used to record physical access to equipment rooms. Visitors to equipment rooms require an escort and must be supervised at all times. The visitor log records visitor name, company, purpose of visit, and times when they entered and exited the building.

An access report is issued quarterly to authorizing directors for high-priority equipment rooms. All cards must be confirmed or removed by the authorizing director. Individual door and key-card reports are provided to the direct supervisor, manager or the audit team.

Remote access mechanisms are defined by the IT remote access standard and the access control servers design and provisioning guidelines. The VPN is governed by SEGRA security policies. Controls specific to remote access specify that all data must be encrypted across public networks and all authentication for remote access must use multi-factor authentication.

SEGRA controlled equipment areas are equipped with fire detection and suppression equipment, hand-held fire extinguishers, dedicated and redundant computer room air conditioning ("CRAC") and HVAC systems, redundant uninterruptible power supply ("UPS") systems and backup generators.

The inspection and maintenance of these devices is performed by external third-party vendors to ensure the devices are in proper working order. Various third-party vendors are contracted to inspect and maintain the fire detection, alarm, and sprinkler systems along with the hand-held fire extinguishers on an annual basis. UPS, CRAC/HVAC systems and the diesel backup generators are inspected on a quarterly basis. Generators are exercised weekly.

HVAC and electric power infrastructure use SNMP to communicate to Netcool, a software application monitored by operations staff 24x7, 365.

SEGRA has a network communications policy that outlines how systems may communicate with each other. To ensure technical communication controls are met, the policy further defines what constitutes a system boundary, defines types of information assets that may be logically grouped with each other, when encryption in transit must be used, and requires documentation and review of communication boundaries. Review of system communication boundaries is conducted at a minimum of once per year.

Ethernet services are segmented and isolated from each other using tunnel and logical isolation technologies such as MPLS, QinQ stacked VLAN tagging, VLANs, and physical isolation using optical wavelengths or fiber optic cables. Wave services are isolated using optical wavelengths or separate physical fiber optic strands.

Internal systems, service providing equipment, and supporting infrastructure are grouped into unique network segments and isolated from each other. Network communications in and out of infrastructure management network areas are protected by a combination of firewalls, authentication, logical isolation and physical isolation. Communications with infrastructure network areas are restricted to authorized staff or systems with a business need to access the infrastructure.

System Operations

Operational policies and procedures are in place for monitoring, escalating, and resolving incidents affecting the services. Those procedures include escalation timelines, ticket handling, and severity level definitions.

Baseline configurations for infrastructure are created by Network Engineering and Planning, reviewed by peers and management, and approved by senior management.

Current configurations for infrastructure are backed up daily and changes are tracked by the infrastructure Element management software and configuration management systems.

Vulnerability scans are conducted quarterly. Availability and integrity of the infrastructure, including environmental, physical or logical changes, resource consumption, failures, or service impacting deviation from baselines, are logged, alerted on and monitored by the NOC 24x7, 365.

Change Management

Change management and maintenance policies and procedures are documented and used by the operational teams to manage infrastructure providing the services. The procedures cover deployment, provisioning, repair and improvements. The change management procedure includes documenting an impact analysis, managerial sign-offs, technical reviews and sign-offs, customer notifications, advanced notification requirements based on activity risk, back-out procedures and escalation paths. Authorized maintenance windows are documented based on activity type, the related risk and business objective impact.

Changes must be submitted using a standard form that includes a description of the change, risk level, impact analysis, scheduling, operational contact information, record of approving parties, and ties to any customer ticket, work order or vendor ticket.

Changes performed outside of change control are detected by NOC systems, investigated and followed up on by management. Corrective actions are taken depending on the impact to the network.

A formal written process is in place to evaluate, design, lab test, document and approve major system changes.

Risk Mitigation

The SEGRA risk management program includes defined rules for mitigating risks. Mitigation activities are proposed and chosen based on the return on investment in terms of cost-of-mitigation to reduction-in-risk. Positive return on investment mitigations are implemented based on resource availability. Risks may also be transferred or accepted. Risks over a certain threshold may not be accepted without executive authorization.

SEGRA maintains a cyber security liability insurance policy with an aggregate limit of liability of $10,000,000.

Vendor risk management includes lab testing new infrastructure to evaluate performance against SEGRA's controls and performance objectives, security team review of new hardware or software, mandatory legal review of any contract greater than $50,000 and mandatory General Counsel and VP level review and approval of any new vendor, hardware or service.

3.4 Description of Controls Relevant to the Availability Trust Services Criteria

Ethernet services are designed for high resilience and availability. Availability requirements and performance requirements are defined. Resilience mechanisms include multiple network paths across physically diverse fiber between MPLS distribution and core devices, MPLS fast reroute, and ethernet rings with sub-50ms protection and recovery switching. Physically diverse building entry, multiple redundant CPE and geo-diverse CPE termination are available as optional features. Link aggregation control protocol is available to provide multiple redundant connections from customer equipment to a single CPE.

DIA services utilize the SEGRA carrier ethernet network for getting traffic from a customer site to an IP router, and inherit those resiliency attributes. IP routers have diverse peerings in multiple cities to multiple Tier 1 providers, direct peerings to popular content providers, and public peering fabrics. If a customer chooses, they may diversely Border Gateway Protocol peer their equipment with multiple SEGRA IP routers for additional resiliency.

3.5 Complementary User Entity Controls

Services are designed with the assumption that certain controls are implemented by user entities. In certain situations, the application of specific controls at the user entity is necessary to meet the applicable trust services criteria. SEGRA's management makes control recommendations to user entities and provides the means to implement these controls in many instances.

This examination was limited to the activities and procedures at SEGRA as they relate to its user entities. Accordingly, the examination did not extend to any activities or procedures in effect at the user entities. It is each user entity's responsibility to evaluate this information in relation to the user entity's internal controls in place in order to obtain an understanding of the internal controls and assess control risk. The portions of the internal controls provided by the user entities and SEGRA must be evaluated together. If effective user internal controls are not in place, SEGRA's controls may not compensate for such weaknesses.

This section describes additional controls that should be in operation at user entities to complement the SEGRA controls. Client considerations include the following recommendations:

#	Complementary User Entity Control	Associated TSP Criteria
1	User entities should establish controls to ensure data is appropriately encrypted while at rest and in transit.	CC6.7
2	User entities should establish controls to ensure best practices are utilized with regards to logical access and security for systems controlled by the users, such as but not limited to the proper management of user accounts, passwords, security settings and network segmentation.	CC6.1
3	User entities should provide assurance that adequate physical and environmental controls are in place for systems residing on the user's premises.	CC6.4
4	User entities should ensure that data sent to the service is complete, accurate and authorized.	CC2.3

#	Complementary User Entity Control	Associated TSP Criteria
5	User entities should assure that data transmitted through the service is in compliance with software license agreements, regulatory requirements and the law.	CC3.2
6	User entities should assure that acceptance testing is satisfactorily completed during the setup or after changes have been made to the service.	CC8.1
7	User entities should assure that appropriate disaster recovery options are in place based upon business needs.	A1.2
8	User entities should assure that appropriate redundancy, diversity and availability options are selected based upon business needs.	A1.2
9	User entities should establish controls to prevent the introduction of unauthorized or malicious software.	CC6.8
10	User entities should establish controls to protect against threats from sources outside the user's system boundaries.	CC6.6
11	User entities should maintain, monitor and evaluate bandwidth capacity of services and order sufficient capacity to meet user objectives.	A1.1

The list of user entity control considerations presented above and those presented with certain specified control objectives do not represent a comprehensive set of all the controls that should be employed by user entities, but represent those controls around which SEGRA's controls are designed. Other controls may be required at user entities. Therefore, each client's system of internal controls must be evaluated in conjunction with the internal control structure described in this report.

