Revolutionary TS/SCI *"SoloSCIF"* Workstation

By TRUSTED SYSTEMS

TRUSTED SYSTEMS

Security Made Simple

Revolutionary TS/SCI *"SoloSCIF"* Workstation

By: Robert Bauman, President/CEO

Trusted Systems, Inc.
2920 Dede Road, Suite A
Finksburg, MD 21048
(410) 756-3300
www.trustedsys.com

Introduction

Today's national security threats move at frightening speed and complexity, enabled by advances in technology and increasing geopolitical risks. Addressing these challenges requires a workforce with low-friction and highly secure access to multiple domains of information. While cyber and other technological advances have changed how attacks are conducted, physical security practices have remained largely unchanged, leaving organizations burdened by expensive, inflexible, and antiquated requirements to build out expensive brick-and-mortar SCIFs tailored to securing a physical space.

Because of the imperative to respond quickly and appropriately, senior decision makers and organizations within the Military, SAP and the Intelligence Communities demand innovation beyond traditional physical security approaches. These mission-owners share the following requirements:

- Rapidly deployable and movable single-seat TS/SCI accredited workstation for JWICS.
- Flexibility beyond expensive and time intensive physical SCIF build outs.
- Increasing number of remote sites requiring secured access.
- Increasing concern for insider threat and security risk.

Therefore, Trusted Systems has heeded this call by developing ***SoloSCIF***, a modular, single-occupant, TS/SCI network access module. Trusted Systems already set the industry standard for Secret high endpoint security solutions for SIPRNet around the world from tactical remote sites to senior leadership offices and residences based on a platform they invented, the GSA Class 5 IPS Security Container with embedded access controls. They have elevated this capability to the TS/SCI world by encasing this secure suite inside a single seat TEMPEST and audio shielded shelter to emulate a full ICD705 SCIF. This combined solution offers a triple layer of protection providing superior defense in depth to that of a traditional SCIF, deployable in a fraction of the time as traditional SCIF build-outs and at low cost.

© 2024 Trusted Systems, Inc.

SCIF Shortcomings

SCIFs were originally designed to protect access to a secured workspace, be it for inter-personnel conversation or for enclosed batch processing computer systems with its database and all I/O activity contained therein. Construction specs have not changed much since. Distributed computing changed the paradigm. Instead of a facility securing **SPACE,** it was expanded to become a network enterprise **PORTAL**. This transformation dramatically increased network exposure and dependency on computing and its vulnerability to attack, more so from software threats where the intelligence of the system could be exploited against itself with each access point a threat vector exposing the entire enterprise. Thus, most of the attention, manpower and funding went to cybersecurity and all things Zero Trust. And so, we find ourselves in a perpetual game of "Cyber Chess", to be confronted but never won.

Meanwhile, physical security stagnated and became an afterthought. The only headway over the years was accomplished at the Secret high level. SIPRNet had evolved with access controlled IPS Containers for protecting network devices and the user interface. Little changed in the TS/SCI world where total reliance on the good old SCIF remained with its inherent shortcomings including expense, time to construct and certify, inflexibility, permanent fixed plant construction, and its need for guards and alarms. But SCIFs were functionally transformed into a network portal, its threats, likewise, were exposed due to two major threat vectors that have been mostly left unprotected, especially against the insider threat:

1.) Computing systems and network communications equipment
2.) Endpoint human interface access control to the network

Once inside a SCIF, cleared personnel had unfettered access to computer systems and communications devices and their attendant networks worldwide, which does little to address the insider threat risks to computer and network systems or verify who is operating the individual portal. This is the antithesis of Zero Trust Architecture on the cyber side. Rather, this is the antiquated castle and moat approach where once inside the castle you can do whatever you want, damsels beware, all trust but no verify.

Single Seat SCIF Solution

The SCIF shortcomings regarding exposed network equipment and the endpoint human interface had countermeasures implemented for years at the Secret level. Trusted Systems developed the IPS Container in the early 90s to house and secure encryption devices, computer systems and comm gear for Secret high networks adapted to SIPRNet and associated coalition networks for on-line, closed-door operation. This became the nucleus of SIPRnet physical security acknowledged by DISA in their STIG as a stand-alone CAA for network equipment protection.

The STIG also mandated that only authorized personnel have access to network equipment, i.e., not the users. This required an access control system to enable network access without opening the IPS Container. From this challenge sprung SIPRGuard, a local biometric two-factor access control system to activate and deactivate the desktop in addition to the normal token/PIN logon.

