Commercial Solutions for Classified (CSfC) Networks

Allowing Command & Control from Anywhere

January 2022

Prepared By:

Open SAN Consulting, LLC
(OSC Edge)
1954 Airport Road, Suite 144
Atlanta, GA 30341

The work environment paradigm for the Department of Defense (DOD) and other federal agencies has shifted dramatically as COVID-19, the "Great Resignation," and other factors have increasingly required workers to stay away from offices and work remotely, where access to enclaves of sensitive or classified data and systems presents challenges. OSC enables remote work from home/anywhere solutions by leveraging Commercial Solutions for Classified (CSfC), where we incorporate modern and commercial hardware and software technologies that provide secure access to multiple enclaves from a single end-user device.

Overview

The ability to share sensitive information, while providing direction to the workforce, is critical for any entity. For DOD and civilian agencies, the exchange of protected or classified information underpins the primary activities and missions of their workforce. However, the need to perform work on these networks, in the age of working remotely, has proven problematic for a functioning organization, as well as recruitment and retention of qualified personnel. The ongoing pandemic ushered in the necessity of working remotely, while the "Great Resignation" and other changes in the demands of the workforce have caused the ability to work remotely to be viewed as an essential employment incentive, on par with other traditional employee benefits such as health insurance[1].

Since the start of the COVID pandemic, US military and civilian leadership has found itself looking for solutions to maintain a centralized command and control that enables the speedy dissemination of information, promotes collaborative educated decision making, and the promulgation of orders and activities in the era of a remote and fluid workforce. Leaders have also found themselves losing employees to competition that allows remote or hybrid work, resulting in negative effects to continuity of operations, mission knowledge, and even technical advantage. Many personnel losses in the US Public Sector (USPS) have been to private commercial entities that have adopted and adapted to a remote workforce.

Even for those employed in the USPS who have been able to work from home, friction and loss of efficiencies due to the uniqueness of the often classified or proprietary nature of the information delivered or shared has persisted. Solutions to enable a fluid and remote workforce are critical as a growing deficiency is felt across leadership, due to a lack of continuity. In addition, the loss of experienced personnel who maintained a great deal of mission memory and knowledge, but are no longer available to impart that knowledge onto less experienced colleagues, is having a significant impact.

CSfC as a DOD Solution for Remote Work on Classified Networks

The US military's network for command and control is the Secure Internet Protocol Router SIPRNetwork (SIPRNet). The OSC CSfC solution has extended that command and control

[1] Remote work continues to shift the work environment paradigm for all organizations, commercial as well as government. Like commercial entities, DOD and Federal agencies that are unable to adapt will likely lose valuable employees and, potentially, their advantage in recruiting talented human capital over the commercial sectors that readily offer this. *Harvard Business Review* cites that nearly 80% of U.S. employees want to work from home at least one day each week, with the average remote work hybrid model desired to include 2.5 days a week (among workers aged 20-65 who earn more than $10k per year). The demand for a hybrid work model as the workplace norm and as a means to ensure work continuity during the pandemic is also evidenced by a June 2021 Survey of Working Arrangements and Attitudes survey that found "56% of employees are more likely to consider a new job with a hybrid working arrangement and that many employees prefer working from home at least part of the week, and they are willing to act on those preferences.

capability to anywhere in the world versus secure workrooms in secure buildings on secure bases, forts, and camps. Having the same workplace functionality, regardless of location, strengthens command and control.

OSC's CSfC networks solution, which is currently already available in certain DOD environments, provides the DOD with capabilities to meet the changing working environment that has affected the post-pandemic workplace in a secure manner. Our solution leverages modern and Commercial Off-the-Shelf (COTS) hardware and software technologies to deliver secure environments that provide timely and relevant cyber-secure communications for rapidly evolving requirements.