Section 4 – Applicable Trust Services Criteria, and Related Controls Provided by MTN Infrastructure TopCo, Inc., dba SEGRA, Tests of Controls and Results of Tests

4.1 Information Provided by the Service Auditor

This report is intended to provide information to the management of MTN Infrastructure TopCo, Inc., dba SEGRA ("SEGRA"), user entities of SEGRA's Ethernet, Wavelength and Dedicated Internet Access System and prospective user entities, independent auditors and practitioners providing services to those entities, who have a sufficient understanding to consider it, along with other information including information about the controls implemented by the user entity. This report is intended to provide information about the suitability of the design of the controls implemented to achieve the service commitments and system requirements based on the criteria relevant to security and availability set forth in TSP section 100, 2017, *Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* ("AICPA, *Trust Services Criteria*") ("applicable trust services criteria"), throughout the period July 1, 2020 to June 30, 2021.

The examination was performed in accordance with the criteria set forth in DC section 200, 2018 *Description Criteria for a Description of the Service Organization's System in a SOC 2® Report.* It is each user entity's responsibility to evaluate this information in relation to the internal control structure in place at each user entity in order to assess the total internal control structure. If an effective internal control structure is not in place at user entities, the SEGRA controls may not compensate for such weaknesses.

This description is intended to focus on SEGRA's controls surrounding the Ethernet, Wavelength and Dedicated Internet Access System, as indicated in Section 3 of this report's Scope and Boundaries section, throughout the period July 1, 2020 to June 30, 2021; it does not encompass all aspects of the services provided or controls performed by SEGRA. Unique processes or control situations not described in the report are outside the scope of this report.

Tests of Controls

Our examination of the description of SEGRA's Ethernet, Wavelength and Dedicated Internet Access System and the suitability of the design and operating effectiveness of the controls to achieve the related service commitments and system requirements based on the services criteria stated in the description involved performing procedures to obtain evidence about the fairness of the presentation of the description of the system and the suitability of the design and operating effectiveness of those controls to achieve the related service commitments and system requirements based on the services criteria stated in the description. Our procedures included assessing the risks that the description is not fairly presented and that the controls were not suitably designed or operating effectively to achieve the related service commitments and system requirements based on the services stated in the description.

As a result of COVID-19, certain procedures, normally performed through inspection during onsite walkthroughs with the IT team, were redesigned. For example, we performed virtual walkthroughs with the IT team during one of the four quarters, and additional alternative and complementary procedures were designed and performed to corroborate the results of our modified tests.

Our procedures also included testing the operating effectiveness of those controls that we consider necessary to provide reasonable assurance that the related service commitments and system requirements based on the services criteria stated in the description were achieved throughout the period July 1, 2020 to June 30, 2021.

Types of testing methods include:

Type	***Description***
Inquiry	Made inquiries of appropriate personnel and corroborated responses with management.
Observation	Observed the application, performance, or existence of the specific control(s) as represented by management.
Inspection	Inspected documents and records indicating performance of the control.
Reperformance	Reperformed the control or processing application to ensure the accuracy of its operation.

4.2 Information Provided by the Entity

When using information produced by the service organization, we evaluated whether the information was sufficiently reliable for our purposes by obtaining evidence about the accuracy and completeness of such information and evaluating whether the information was sufficiently precise and detailed for our purposes.

4.3 Common Criteria to Security

The trust services criteria relevant to security address the need for information and systems to be protected against unauthorized access, unauthorized disclosure of information, and damage to systems that could compromise the availability, integrity, confidentiality, and privacy of information or systems and affect the service organization's ability to achieve its service commitments and system requirements.

Security refers to 1) the protection of information during its collection or creation, use, processing, transmission, and storage and 2) systems that use electronic information to process, transmit or transfer, and store information to enable the achievement of MTN Infrastructure TopCo, Inc., dba SEGRA's ("SEGRA") service commitments and system requirements. Controls over security prevent or detect the breakdown and circumvention of segregation of duties, system failure, incorrect processing, theft or other unauthorized removal of information or system resources, misuse of software, and improper access to or use of, alteration, destruction, or disclosure of information.

CC1.1 - The entity demonstrates a commitment to integrity and ethical values.			
	SEGRA's Controls	**BPS Tests of Controls**	**Results of Tests**
CC1.1.1	Management has put in place an organizational structure that defines reporting lines, authorities, and responsibilities for the design, development, implementation, operation, monitoring and maintenance of each respective area.	Inspected organizational chart and a sample of employees noting that the roles and responsibilities align with reporting lines.	No exceptions noted.

CC1.1 - The entity demonstrates a commitment to integrity and ethical values (continued).			
	SEGRA's Controls	**BPS Tests of Controls**	**Results of Tests**
CC1.1.2	Formal hiring procedures are in place and performed by the Human Resource Department including criminal background checks, drug tests, financial checks if relevant to the position, and reference checks prior to hiring.	Inspected files for a sample of newly hired employees noting that reference, background and drug checks were performed. The circumstances that warrant the operation of a financial check did not occur in the sample selected during the examination period. In performing the testing above, we tested that no sampled employees met requirements for a financial check. As a result, this part of the control could not be tested.	No exceptions noted. The circumstances that warrant the operation of a financial check did not occur in the sample selected during the examination period. As a result, this part of the control could not be tested.
CC1.1.3	Performance evaluations are conducted by the Human Resources Department at least annually as outlined in the human resources policies and procedures document. Employees are evaluated against SEGRA core values.	Inspected completed performance evaluations for a sample of employees noting that the evaluations align with core values.	No exceptions noted.
CC1.1.4	SEGRA has documented the code of business conduct and ethical standards which are reviewed, updated if applicable and approved by the board of directors and senior management annually.	Inspected code of conduct and ethical standards noting that the board of directors and senior management reviews and approves the documents at least annually.	No exceptions noted.

CC1.1 - The entity demonstrates a commitment to integrity and ethical values (continued).			
	SEGRA's Controls	**BPS Tests of Controls**	**Results of Tests**
CC1.1.5	Personnel are required to read and accept the code of conduct and ethics upon their hire and formally reaffirm them annually thereafter.	Inspected files for a sample of newly hired and long-term employees noting that each signed acknowledgement of the code of conduct and ethics requirements.	No exceptions noted.
CC1.1.6	Management has put into place multiple anonymous whistleblower hotlines, depending on the severity, for reporting ethical or integrity violations to the board of directors and management.	Inspected methods for whistleblowing communications noting that the issues reported through independent third-parties to management and the board of directors are received with initiator both identified and anonymous.	No exceptions noted.

