PROMETHEUS
SECURITY GROUP GLOBAL

PSG - LOW COST SCIF SOLUTION

PRODUCT OVERVIEW:

PSG's SCIF solution is ICD 705 compliant and a modernized low-cost integrated Intrusion Detection and Access Control system. It leverages PSG's extensive PL1N background and product suite the Universal Field Panel (UFP) with Digital Encrypted Security Interface (DESI) technology combined with PSG's Command & Control (C2) software. The basic system configuration provides local management of up to sixty-four DESI I/O devices and eight access controlled doors. The secure/access control (SEC/ACC) function is provided by a touch-screen LCD keypad. Optional 3rd party FIPS 140 encryption (VPN Tunnels, Modems, Network Switches) are available for networked SCIF applications.

Features	Benefits
Embedded Browser Based Command and Control (C2)	- No additional Application servers required
Zero Trust Architecture (ZTA) compliant	- Secure FIPS PKI Authenticated Data - Edge to Enterprise
Universal Field Panel with PKI (DESI)	- Upgrades legacy field panels and old end-of-line resistors
Zone Control (Touch Screen Keypad)	- Simple, text-based touch screen zone control
TAA/NDAA compliant	- Made in the USA
ICD-705 compliant solution for SCIF applications	- 3rd party FIPS 140 encryption available for remote monitoring
Intrusion & Access Control	- Low cost per input field panel, scalable up to 128 alarm points & 8 doors.
UL 2050 compatible (w/req. API)	- MOSA - Modular Open Systems Approach (any UL 2050 3rd party monitoring sol).

PSG (C2) Software: PSG's C2 software is browser based and embedded directly on the UFP-GW. Includes user-friendly intrusion detection and access control configuration, command and control and user credential enrollment - all available via users client-based web browsers. Eliminates need for dedicated clients and servers. The PSG C2 provides users US Dept. of Energy (DOE) /Dept. of Defense (DOD) nuclear asset approved (PL1N) security software at commodity pricing.

Universal Field Panel (UFP) with Digital Encrypted Security Interface (DESI) : UFP is the next generation of open architecture secure IoT devices that provide integrated data gathering and control from the edge to the enterprise. The UFP consists of a gateway and optional expansion modules which implement the physical security mission. The solution combines intrusion detection, access control and industrial data gathering controls into a cost-effective footprint. The UFP, combined with DESI, provides users Zero Trust FIPS level PKI encryption & authentication of data between edge devices (dry contact input/control outputs) and the enterprise.

Cyber Secure: The UFP/DESI delivers a set of current security tools including but not limited to support for Security Technical Implementation Guide (STIG), Trusted Platform Module (TPM 2.0), Secure Boot, Secure Key Storage for communications and FIPS encryption (PKI) and authentication stack.

Cost Effective Event Processing and I/O Device: The UFP delivers a MOSA (Modular Open System Approach) concept to the edge computing needs of the any security mission solution. The C2 software is included with the UFP, the UFP is truly open, providing database, computing and container services that enable hosting of third-party applications, both commercial-off-the-shelf (COTS) and/or government-off-the-shelf (GOTS). It supports third party integration via MQTT communications protocol. The UFP secure computing environment enables modernization of sensing and control applications for Intrusion Detection, Access Control, and SCADA environments.

UL 2050 Commercial Central Stations: SIA Standard internet protocols allowing for seamless ICD 705 compliant integration. Making it possible for the benefits of UFP/DESI to be leveraged by the operators of UL2050 central stations.