Our CSfC solution allows commercial products to be used in layered encrypted solutions to protect classified National Security Systems (NSS) data and provide secure communication solutions that can be fielded in months. Implementing Capability Packages that incorporate encrypted hardware and software solutions, along with ***Red / Gray / Black*** networks, enables secure access to information, data, systems, and applications <u>from virtually anywhere.</u>

While some employees can answer emails on their phones, there is often a misperception that work is being done and one is as productive as being in an office. Although communications have been enhanced by smartphones, work on a desktop or laptop is typically more productive and allows for more complete functionality. Our CSfC solutions work on approved desktops, laptops, and other mobile devices. OSC's currently deployed CSfC solution enables a true desktop or laptop experience for the warfighter, providing complete workplace functionality anywhere, up to a Secret level, without the risk and vulnerabilities of working and storing classified information on other types of devices in non-secure environments.

More importantly, this CSfC solution can be engineered and implemented quickly and effectively despite the common belief that such solutions take too long to bring to market. With the onset of the pandemic, OSC was able to design and implement our solution for remote work on classified networks in just three months. During this time, OSC met with the customer, defined requirements, prototyped the solution, planned for the implementation, initiated equipment acquisition, initiated NSA accreditation, fielded the production solution, and finalized NSA accreditation and an Authority to Operate (ATO). OSC's CSfC subject matter experts can develop the requirements for any customer and field a tailored solution in the same amount of time it would take to develop a continuity of operations plan. With the OSC CSfC solution, the continuity of operations is built into the CSfC solution, providing a capability that can scale to any size envisioned by the customer and engineered into their unique solution.

Modernization and standardization are part of the process. Utilizing current laptops, desktops, and certain infrastructure is not usually possible, in most cases. An investment in a CSfC solution will mean an investment in IT infrastructure. The equipment used in the solution must be on the approved National Information Assurance Partnership (NIAP) List and suitable for CSfC Solutions and must be configured in such a way that is passes stringent security requirements set forth by the NSA. While there is an initial investment, it does allow for savings in other areas that could allow for a lowered Total Cost of Ownership -- brick and mortar facilities would not need structured cabling, secure areas can be added ad hoc and set up on-the-fly with strategically placed wireless access points enabling open format workspaces, and access to different enclaves can be provided though a single encrypted connection instead of through separate infrastructures. In addition, an uptick in employee satisfaction and efficiencies may be realized through a more modern working environment that disrupts the commuting costs associated with employees being tied to physical locations.

CSfC Systems Integration

Engineering, implementing, and maintaining the CSfC solution requires a range of subject matter experts to ensure the proper integration of the solution within an existing enterprise network, the delivery of the solution, and the operations and maintenance of the solution once integrated. OSC's CSfC solution architects have the proven experience to create a compliant system that provide the capabilities and scalability required. Our NSA accreditation specialists are knowledgeable of the intricate needs of securing these solutions and shepherding the process through the AO and NSA accreditations. Our knowledge of the accreditation paperwork, deviation packages, and security plans will speed the deployment of any solution and ensure a solution is quickly brought to a Fully Mission Capable (FMC) status. OSC has an in-house team of Network and Systems Engineers and Administrators, VoIP Engineers, VTC Technicians, Cabling Specialists, Service Desk Specialists, and Back Office Support that specializes in CSfC implementations and operations and maintenance.

Our CSfC solutions can span a single network/enclave or several of them at the same time. The infrastructure is similar for both solutions, the main difference being that a Cross Domain Solution Element (CDSE) is incorporated into those that include multiple networks and/or enclaves. If the specific CSfC solution is not spanning different networks or enclaves, i.e., NIPRNet and SIPRNet, the CDSE is not required. This can significantly reduce the amount of time required to implement the solution. However, if a Cross Domain Solution is needed, the OSC CSfC solution can provide the COTS system with ***Access and Transfer*** solutions recognized by the NSA's National Cross Domain Strategy Management Office (NCDSMO).

Our CSfC logistics team is continuously vetting hardware and software products found on the NIAP approved equipment list. We maintain relationship with these vendors so that there is OEM reach back for troubleshooting and enhancements. This team has established relationships that guarantee ready access to these vendors and their products for Zero, Thin and Fat Clients, Network Infrastructure, and Mobile and End-User Devices.

