CYBER OPERATIONS NETWORKS
ANTI NETWORK TERRORISM
TEST REPORT

12 SEPTEMBER 2002
DISA CENTER FOR IA APPLICATIONS

PREPARED FOR:
CENTER FOR INFORMATION ASSURANCE ENGINEERING
AND THE DISA INFORMATION ASSURANCE EXECUTIVE

Executive Summary

Background. Cyber Operations Anti Network Terrorism (A.N.T.) was tested and evaluated during August 2002 for deployment in the internet-NIPRNET gateway. The purpose of the testing was to:

Assess interoperability and interface compatibility with existing architecture
Assess any risk to network operations, including security evaluation of the A.N.T. system
Assess the detection operating characteristics of the A.N.T. system for specific denial of service (DOS) attacks
Assess the device management characteristics of the A.N.T. system
Assess the filter management characteristics of the A.N.T. system

Results. Testing and evaluation was satisfactorily completed on 9 August 2002. Major findings are as follows:

The system is interoperable with the existing architecture and leverages existing data capture functions.
The system does not introduce any measurable risk to operations or security vulnerabilities
The system is capable of threshold device management
The system is capable of threshold filter management
The system can successfully detect, in near-real time, specific DOS and DDOS attacks
The system produces an automated mechanism for creating access control entries that can counter the DOS attack

Recommendation. The system is recommended for further testing when OC-3 interfaces and Juniper compatibility are available. It can provide detection capabilities that are not currently available in the existing network. The DISA managed DOD network regions are the appropriate locations for early indication and warning of DOS attacks against network service subscribers.

The filter management system performed very well. The ability to merge existing filter lists and manage multiple filters lists is a key requirement. The A.N.T. filter management system does need to incorporate Juniper devices and a more granular (i.e. line by line) filter merging tool to meet the current requirements.

The device management system also performed well. The potential to perform world-wide configuration changes, regardless of the type of device, is most impressive.