NetworkIntegrity
SYSTEMS

INTERCEPTOR™
Optical Intrusion Detection System

Purpose-Built. Mission-Proven.
Trusted for National Security.

INTERCEPTOR™: SMART ALARMED PDS ENSURING END-TO-END SECURITY AND COMPLIANCE

For more than two decades, INTERCEPTOR™ has stood as the industry benchmark for securing classified and mission-critical networks. The latest generation—INTERCEPTOR^NX™—continues that legacy with purpose-built innovation, unmatched performance, and the trusted reliability demanded by the U.S. Government and Military. Fully compliant with CNSSI 7003, INTERCEPTOR^NX delivers real-time threat detection, superior optical performance, and smart capabilities that multi-purpose systems simply can't match.

When your mission demands precision, scale, and security without compromise, choose the solution engineered exclusively for the job—INTERCEPTOR^NX™.

MADE IN THE USA, FOR THE USA

Network Integrity Systems(NIS) based in Hickory, NC, USA, designs, engineers, and supports the entire INTERCEPTOR^NX platform in-house including all firmware and software. Our integrated portfolio ensures full CNSSI 7003 compliance and seamless performance across your infrastructure.

WHAT SETS INTERCEPTOR^NX™ APART

Superior Optical Performance
Makes the entire cable a sensor:
- When any component of the cable is abnormally handled, a pair of monitored fibers inside the protected cable senses

the disturbance—offering improved sensitivity compared to using a single sensing fiber.
- Uses standard LAN infrastructure connections
- Industry-leading dynamic range, without compromising signal quality or detection performance.
  - 55dB for single-mode
  - 50dB for multimode
- Supports patented point-to-multipoint architecture, slashing hardware requirements and cost while maximizing coverage.
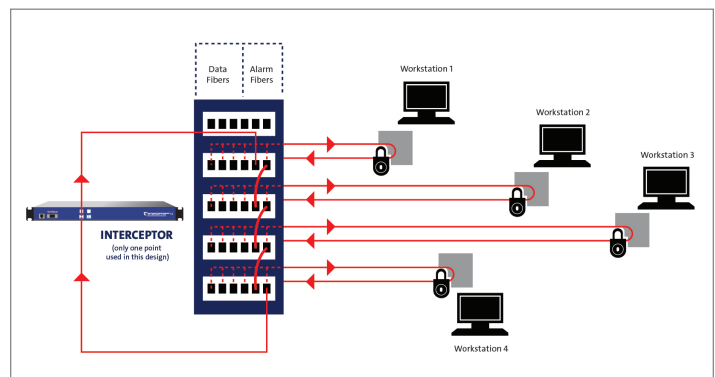
Purpose-Built for Classified Networks
- Exclusively for U.S. Government Protected Distribution System (PDS) applications, featuring detection algorithms specifically tailored for U.S. Government networks. This solution is not available for commercial sale or to foreign governments.

