Commercial Satellite Survivability

Issue Background

Industry and the Government increasingly rely on the satellite infrastructure for data, voice, and video communications and services. The national security and homeland security communities use satellites for critical activities such as military support, intelligence gathering, and disaster preparedness. The Government uses satellite communications nationally and globally. Although the *Homeland Security Act of 2002* recognizes satellite infrastructure as a critical infrastructure, previous security issues regarding national security and emergency preparedness (NS/EP) satellite programs focused on providing an alternative means of communications under nuclear attacks.

History of NSTAC Actions

At its first formal meeting on December 14, 1982, the President's National Security Telecommunications Advisory Committee (NSTAC) established the Commercial Satellite Survivability (CSS) Task Force to assess the vulnerability of the commercial satellite communications network and to determine what enhancements commercial carrier satellites and Earth terminals could provide to the NS/EP telecommunications infrastructure. The NSTAC's examination of select Federal satellite initiatives resulted in the development of a 12-point plan for improving the survivability and robustness of commercial satellite communications resources. In 1987, based on NSTAC recommendations, the Government established the Commercial Satellite Communications (SATCOM) Interconnectivity (CSI) Program Office, which proposed objectives for employing new commercial SATCOM technologies in emergency environments. The NSTAC reviewed these proposals, concluded that the program's approach was reasonable, and recommended steps the Government should take to improve access to and interoperability of satellite communications in the United States and abroad.

In 2003, the Director, National Security Space Architect, asked the NSTAC to examine ways industry and Government could mitigate satellite infrastructure vulnerabilities and to determine whether foreign satellite ownership posed a security risk. After engaging satellite owners and operators, trade associations, Government agencies, and other technical experts, the NSTAC recommended that the President direct Federal officials to develop commercial SATCOM provisioning and management policies in recognition of industry's unique capabilities it provides to military, diplomatic, and homeland security missions. The White House included several of these recommendations in its 2004 revision of the National Space Policy.

Recent NSTAC Activities

The NSTAC's 2004 recommendations primarily addressed infrastructure vulnerabilities and provided a cursory look at risks to the global positioning system (GPS). At the 2007 NSTAC Meeting, the NSTAC determined the issue warranted further investigation. The NSTAC's Industry Executive Subcommittee established the GPS Working Group in June 2007 to examine the commercial communications industry's use of and reliance on GPS and the impact that loss or degradation of GPS signals would have on commercial communications networks and operations.

For more information on the NSTAC, visit www.ncs.gov/nstac/nstac.htm or call (703) 235-5516.