



TRANSMISSION OF INTRUSION DETECTION SYSTEM (IDS) DATA VIA ARMY LOCAL AREA NETWORKS (LANs)



By Craig Zeigler

In the U.S. Army, IDS data is, by regulation, transmitted via dedicated networks. Army Regulation (AR) 190-13, *The Army Physical Security Program*, states: "Transmission lines for the alarm circuits shall be electrically supervised and dedicated to minimize undetected tampering." The Office of the Provost Marshal General (OPMG) has clearly documented an interpretation of this policy statement to mean that transmitting IDS data over LANs or other shared systems is prohibited. This prohibition applies most notably to the Army installation level, where LAN connectivity typically extends to all facilities, making it an otherwise attractive choice for IDS data transmission.

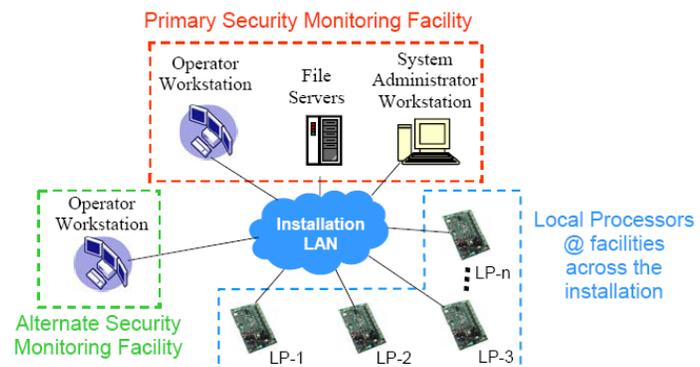
Regardless of the policy, employing dedicated, stand-alone networks truly provides the most secure routing of IDS signals. The reluctance to leverage anything other than a dedicated network for IDS data transmission is understandable, and using a dedicated, stand-alone data transmission system (DTS) should be the primary choice for IDS data. However, today's networking technologies provide other options for transmitting IDS data, including LANs, wide area networks (WANs), and even the Internet.

Provided specific conditions are met, data transmission outside of a dedicated network can be performed with a high degree of security and low risk, and it is important to note that the OPMG is considering revising AR 190-13 and AR 190-11

Physical Security of Arms, Ammunition, and Explosives to allow transmission of IDS data over networks that are not dedicated to the security system. The OPMG is considering this policy change to facilitate leveraging state-of-the-art networking technologies while dictating minimum functional and security

requirements for a DTS, regardless of the communications media and protocols used. The OPMG policy revision being considered will likely reflect the following provisions:

1. The primary choice for a DTS used to communicate IDS data is a stand-alone, autonomous, supervised network, operated and maintained by security personnel.
2. The DTS used to communicate IDS data shall assure complete data availability, confidentiality and integrity throughout the system, end-to-end. The DTS shall be secured against tampering, jamming, interception, interference and intrusion by employing line supervision, tamper detection and, when required by specific system security standards, data encryption.
 - A. The system shall supervise the signal lines by monitoring the circuit for changes or disturbances in the signal, and for conditions as described in Unified Facilities Guide Specification 28 20 01.00 10, *Electronic Security System* for line security equipment. The system shall initiate an alarm in response to a change or disturbance in the signal. The system shall also initiate an alarm in response to opening, closing, shorting, or grounding of the signal.
 - B. When encryption is required, IDS data shall be encrypted using a National Institute of Science and Technology (NIST) approved algorithm with a minimum of 128-bit encryption.
3. If a dedicated network is not available, achievable or deemed not cost effective, an alternative DTS may be used. An alternative DTS may consist of a LAN, WAN, wireless communications system or a combination of these technologies.



Concept for IDS Data Transmission via LAN at Army Installations



**TRANSMISSION OF INTRUSION DETECTION SYSTEM DATA
VIA ARMY LOCAL AREA NETWORKS (continued)**



The decision to employ an alternative DTS should be based on the results of a risk assessment conducted jointly by designated representatives of the installation commander, the using unit or activity, and the supporting installation provost marshal or equivalent security officer representative. The risk assessment shall be conducted in accordance with the requirements in AR 25-2 and be performed according to the guidance found in the NIST Special Publication 800-30, "Risk Management Guide for Information Technology Systems." The following provisions apply to the alternative DTS:

- A. The DTS must provide an equivalent, or higher, level of security for the IDS data compared to a dedicated network.
- B. Vulnerabilities identified during the risk assessment and corresponding mitigation measures must be documented.
- C. The Designated Approving Authority (DAA) accepts and approves the risk assessment report, including the mitigation measures identified and incorporated into the design and installation of the DTS.
- D. If a LAN is selected as the DTS, the LAN must have a minimum availability rating of 99.9%. This equates to a total yearly downtime of less than nine hours.
- E. If the selected DTS cannot achieve an equivalent, or higher, level of protection for the IDS data a dedicated network provides, a second independent means of communicating the data from the protected area to the monitoring station should be provided. The dual transmission equipment must continuously monitor the integrity of both links. Upon loss of either communications path, the system must immediately send a communications fault alarm to the monitoring facility via the active link and then automatically switch to this link for any subsequent IDS alarms.

Although shared networks offer potential for economical and effective IDS data transmission, it is clear that, until OPMG revises the applicable regulations, transmitting IDS data over an Army installation LAN, or any other network not dedicated to the security system, is prohibited. If future revisions to Army policy do allow the use of an alternative DTS, project planning and network integration will be the keys to success.

The Directorate of Information Management (DOIM) must be consulted early in the project planning phase when considering an installation LAN for transmitting IDS data. A few of the more important issues to resolve relative to the LAN infrastructure (cables, hubs, switches, routers, servers, etc.) are emergency backup power, physical & electronic protection, IDS data rate & latency, supervision & encryption of virtual IDS circuits, and priority of IDS data on the network. Another important topic to address with the DOIM is the DoD Information Technology Security Certification and Accreditation Process (DITSCAP) as it applies to IDS processors, file servers, workstations, and system software. Finally, the day-to-day operation and maintenance of the LAN, to include the technical and security qualifications of DOIM technicians, should be discussed.

*This article was extracted from the **Electronic Technology Systems Center Technical Bulletin**. To find more articles on best security practices and other information, visit our web site at <http://www.hnd.usace.army.mil/esc> and click on the Resources link.*