CC1.2 - The board of directors demonstrates independence from management and exercises oversight of the development and performance of internal control.			
	SEGRA's Controls	**BPS Tests of Controls**	**Results of Tests**
CC1.2.1	The board of directors of MTN Infrastructure TopCo, Inc., dba SEGRA, are appointed by EQT Partners and act on behalf of the owners by exercising oversight of the management team. An Audit Committee consisting of a mixture of board members and management oversees the development and performance of internal control.	Inspected charters and a sample of minutes noting that the board of directors and Audit Committee provide oversight over internal control.	No exceptions noted.
CC1.2.2	The majority of the members of the board of directors do not hold SEGRA management positions.	Inspected organizational chart and members of the board of directors noting that a majority of the board is non-management.	No exceptions noted.
CC1.2.3	SEGRA, has a Cyber Security Committee governed by a Cyber Security Committee charter that provides support to management and the board of directors.	Inspected Cyber Security Committee charter and a sample of minutes noting that open lines of communication exist with both management and the board of directors.	No exceptions noted.

CC1.3 - Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives.			
	SEGRA's Controls	**BPS Tests of Controls**	**Results of Tests**
CC1.3.1	Management has put in place an organizational structure that defines reporting lines, authorities, and responsibilities for the design, development, implementation, operation, monitoring, and maintenance of each respective area.	Inspected organizational chart and a sample of employees noting that their roles and responsibilities align with reporting lines.	No exceptions noted.

CC1.4 - The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.			
	SEGRA's Controls	**BPS Tests of Controls**	**Results of Tests**
CC1.4.1	Management writes job requirements, obtains resumes and conducts interviews prior to hiring personnel.	Inspected files for a sample of newly hired employees noting that job requirements are written, resumes are retained and interviews are performed.	No exceptions noted.
CC1.4.2	Management has established tuition reimbursement and training programs to help with retention.	Inspected a sample of quarterly training reports and tuition reimbursement reports noting that employees are provided reimbursement and training is completed.	No exceptions noted.

CC1.5 - The entity holds individuals accountable for their internal control responsibilities in the pursuit of objectives.			
	SEGRA's Controls	**BPS Tests of Controls**	**Results of Tests**
CC1.5.1	Management conducts appraisals annually, and raises are performance-based.	Inspected annual reviews for a sample of employees noting that there is a correlation between performance results and salary modification.	No exceptions noted.
CC1.5.2	Management has established disciplinary policy and procedures that include steps such as coaching, written warnings, final warnings and conditions for termination of employment.	Inspected files for a sample of terminated employees noting that the disciplinary discussions are acknowledged by each employee prior to termination.	No exceptions noted.

CC2.1 - The entity obtains or generates and uses relevant, quality information to support the functioning of internal control.			
	SEGRA's Controls	**BPS Tests of Controls**	**Results of Tests**
CC2.1.1	SEGRA identifies information and process requirements via an annual assessment to identify data and process flows.	Inspected feedback and correspondence from process and control owners for a sample of months noting that data and process flows are evaluated on an ongoing basis.	No exceptions noted.
CC2.1.2	SEGRA communicates critical controls via a document review procedure and email distribution.	Inspected a sample of e-mail chains and intranet discussions noting the review and distribution of critical controls.	No exceptions noted.

CC2.2 - The entity internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.			
	SEGRA's Controls	**BPS Tests of Controls**	**Results of Tests**
CC2.2.1	Risk and control effectiveness are reported to management during quarterly meetings between Security Architecture, Operations, IT and senior management.	Inspected a sample of quarterly meeting minutes noting that those responsible for control implementation are in attendance and discussions align with risk and control effectiveness.	No exceptions noted.
CC2.2.2	Senior management has established whistle-blower hotlines for employees to anonymously report ethics or policy violations.	Inspected methods for whistleblowing communications noting that the issues reported through independent third-parties to management and the board of directors are received with the initiator both identified and anonymous.	No exceptions noted.
CC2.2.3	Change management and incident response procedures provide communication trees and escalation time-lines for internal communication of routine incidents and non-routine disasters.	Inspected Change Management and Incident Response Policies noting the inclusion of communication trees and internal correspondence requirements.	No exceptions noted.

CC2.3 - The entity communicates with external parties regarding matters affecting the functioning of internal control.			
	SEGRA's Controls	**BPS Tests of Controls**	**Results of Tests**
CC2.3.1	Media and Investor Communications Policy defines and restricts communications to media, analysts or investors to appropriate named executive staff and supporting personnel.	Inspected a sample of external communications noting that media releases are prepared and provided by the appropriate sources in accordance with its Media and Investor Communications Policy.	No exceptions noted.
CC2.3.2	Change management and incident response procedures provide communication trees and escalation time-lines for external communication of routine incidents and non-routine disasters.	Inspected Change Management and Incident Response Policies noting that communication trees and internal correspondence requirements are documented. Inspected a sample of internal and external communications noting policy compliance.	No exceptions noted.
CC2.3.3	Customers may elect to receive routine reporting on SLA performance as an optional service feature for the ELINE and E-Access products.	Inspected a sample of SLA performance reports noting that the measurement of actual results and service level requirements are communicated to the customer.	No exceptions noted.
CC2.3.4	Elite Care and Critical Care customers are assigned a Technical Support Manager and a Client Program Manager ("CPM") to keep the customer informed of internal SEGRA activities relating to the customer's service such as monthly operational/incident reports and upcoming maintenance or service enhancement activities. The CPM acts as an advocate for the customer working within SEGRA.	Inspected correspondence for a sample of Elite Care and Critical Care correspondence noting that the assigned CPM communicates maintenance or service enhancements to the customer.	No exceptions noted.

CC3.1 - The entity specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives.			
	SEGRA's Controls	**BPS Tests of Controls**	**Results of Tests**
CC3.1.1	Security Architecture meets with General Counsel at least quarterly to identify changes in law or regulatory requirements to be incorporated into the risk management process.	Inspected a sample of minutes of meetings noting that regulatory issues and risk management are discussed.	No exceptions noted.
CC3.1.2	Contract terms and commitments are maintained by the General Counsel's office. Updates and modifications to contractual terms are approved by the legal department prior to contract approval. Terms are incorporated into the risk assessment and review process.	Inspected a sample of contracts noting that the legal department approves modifications and internal risks surrounding contract terms are considered.	No exceptions noted.

