



### **Introduction:**

Over the last 24 months, the Department of Defense (DoD) and the Department of Homeland Security (DHS) have experienced a tremendous increase in the deployment of secure networks carrying classified or Sensitive But Unclassified (SBU) information. Within the Department of Defense, the deployment of the Global Information Grid (GIG) and the expansion of its associated bandwidth up to 10-Gigabit Ethernet have given many DoD installations and combat units their proverbial ‘on-ramp’ to the SIPRNET super information highway. With SIPRNET access, military units are able to leverage the many communication and collaboration tools that have been deployed by DISA’s Network Centric Enterprise Strategy (NCES) to enhance command and control and our underlying combat effectiveness. Within the Department of Homeland Security (DHS), the Homeland Secure Information Network (HSIN) is providing essential connectivity and information sharing between state, local, and federal agencies on counterterrorism. HSIN provides government officials and civil authorities with real time sharing of threat information and improving situational awareness.

### **Secure Connectivity Requirements:**

However, in spite of all of the benefits that both SIPRNET and HSIN can provide, nothing is possible without first providing authorized personnel with the ability to access or connect to the secure network in a timely and reliable fashion. Due to the sensitive or classified nature of the underlying information, deployment of secure networks must adhere to strict guidelines designed to protect the confidentiality, integrity, and availability of the information and the associated networks. For years, this meant that secure networks had to either deal with the bandwidth limitations associated with Type I encryption or to take extraordinary measures to protect the unencrypted networks using a Protected Distribution System (PDS). Historically, a PDS is deployed using either concrete-encased duct banks for campus or wide area networks, or installing cables inside of EMT for local area networks. While encryption is the undisputed choice for protecting information across long-haul or metropolitan networks, a majority of DOD units use PDS for secure network access on military installations and within facilities. Encryption is just too costly, too limiting on network performance, and requires too much time to manage the Public Key Infrastructure and COMSEC issues. In fact, many units that have previously deployed encrypted connections ‘tunneled’ across unclassified networks are now being challenged by approval authorities to re-assess the protection being provided to BOTH the information and the network infrastructure being used to transmit it- especially considering the strategic dependence on the networks, and the increasing focus by our enemies to degrade them.

While EMT and concrete-encased duct banks have been deployed for years as part of a PDS system, both approaches are very complex, time-consuming, and costly. In the past, secure network distribution on a military installation would be limited to a few buildings; today, that same military installation must provide pervasive connectivity to a majority of the buildings. This has caused a dilemma in the cost and complexity associated with providing access to secure networks – especially in light of continued budget

pressures with the ongoing military operations on the ongoing war against terror, and the counterterrorism programs and activities here in the United States. The dilemma for DoD and DHS is how to meet BOTH the functional and security requirements for the network – while also balancing the need for increased deployment with diminishing resources. Another element that makes the situation even more complex is that change has become a constant in DoD and DHS. Organization re-structuring and unit re-assignments and deployments have become commonplace – forcing agencies and units to consider Total Cost of Ownership and the transferability of any solution to a new work center, facility, installation, or geographical location.

With the growing demand for secure network connectivity, network managers, facility owners, and end users alike are looking for new solutions that significantly reduce the cost of SIPRNet deployments – without creating any bandwidth bottlenecks or reducing the performance of the network that the war fighter depends upon.

### **Introducing INTERCEPTOR™:**

A new innovative solution is available. This technology, developed for ‘alarming’ a PDS system rather than ‘hardening’ it with concrete or EMT, has, to-date, been one of the Intel communities best kept secrets.

The Interceptor™ Optical Network Security System from Network Integrity Systems was developed in part with DoD funding to monitor and protect the physical integrity and availability of networks links transporting SECRET or above traffic. Interceptor works as an in-line network Protected Distribution System (PDS) that can be easily installed on new or existing fiber optic cables. Interceptor is fully compliant with NSTISSI 7003 and the corresponding implementation guidelines of the various agencies and services, and has been leveraged in support of projects at the Pentagon, DHS, DIA, NRO, Army INSCOM, Air force INTEL, CENTCOM, Department of Justice and SPAWAR.

### **Functional Requirements for Secure Network Connectivity**

- 1) Cost-effective
- 2) Fast / High-Bandwidth
- 3) Scalable
- 4) Easy to Install
- 5) Minimal O&M Impact
- 6) Transferrable / Transportable



Rather than requiring extensive planning and construction for a hardened PDS system with concrete encasement, INTERCEPTOR™ enables the option of leveraging either existing cables or pulling new cables into existing duct banks or pathways. By simply installing INTERCEPTOR™ equipment on one or both ends of the fiber optic cable, the point-to-point connection is quickly and easily protected – requiring little to no intrusive installation or activity along the cable route. In fact, INTERCEPTOR™ can be installed on lit or dark fibers, and can protect up to a 144-fiber cable using only a single pair of fibers for monitoring. Even when installed on active fibers, INTERCEPTOR™ utilizes an out-of-band signal for monitoring which negates any potential bandwidth ‘bottlenecks’ or degradation of network performance typically experienced with in-line network encryptors.