Smart, Patented Capabilities
- Smart Filter Detect™ (SFD) eliminates false alarms through real-time analysis and adaptive response.
- Auto-configuration minimizes setup time and ensures optimal performance from day one.
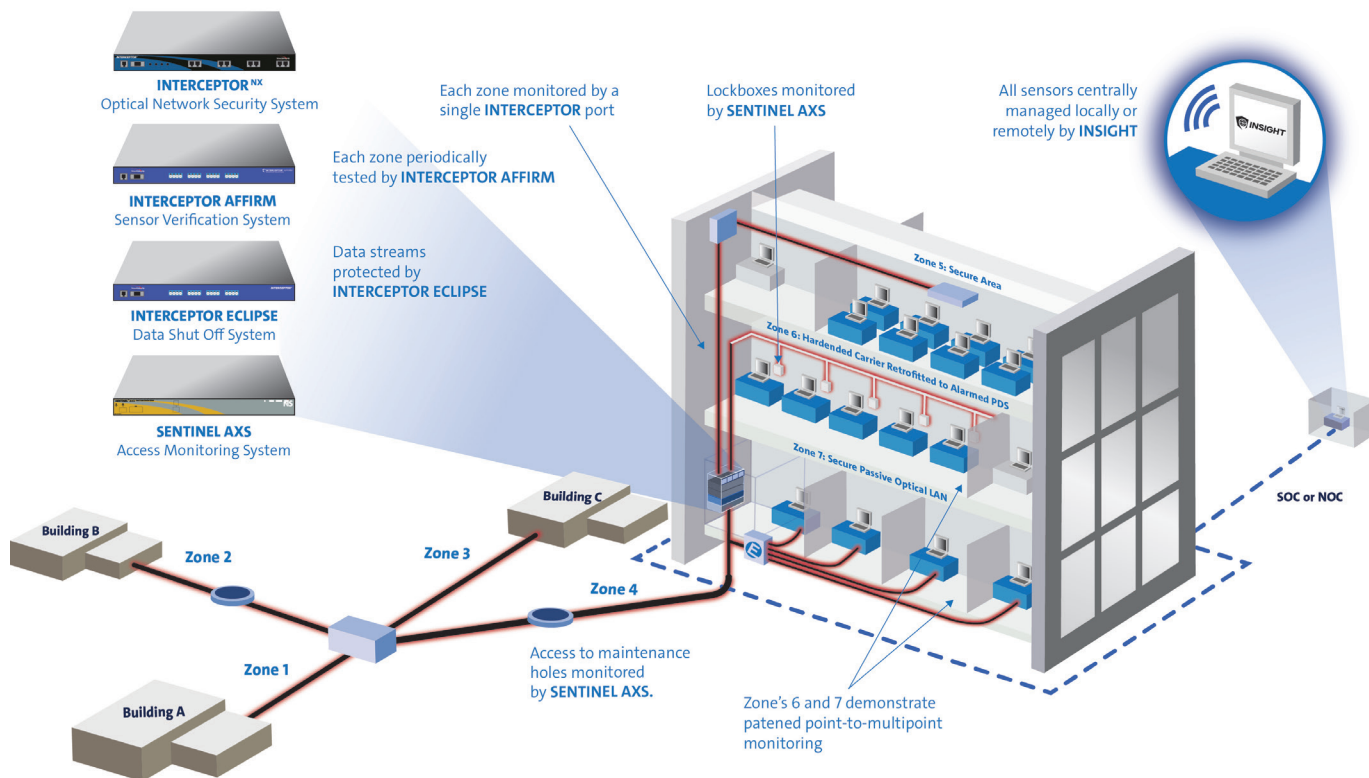
Advanced OS 3 Firmware
- Enhanced user experience with improved algorithmic performance, and hardened cybersecurity through a custom API that reduces attack vectors.

COMPLETE SOLUTION FOR CNSSI 7003 COMPLIANCE

NIS has developed a suite of ancillary, purpose-built products that complete the solution and help ensure compliance with CNSSI 7003 for classified network protection.

