SECURING MOBILE COMMUNICATIONS FOR COMMS KITS

Attila's GoSilent provides a low cost, high-bandwidth solution to protect data, voice and video communications in comms kits.

> *"The Agency needed the ability to establish military-grade secure communication channels anywhere in the world in just minutes."*

END USER PROFILE

An agency within the Department of Defense requiring on-demand, secure command and control network communications to keep its key leaders connected via voice, video, email and data from anywhere in the world.

CHALLENGE

Communications kits generally consist of a lightweight, compact carbon fiber chassis with a handset for secure voice calls, built-in cellular and WiFi transport options, a USB port for laptop or other device and an integrated power supply with battery backup. Some kits are designed and approved to send sensitive, unclassified information, whereas others may transport classified data or both classified and unclassified data.

There are two primary issues that generally plague communications kits: 1) security breaches and 2) long set-up time. In order to send and receive highly sensitive, classified communications, the Agency was seeking a Commercial Solutions for Classified (CSfC)-certified solution for mobile applications. CSfC is quickly becoming the new government standard replacing antiquated and costly Type 1. Due to the size of the comms kit, it was important that the security solution have a small form factor. Lastly, the nature of the Agency’s work required the ability to communicate in a highly mobile situation. It was essential to have a minimal set-up time and to be able to send and receive communications in real-time.

> *“GoSilent addressed the two primary issues that plague executive communications kits: security breaches and long set-up time.”*

THE ATTILA SOLUTION

GoSilent was determined to be the only truly CSfC-certified security solution that met the Agency’s mobile applications communications needs as well as its additional criteria of compact size, portability and ease of use.

Executive communications kits are capable of transmitting data over IP-based cellular, satellite and wired/wireless transport. Those which are transporting information that is classified (vs. sensitive unclassified) require a Commercial Solutions for Classified solution. CSfC was established by the NSA to enable U.S. government agencies and contractors to leverage emerging technologies and avoid the long development lead times and high maintenance costs associated with many custom solutions. Products that comply with strict cryptography and secure protocol standards may be deemed CSfC certified and therefore cleared to secure classified data. GoSilent meets the NSA Capability Package for mobile access which calls for three firewalls in combination with double encryption. The CSfC designation means that GoSilent has been approved for use in protecting the nation’s most critical information and systems against cyberattacks.

Not surprisingly, executive communications kits are prime targets for cyber attacks. The GoSilent portable VPN/firewall offers robust encryption protection algorithms against cyber threats, including those most frequently targeted at executive communications kits:

- **Remote Access Trojan (RAT)** - Malicious code that gets downloaded invisibly as an attachment or user-requested program. Once the application is installed, the attacker has the ability to control the communications kit.
- **IP Exfiltration** - Unauthorized data transfer conducted through malicious code.
- **Man-in-the-Middle Attack** - Attackers gain access to the network by brute force or packet injection and invisibly intercept and eavesdrop on communications.
- **SCADA Connection Attack** - Bad actors use the communications kit to gain access to an enterprise's SCADA (supervisory control and data acquisition) system.

> *"GoSilent layers on top of the comm kit - regardless of what devices are employed in the kit. No time-consuming or costly reconfiguration is necessary."*

GoSilent layers on top of existing devices in the communications kit, with no time-consuming or costly reconfiguring necessary. GoSilent met the criteria for an out-of-the-box, CSfC-certified solution for mobile communications and also satisfied the demanding characteristics that government-grade security must provide, such as:

- **Virtual Server** – NIAP certification for 2 protection profiles; stateful layer 7 application firewall and VPN Gateway.
- **PC Protection** – Filters all data traffic. Protection from cyber-attacks, identity theft and malware.
- **Commercial National Security Algorithm (CNSA) Suite** – Built in, Top Secret (TS) level cryptography.
- **Captive Portal Isolation** – Isolates end user devices from attempts to intercept and alter the connection between the user and the site they are trying to visit.
- **IP Obfuscation** – Randomizes the IP addresses of all in and outbound data traffic.

ADVANTAGES

- **HIGHLY SECURE** - Top Secret (TS) level CNSA/Suite B encryption for secure data transport.
- **GOVERNMENT-GRADE PROTECTION** - Listed on the US NIAP Product Compliant List and pending certification for 2 Common Criteria Protection Profiles: Stateful Firewall and Gateway VPN (IPSec IKEv1 and IPSec IKEv2), and CSfC-certified for secure mobile communications of classified information.
- **PLUG-AND-PLAY** - Works instantly with any IP-enabled device.
- **PORTABLE** - Small form factor (2.5x2x1 inch, 3oz) fits easily into compact communication kits.
- **FLEXIBILITY** - Layers on top of any existing communications kit. Integrates seamlessly with existing solutions already in use within the kit.
- **DEPLOYMENT** - Fast deployment via cloud. Self-provisioning automatically applies enterprise policies to any device.
- **OBFUSCATION** - IP address randomization for all in-/outbound data.
- **ISOLATED** - Fully isolates user devices from Captive Portal exploits.
- **AFFORDABLE** - Highly cost effective when compared to other solutions or device re-configuration.

