Red River

Red River: A Trusted Integrator For Commercial Solutions for Classified (CSfC):

WHAT IS COMMERCIAL SOLUTIONS FOR CLASSIFIED (CSfC)?

CSfC is the NSA's commercial strategy for leveraging industry innovation to deliver Information Assurance (IA) solutions efficiently and securely. The program is founded on the principle that when properly configured, layered solutions can provide adequate protection of classified data in a variety of different applications.

The CSfC Program harnesses the power of commercial industry, providing a secure alternative for government-off-the-shelf IA solutions. It has transformed the delivery of IA solutions to combatant commands, military service, and agencies by enabling NSS customers to securely communicate using an increasingly diverse set of commercial products. Customers can efficiently meet their needs for protecting classified information due to NSA investment in the research and application of commercial technologies. Benefits include:

- **END-TO-END SOLUTIONS** – Provides NSA designed and approved solutions, leveraging a cadre of vetted, trusted system integrators

- **FLEXIBILITY AND TRANSPARENCY** – Leverages NIAP-validated components, satisfying US and collaborative protection profile requirements, validated against internal common criteria

- **COST EFFECTIVENESS AND EFFICIENCY** – Allows clients to keep pace with technological progress and employs the latest capabilities in their systems and networks, while reducing the time it takes to build, evaluate and deploy IA solutions by utilizing mature technologies already available to the commercial sector. Potential cost savings may be realized through marketplace competition and rapidly deployable, scalable commercial products

- **STANDARDS BASED** – Solutions leverage open, non-proprietary interoperability and security standards

- **MONITORING AND RESPONSE** – Provides situational awareness about components use and location, as well as documented incident handling procedures

- **TECHNICAL EXPERTISE** – Driven by NSA's world-class team of system engineers, threat analysts, and cyber experts

Commercial Solutions for Classified (CSfC) is NSA's commercial Cybersecurity strategy that leverages industry innovation to deliver solutions with efficiency and security. The program is founded on the principle that properly configured and layered solutions can provide adequate protection of classified data in a variety of different applications. NSA/CSS policy **mandates** CSfC as the first option to be considered to satisfy a CS requirement.

CSFC CAPABILITIES PACKAGES

MULTI-SITE CONNECTIVITY (MSC CP)

The MSC Solution uses two nested, independent encryption tunnels to protect the confidentiality and integrity of data as it transits the untrusted network. The two encryption tunnels protecting a data flow can use either Internet Protocol Security (IPsec) generated by a Virtual Private Network (VPN) Gateway or Media Access Control Security (MACsec) generated by a MACsec Device. VPN Gateways and MACsec Devices are implemented as part of the network infrastructure.
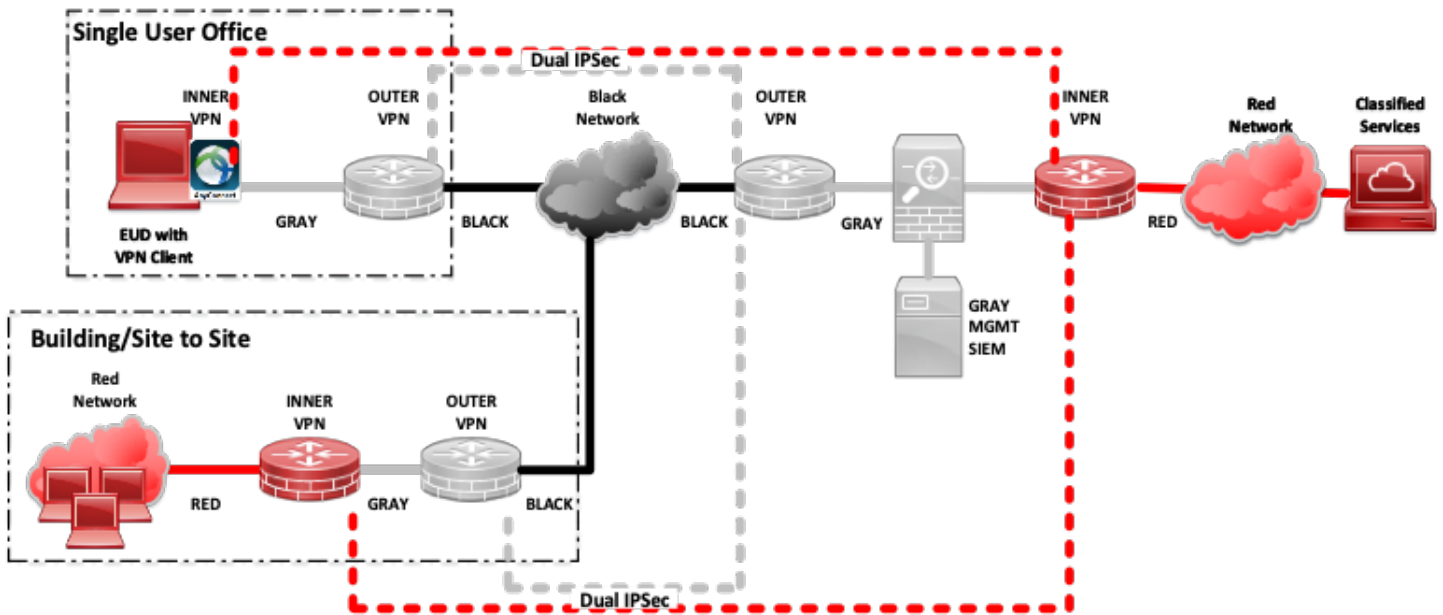
MOBILE ACCESS CAPABILITY PACKAGE (MA CP)

The MA CP describes a general mobile access solution that protects classified information as it travels across either an untrusted network or a network consisting of multiple classification levels. This includes protecting classified data transiting wired networks, domestic cellular networks, and trusted wireless networks to include government private cellular networks and government private Wi-Fi networks. This solution supports connecting end user devices (EUDs) to a classified network via two layers of encryption terminated on the EUD, if the EUD and the network operate at the same security level. The MA solution uses two nested, independent tunnels to protect the confidentiality and integrity of data (including voice and video) as it transits the untrusted network. The MA solution utilizes IPsec as the outer tunnel and, depending on the solution design, IPsec or Transport Layer Security (TLS) as the inner layer of protection.

