C A S E S T U D Y

Meeting the Demand for Compliant, Secure Classified Network Deployments in the Industrial Environment; Using Advanced Alarmed PDS Technology

Background

Private enterprises performing contractual work for the U.S. Government in projects where National Security Information is communicated via the contractor's private networks, must undergo Command Cyber Readiness Inspections (CCRI) to obtain and maintain an Authority to Operate (ATO) the networks. A significant component of the CCRI is verification that an authorized method for assuring the confidentiality, integrity, and availability of the information transmitted over the network is in-place. A common security practice is to utilize NSA approved Type-1 encryption devices within the network. However, there are several disadvantages associated with the use of Type-1 encryption such as high cost, network bandwidth restrictions, un-acceptable lead-times to acquire equipment and cumbersome encryption-key management processes. When encryption isn't in-place, these organizations, as their DoD clients do, must comply with National Security Telecommunications and Information Systems Security Instruction (NSTISSI) 7003, Protective Distribution Systems (PDS) which provides guidance for the protection of wireline and optical fibers transmitting unencrypted National Security Information. In many cases however, operating, maintaining and insuring the security of a conventional PDS complaint with NSTISSI 7003 guidance is becoming increasingly difficult to achieve.

With an Intelligent PDS, all of the prior disadvantages of PDS, which are most likely the reasons for its non-compliance, have been eliminated.

Situation

Recently, Network Integrity Systems (NIS) worked with two industry leading government defense contractors, each working on mission critical projects, which failed their (CCRIs) due to non-compliant PDS. In each case, these organizations were left unable to obtain authority to connect to the classified government network and exchange information necessary for the performance of their contracts. Over the years, NIS has seen this scenario on many occasions.

Solution

Fortunately, a new breed of Protective Distribution System is available today. Called Alarmed PDS or in some cases Alarmed-Armored-PDS™, all of the prior disadvantages of PDS which are most likely the reasons for its non-compliance, have been eliminated. This "Intelligent" PDS solution consists of the INTERCEPTOR™ Optical Network Security system from Network Integrity Systems and the CyberSecure Infrastructure Monitoring System (IMS) from CyberSecure IPS. This combined solution quickly and efficiently creates a centrally managed Alarmed Carrier PDS that is fully compliant with NSTISSI 7003, holds a Certificate of Networthiness (CON) and has been used to protect networks and provide ATOs in networks carrying data up to the TS/SCI level including SIPRNet, JWICS and in high threat level environments. INTERCEPTOR incorporates technology to monitor unused fibers within the cables requiring protection to detect unauthorized tampering with the infrastructure. Smart-filtering™ technology eliminates false alarms by learning the normal day-to-day activity within the environment. Cyber Secure IMS, enables centrally managed monitoring, situational awareness, site-specific standard operating procedure creation and case resolution audit trail generation, all of which simplifies Information Assurance Management. Together, this solution provides robust protection against physical infrastructure intrusion attempts.

Network Integrity SYSTEMS

We Bring Security To Light™

877.NIS.4PDS

Passing the PDS Inspection The First Time, Every Time

Both of the aforementioned contractors selected this solution to rapidly and cost-effectively solve their accreditation issues. From the Defense Security Systems (DSS) perspective, this solution made accreditation of the networks quick and easy as the CyberSecure software was able to implement the DSS Systems Security Plan template into a wizard where the user was walked through the compliance procedures, question and answers. This culminated in the presentation of a of a full PDS plan in PDF format that they could submit directly to the approval authority.

This combined solution resulted in both contractors gaining compliance and authority to connect to the secure government network within 30 days after making original contact with Network Integrity Systems. The Information System Security Managers responsible for these networks now have the ability to monitor and protect the physical security of their network infrastructure as well as implement site-specific NSTISSI 7003 compliant operating procedures and generate unique case resolution audit trails, simplifying information assurance management and PDS inspection. All of this is possible with no bandwidth constraints on the network and a total deployment cost that was significantly less than other alternatives.

Network Integrity Systems

WE BRING SECURITY TO LIGHT™

1937 Tate Boulevard, SE
Hickory, North Carolina 28602, USA
Call 877.647.4737

Network Integrity Systems (NIS) develops and manufactures products that enable organizations to protect their networks quickly and cost-effectively. Founded by optical engineers and management personnel from a global fiber optics leader, NIS has responded to the growing need to protect the confidentiality, integrity and availability of critical network infrastructures. NIS has spent the last 10 years as a leading innovator in this space and holds over 15 U.S. and International patents related to fiber optic network security and monitoring.