Comprehensive Network Infrastructure Security Solution

INTERCEPTOR NX
Optical Network Security System

INTERCEPTOR AFFIRM
Sensor Verification System

INTERCEPTOR ECLIPSE
Data Shut Off System

SENTINEL AXS
Access Monitoring System

Each zone monitored by a single **INTERCEPTOR** port

Each zone periodically tested by **INTERCEPTOR AFFIRM**

Data streams protected by **INTERCEPTOR ECLIPSE**

Lockboxes monitored by **SENTINEL AXS**

All sensors centrally managed locally or remotely by **INSIGHT**

Zone 5: Secure Area

Zone 6: Hardended Carrier Retrofitted to Alarmed PDS

Zone 7: Secure Passive Optical LAN

SOC or NOC

Building B

Building C

Zone 2

Zone 3

Zone 4

Zone 1

Building A

Access to maintenance holes monitored by **SENTINEL AXS.**

Zone's 6 and 7 demonstrate patened point-to-multipoint monitoring

INSIGHT™ ALARM MANAGEMENT SOFTWARE

INSIGHT is a sophisticated, customizable, purpose-built alarm response and management application designed to integrate seamlessly with the INTERCEPTOR^NX and other systems. Developed from the ground up with strict adherence to U.S. Government Security Technical Implementation Guides (STIGs), INSIGHT prioritizes cybersecurity at every level. It is offered as a perpetual license, eliminating the need for mandatory annual renewals. To help customers leverage their existing alarm response infrastructure, INSIGHT offers INTERLINK™—a flexible integration feature set that allows third-party sensor data to be seamlessly incorporated into current systems. INTERLINK can also operate independently of the full INSIGHT platform, enabling an easy transition while preserving and enhancing the value of previous security investments. Plus, it comes at a lower price than the complete INSIGHT package.

To validate its security posture, Network Integrity Systems engaged a certified C3PAO, to assess compliance with NIST SP 800-53 Rev. 5 (Moderate). This assessment included a rigorous review of INSIGHT's architecture, documentation, and security, ensuring alignment with DoD Application Security and Development STIG requirements.
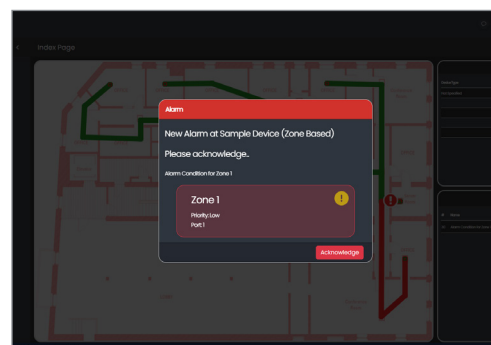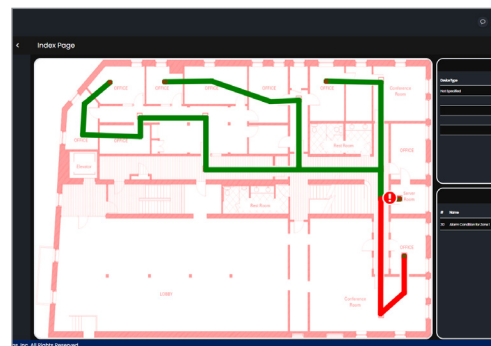
INTERCEPTOR AFFIRM™ AUTOMATED SENSOR VERIFICATION SYSTEM

An integral component of the INTERCEPTOR^{NX} Alarmed Carrier PDS solution. Engineered to automate the essential periodic testing of the system, INTERCEPTOR AFFIRM seamlessly integrates with INSIGHT, conducting automatic tests for each zone without any human intervention.

## INTERCEPTOR ECLIPSE™ DATA SHUTOFF SYSTEM

Integrates with INSIGHT to disable data traffic when an intrusion attempt is detected. This feature enhances security and assists with alarm responses outside of regular business hours.

Unlike competitive products that incorporate the functions of INTERCEPTOR AFFIRM and INTERCEPTOR ECLIPSE into one device, we have designed them as separate products with different fail-safes so the security of your data is never in question.

SENTINEL AXS™ AUTOMATED OPEN/CLOSE SENSORS FOR PDS SYSTEMS

This versatile solution is designed to detect open and close events, making it ideal for lock boxes, maintenance holes, and other locations where a verified open or closed state is critical. The system leverages new technology that reduces cost and simplifies maintenance, with standard sensors that can be deployed anywhere. Fully integrated with INSIGHT™ software, it supports single-mode fiber and is available in 1, 2, and 4-port models. The use of passive sensors means no power is required in the field, further enhancing reliability and ease of deployment.
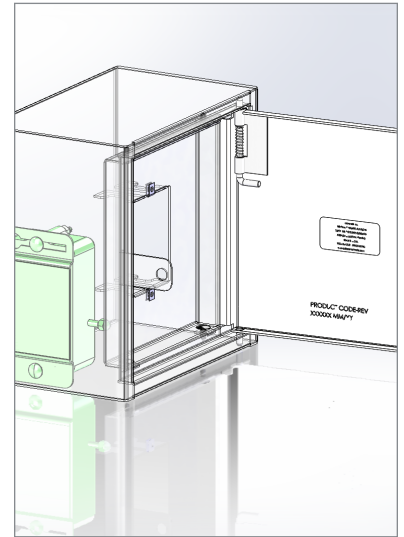
INTERCEPTOR NX™ ENGINEERED FOR PERFORMANCE. TRUSTED FOR NATIONAL SECURITY.

