

FOR IMMEDIATE RELEASE

Media Contact: Amanda Simpson
828.322.2181
amandas@networkintegritysystems.com

INTERCEPTOR Selected for Major Army Secure PON Network Modernization Project

HICKORY, N.C. (May 7, 2013) –The [INTERCEPTOR](#)™ Optical Network Security System has been selected for the Network Modernization Project at Greely Hall on Ft. Huachuca, home of the US Army's Network Enterprise Technologies Command (NETCOM). Secure PON (S-PON) delivers the immense cost savings and feature benefits of Gigabit Passive Optical Network (GPON) Optical LAN technology combined with the best-of-breed infrastructure security of INTERCEPTOR Alarmed-Armored PDS™.

INTERCEPTOR Alarmed-Armored PDS™, leveraging flexible interlocking armored optical cable to enable concealment of the Protective Distribution System (PDS), allows for SIPR connections to be deployed to any location within a facility rapidly, and at a low cost. With this award, INTERCEPTOR has been selected for all of the prominent US government S-PON deployments, including the new Department of Homeland Security's consolidated headquarters at the St. Elizabeths campus in Washington, D.C., and the Air Force District of Washington's Headquarters (AFDW), at Joint Base Andrews.

As a result of INTERCEPTOR's unanimous selection in these projects, industry leading layer 1 manufacturers have been developing best-of-breed components for S-PON infrastructures to enable systems integrators to offer INTERCEPTOR-integrated Alarmed-Armored PDS™ solutions including advanced tools for infrastructure and alarm-response management. INTERCEPTOR is the only data cable monitoring system available with millions of hours of past performance monitoring dark fibers within the cables being secured. Since INTERCEPTOR was developed specifically for data infrastructure security, it has many technical and operational advantages over products that were developed for and derived from perimeter security technology. These advantages, which combine to make INTERCEPTOR uniquely capable of addressing the flexible S-PON zone architecture requirements, include:

- The patented ability to directly monitor single mode fibers – the standard fiber type used in GPON cabling. Systems with only multi-mode capability would require an expensive specialty hybrid cable in a GPON solution.
- Ample dynamic range to protect more than the standard 32 end-user drops in a single GPON zone using a *single monitoring port* (or zone). This means

that a 4-port INTERCEPTOR can protect up to 4 or more GPON zones (or over 128 users); using standard fiber connectors and patch panels, surpassing competing models with 8 ports which have a fraction of the dynamic range of an INTERCEPTOR.

- Enables the construction of the monitoring circuit within the zone with low-cost, easy to install mechanical connectors or splices (other systems relying on reflective termination devices, require an inconvenient, difficult to modify, *all-fusion spliced circuit in order to extend to multiple drop locations*).
- The ability to change the length of the zones, for instance when moves, adds or changes are required, without the need to reconfigure the physical placement of the cables in the alarm system.
- INTERCEPTOR alleviates the need to reprogram the alarm management server every time a zone changes. In fact, such systems can be programmed to enable the INTERCEPTOR to learn new drops or reconfigurations made to the infrastructure as moves/adds/changes are performed on the network.
- The patented ability to *automatically* learn the ambient state of the network infrastructure to prevent nuisance alarms, and to relearn when conditions change without monitoring downtime, and without manual assistance from factory certified personnel required on the job site.
- The ability to quickly, easily and securely integrate the INTERCEPTOR directly to existing network management systems or custom software solutions using SNMPv3 traps.
- Capacity to capture event log information without an external PC attached to every alarm unit, and the ability to send a daily health report of the systems and the physical network. This is important for Information Assurance and future inspection audit requirements.

Contact Network Integrity Systems for more information on how your organization can benefit from modern network design and infrastructure protection.

About the INTERCEPTOR™ Optical Network Security System

INTERCEPTORs have been deployed since 2003 across the globe and have recorded in excess of 50-million port-hours protecting U.S. government classified networks.

Traditional methods to protect the infrastructure of unencrypted networks carrying national security information, such as hardened PDS, cannot scale with today's demand for access to those classified networks. Alarm systems designed for perimeter security applications are ill suited for fiber-to-the-desk architectures such as PON. In contrast, INTERCEPTOR was design specifically for data communications security, and with years of customer feedback regarding the specific requirements for securing network cabling. Demonstrating their confidence in the INTERCEPTOR, Information Assurance authorities have authorized its use in networks carrying data up to the TS/SCI level including SIPRNet, JWICS and in high threat level environments.

About Network Integrity Systems, Inc.

Network Integrity Systems, Inc., (NIS) develops and manufactures products that enable organizations to protect their classified networks faster, more economically, and less intrusively than ever before possible with legacy systems. Founded by optical engineers and management personnel from a global fiber optics leader, NIS helps solve key issues associated with the growing need to guard the confidentiality, integrity and availability of National Security Information.

Visit www.networkintegritysystems.com for more information, or call 1-877-NIS-4PDS.