Our relationships extend also to needed software vendors and their products. We maintain a regular cadence of communications with software companies that provide high-state encryption, system monitoring, system governance, and Security Information and Event Management (SIEM) tools. The regular communications keep us abreast of technological improvements and innovations that we in turn standardize and incorporate into our solution.

CSfC Capabilities Packages

There are several capabilities packages that the National Security Agency (NSA) Central Security Service (CSS) has published for use in the CSfC solution. These packages include the following:

- ***Campus WLAN Capability Package***
- ***Mobile Access Capability Package***
- ***Data at Rest Capability Package***
- ***Multi-Site Connectivity Capability Package***

Campus WLAN Capability Package: This CSfC Campus Wireless Local Area Network (WLAN) Capability Package meets the demand for commercial End User Devices (EUD) (i.e., tablets, smartphones, and laptops) to access secure enterprise services over a campus wireless network. Cryptographic algorithms, known as Commercial National Security Algorithms (CNSA), are used to protect classified data using layers of COTS products.

This solution is supported using wireless devices to access sensitive data and enterprise services while minimizing the risk when connecting to existing government enterprise networks. Government-managed, campus-area wireless networks provide controlled connectivity between mobile users and the broader government enterprise. The term *campus* is used in this document to refer to any area that is physically protected to the highest classification level of the enterprise network where multiple enclaves are supported. This physical area includes secure facilities and tactical environments when the physical controls are deemed appropriate by the Authorizing Official (AO).

Mobile Access Capability Package: This CSfC Mobile Access (MA) Capability Package meets the demand for mobile data in transit solutions (including Voice and Video) using approved cryptographic algorithms and National Information Assurance Partnership (NIAP) evaluated components. These algorithms, known as the Commercial National Security Algorithm (CNSA) suite, are used to protect classified data using layers of COTS products.

This MA solution protects classified information as it travels across either an untrusted network or a network consisting of multiple classification levels. The solution supports connecting end-user devices (EUDs) to a classified network via two layers of encryption terminated on the EUD, provided that 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 uses Internet Protocol Security (IPsec) as the Outer Tunnel and depending on the solution design, IPsec, or Transport Layer Security (TLS) as the Inner layer of protection.

Data at Rest Capability Package: This CSfC Data-at-Rest (DAR) Capability Package meets the demand for DAR solutions using the Commercial National Security Algorithm (CNSA) Suite. These algorithms are used to protect up to top secret data using layers of COTS products.

The goal of the DAR solution is to protect classified data when the EUD is powered off or unauthenticated. Unauthenticated is defined as the EUD state prior to a user presenting and having their credentials (i.e., password, tokens, etc.) validated by both layers of the DAR solution. The DAR solution is composed of dual encryption layers, an outer and inner layer. The outer layer is considered the layer that is authenticated to first, while the inner layer is authenticated to second. The data owner determines specific data that must be protected.

Multi-Site Connectivity Capability Package: This CSfC Multi-Site Connectivity (MSC) Capability Package meets the demand for data in transit solutions using approved cryptographic algorithms and National Information Assurance Partnership (NIAP) evaluated components. These algorithms, known as the Commercial National Security Algorithm (CNSA) Suite, are used to protect classified data using layers of COTS products.

This solution supports interconnecting two or more networks operating at the same security level via encryption tunnels, where the security level encompasses the classification level, list of compartments, dissemination controls, and other such controls over information. The solution provides sufficient flexibility to be applicable to many use cases of MSC implementations.

These secure communication solutions have been developed to guard against ***Passive Threats, Active Threats, Insider Threats,*** and ***Supply Chain Threats.*** They can be used separately or together depending on the requirements derived for each customer through customization of the CSfC solution.

CSfC Solution Applications

The CSfC solution can be utilized in both military and commercial environments for a variety of needs and to meet different requirements. Capabilities packages can be utilized individually or as a bundle to meet the unique needs of each customer.