CC3.2 - The entity identifies risks to the achievement of its objectives across the entity and analyzes risks as a basis for determining how the risks should be managed.			
	SEGRA's Controls	**BPS Tests of Controls**	**Results of Tests**
CC3.2.1	A risk management process is established.	Inspected Security Risk Management Policy noting that a risk management process is established.	No exceptions noted.
CC3.2.2	IT assesses and responds to security risks on an ongoing basis by reviewing authentication and access logs monthly, and to a lesser extent daily, performing quarterly vulnerability assessments, annual penetration tests, and conducting formal risk assessments annually or when there is a significant change to the environment.	Inspected minutes for a sample of Information Security Team meetings noting that risk management is incorporated in the discussion. Inspected a sample of access log reviews and vulnerability assessments or penetration tests as documented in the CC6 portion of Section 4 of this report. Inspected a sample of daily security reports noting that the risk assessment plan incorporates findings into its process.	No exceptions noted.
CC3.2.3	Strategy and operations, risk considerations and other factors critical to the business are discussed at least quarterly at meetings between Security Architecture, operations, IT and executive management.	Inspected minutes from a sample of Executive Security Updates noting that the meetings are conducted at a frequency greater than quarterly.	No exceptions noted.

CC3.2 - The entity identifies risks to the achievement of its objectives across the entity and analyzes risks as a basis for determining how the risks should be managed (continued).			
	SEGRA's Controls	**BPS Tests of Controls**	**Results of Tests**
CC3.2.4	Risks are calculated and ranked using methodology that measures impact and likelihood using factors from the security or operations teams and business impact factors from operations, legal and executive management, such as impact to critical products, compliance or major accounts.	Inspected a sample of Monthly IT Assurance Summaries noting that severity ratings were assigned to internal and external events, which were documented in detail to include resolutions and risk management strategies in accordance with the Risk Management Policy.	No exceptions noted.
CC3.2.5	Risk assessment includes considering how the risk should be managed and whether to accept, avoid, reduce, or share the risk.		

CC3.3 - The entity considers the potential for fraud in assessing risks to the achievement of objectives.			
	SEGRA's Controls	**BPS Tests of Controls**	**Results of Tests**
CC3.3.1	Management collaborates with an external third-party to assess fraud potential at least annually.	Inspected internally and externally prepared annual risk assessments noting that the potential for fraud is considered.	No exceptions noted.
CC3.3.2	Management investigates all identified and reported fraud and applies corrective action as appropriate.	The circumstances that warrant the operation of this control did not occur during the examination period. Inspected Fraud Risk Assessment Policy noting that the steps for addressing fraud are documented; no instances of reported fraud were noted based on our review of the available methods for reporting fraud.	The circumstances that warrant the operation of this control did not occur during the examination period. As a result, the control could not be tested.

CC3.4 - The entity identifies and assesses changes that could significantly impact the system of internal control.			
	SEGRA's Controls	**BPS Tests of Controls**	**Results of Tests**
CC3.4.1	The SEGRA financial planning and analysis team, security team and senior management, through its ongoing risk assessment process, evaluate changes in business, economic, regulatory and technology environments.	Inspected a sample of Monthly IT Assurance Summaries noting that internal evaluation and risk assessment relevant to business, economic, regulatory and technology changes is incorporated.	No exceptions noted.

CC4.1 - The entity selects, develops, and performs ongoing and/or separate evaluations to ascertain whether the components of internal control are present and functioning.			
	SEGRA's Controls	**BPS Tests of Controls**	**Results of Tests**
CC4.1.1	Penetration testing is performed at least annually.	Inspected the results of the annual penetration test noting that the external assessors identified no significant issues.	No exceptions noted.
CC4.1.2	Vulnerability assessments are performed quarterly.	Inspected a sample of vulnerability assessments noting that they were conducted at least quarterly.	No exceptions noted.
CC4.1.3	Audits against established specifications and formal security and risk assessments are performed when there are major changes to the environment.	Inspected a sample of baseline configuration change audits noting that only intended changes occur. Inspected a sample of changes to the system noting that risk levels are identified.	No exceptions noted.
CC4.1.4	Infrastructure utilization is monitored by software systems and IT initiates infrastructure capacity upgrades at predefined thresholds of utilization.	Inspected a sample of method of procedure tickets noting that the need for capacity increases are tracked and upgrades are initiated and carried out at predefined thresholds.	No exceptions noted.
CC4.1.5	Infrastructure is monitored using dry contact alarms, SNMP traps, syslog, ethernet CFM and software monitoring systems to aggregate, parse and display monitoring and alarming data. The Operations Team monitors the system 24x7, 365 and initiates incident recovery as necessary.	Inspected a sample of network devices noting that monitoring is ongoing in the Network Operations Center ("NOC"). Inspected the ticketing system log for a sample of days noting that alarm originated tickets are resolved by the NOC.	No exceptions noted.

CC4.2 - The entity evaluates and communicates internal control deficiencies in a timely manner to those parties responsible for taking corrective action, including senior management and the board of directors, as appropriate.			
	SEGRA's Controls	**BPS Tests of Controls**	**Results of Tests**
CC4.2.1	Evaluation and results, deficiencies and corrective actions are reviewed quarterly by executive management.	Inspected a sample of minutes from executive management meetings noting that risk management is discussed.	No exceptions noted.
CC4.2.2	Troubles, incidents, their resolution and SEGRA's performance in resolving those troubles and incidents are documented, tracked and reported on using the ticket system.	Inspected a sample of tickets noting that issues are documented and timestamped throughout the resolution process in the ticketing system.	No exceptions noted.

CC5.1 - The entity selects and develops control activities that contribute to the mitigation of risks to the achievement of objectives to acceptable levels.			
	SEGRA's Controls	**BPS Tests of Controls**	**Results of Tests**
CC5.1.1	Management segregates incompatible duties such as a separation of operations and engineering design, and lab/development and production. This is reflected in the organization chart, documented job responsibilities, and the technical segregation of lab/test environments. This segregation is also reflected in logical access privileges in the form of separate accounts per role, or limited privileges to production for engineering and design staff.	Inspected organizational chart noting that responsibility-based segregation of duties is clearly defined. Inspected roles and responsibilities for a sample of newly hired and long-term employees noting that their access levels align with their position and responsibilities.	No exceptions noted.

CC5.2 - The entity also selects and develops general control activities over technology to support the achievement of objectives.			
	SEGRA's Controls	**BPS Tests of Controls**	**Results of Tests**
CC5.2.1	Management develops a list of control activities to manage technology infrastructure and security risks identified during the annual risk assessment.	Inspected control activities as documented in formal procedures and policies and throughout testing noting that a risk-based approach to system management is taken.	No exceptions noted.
CC5.2.2	Management has established technology acquisition, development and maintenance processes that requires new technologies to be evaluated against and designed for performance objectives including security control capabilities.	Inspected a sample of technology implementations noting that each is evaluated against performance objectives and approved prior to release. Inspected a sample of potential new technology acquisitions that did not meet network standards noting that they were not incorporated into the system.	No exceptions noted.

