

Commercial Solutions for Classified

from Telos Corporation

Telos is your partner for CSfC solutions that reduce costs and enhance efficiency and productivity in secure/classified environments.

- Eliminate the need for expensive Protected Distribution Systems, COMSEC CCI equipment, network monitoring and COMSEC CCI logistics
- Integrate multiple security domains in a single network
- Give senior military and civilian leaders access to classified information over commercial networks
- Enable senior leaders to use classified networks wherever they are for day-to-day operations instead of relying on the increasingly vulnerable NIPRNet
- Allow users mobile access to classified networks from any location

Greater threats mean greater need for network security.

Government agencies are experiencing tremendous pressure from their end users to support commercial, consumer-grade mobile devices. Over the past decade, military, intelligence community and civilian agencies have been transitioning to network-centric applications to support their operations.

The most important of these applications reside on tactically secret networks, such as the U.S. Department of Defense SIPRNET. As a result, classified networks have experienced a dramatic increase in importance and usage. Further, the non-classified NIPRNet has shown vulnerabilities, putting a focus not only on strengthening our cyber security posture, but also a move toward more use of the SIPRNet versus relying on the NIPRNet.

Older, wired SIPRNet infrastructure is being evaluated for replacement and upgrade, and the latest classified communications technologies and architectures are being pursued for this replacement rather than relying on the very expensive and logistically intensive Protected Distribution Systems (PDS) and Communications Security (COMSEC) Controlled Cryptographic Items (CCI).



CSfC: Opening new channels for secure communication.

NSA has developed a program called Commercial Solutions for Classified (CSfC) and has 1) established architecture guidelines for point-to-point VPN, campus WLAN, and mobile access, 2) established policy and processes for the approval of commercial products to be used in these architectures, and 3) established policy and processes for approval of companies to develop, implement, and support CSfC architectures as NSA Trusted Integrators.

CSfC architectures, when implemented properly and approved by NSA, provide the ability to transmit secret and top secret information over commercial networks. As of November 2015, there are 94 approved products in 19 categories and there are 24 Trusted Integrators.

Telos: CSfC architectures for secure mobility.

Telos Corporation can provide a full line of professional services capabilities to design, develop, and implement CSfC architectures, coordinate efforts between the end user and NSA representatives, and provide necessary documentation to complete the CSfC package.

Telos is a NETCENTS Network Operations (NetOps) contract holder with 20 years' experience delivering wireless and mobile solutions. The CSfC services are available under this contract for Air Force and any other DoD customer.

