NOTE: Because this report assesses potential vulnerabilities in IT security, only a summary of the report is posted.

Report Title: Audit of NARA's Network Perimeter
Report Number: 06-01
Date Issued: December 15, 2005

Audit of NARA's Network Perimeter

The NARA OIG performed an audit of NARA's network perimeter[1] to determine whether the controls surrounding the boundary of NARA's network (NARAnet) provide reasonable protection from external intruders.

Our audit revealed that NARA's network perimeter security was not adequate and exposed the agency to significant information security risks. This condition existed because management has not adopted, incorporated, and enforced pertinent standards promulgated to reduce risk to an acceptable level. Numerous NIST Special Publications, highlighted in the detailed findings, document the minimum requirements that should be considered, implemented, and tested concerning local and wide area network perimeter security. When the network perimeter is not adequately protected, not only does the risk of intrusion increase, but the network is more vulnerable to nefarious individuals or groups seeking to harm the network infrastructure.

We made eight recommendations to improve and secure NARA's network perimeter security. Management concurred with all but one recommendation and promptly initiated management action to address our recommendations.

[1] A perimeter is the fortified boundary of the network that might include routers, firewalls, IDSs, VPN devices, software, DMZs, and screened subnets.