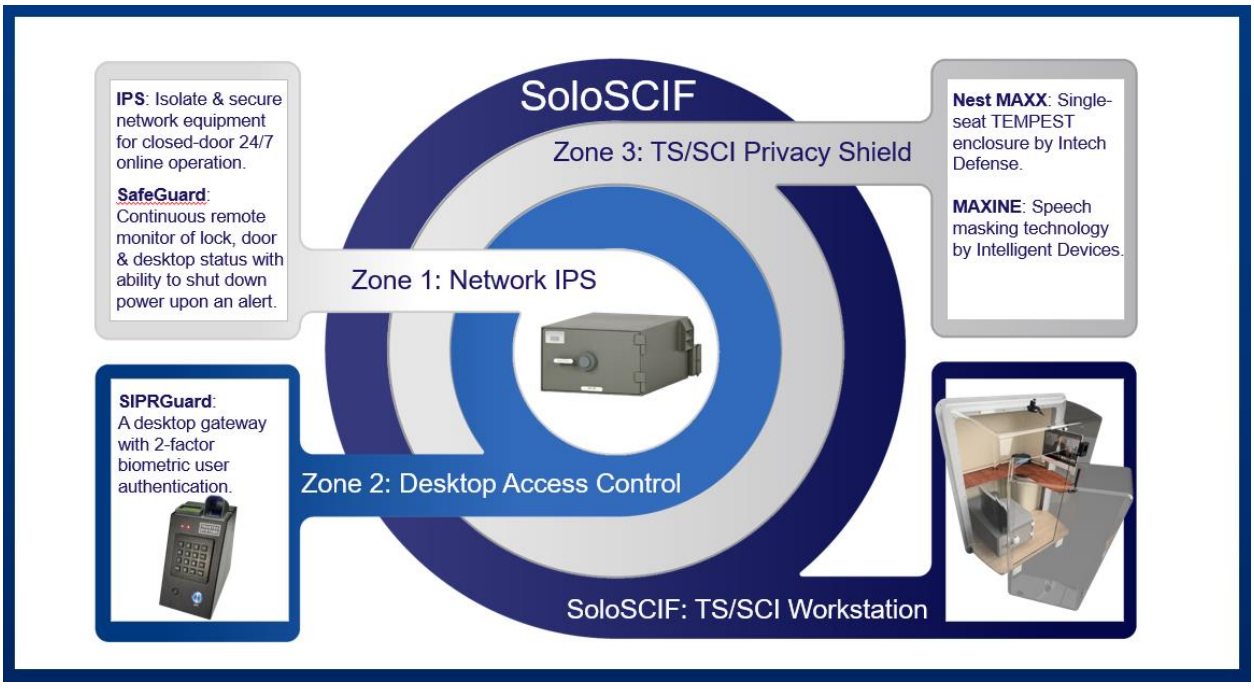
© 2024 Trusted Systems, Inc.

To audit the IPS Container's lock and door status, an IP addressable remote monitor and control system, called SafeGuard, provides a continuous monitor to detect any attempt to open the door to access the network devices. Based on smart PDU technology in response to an alert, the dispatcher or guard can immediately power down all equipment remotely to prevent a compromise. This protects the network equipment while SIPRGuard protects the network access. SafeGuard is also capable of remote monitoring and controlling of the on/off status of SIPRGuard to prevent unauthorized exposure of the desktop.

Full TS/SCI SCIF capability is achieved by surrounding this SIPRNet solution suite inside a single seat TEMPEST and audio shielded shelter. It consolidates protection into three concentric zones of control, each layer protecting and controlling access to the other.

The SoloSCIF – Three in One

SoloSCIF embraces a revolutionary design concept in SCIF construction and functionality that conforms to all the performance criteria set forth in the ICD705 SCIF Specifications but in a unique form factor. Rather than securing a single space with level of protection for TS/SCI multifunctional activity for any number of cleared personnel, ***SoloSCIF*** has been designed for optimizing security for restricted access as a single seat workstation allowing for the sole desktop function as a TS/SCI network portal. This unique capability is achieved with three concentric zones of control as shown in the diagram below, each with its own unique function, isolated from each other but interconnected with integral access controls to manage seamless defense in depth to enable complementary remote monitoring and control.



© 2024 Trusted Systems, Inc.

Zone 1: Network IPS Container – referred to as the "Network IPS", consists of the GSA Class 5 IPS Container with an X10 lock housing and protecting all electronic devices: computers or thin/zero clients, switches, routers, encryption devices and control modules for SIPRGuard. It includes the smart PDU for SafeGuard to monitor the X10 lock, safe door, SIPRGuard status, and outer door status to enable remote control of power shutdown upon an alert.

Zone 2: Desktop Access Control – consists of the operator workspace with its desktop, chair, desktop KVM/VTC peripherals, optional VOIP phone, the JWICS token reader, along with the SIPRGuard desktop biometric fingerprint/PIN reader. The operator has no access to the IPS Container, and its contents, once seated inside. The desktop peripherals are activated only after the outer door is closed and sealed and a successful fingerprint/PIN authentication. Once activated, the normal JWICS logon procedure will commence.

Zone 3: TS/SCI Privacy Shield – consists of the outer carbon fiber composite TEMPEST shell with latching access door, internal lighting, thermostatically controlled air conditioning, (4) external surveillance cameras, filtered power and data ports with battery backup. No network connection activity is enabled until the operator is seated with the outer door closed and latched. The acoustic shielding is embedded into all inner surfaces of the shell using approved TS/SCI speech masking technology. The outer door exterior lock may be an X10, CAC/PIN door access, digital/FOB lock or other lock deemed acceptable by the controlling authority.