TECHNOLOGY DECISIONS AREN'T BLACK AND WHITE. THINK RED.
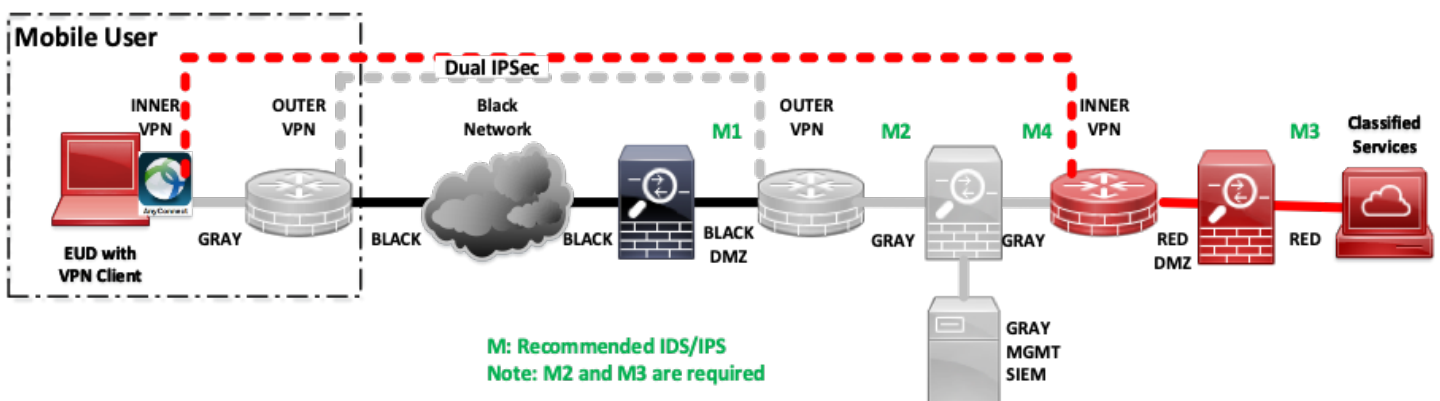
WIRELESS LAN (WLAN CP)

The WLAN CP enables the client to meet the demand for commercial End User Devices (EUDs) -- such as tablets, smartphones, and laptop computers -- to access secure enterprise services over a campus wireless network. The Campus WLAN CP enables the client to implement layered encryption between a secure network and an EUD. The WLAN CP provides a reference architecture and corresponding configuration information leveraging the list of COTS products from the CSfC Components List. Approved COTS devices will be used for the client's Campus A wireless local area network (WLAN) solution which, when properly configured, will achieve a level of assurance sufficient for protecting classified data while in transit. CNSA algorithms use layers of COTS products to protect classified data.
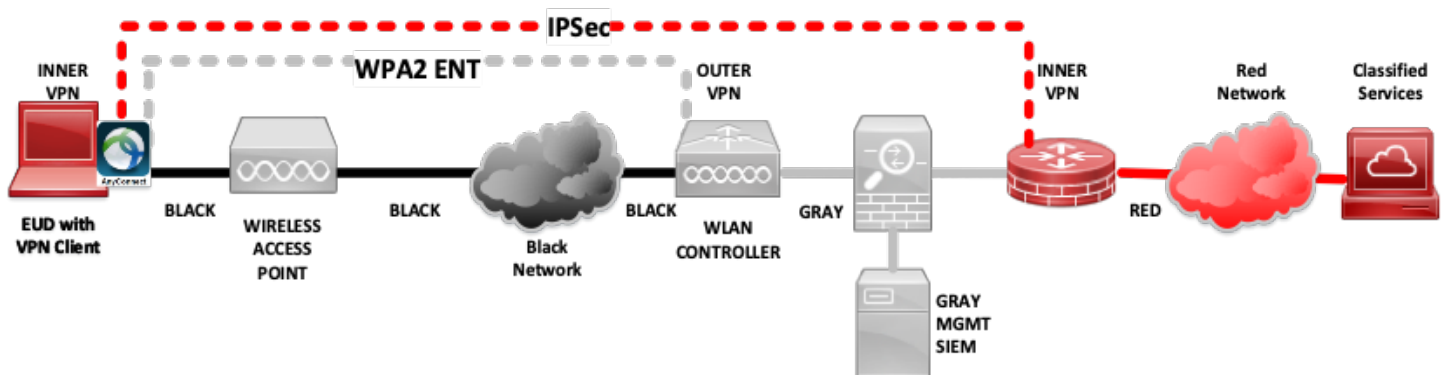
DATA AT REST (DAR CP)

The DAR CP enables customers to implement two independent layers of encryption for providing protection for stored information using NSA approved cryptography while the End User Device (EUD) is powered off or in an unauthenticated state (defined as prior to a user presenting credentials and being validated by both layers of the DAR solution). Specific data to be protected must be determined by the data owner.

CONTACTS

Matt Conklin	Jamie D'Alessandro	Keith Stacy
Director, DoD Sales	Director, DoD	Customer Solutions Architect
843-817-0497	703.585.4415	813.573.1268
matt.conklin@redriver.com	**jamie.dalessandro@redriver.com**	**keith.stacy@redriver.com**

Red River