Booz | Allen | Hamilton®

TACTICAL COMMERCIAL SOLUTIONS FOR CLASSIFIED (CSfC)

The rapid pace of emerging technologies, coupled with increased cyber threats, led the National Security Agency (NSA) to develop new processes that rapidly deploy cost-effective, flexible solutions with security engineered up front. As an NSA-approved CSfC Trusted Integrator, Booz Allen harnesses current commercial technology, in accordance with NSA-developed security architectures, to design solutions for sensitive missions including tactical use cases. Operators at the tactical edge frequently require secure access to command-and-control (C2) applications and classified information. Booz Allen's tactical CSfC solution utilizes a commercially available ruggedized server system and both commercial/private 5G cellular and tactical radio transport networks for an always-on secure capability to enable decision making at the edge.

The NSA's CSfC program offers multiple technology requirement baseline capability packages (CP) which can be coupled to meet mission needs:

MACP

Mobile Access CP

Describes how to protect classified data in mobile access solutions transiting wired, domestic cellular, and trusted wireless networks, including government private cellular and Wi-Fi networks

CWLAN CP

Campus Wireless LAN CP

Enables customers to meet the demand for commercial end-user devices (e.g., tablets, smartphones, and laptop computers) to access secure enterprise services over a campus wireless network

MSC CP

Multi-Site Connectivity CP

Describes how to protect classified information as it travels across either an untrusted network or a network of a different security level

DAR CP

Data-at-Rest CP

Enables customers to implement two independent layers of encryption to provide protection for stored information using NSA-approved cryptography while the EUD is powered off or in an unauthenticated state

ABOUT BOOZ ALLEN CSfC INTEGRATION SERVICES

Design and Architecture: The mission need is identified through rapid requirements gathering, and a candidate architecture solution with the necessary security functions is then incorporated into the enterprise.

Integration and Deployment: Driven by the final architecture and the procured products, the components are configured and tested to comply with the requirements of the selected CP.

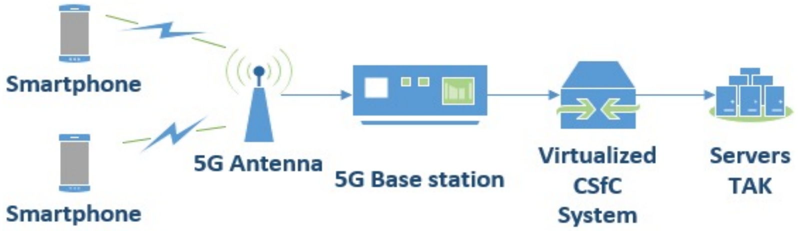
Assessment: Device configurations are validated, and infrastructure components are deployed to ensure CP compliance. In addition, a security test is conducted to determine any residual risk to the enterprise.

CSfC Features and Benefits

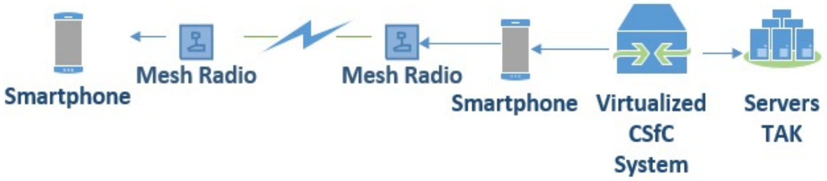
- ✓ **NSA-Approved Secure Solutions:** Leverages NSA-developed framework/approach and pre-vetted system integrators
- ✓ **Operational Flexibility:** National Information Assurance Partnership-validated commercial components and use of commercial "black" transport networks
- ✓ **Standards-Based:** Provides non-proprietary interoperability, while implementing NSA security standards
- ✓ **Cost Efficient:** Potential cost reduction through use of commercially available products
- ✓ **Expedited Speed-to-Solution:** Rapidly deployable, scalable solutions fielded in months vs. years; Lifecycle refresh at commercial speed

APPLICABLE TACTICAL USE CASES

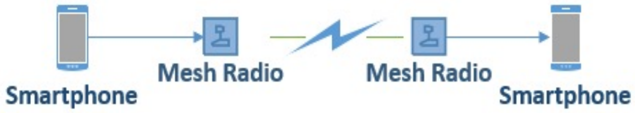
5G transport provides access to C2 applications and the CSfC network: A tactical user will connect a CSfC-approved smartphone through a 4G/5G network to the CSfC system. Once connected, the user will be able to locate other CSfC smartphone users on a Android Team Awareness (ATAK) map screen and send maps, chat messages, and data files.



Tactical mesh radio transport provides access to C2 applications and the CSfC network: The tactical user connects their CSfC smartphone with an Ethernet cable to the CSfC system. Smartphones are then connected to mesh radios to receive ATAK and C2 information through the CSfC system.



Tactical mesh radio transport disconnected from the CSfC network, with localized C2 applications on end user device: Tactical users connect the CSfC smartphone to mesh radio via cable for peer-to-peer connectivity. The radios will provide a backhaul network for ATAK application communication (location data, chat, and local data sharing) localized on each device, with no CSfC system connectivity.



CLIENT SUCCESS STORIES

Defense Information Systems Agency DOD Mobility Portfolio Management Office: CSfC Trusted Integrator for Department of Defense (DOD) enterprise Secret and Top Secret (TS) mobility systems. Developed Android-based enterprise CSfC Mobile Access Capability Package-registered solutions and implemented a Windows 10 data-at-rest solution capable of enterprise services reachback.

Indo-Pacific Command (INDOPACOM): Developed and implemented a tactical CSfC mobility system using virtualized networking functions on a ruggedized server. Integrated District Defend® location-based security using Wi-Fi geofencing techniques.

NAVAIR: Designed and engineered CSfC Campus Wireless Local Area Network (CWLAN) CP-compliant (Secret) electronic kneeboard solution. Successfully integrated hardened Samsung tablets with tactical extensions of CSfC red/gray infrastructure to enable NAVAIR pilot access to electronic data while in flight, reducing the weight associated with paper manuals.

About Booz Allen

Booz Allen is the premier digital integrator for the Department of Defense, blending decades of mission experience with state-of-the-art AI/ML, next-generation data solutions, networking, cyber, and advanced software development to help DOD achieve information dominance. We bring our defense clients the best emerging technology to help them quickly and easily modernize, achieve interoperability, and win.

Contact Information

BOOZ ALLEN TRUSTED INTEGRATOR TEAM
CSfCIntegrator@bah.com

JEFF PREVETT
BD Director, CSfC and Mobility Programs
Prevett_Jeffrey@bah.com

NEAL BURKHART
Senior Lead Engineer
Burkhart_Neal@bah.com

MARK BATTAGLINI
Business Operations Lead
Battaglini_Mark@bah.com

For additional resources, go to BoozAllen.com/Defense