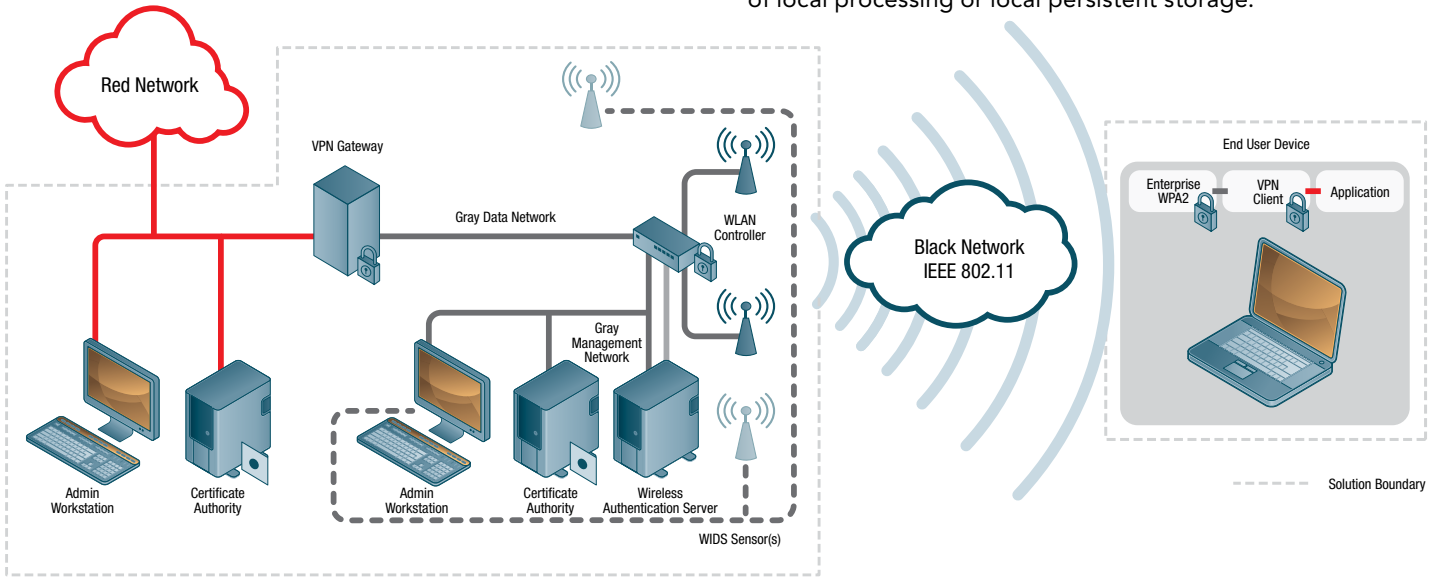
Components of the CSfC Architecture

Red Network - A Red network contains unencrypted classified data and is logically located behind an Inner VPN Gateway. The networks connected to end user devices through the campus WLAN solution are Red networks.

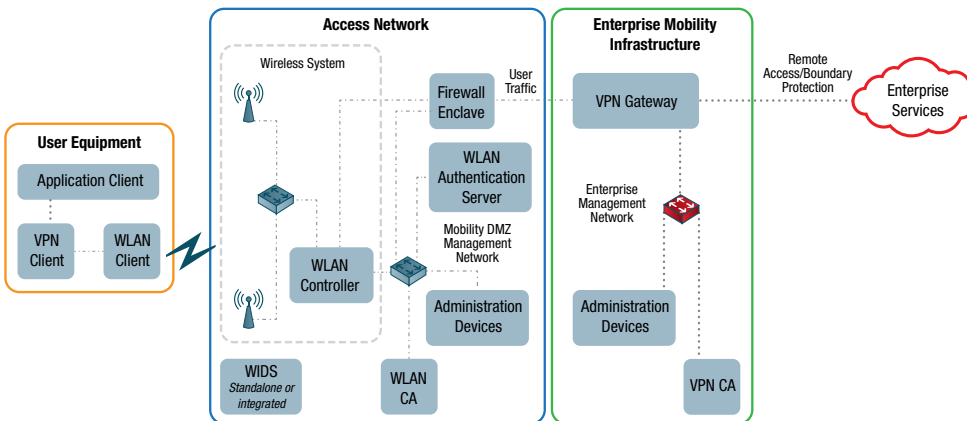
Gray Network - A Gray network contains classified data that has been encrypted once. The network between an inner VPN gateway and the wireless system is a Gray network.

Black Network - A Black network contains classified data that has been encrypted twice. The wireless network between the end user device and the wireless system in which data is protected with two layers of encryption is a Black network.

End User Device - The end user device is a commercial tablet, laptop computer, or similar computing device that supports Wi-Fi connectivity options. It may run applications that make use of local processing or local persistent storage.



Campus WLAN Architecture



Outer Tunnel Layer 2 Secure Wi-Fi

- Mobility Controllers terminate "outer" tunnel (WPA2 Enterprise) Access Points
- RSA or EC Computer Certificates with Layer 2 supplicant (EAP-TLS)

Inner Tunnel Layer 3 IPsec VPN

- Other vendor VPN client & gateway supporting Suite-B algorithms

Dual Tunnel Client to Core AES Crypto

Please contact us to get started streamlining your secure and classified environments with CSfC solutions from Telos. We look forward to working with you.



info@telos.com | 800.70.TELOS (800.708.3567)
 www.telos.com | twitter.com/telosnews
 facebook.com/teloscorporation
 linkedin.com/company/telos-corporation