Building a Secure Federal Network

The need for federal government agencies to adopt the most up to date information security measures is critical to mission success. Adversaries seek any opportunity to exploit cybersecurity gaps across all aspects of an agency's network. That is why the government has established stringent certification requirements – including Trade Agreements Act (TAA) compliance – for products that are deployed into a federal network.

In order for agencies to ensure they comply with these requirements; they need to work with industry partners who can help build and maintain a secure network that protects the often sensitive or classified information traversing the network. Agencies must consider the following when building a secure network:

- Wired and wireless infrastructure
- Secure network access
- Network management

CommScope provides an end-to-end secure network solution that is TAA compliant and can address each area of consideration.

COMPONENTS OF A COMMSCOPE-DELIVERED SECURE NETWORK:

Wired & Wireless Infrastructure	Secure Network Access	Network Management
• Wiring for the network, fiber, copper, switch port security and locking, cable attachment security, color coding – new powered fiber cable • FIPS certified switches to interconnect all devices and buildings across a campus • IPS certified access points used to obtain access to the network	• On-boarding devices for both employee secure access and guest access • Ability to on-board devices of various operating systems and network abilities	• Centralized management for wired and wireless environments • Ability to monitor and provide visibility into the status of the physical layer
CommScope solutions: • SYSTIMAX® powered fiber • RUCKUS® ICX® switches • RUCKUS access points	**CommScope solution:** • Cloudpath®	**CommScope solutions:** • SmartZone network controllers • imVision automated infrastructure management

COMMSCOPE®
RUCKUS®

CommScope offers ongoing management services which optimizes both wired and wireless networks. Our long-term approach to system management takes the responsibility off of your agency and allows us to keep your networks secure and running efficiently. This includes:

- **Unified policy:** One access policy for granular control and access rights along with consistent on-boarding and guest management utilizing Cloudpath.
- **Unified management:** Single pane of glass with either SmartZone-based on-premises management or unified RUCKUS Cloud management.
- **Optimized access:** Purpose-built affordable multi-gigabit solutions optimized for 802.11ac wave 2.
- **Reporting and analytics:** Long-term reporting across wired and wireless networks with SmartCell Insight (SCI), providing performance history of how the network is being used as well as insights into the overall user experience.

Certification requirements for secure network

- FIPS 140-2 – Federal Information Processing Standard (140-2)
- Common Criteria
- USGv6 – United States Government initiatives in IPv6 adoption
- DoDIN APL – Department of Defense Information Network Approved Products List
- CSfC – Commercial Solutions for Classified

Additionally, CommScope works with you to install your network to help keep your agency's information protected. We offer:

- **High Reliability:** RUCKUS APs uniquely deliver reliable service in the most challenging environments, including those characterized by high loss or high interference.
- **Stable mobile client connectivity:** High-gain, directed signals and adaptive beam-steering avoids interference and steers transmissions over the best performing path.
- **Application support:** Automatic interference mitigation ensures glitch-free streaming of IP video and voice for applications such as information displays.
- **Government security compliance:** All of our services are compliant with DoDIN APL, FIPS 140-2, USGv6, and Common Criteria standards.
- **Elegant, simplified BYOD and guest networking:** Separate WLANs provide secure staff and guest access with associated devices and role enforcement.
- **No new cabling:** Highly adaptive and reliable smart Wi-Fi meshing eliminates the need to cable every access point and provides self-healing capabilities.
- **Flexible deployment options:** Deploy access points with or without a local controller and receive full geo-separated clusters for redundancy.
- **Easy to configure and deploy:** Graphical user interface with easy to understand point and click commands.

Now meets next

At CommScope Federal, we push the boundaries of communications technology to create the world's most advanced networks. Across the globe, our partners and their solutions are redefining connectivity, solving today's challenges and driving the innovation that will meet the needs of what's next.

commscope.com/federal

Visit our website or contact federalsales@commscope.com for more information.

CO-115175-EN (11/20)