

TACTUS KEEP IN TOUCH.



THE CHALLENGES WITH SMARTPHONE RESTRICTIONS IN CONTROLLED ACCESS AREAS

Federal government and military employees today use government-issued and personal smartphones for primary, work-related communication and point of contact – phone calls, text messages, e-mail, and mobile apps. But, due to security risks, smartphones are not permitted into Controlled Access Area (CAA) or Sensitive Compartmented Information Facility (SCIF), which limits an employee's ability to perform a variety of necessary work functions on cellular devices.

**SMARTPHONE ACCESS
AND FUNCTIONALITY
WITHIN A CAA OR SCIF**

Employees can spend
up to 30% of the workday
outside a CAA or SCIF,
and away from their
workspace to gain access to
their smartphone.



**\$300,000 ANNUAL COST OF A FEDERAL EMPLOYEE
X 30% LOSS IN DAILY PRODUCTIVITY**

\$90,000 ANNUAL COST OF LOST PRODUCTIVITY

Enterprise solutions offer only selective access to a user's smartphone apps and require IT staffing, hardware, software development, patching and upgrades, backup and recovery, and agency program office management. Tactus requires no maintenance, updates, or patches. And unlike current enterprise solutions, Tactus provides 100 percent smartphone access and functionality within a CAA or SCIF, including WhatsApp, Signal, Microsoft Teams and Office 365, incoming and outgoing calls (including emergency calls to Regional Security Office), and text messages.

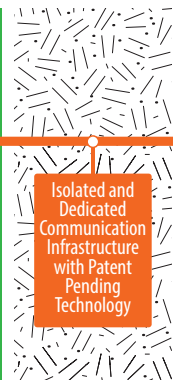
INTRODUCING TACTUS

What if an employee or contractor could access their smartphone inside a CAA or SCIF? Conceras introduces **Tactus 1000**, a two-part device designed to uniquely combine Telecommunications Security Group (TSG) certification and a proprietary, patent pending technology, offering the ability to access a smartphone (iPhone 15 and Samsung DEX enabled phone) on a remote desktop unit within a CAA or SCIF. **Tactus 1000L** will be released in late 2024 which supports legacy iPhones from versions 8 through 14.



iPhone 15, Samsung
with DEX & Other
Android Models

NON-SECURE SPACE



Isolated and
Dedicated
Communication
Infrastructure
with Patent
Pending
Technology

**TACTUS
1000**

SECURE SPACE



Mirrored Phone with
access to ALL functions
on smartphone to
include WhatsApp,
Signal, MS Teams,
incoming & outgoing
calls, & text messaging

Meets all federal TSG
security requirements

KEY FEATURES FOR TACTUS 1000

- + Tactus is an electromechanical solution with no software on desktop unit within the CAA or SCIF; all software functionality resides on the smartphone outside of CAA or SCIF
- + Tactus has an isolated and dedicated communication system, and doesn't operate on government IT infrastructure

ISO 9001: 2015 QUALITY

- + All business processes, procedures, and quality recordkeeping are subject to regular audit by an ISO 9001 registrar

U.S. MANUFACTURING EXCEEDS SECURITY STANDARDS

- + All Tactus components are manufactured in the U.S.
- + The product has Certified Technical Security Safeguard (TSS) test points for agency TSG Committee on National Security Systems (CNSS) approval
- + Tactus has a secured supply chain to meet federal requirements
- + Tactus' manufacturer manages strict change control, field inspection, and test regimes required by TSG-6
- + Design engineering includes electronic, Printed Circuit Board (PCB) design, and mechanical engineering

TACTUS MEETS REGULATORY, SAFETY, ENVIRONMENTAL, AND RELIABILITY TESTING

- + Tactus' manufacturer is International Traffic in Arms Regulations (ITAR) registered
- + Our staff is trained to manage materials and information that are subject to export control (such as for TEMPEST security products)
- + Manufacturing procedures comply with the Defense Priorities and Allocations System (DPAS), used to prioritize defense-related orders in the U.S. supply chain
- + Documented Counterfeit Components Prevention Procedures based upon Aerospace Standard AS5553

CUSTOMER BENEFITS

- + **Tactus 1000** provides 100 percent smartphone access and functionality within a CAA or SCIF. Tactus also provides international call capability Microsoft Teams phone numbers.
- + **Tactus 1000's** desk set touchscreen within the CAA or SCIF mirrors the user's smartphone screen located outside of the CAA or SCIF. Tactus' desk set also acts as a simulated workstation, a functional desktop computer in a cloud environment. A keyboard and mouse can be connected to the desk set device in the CAA or SCIF, if desired.
- + Audio input and outputs are positively disconnected via a switch on the handset or an electrical mechanical circuit, depending on customer requirements. When Tactus is not in use, nefarious actors cannot remotely listen in on sensitive conversations.
- + Tactus requires no licensing fees, maintenance, updates, or patches.

ASK US ABOUT

- + Our pre-terminated fiber for self-installations or cleared technicians for full-service installations.
- + Your needs to have Tactus function with a different smartphone or cellular device.
- + Our secure cable plant infrastructure design and installations for larger projects.



Conceras

11350 Random Hills Road, 8th Floor
Fairfax, VA 22030
www.conceras.com
tactus@conceras.com

CONTACT US:

Tom Woodward

Sales
703.786.8529
thomas.woodward@conceras.com

Joe Cole

Chief Telecom Engineer
571.243.1656
joseph.cole@conceras.com