When national security is on the line, don't settle for repurposed solutions. Choose the platform trusted by the U.S. Government for over 20 years—a solution built from the ground up for one mission: to protect the nation's most sensitive communications.

WARRANTY AND SUPPORT PROGRAM (WSP)

The NIS Warranty and Support Program (WSP) provides up to 5 years of comprehensive hardware coverage and flexible support options tailored to your needs. Backed by industry-leading service, WSP gives you peace of mind. Choose from three levels of support—ranging from online and phone assistance to on-site service—for 1, 3, or 5 years. We're committed to ensuring an exceptional experience with every product.

HOW INTERCEPTOR^{NX}™ ALARMED PDS REPLACES IN-BUILDING TACLANES WITHOUT SACRIFICING SECURITY

The U.S. government have traditionally turned to TACLANE® encryptors to safeguard data in transit. While effective, this approach adds complexity, cost, and logistical burden—especially within secured buildings. The INTERCEPTOR™ Alarmed PDS offers a smarter, streamlined alternative: a high-assurance solution that eliminates the need for in-building TACLANEs while still meeting the strictest security requirements.

SUMMARY COMPARISON OF TACLANES/TYPE-1 ENCRYPTION VERSUS INTERCEPTOR^{NX}

	Type-1 Encryption	INTERCEPTOR^{NX} Alarmed PDS
Equipment Expense	**HIGH** Individual encryptor required per fiber-link and per DWDM wavelength channel per fiber link	**LOW** Requires only one port of one device to secure all fibers and all DWDM wavelength channels in each fiber in a cable
Operating Expense	**HIGH** • Daily PKI processes • COMSEC management • Frequent software updates	**VERY LOW to LOW** • Automated alarm circuit verification • Human inspection upon alarm • Infrequent software/firmware updates
Speed of Deployment (Lead Times)	**HIGH** Long lead times, currently 12-18 months	**LOW** Short lead times, currently 4-6 weeks
Network Bandwidth	**LIMITED** • Encryption touches all data • Dependent on Encryptor speed	**UNLIMITED** • INTERCEPTOR^{NX} doesn't touch the data • No bandwidth restrictions
Cyber Security Profile	**IGNORES DATA THEFT** Relies on intruders' inability to decipher information	**PREVENTS DATA THEFT** Detects tapping and disruption of fibers
Dave Availability Profile	**NONE** Does not assure data availability	**CONTINUOUS MONTIORING** Detects tampering with cables as a precursor to a denial-of-service attack

NOT ALWAYS COMPETITORS: HOW TACLANES AND INTERCEPTOR^{NX} CAN WORK TOGETHER FOR STRONGER NETWORK SECURITY

In many secure network environments, TACLANEs and INTERCEPTOR can serve complementary roles, enhancing overall protection by addressing different layers of security. While TACLANEs focus on encryption, INTERCEPTOR strengthens network infrastructure integrity. Together, they create a more robust defense.

Ultimately, both TACLANEs and INTERCEPTOR serve critical roles in securing classified networks—but they solve different problems. Where encryption is required for protecting data over untrusted or external networks, TACLANEs remain essential. However, for in-building cable runs within controlled spaces, INTERCEPTOR delivers a simpler, more cost-effective solution that meets or exceeds federal security standards without the overhead of encryption devices at every endpoint. As agencies look to modernize and streamline their infrastructure, INTERCEPTOR stands out as the preferred path to high-assurance network security inside the building.