### **PDS Deployment Options for OSP Networks:**

For decades, the construction of a hardened PDS system using concrete-encasement has been a de facto standard for new building construction and OSP network deployments or modernizations. However, recent price increases and availability of key ingredients such as Kevlar have made concrete encasement much more costly and more difficult to obtain. With increasing focus on Green Building standards and LEED criteria, many General Contractors and Federal agencies are looking for alternatives to concrete-encasement in order to reduce the over-order waste that can contribute up to 30-50% of a construction project's total waste. In fact, using technologies like INTERCEPTOR™ - that negate the need for concrete-encasement - actually qualify the contractor for a credit towards the federally-mandated LEED Silver certification for government facilities.

For those not familiar with new facility construction costs or OSP Network deployment costs, it is easy to dismiss concrete-encasement as a ‘necessary evil’ or ‘cost of doing business.’ However, the truth is that concrete-encasement is NOT a common practice in private industry or as part of network deployments by public telephony or CATV operators. In fact, concrete-encasement of duct banks is a top cost contributor to any construction or network deployment project. For the US Army’s Installation Infrastructure Improvement and Modernization Program (I3MP), concrete encasement is routinely in the top 3 of all materials and project cost contributors – totaling well over \$1 million per Army installation. Given the increasing pressure on federal budgets, finding cost-effective alternatives to concrete encasement represents a huge potential cost savings – savings that could be recouped and re-utilized for other requirements. On the I3MP program, alone, if 4 installations are upgraded per year – it represents a potential cost savings of over \$5 million for the US Army, and the indirect benefit of being more environmentally-friendly and adhering to newly established LEED criteria for DoD construction projects.

**Joint Command Case Study:** To give a specific example of the potential cost-savings and other benefits of leveraging the INTERCEPTOR™ Optical Network Security System, a joint command in Florida was evaluating the PDS requirements associated with the construction of a new facility. The J2/J6 personnel had determined that encryption was too costly and too restrictive for the project given the large number of connections required and increasing bandwidth demands, and instead started focusing on the installation of a concrete-encased duct bank along the 400' cable route to the new facility. As part of the project planning, the command personnel were faced with the costs and deployment considerations highlighted in Figure X.

**Concrete-Encasement Deployment Profile**

**Total Cost:** \$800,000  
**Time Required:** 2 Weeks On-site  
*(after a 4 week delay to start)*  
**Equipment Needed:** Excavator  
*(to dig 4' wide trench)*  
**Impact on Base:** Very Intrusive  
 - Road Closures / Detours  
 - Loss of Parking Lot  
 - Noisy Equipment  
 - Potential damage to other buried infrastructure  
**Landfill Impact:** 20% Over-Order Waste  
*(Waste fee not included)*

After learning about another DoD agency's deployment of Interceptor, the command personnel engaged their Information System Security Officer (ISSO) to evaluate the applicability of the INTERCEPTOR™ to reduce the cost and complexity of their upcoming deployment. While the reduction of the deployment's cost and complexity were key considerations, the ISSO needed to assess the level of protection that INTERCEPTOR™ would provide for their SIPRNET and JWICS networks that were planned. After evaluating INTERCEPTOR™, the ISSO and command personnel concluded that INTERCEPTOR™ provided enhanced security for the

**INTERCEPTOR™ Deployment Profile**

**Total Cost:** \$180,000  
**Time Required:** 2 Days On-site  
*(doable over a weekend)*  
**Equipment Needed:** Ditch - Witch  
*(to direct bury duct)*  
**Impact on Base:** Minimal  
 - No impact on roads or traffic  
 - Almost transparent to adjacent facilities  
 - Completed over Weekend  
**Landfill Impact:** None

network above and beyond a traditional 'hardened' PDS system in that INTERCEPTOR™ would negate the need for costly and potentially unreliable system to monitor manholes. In fact, the command personnel were delighted to discover that INTERCEPTOR™ would provide a cost-effective yet secure alternative and enable the deployment profile highlighted in Figure X. As a result of the successful deployment, the command is now considering increased deployment of INTERCEPTOR™ equipment for other projects and facilities.

**Conclusion:**

With the increased deployment of secure networks by DoD, DHS, and other federal and state agencies, new technologies are needed to provide high-assurance, cost-effective protection for the networks. When we consider the role that technology development has played in the evolution of our network-centric strategy, we must also consider that similar technology

advances could benefit us with regards to the protection of the network(s) as well. Specific to new construction projects and OSP network deployments, there are millions of dollars in potential cost savings that could be realized by leveraging an Alarmed PDS with the INTERCEPTOR™ Optical Network Security System as an NSA-approved alternative to concrete-encased duct banks. In fact, with the increased focus on environmentally-friendly construction and the need for enhanced security of our networks, the INTERCEPTOR™ Optical Network Security System is well-positioned to serve as the next-generation de facto PDS solution.