CC5.3 - The entity deploys control activities through policies that establish what is expected and in procedures that put policies into action.			
	SEGRA's Controls	**BPS Tests of Controls**	**Results of Tests**
CC5.3.1	Information security policies and operating procedures address controls over significant aspects of operations. Policy sections include access control, network communications, risk assessment, user provisioning, change control, incident response, physical security, and vendor relations.	Inspected control activities as documented in formal procedures and policies and throughout testing noting that a risk-based approach to system management is taken.	No exceptions noted.
CC5.3.2	The SEGRA Cyber Security Committee is charged with establishing, maintaining and enforcing the overall security policies and procedure.	Inspected Cyber Security Committee charter and IT security policies noting that the approvals and timing of reviews align with committee requirements.	No exceptions noted.

CC6.1 - The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity's objectives.			
	SEGRA's Controls	**BPS Tests of Controls**	**Results of Tests**
CC6.1.1	Information assets are inventoried and tracked using inventory and asset management software systems.	Inspected a sample of inventory systems for reasonableness and traced a sample of network equipment through the inventory reports.	No exceptions noted.
CC6.1.2	Access is granted in accordance with the Company's Access Control Policy, which requires access level to align with job duties and requires recorded authorization.	Inspected recorded access authorization for a sample of newly hired and long-term employees noting that access levels align with the position and responsibilities.	No exceptions noted.
CC6.1.3	Shared, generic or group passwords used for emergency override in the event of an authentication systems failure must be changed every six months.	Inspected admin password change logs for a sample of months noting that admin passwords are changed at least every six months.	No exceptions noted.
CC6.1.4	Every user or system must have unique credentials for access to multi-user systems and computers. Shared, generic or group credentials may only be used if absolutely necessary.	Inspected a sample of logical access reports noting that all users have unique user names. Inquired on a sample of admin accounts to determine access holders and inspected organizational chart, position and role noting that their access was appropriate.	No exceptions noted.
CC6.1.5	Passwords must meet length and complexity requirements in accordance with internal policies.	Inspected length and complexity requirements per internal policy noting that access rules for each software align with internal policies. Reperformed password change procedures noting that non-complex passwords are rejected.	No exceptions noted.

CC6.1 - The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity's objectives (continued).			
	SEGRA's Controls	**BPS Tests of Controls**	**Results of Tests**
CC6.1.6	Access attempts are logged.	Inspected a sample of access reports noting that failed attempts and successful logins are logged.	No exceptions noted.
CC6.1.7	Individual user accounts are locked out after 6 failed attempts.	Reperformed incorrect input six times noting that the device locked requiring administrator intervention to unlock.	No exceptions noted.
CC6.1.8	Remote access encrypts data in transit.	Inspected remote access traffic for a sample of days noting that all remote data in transit was encrypted.	No exceptions noted.
CC6.1.9	Remote access requires the use of multi-factor authentication.	Inspected remote access configurations noting that multi-factor requirements were in place.	No exceptions noted.
CC6.1.10	SEGRA's controlled equipment areas are equipped with fire detection and suppression, hand-held fire extinguishers, dedicated and redundant CRAC and HVAC systems, redundant UPS systems, and backup generators. HVAC inspection and maintenance are performed by third parties 2-4 times a year to ensure the devices are in working order. Backup generators and UPS batteries are inspected quarterly. Generators are exercised weekly.	Inspected fire detection and suppression systems noting that inspections occur at a frequency greater than quarterly. Inspected backup power systems noting that inspections occur at a frequency greater than quarterly. Inspected a sample of generator logs noting that load and failover testing occurred weekly.	No exceptions noted.

CC6.1 - The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity's objectives (continued).			
	SEGRA's Controls	**BPS Tests of Controls**	**Results of Tests**
CC6.1.11	HVAC and electrical power infrastructure communicate alerts using SNMP to the monitoring software system. The software is monitored by operations staff for actionable events 24x7, 365.	Inspected a sample of network devices noting that the NOC monitors the sampled device and it is configured so that alerts are generated.	No exceptions noted.
CC6.1.12	Network segregation requirements are defined in a formal written policy defining network boundaries, requiring networks to be segmented into logical areas based on risk and trust levels, mandating the use of control mechanisms to enforce segregation such as firewalls, physical isolation or tunneling, and requiring firewall devices between different network segments that must communicate with each other.	Inspected network diagrams and network requirements defined in the Information Security Policy noting that the design used is intended to segregate areas from each other where communication is not necessary and to require protection between areas where it is necessary.	No exceptions noted.
CC6.1.13	Control mechanisms between logical network boundaries must be documented and reviewed annually.	Inspected Information Security Policy noting that logical boundaries are documented and reviewed at a frequency greater than annual. Inspected a sample of boundary devices noting that the configurations and rules were reviewed and updated where needed at least annually.	No exceptions noted.

CC6.1 - The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity's objectives (continued).			
	SEGRA's Controls	**BPS Tests of Controls**	**Results of Tests**
CC6.1.14	Ethernet services are segmented and isolated from each other using tunnel and logical isolation technologies such as MPLS, QinQ, VLANs, and physical isolation using optical wavelengths or separate fiber optic strands.	Inspected engineering test plans and results for a sample of in-place and new network devices noting that implementation is tested and passed by engineering on service isolation prior to turning up new equipment.	No exceptions noted.
CC6.1.15	Communications with infrastructure management networks are restricted to authorized staff in accordance with the Company's Access Control Policy.	Inspected roles and responsibilities for a sample of staff able to access infrastructure noting that their access levels align with the Access Control Policy.	No exceptions noted.

CC6.2 - Prior to issuing system credentials and granting system access, the entity registers and authorizes new internal and external users whose access is administered by the entity. For those users whose access is administered by the entity, user system credentials are removed when user access is no longer authorized.			
	SEGRA's Controls	**BPS Tests of Controls**	**Results of Tests**
CC6.2.1	Requests for access are logged and require approval from the operations manager responsible for the system the access request is for.	Inspected access requests for a sample of newly hired employees and changes for a sample of long-term employees noting that the access was authorized by the system's manager.	No exceptions noted.
CC6.2.2	Access permissions are reviewed quarterly to ensure the business need for the access is still relevant.	Inspected access reviews and report issuance correspondence for a sample of systems and high-priority equipment noting that the reviews occurred at a frequency greater than quarterly.	No exceptions noted.
CC6.2.3	A physical access report is issued quarterly to authorizing directors for high-priority equipment. All cards must be confirmed as still necessary or they will be deactivated.		
CC6.2.4	A visitor log is used to record physical access to equipment rooms.	Inspected visitor logs in a sample of secure equipment rooms noting that the logs are being used.	No exceptions noted.
CC6.2.5	Accounts are revoked by IT and system owners based on notices of termination sent from Human Resources.	Inspected timeliness of termination correspondence and system owners' revocation for a sample of terminated employees noting same day access removal.	No exceptions noted.

