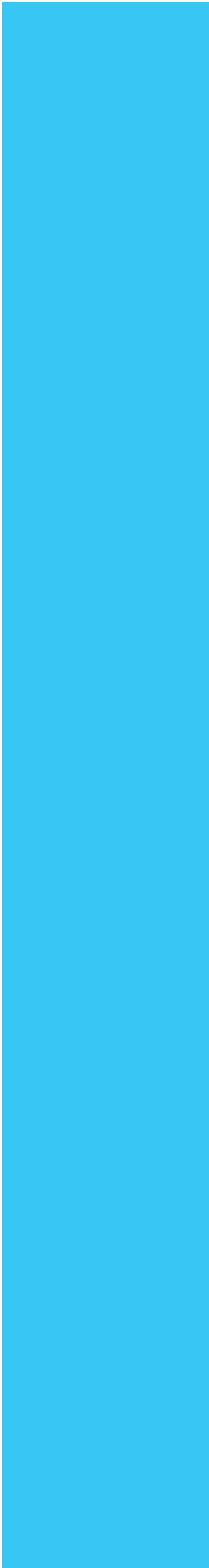# Lumen as a Custom Network Integrator

LUMEN®
TECHNOLOGIES

Lumen is keenly aware of the challenges the U.S. Government faces as it develops a modern communications architecture that will transmit data robustly and reliably across various locations, environments, and conflict conditions. As a Tier 1 carrier, Lumen integrates diverse assets into a single compliant, reliable, and scalable network. Lumen's infrastructure includes assets from Qwest, US West, Embarq, CenturyLink, Global Crossing, Time Warner, and Level 3. We leverage our years of experience, methods, procedures, and tools integrating our corporate backbone to provide a low risk, agile, scalable solution to best meet U.S. Government mission needs today and into the future.

Corporately, Lumen uses its extensive networking lab in Littleton, CO to test all hardware and software before it is installed into our worldwide core network infrastructure. We test vendor interoperability, standards, scalability, reliability, etc. and use this same approach to develop custom networking solutions for our U.S. Government customers.

LUMEN®
TECHNOLOGIES

Use case: CSfC Trusted Integrator

Lumen Technologies Government Solutions, Inc. was recently named a Commercial Solutions for Classified (CSfC) Trusted Integrator by the NSA. Lumen® has a long history of designing and deploying secure communication systems for the government. Joining the CSfC Program was a natural fit for our team. Not only can we design, deploy, and operate classified global networks but we also have experience in building accredited and scalable cyber systems for our mission customers. Our team fuses the knowledge and experience of operating a global internet service provider with system integration best practices. Our approach to the deployment of CSfC is to do so right in the same network that we provide today. The Lumen solution can bring enterprise and mission access, accredited solutions, and be your trusted partner. Come see how Lumen Technologies Government Solutions can partner with your organization, deploy next-generation encryption technologies, and enable your network to do great things.

Use case: Large Research Network

We transitioned services from a virtual WAN built on a commercial communications network to our backbone network. We provided digital data transfer services between defined Service Delivery Points (SDP) with an advanced technology, high-speed, high availability network service. We implemented secure gateways to existing federal and civilian networks to connect defense scientists and engineers at various research entities, laboratories, and test facilities across the U.S. We provided increased bandwidth to provide high-availability, high-performance connectivity at new sites and inserted new technology across the new network service to support the customer mission. The network supported almost 200 sites, and included a mix of Ethernet, IP, and Optical Wavelength Service (OWS) at speeds from 50 Mbps to 40 Gbps with a Virtual Private Network Service (VPNS) with IPv6 for monitoring while continuing to support IPv4. Our engineers designed software-defined networking (SDN) and network functions virtualization (NFV) with a deterministic routing (data path symmetry) that is agnostic of the

LUMEN®
TECHNOLOGIES

hardware vendor. Control protocols, such as Bi-directional Forwarding Detection (BFD), use the same data pipe for transmission. Additionally, our engineers designed and deployed network management controls that use the IPv6 protocol in a dual stack architecture — IPv4 / IPv6 multicast.

Use case: Large Federal Government Private Network

We managed and operated a large scale classified 100G mission-critical network and met or exceeded the uptime service-level agreements (SLA's) over the contract term. We built and managed multiple Internet Access Points (IAP) globally that aggregate large amounts of network traffic for the customer globally. We implemented "assured delivery" on the network allowing the customer to prioritize certain traffic during critical events. We deliver a full suite of security services as an integrated managed service. Services included:

- A custom, automated global firewall service which dynamically updates firewall rules every 10 seconds worldwide in response to rapidly changing threat indicators.
- Dynamic active threat blocking capabilities that remove known bad traffic to include Geo-Based IP, Anonymous, and Scan.
- Generation and delivery of flow data on all traffic, and reporting on all blocked traffic for situational awareness.
- Integrated Distributed Denial of Service (DDOS) detection with automated-mitigations within the customer IAPs.
- Support for the network and security services via a 24/7/365 global NOC/SOC.