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.

To ensure they comply with these requirements, agencies 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. They need the ability to support a zero trust approach that explicitly verifies trust before allowing access. Agencies should consider the following when building a secure network:

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

COMPONENTS OF A COMMSCOPE RUCKUS—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 • RUCKUS Analytics™ for AI/ML-powered automatic classification of service incidents*
CommScope RUCKUS solutions: • SYSTIMAX® powered fiber • RUCKUS® ICX® switches • RUCKUS access points (APs)	**CommScope RUCKUS solution:** • Cloudpath® Enrollment System	**CommScope RUCKUS solutions:** • SmartZone network controllers • imVision® automated infrastructure management

* Consult your account team.

RUCKUS® COMMSCOPE

CommScope RUCKUS offers ongoing management services That optimize 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 Enrollment System.
- **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 and 802.11ax (Wi-Fi 6).
- **Reporting and analytics:** RUCKUS Analytics for incident analytics and network health monitoring, and more, as well as 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

- 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
- TAA—Trade Agreements Act

In addition to our hardware, CommScope RUCKUS can provide support to ensure your network is installed and secure to keep your agency and our country'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 signal antenna technology and beam-steering (RUCKUS BeamFlex+) technology steers signals to high-quality paths for greater speed, fewer errors, rapid bandwidth, and optimized user connectivity.
- **More efficient cable performance:** In most cases, CommScope AP coverage performance requires fewer APs and less network cabling. RUCKUS SmartMesh technology allows for automatic AP-to-AP connectivity in locations with distance limitations, or where cabling is difficult to provide.
- **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.

CommScope RUCKUS provides an end-to-end secure network solution that is compliant with the latest certification requirements and can address your needs.

ruckusnetworks.com/federal

Visit our dedicated website or contact us and a local RUCKUS sales representative will get in touch with you.

CO-115175.1-EN (03/23)