CC6.3 - The entity authorizes, modifies, or removes access to data, software, functions, and other protected information assets based on roles, responsibilities, or the system design and changes, giving consideration to the concepts of least privilege and segregation of duties, to meet the entity's objectives.			
	SEGRA's Controls	**BPS Tests of Controls**	**Results of Tests**
CC6.3.1	Access is granted to a system based on business need pending approval from authorized approving managers.	Inspected access changes for a sample of newly hired and long-term employees noting that access is granted by the system manager on an as-needed basis only.	No exceptions noted.
CC6.3.2	Accounts are revoked by IT and system owners based on notices of termination sent from Human Resources.	Inspected timeliness of termination correspondence and system owners' revocation for a sample of terminated employees noting same day access removal.	No exceptions noted.
CC6.3.3	Role based access control is used to support segregation of incompatible functions. Communication and access controls are based on internal group memberships.	Inspected organizational chart noting that responsibility-based segregation of duties is clearly defined. Inspected roles and responsibilities for a sample of newly hired and long-term employees noting that their access levels align with position and responsibilities.	No exceptions noted.

CC6.4 - The entity restricts physical access to facilities and protected information assets (for example, data center facilities, back-up media storage, and other sensitive locations) to authorized personnel to meet the entity's objectives.			
	SEGRA's Controls	**BPS Tests of Controls**	**Results of Tests**
CC6.4.1	Physical access to SEGRA's facilities is controlled by an electronic key card badge system. Physical access is controlled by responsibility role-based access control. Changes to responsibility-based access are documented via the trouble ticket system, approved by the director of the individual requesting additional access, and executed by the facilities team.	Inspected physical access points for a sample of equipment rooms noting that a key card is required for entry. Inspected access changes for a sample of newly hired and long-term employees noting that access is manager approved, facilities team granted, and on an as-needed basis only.	No exceptions noted.
CC6.4.2	Physical access is logged through the badging system.	Inspected badging system reports for sample of days and facilities noting that access is logged.	No exceptions noted.
CC6.4.3	Physical access logs are reviewed quarterly for unauthorized access by facilities, operations, and/or the security team.	Inspected physical access reports, tickets and correspondence noting that management's review occurs at a frequency greater than quarterly.	No exceptions noted.
CC6.4.4	A visitor's log is used to record physical access to equipment areas. Visitors to equipment areas require an authorized escort. The visitor log records the name of the visitor, the times and purpose of visit, and the company of visitor.	Inspected visitor logs in a sample of secure equipment rooms noting that the visitor name, time in/out, date, visitor's company and the visitor's purpose is recorded.	No exceptions noted.

CC6.5 - The entity discontinues logical and physical protections over physical assets only after the ability to read or recover data and software from those assets has been diminished and is no longer required to meet the entity's objectives.			
	SEGRA's Controls	**BPS Tests of Controls**	**Results of Tests**
CC6.5.1	Prior to removal from company facilities, all digital media is removed, destroyed, or otherwise sanitized to remove any confidential data or software.	Inspected digital media storage facility housing decommissioned hardware and sanitization logs noting that the equipment is wiped prior to removal or destruction.	No exceptions noted.

CC6.6 - The entity implements logical access security measures to protect against threats from sources outside its system boundaries.			
	SEGRA's Controls	**BPS Tests of Controls**	**Results of Tests**
CC6.6.1	Management has established formal written policies and procedures to restrict logical access, establish boundary protection systems, and define additional authentication controls for remote access.	Inspected Access Control and Network Segmentation Policies noting that the policies are reviewed, approved, and maintained current.	No exceptions noted.
CC6.6.2	DDoS mitigation appliances are placed at every autonomous system border at which SEGRA receives full Internet routes or a default route.	Inspected a sample of border devices and DDoS appliances, noting that defense systems are active for each downstream provider.	No exceptions noted.
CC6.6.3	Boundaries between network areas are protected by firewalls, physical isolation or tunneling.	Inspected a sample of boundary devices, defense devices and applications noting that protections are in place.	No exceptions noted.
CC6.6.4	Network boundaries and the controls between them (such as firewall rules) are documented and reviewed by the security team annually.	Inspected Network Boundaries Policy noting that the security team reviews and approves at a frequency greater than annually. Inspected firewall dashboard for a sample of devices noting that default, ingress and egress firewall rules, network address translation, and denial of service rules are implemented.	No exceptions noted.

CC6.7 - The entity restricts the transmission, movement, and removal of information to authorized internal and external users and processes, and protects it during transmission, movement, or removal to meet the entity's objectives.			
	SEGRA's Controls	**BPS Tests of Controls**	**Results of Tests**
CC6.7.1	Company laptops and iPads use encryption-at-rest.	Inspected encryption method and settings on a sample of devices noting that encryption at rest is active.	No exceptions noted.
CC6.7.2	VPN technologies are used to provide encryption across public networks.	Inspected remote access traffic for a sample of days noting that remote data in transit is encrypted.	No exceptions noted.

CC6.8 - The entity implements controls to prevent or detect and act upon the introduction of unauthorized or malicious software to meet the entity's objectives.			
	SEGRA's Controls	**BPS Tests of Controls**	**Results of Tests**
CC6.8.1	The monitoring system logs and notifies the NOC of software installations or attempted software installations.	Inspected a sample of executable files and devices noting that install activity is recorded and NOC is alerted.	No exceptions noted.
CC6.8.2	Only authorized staff are able to install software on infrastructure devices. Authorized software is defined in engineering approval notices that are approved by executive management.	Inspected install rules for a sample of users noting that read-only, authorization required or execute allowable appropriately aligns with the device owner's role within the system.	No exceptions noted.
CC6.8.3	Antivirus and anti-malware software are implemented.	Inspected a sample of the system's multi-layered protection applications noting that threats are blocked and definitions are current.	No exceptions noted.

CC7.1 - To meet its objectives, the entity uses detection and monitoring procedures to identify (1) changes to configurations that result in the introduction of new vulnerabilities, and (2) susceptibilities to newly discovered vulnerabilities.			
	SEGRA's Controls	**BPS Tests of Controls**	**Results of Tests**
CC7.1.1	Configuration standards and baselines are defined by engineering provisioning guidelines, which are approved by management.	Inspected a sample of provisioning guidelines and baseline configurations noting that management approves the guidelines.	No exceptions noted.
CC7.1.2	The monitoring system software logs when changes are made to production configurations. The NOC monitors these logs 24x7, 365.	Inspected a sample of configuration changes noting that the activity is recorded and the NOC was alerted.	No exceptions noted.
CC7.1.3	A configuration management tool collects active configurations from infrastructure devices at least daily.	Inspected full configurations for a sample of infrastructure devices and days noting that configuration mirroring occurs at a frequency greater than daily.	No exceptions noted.

CC7.2 - The entity monitors system components and the operation of those components for anomalies that are indicative of malicious acts, natural disasters, and errors affecting the entity's ability to meet its objectives; anomalies are analyzed to determine whether they represent security events.			
	SEGRA's Controls	**BPS Tests of Controls**	**Results of Tests**
CC7.2.1	Availability and integrity of the infrastructure, including environmental, physical or logical changes, resource consumption, failures, or deviation from baselines, are logged, alerted on, and monitored by the NOC 24x7, 365.	Inspected a sample of alarm data noting that unusual activity, near capacity thresholds, out-of-spec environmental monitoring and system changes are recorded, alerted and NOC monitored.	No exceptions noted.