System Integration

SoloSCIF is currently in its final stages of development with our partners at Intech Defense and Intelligent Devices, both best of breed in their respective fields. Intech Defense pioneered the deployment of portable shielding solutions, such as TEMPEST tents, for high level VIP travel comms worldwide. They have embarked on creating a hard-shell composite single seat TEMPEST enclosure, called the "Nest", to create a more permanent single seat TS/SCI workspace.

Intelligent Devices, with funding from DARPA and NSA, developed the "Maxwell/Maxine" speech masking technology, the de facto industry standard for acoustic protection for high side remote conversations worldwide, embedded in the Intech Defense TEMPEST tents or the Nest. This technology coupled with passive sound absorbing material is embedded into all surfaces providing optimum acoustic protection.

For robust physical security to complete the TS/SCI workstation trifecta incorporates the Trusted Systems IPS Container. Renowned for its field-proven performance, the container boasts integrated access controls protected by the X10 lock, ensuring a GSA Class 5 rating for superior protection. This setup is designed to leverage the benefits of SafeGuard and SIPRGuard to isolate the network equipment and control the human interface to it without opening the container to do so.

For high profile executive environments requiring discreet security solutions, Trusted Systems presents the INCOGNITO line — finished wood cabinetry designed to integrate ***SoloSCIF*** seamlessly with the

© 2024 Trusted Systems, Inc.

room's décor. These custom-finished cabinets blend with existing furniture, offering an elegant solution to house TS/SCI network access inconspicuously. ***SoloSCIF***'s incorporation ensures high side classified communications are not only centralized but also artfully concealed within the executive space, maintaining a clean look, consolidating network communications.

Accreditation

The attributes described above, when combined, proffer defense in depth that encompasses physical security, emanation security, and environmental protection far beyond what an ICD-705 SCIF provides. In this light, Trusted Systems posits that ***SoloSCIF*** is not only equivalent to a SCIF by design but superior to a traditional SCIF due to its additional protection for the human interface and the network devices. This entails a paradigm shift in the criteria of ICD705 to meet emerging security threats.

The Trusted Systems IPS Container offers high-end compartmented, GSA Class 5 protection for Secret and TS high applications residing within the confines of the TEMPEST shielded *Nest Maxx*. All red network cabling resides inside the container away from the user and without the need for any plugging or unplugging to get online. All cabling outside the container is encrypted except for the desktop cable connections, which are only active when the operator is present and authenticated, and the outer door is properly closed to maintain TEMPEST integrity. No such capabilities exist inside a traditional SCIF.

SafeGuard augments the traditional exterior alarm systems as specified in the ICD705 spec by providing continuous remote monitoring of the outer door access to ***SoloSCIF*** and the IPS Container spin dial, lock, and door. Where SafeGuard differentiates itself from other SCIF alarm systems, it also controls power to the network devices that can be immediately shut down upon an alert including “zeroizing” encryption devices, not waiting 10-15 minutes for a guard response.

SoloSCIF has only one operational function, that is a network portal for a single user. Supplemental two-factor biometric authentication restricts the user to online network access only, without access to any network devices except those on the desktop.

The speech masking technology was developed at Intelligent Devices based on DARPA and NSA-funded projects called *Maxwell/Maxine*. It has emerged as the de facto standard for secure TS/SCI comms at US Government and Military facilities CONUS and OCONUS, and remote off-site locations, such as hotels.

Intech Defense has deployed TEMPEST tents for mobile deployments and senior leadership travel destinations, accepted for use at the TS/SCI required security levels worldwide. This experience has been leveraged to create the *NEST* hard-shell version incorporating all the features of the TEMPEST tents including integrating *Maxwell/Maxine* speech masking and internal air conditioning.

With each component system above already individually accepted for use up to TS/SCI levels, the aggregate security solution should generate ample impetus for consideration to gain accreditation at least as a T-SCIF or accepted as a single-seat SCIF alternative unto itself.

It is expected that the ultimate configuration will be generated by the Government sponsor with specific use case requirements submitted in a package from the SSO for review and evaluation at the MAJCOM

© 2024 Trusted Systems, Inc.

level. In concert with DIA, a final ATO on a T-SCIF basis or otherwise accepted by the reigning authority could be issued. Each use case package would be evaluated separately under its own merits.

Summary

Our philosophy at Trusted Systems entails simplicity at its core. Since simplicity is not easily achieved, we innovate security improvements while incrementally advancing the state-of-the-art using known and accepted standards, procedures, and products. Our simple approach embracing the convergence of compliance and convenience has allowed us to successfully advance the interests of the SIPRNet community, in addition to supporting the TS/SCI environment. Trusted Systems is well on the way to achieving an integrated single-seat SCIF Workstation that is simple, convenient, and compliant. We believe that ***SoloSCIF*** presents an optimal solution for single seat JWICS and other TS/SCI based networks, like NSANet, with its cost-effectiveness, timeliness for deployment, non-obsolescence, self-contained design, and adaptability to nontraditional work environments.

The next step forward is to uncover specific use cases to demonstrate ***SoloSCIF*** in action to evaluate and validate the claims made herein, make refinements where necessary, and to eventually attain ATO acceptance throughout the TS/SCI community.

© 2024 Trusted Systems, Inc.