Secure Mobile NIPR/SIPR Network Access: Creates an on-the-move workforce for both command and control within the military as well as information sharing and continuity across sectors and industries. CSfC creates the ability to incorporate a secure office-without-walls workspace environment when used in conjunction with a VDI Solution. This is the perfect solution for new construction, rehab construction, dense workspaces, or ad-hoc workspaces.

Wireless Solution for New Campus/Building Construction: Eliminates or reduces the costs associated with wired infrastructure. The CSfC solution is entirely scalable for new campus additions and/or redesignation of workspaces by just adding new Access Points (APs) and related infrastructure allowing for Secure Zero Trust Architecture while leveraging existing Identity Access Management (IDAM) infrastructure.

Secure Access for Select Individuals: Allowing designated networks for certain individuals from remote locations. Our CSfC solution provides the ability to work with the same capabilities and functionality as one would have at the office, or in garrison for our warfighters, from remote locations (home, secure field conditions, etc.) for select individuals. This solution is perfect for travel, unsecure workspaces, inclement weather and natural disaster response and national emergencies.

Zero or Thin Clients that Have no Resident Data: After shutdown, no data is left on the secure end user device. CSfC enables a secure on-the-move plug and work environment. This solution will be perfect for secure workspaces, non-secure workspaces, workspaces without classified storage, and remote unsecure workspaces.

Active OSC CSfC Solutions

OSC is responsible for two active instances of the CSfC solution. One is supporting an Army customer located in the Contiguous US (CONUS). This instance went from pilot to fielded solution in three months. It currently supports approximately 840 end users, with 83 of them being VIPs. For one of the active instances, the architecture developed and implemented allows easy scalability to 2000 users. Scalability is limited only by the underlying hardware present at the customer's site. However, the solution overall has unlimited scalability with the procurement of additional hardware. Our solution is also capable of certificate auto-enrollment over the wire, removing the need to ship the end user devices back to hub for reimaging every year.

The second instance is supporting a different Army customer located Outside the Contiguous US (OCONUS). This instance includes multi-site capability through site-hopping utilizing geo-location. The solution provides access from anywhere, up to the SIPRNet level, and has the added advantage of the warfighter deploying from CONUS to OCONUS and back again with the same end user device, utilizing the same credentials. The need to relocate CSfC stacks or reimage end user devices is eliminated, and the solution allows for ruggedized mobile devices.

Summary

The OSC CSfC solution will revolutionize the way remote work will be accomplished. Currently the CSfC solution is a Secret and Below Interoperability (SABI) certified solution. However, there is an option for a Top Secret/SCI and Below Interoperability (T-SABI) certification that OSC can assist customers with initiating. The initial pilot for the CSfC was meant to modernize the Army's IT infrastructure during a renovation and originally required a one-wire solution to each building, regardless of the number of networks or enclaves being supported. The customer wanted to access multiple networks from the same device and establish an open area where SIPRNet could be accessed without the need to lock up the machines.

OSC's knowledge and understanding of CSfC solutions has enabled enhancements of our original pilots and implementations to vastly increase capabilities of the original solution intents. For instance, our first pilot was for a single-wire solution, the addition of the wireless end user devices providing SIPRNet access from anywhere, is now being utilized by nearly four times the personnel it was originally intended for. This includes 83 VIPs—General Officers (GOs) and Senior Executive Service (SES) personnel. Our solutions are currently being leveraged to provide increased secure communication capacity at commands in the continental United States, Southwest Asia, Europe (EUCOM) and the Pacific (PACOM).

Our solution provides leaders secure access to the SIPRNet command and control network from anywhere in the world, without storing any information on the end user device or opening the network to hostile action. It provides an on-the-move solution for travelling personnel, personnel needing access to select enclaves and personnel responsible for ensuring the safety and direction of men and women in harm's way. Our solution is scalable, reliable, and secure. It eliminates the need to look for a secure building or room to communicate at the SIPRNet level, as well at the need to wait to provide guidance as a leader. Most importantly, it eliminates the worry and concern about a device with sensitive information being exploited.