CC7.3 - The entity evaluates security events to determine whether they could or have resulted in a failure of the entity to meet its objectives (security incidents) and, if so, takes actions to prevent or address such failures.			
	SEGRA's Controls	**BPS Tests of Controls**	**Results of Tests**
CC7.3.1	Security incidents are reported and evaluated by the security team. The security team recommends mitigations, and reports on incidents in a monthly report. Non-routine incidents of sufficient severity are escalated to senior management.	Inspected a sample of daily traffic reports and monthly assurance summaries noting that non-routine incidents are evaluated, tracked through resolution, and escalated to senior management, when necessary, using the internal ticketing system.	No exceptions noted.

CC7.4 - The entity responds to identified security incidents by executing a defined incident response program to understand, contain, remediate, and communicate security incidents, as appropriate.			
	SEGRA's Controls	**BPS Tests of Controls**	**Results of Tests**
CC7.4.1	All incidents follow the incident response or disaster recovery plans depending on the severity. Plans include roles, communication trees, and escalation timelines.	Inspected Incident Response Plan, Disaster Recovery Plan and a sample of incidents noting that the maintenance of current contacts, escalation rules and timelines were included in the investigation process.	No exceptions noted.

CC7.5 - The entity identifies, develops, and implements activities to recover from identified security incidents.			
	SEGRA's Controls	**BPS Tests of Controls**	**Results of Tests**
CC7.5.1	Software updates related to flaw remediations are tested for effectiveness and potential side effects in a segregated environment before installation to production. A roll back procedure is determined before upgrading or patching.	Inspected roll-back and test lab procedures for a sample of patches noting that a segregated environment is used for testing prior to production release and roll-back data is stored.	No exceptions noted.
CC7.5.2	Incidents related to the security of the system are logged, tracked and communicated to senior management and affected parties according to the incident level. Escalation procedures remain in place until resolution.	Inspected Incident Response Plan and Disaster Recovery Plan noting the maintenance of current contacts, escalation rules and timelines. Inspected a sample of incidents noting that each was logged, tracked, escalated and resolved in accordance with documented procedures.	No exceptions noted.

CC8.1 - The entity authorizes, designs, develops or acquires, configures, documents, tests, approves, and implements changes to infrastructure, data, software, and procedures to meet its objectives.			
	SEGRA's Controls	**BPS Tests of Controls**	**Results of Tests**
CC8.1.1	A change management policy is in place to evaluate, design, test, document and approve significant changes.	Inspected engineering process and Change Management Policy noting that changes include design documents, testing, reviews and approvals.	No exceptions noted.
CC8.1.2	Risks and impacts of changes are identified and documented as a part of the change approval process.	Inspected a sample of system changes noting that risks are evaluated, reviews are multi-layered, and communication and approvals occur prior to implementing system changes.	No exceptions noted.
CC8.1.3	Changes are formally documented, reviewed, communicated to the appropriate parties and approved.		
CC8.1.4	Baseline configurations are stored in the configuration backup tool for roll back capability before a change is made.	Inspected a sample of device provisioning guidelines and baseline configurations noting that configurations are stored prior to change and roll-back procedures exist.	No exceptions noted.
CC8.1.5	Non-routine changes are developed and tested in a separate development or test environment before implementation.	Inspected roll-back and change procedures for a sample of non-routine changes noting that testing occurred in a segregated environment prior to system release.	No exceptions noted.

CC9.1 - The entity identifies, selects, and develops risk mitigation activities for risks arising from potential business disruptions.			
	SEGRA's Controls	**BPS Tests of Controls**	**Results of Tests**
CC9.1.1	A documented risk management procedure is in place that includes guidance on the identification of threats, rating the significance of risk associated with the threats, and mitigation strategies for those risks.	Inspected Security Risk Management Standard noting that risks are categorized, ranked based on threat level and the Standard is designed such that risk assessment is prioritized based on level.	No exceptions noted.
CC9.1.2	A risk assessment is performed on at least an annual basis. As part of this process, threats and environmental, regulatory and technological changes to service commitments, policies and procedures are identified and the risks are formally assessed.	Inspected risk assessments performed by an external 3rd party and the internal security team noting an occurrence frequency greater than annual.	No exceptions noted.
CC9.1.3	The risk management procedure includes the use of insurance to minimize the financial impact of any loss events.	Inspected insurance policy noting that coverage exists throughout the period.	No exceptions noted.

CC9.2 - The entity assesses and manages risks associated with vendors and business partners.			
	SEGRA's Controls	**BPS Tests of Controls**	**Results of Tests**
CC9.2.1	Formal information sharing and confidentiality agreements are in place with related parties and vendors.	Inspected a sample of 3rd party agreements noting that protections are in place.	No exceptions noted.
CC9.2.2	General Counsel and the relevant vice president review and approve any new vendor, hardware or service.	Reviewed a sample of contract modifications noting that the General Counsel and Vice President reviews and approves new vendors prior to initiation.	No exceptions noted.

4.4 Additional Criteria to Availability

The availability principle refers to the accessibility of the system, products or services as committed by contract, service-level agreement, or other agreements. This principle does not, in itself, set a minimum acceptable performance level for system availability. The availability principle does not address system functionality (the specific functions a system performs) and system usability (the ability of users to apply system functions to the performance of specific tasks or problems), but does address whether the system includes controls to support system accessibility for operation, monitoring, and maintenance.

A1.1 - The entity maintains, monitors, and evaluates current processing capacity and use of system components (infrastructure, data, and software) to manage capacity demand and to enable the implementation of additional capacity to help meet its objectives.			
	SEGRA's Controls	**BPS Tests of Controls**	**Results of Tests**
A1.1.1	Provider network capacity is measured, forecasted and upgraded according to capacity management standards and procedures.	Inspected a sample of network planning projects noting that near-threshold capacity is increased in accordance with internal policy.	No exceptions noted.

A1.2 - The entity authorizes, designs, develops or acquires, implements, operates, approves, maintains, and monitors environmental protections, software, data back-up processes, and recovery infrastructure to meet its objectives.			
	SEGRA's Controls	**BPS Tests of Controls**	**Results of Tests**
A1.2.1	Environmental threats are monitored, detected, alerted, and addressed using SNMP monitoring and the internal ticketing system.	Inspected a sample of equipment room hardware noting that alarming devices are attached and traced a sample of hardware related tickets through NOC monitoring equipment.	No exceptions noted.
A1.2.2	Full infrastructure configuration data is backed up daily.	Inspected full configuration backups and backup logs for a sample of days noting that mirroring occurs at a frequency greater than daily.	No exceptions noted.
A1.2.3	Alternate processing infrastructure is in place to ensure data can be accessed using multiple routes.	Inspected alternate versus explicit processing routes noting that multiple traffic paths are available and utilized based on predefined efficiency or customer driven parameters.	No exceptions noted.