> *“The right solution required the ability to deploy instantly to enable secure communications in highly mobile situations.”*

CONCLUSION

Government agency officials working in the field need secure, real-time communications access to their home base staff as well as to DoD colleagues operating in other parts of the world. An executive communications kit outfitted with the CSfC-certified GoSilent product suite creates a secure mobile workspace that is flexible enough to be set-up and taken down instantly. In addition, the Agency can easily scale this cost-effective solution to any number of remote decision makers or deployed teams.

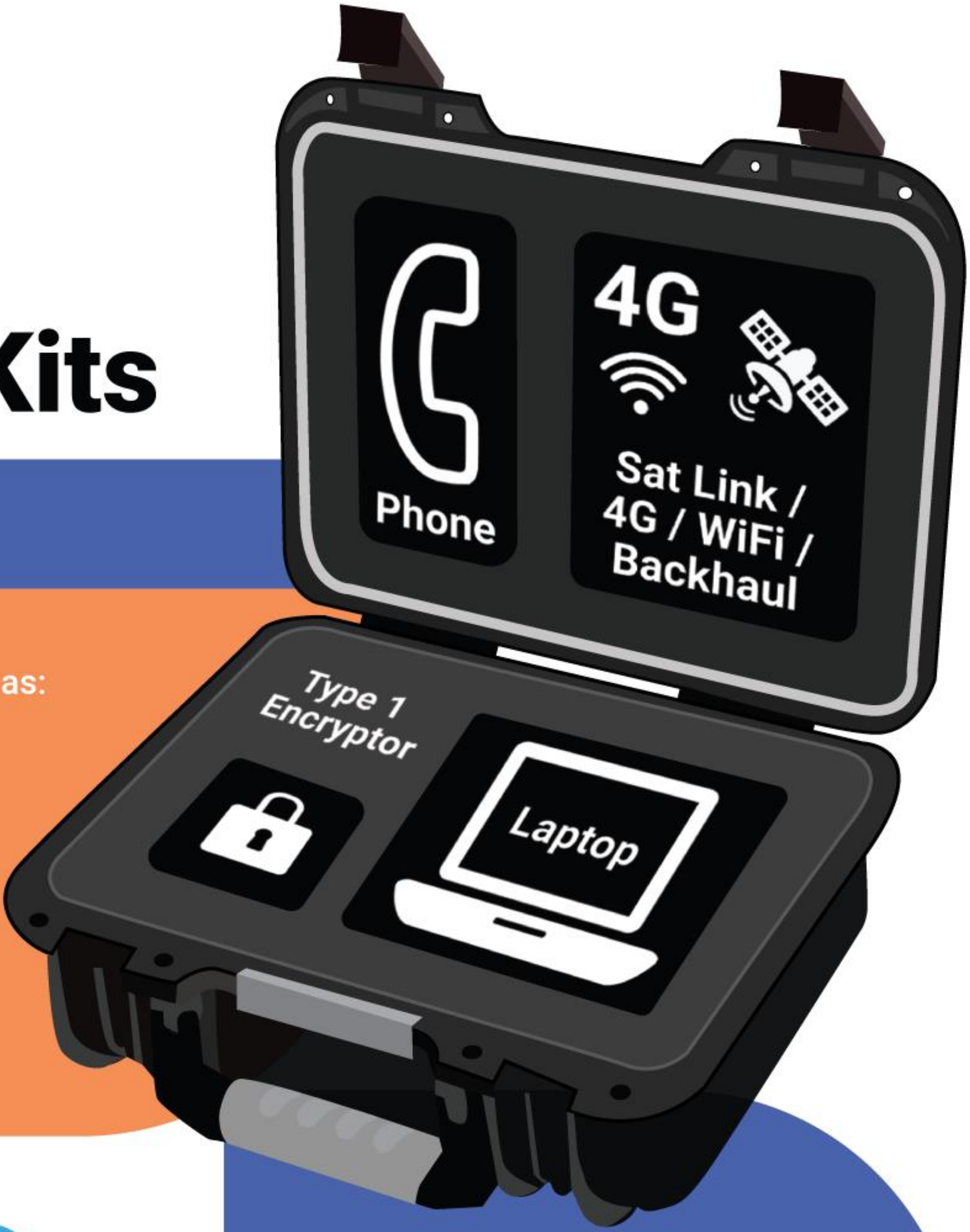
attila SECURITY
presents

Secure Comms Kits

The Basics

Secure comms kits can contain built-in tech such as:

- Firewalls
- VPNs (multiple)
- Laptops
- Phones
- Satellite link
- 4G
- WiFi hotspot
- Backhaul
- Router



All can include

DATA VOICE VIDEO

over any combination of transport:

WIRED WIRELESS IP-BASED CELL SATELLITE

Why migrate to CSfC?

- Better performance
- Requires fewer resources
- More flexibility
- Modern protocols
- Easier to use
- Removes requirement for ComSec Manager & ComSec accountability

THE EASIEST WAY TO CONVERT A TYPE 1 COMMS KIT TO CSfC IS WITH ATTILA SECURITY