Core Assurance and Physical Security

Issue Background

The core network is defined as the variety of components that together form the communications infrastructure that consumers, businesses, and the Federal Government utilize on a day-to-day basis. The networks are not only critical to the continued operation of business and Government, but also to national security and emergency preparedness (NS/EP) communications. Without this infrastructure, communications can become difficult or impossible. To ensure continuity of communications, it is essential to maintain and protect the infrastructure from situations which could harm or disable them. Recent national and international events have shed light upon the importance of ensuring the physical security of the core network.

History of NSTAC Actions

In 1990 the President's National Security Telecommunications Advisory Committee (NSTAC) began an examination of the physical security of the public switched network and coordinated with the National Communications System (NCS) to investigate physical security of the telecommunications infrastructure due to issues surfaced by a National Research Council report on the growing vulnerability of the Nation's communications network. The study included results from a questionnaire given to the National Coordinating Center's industry representatives on physical security policy, operational procedures, and methods, and also documented past NCS efforts regarding physical security of NS/EP telecommunications facilities, sites, and assets and relevant conclusions and recommendations of those past efforts.

The NSTAC again addressed physical security concerns of the telecommunications infrastructure during the business and executive sessions of the April 2003 NSTAC Meeting, resulting in the creation of the Vulnerabilities Task Force (VTF). Through the VTF, the NSTAC submitted four reports to the President addressing various topics regarding concentrated telecommunications assets: *Chain of Control, Telecom Hotels, Trusted Access, and Internet Peering Security*. In direct response to the *Vulnerabilities Task Force Report on Trusted Access*, the NSTAC began an examination of how industry and Government can work together to address concerns associated with implementing a national security background check program for access to key facilities. The examination resulted in the establishment of a pilot program to use Federal terrorist lists and Government databases to pre-screen a small group of industry employees who may need access to physical sites or critical information concerning national special security events and associated facilities.

Recent NSTAC Activities

In response to a request from the Executive Office of the President, in 2008, the NSTAC began to examine infrastructure threats and issues concerning physical security of the core network to re-educate Government stakeholders and determine what, if any, mitigation measures the Government can implement to assure physical security of the core network and its key functions. The NSTAC developed the *NSTAC Report to the President on Physical Assurance of the Core Network* and an accompanying Appendix, which it approved in November 2008 and February 2009, respectively.

For more information on the NSTAC, visit www.ncs.gov/nstac/nstac.htm or call (703) 235-5525.