A1.3 - The entity tests recovery plan procedures supporting system recovery to meet its objectives.			
	SEGRA's Controls	**BPS Tests of Controls**	**Results of Tests**
A1.3.1	The integrity and completeness of infrastructure back-up data is tested quarterly.	Inspected a sample of infrastructure backups noting that restoration testing occurs at a frequency greater than quarterly.	No exceptions noted.
A1.3.2	The business continuity plan is tested annually and updated as needed.	Inspected a sample of business continuity plan tests noting that testing occurs at least annually.	No exceptions noted.

SEGRA

Segra's Implementation Plan

We believe service doesn't end with sales.

Once you sign the proposal, that's when our customer service really kicks in. In fact, we've re-engineered our entire company operations to put you – our customer – at the very center of what we do. We listen, we show respect, and we make every conversation count.

Guide to Successful Implementation

Thank you for doing business with Segra. Here is a simple guide to ensure your service installation is smooth and successful. You are one of the four key players involved in ensuring successful implementation of your Segra services.

The other key players are:

- Your Segra Project Coordinator
- The vendors who maintain your telephone system and computer network
- Segra Network Partners

The following steps must be completed before we can enter your order and provide you with a due date:

1. Segra must have complete and accurate information for your order to be entered into our systems.
2. Based on the services ordered, a Segra Engineer may call you (and, if applicable your phone/ data equipment vendor) to collect the technical specifications and physical site requirements to support the services ordered. Please be ready to provide the information to the Segra Engineer and ensure it is complete and accurate.

* Delays in obtaining complete and accurate information may delay the delivery of your service.

Once we have received your information, your Project Coordinator will work with you throughout the service delivery process. Following these steps your P.C. will:

1. Contact you to discuss a Target Due Date for the activation of your service.
2. Provide you with a Firm Order Commitment (FOC).
3. Contact you to finalize the date your services will be installed.
4. Before your scheduled installation date, you will be contacted to ensure you are prepared for the delivery of your service.
5. The following items must be available prior to your service delivery date:
    a. Please make sure your installation site has adequate space and power.
    b. Provide building access to your premises for Segra or our network partner to install your services.
    c. A cable run may be required from the Segra router (if applicable) to your network hub. If so, please ensure that this is provided and that your computers are networked.
    d. Please ensure you or your vendors are available on your service delivery date to perform testing with Segra.

Delays in the items above may result in additional charges and could delay your service delivery date. Your Project Coordinator will interact with all key players to make your service delivery date a success.

THANK YOU FOR CHOOSING SEGRA!

Implementation Specifics

Once an Agreement is in place, an external kickoff call will be completed by the account team, customer and project team to discuss services purchased. The agenda will include face-to-face introductions to key contacts of the Project Management team and a review of the below project outline that spells out the process from contract execution to post-cut follow ups.

1. Data Gathering Stage

a. Pull Customer Service Record
    i. Acquire Customer Service Record from current LEC, compile number inventory and identify respective location BTN, 1FB Copper Lines, Toll-Free Routing/Ring-To, etc.
b. Vendor Contact Info and Introductions
    i. Gather voice and data vendor contact info / POC for each customer premise
    ii. Voice Configuration – PRI Protocol / DNIS digits / Channel Type / Digits Out=Pulsed / Caller ID and CNAM Control
    iii. Data Configuration – MPLS WAN and LAN topology and addressing / Firewall Configuration and policies/DHCP requirements / LAN Servers requiring Public IP Addressing / DNS / etc.
c. WAN mapping and design – meeting or conference call with Segra Engineer(s) to review Segra Network Design and establish Network Drawing for Implementation
d. Billing/Account Set-Up – Account Executive and Customer review Group Billing Form, Customer Proprietary Network Information Authorized Contact(s) Form, Billing Address and Contact, etc.

2. Submit Service Order Change

a. Credit Approval – Submitted and Approved by Segra Accounting Chair, Luci Mackie
b. Group Billing / Account Detail – per customer specifics and paperwork, list sub-account titles and address(s)
c. Customer Premise Site Survey – Segra Engineer or Local Market Install Technician to visit each site to confirm rackspace/backboard availability, document DEMARC extensions needed for service, confirm A/C power availability
d. Initiate Service Orders – Account Executive and Sales Engineer to submit voice and data orders to Segra Order Entry team, key SO#s within Work Flow System
e. Project Assignment and Contact

3. Status Updates & Milestones - What to Expect

a. Bi-weekly status calls with Project Coordinator – Beginning 15 Days after submittal of final Service Orders (estimated 30 business days after contract award)
b. Customer Project Package – working document with a compiled list of Service Orders, Dependencies, FOC, Contacts, Scope of Work and Milestone Dates
c. Milestones – Reviewed via status calls / conference bridge including Firm Order Confirmation (FOC) and updates on circuit construction, DOT and City/County Permits (relevant to fiber or ethernet circuits), Copper 1FB FOC, Port Order FOC (from current LEC)

Implementation Specifics

4. Pre-Conversion Stage

a. Circuit Delivery by Segra or LEC (fiber and copper circuits) – day of week and window of time provided by Segra, requiring only access to customer DEMARC
b. Test and Turn-Up of Circuit – Segra or LEC confirms delivery of circuit/transport, tests circuit for MINIMUM of 48-72 hours to prove reliability, transport speed, build into MPLS core routing
c. Pre-Install of Segra Equipment – Scheduled per customer availability, local Segra to each market/SCLS location to pre-install Segra voice CPE, MPLS router, locate new 1FB copper lines. This stage is NON-service affecting.

5. Conversion

a. Local Segra tech(s) assigned to each location with assignment from applicable customer contact and/or Voice/Data Vendors
b. Phased Cut Approach versus Single Cut Approach

* Segra Project Management team and Customer / Customer Vendors will discuss and agree upon best practice for implementation of Voice / Data transitions and scheduling (i.e. cut MPLS network all sites one day, followed by voice cut the next day OR phased site-by-site implementation)

**Estimated installation window is 90-120 calendar days from receipt of contract\award, can be adjusted/expedited per customer request

6. Post-Conversion Stage

a. Account Executive to schedule meeting with customer primary contact and customer primary billing contact to review first Segra invoice cycle, confirm accuracy and invoice delivery method is satisfactory (i.e. PO Box, Via Email - PDF)
b. Account Executive to provide customer with hard copy of Segra escalation list for following departments: Customer Care and Order Entry, Billing Operations, Network Operations Center)

STRATEGIC ACCOUNT TEAM MEMBERS

Gregory Florence	GOVERNMENT ACCOUNT EXECUTIVE II	(304) 414-0411 Greg.Florence@segra.com
David Jones	SR. SALES ENGINEER - GOVERNMENT	(724) 216-9003 David.Jones@segra.com
Michael Brisson	STRATEGIC ACCOUNT SPECIALIST	(757) 274-2904 Michael.Brisson@segra.com
Gary Crocco	DIRECTOR - GOVERNMENT SALES	(804) 874-4105 Gary.Crocco@segra.com
Daniel Eskew	VP - ENTERPRISE SALES	(803) 726-0018 Daniel.Eskew@segra.com

SEGRA℠

SEGRA.COM | 833.GO.SEGRA