THE PRESIDENT'S
NATIONAL SECURITY TELECOMMUNICATIONS
ADVISORY COMMITTEE

SATELLITE TASK FORCE REPORT

FACT SHEET

February 2004

EXECUTIVE SUMMARY

In January 2003, the Director, National Security Space Architect, requested that the President's National Security Telecommunications Advisory Committee (NSTAC) consider embarking on a study of infrastructure protection measures for commercial satellite communication (SATCOM) systems. The NSTAC established the Satellite Task Force (STF) to review and assess policies, practices, and procedures for the application of infrastructure protection measures to commercial SATCOM networks used for national security and emergency preparedness (NS/EP) communications. Specifically, the STF was established to (1) review applicable documentation addressing vulnerabilities in the commercial satellite infrastructure, (2) identify potential policy changes that would bring the infrastructure into conformance with a standard for mitigating those vulnerabilities, (3) consider Global Positioning System (GPS) timing capabilities during the deliberations, (4) coordinate this response with representatives from the National Communications System (NCS) and others, and (5) draft a task force report with findings and recommendations.

The STF engaged broad and active participation from representatives of NSTAC member companies, non-NSTAC commercial satellite owners and operators, commercial satellite trade associations, Government agencies, and technical experts. The task force examined all types of commercial SATCOM systems, including Fixed Satellite Service, Broadcast Satellite Service, Mobile Satellite Service, and Satellite Digital Audio Radio Service. To gain a broad understanding of vulnerabilities, the STF compared the difficulty of potential threats against the degree of susceptibility of key elements in these services, including the radio frequency links, ground segment, cyber segment, and space segment.

The STF conducted two surveys to contribute to the task force's understanding of Federal agency use of commercial SATCOM systems and services for NS/EP, as well as vulnerabilities in that infrastructure. With the assistance of the NCS, 14 Federal departments and agencies provided input on their use of commercial satellites and services, backup communications plans, and anticipated communications requirements. As part of its contribution to the STF, the Satellite Industry Association surveyed its member satellite operators to provide a voluntary self-assessment of the industry's vulnerabilities and mitigation techniques currently in use. The Federal agencies and satellite operators were very responsive to the surveys, providing valuable input to the task force work.

Although commercial SATCOM is important to NS/EP communications, the task force found that the Government does not fully optimize or protect the satellite infrastructure. Within civil agencies there is a shortage of in-house technical expertise that can integrate satellite communications into their network architectures, and agency procurement processes do not allow them to compete effectively for commercial SATCOM capacity.

In its satellite infrastructure vulnerability analysis, the task force found that all components of commercial satellite systems are susceptible to intentional and

unintentional threats to varying degrees. While the satellite industry has already taken steps to ensure that the security of the infrastructure adequately protects its commercial business interests, individual Federal agencies must decide which additional mitigation techniques to require and whether their missions make it necessary to actively address the less likely and more expensive threats. In addition, the task force found that the Government does not have an adequate proactive information assurance policy.

Based on its STF analysis and review of related policy issues, the NSTAC recommends, in accordance with responsibilities and existing mechanisms established by Executive Order 12472, *Assignment of National Security and Emergency Preparedness Telecommunications Functions,* and other existing authority, that the President—

- Direct the Assistant to the President for National Security Affairs, Assistant to the President for Homeland Security, and Director, Office of Science Technology Policy, to develop a national policy with respect to the provisioning and management of commercial SATCOM services integral to NS/EP communications, recognizing the vital and unique capabilities commercial satellites provide for global military operations, diplomatic missions, and homeland security contingency support.
- Fund the Department of Homeland Security to implement a commercial SATCOM NS/EP improvement program within the NCS to procure and manage the non-Department of Defense satellite facilities and services necessary to increase the robustness of Government communications.
- Appoint several members to represent service providers and associations from all sectors of the commercial satellite industry to the NSTAC to increase satellite industry involvement in NS/EP.

To guide rapid implementation of these recommendations with specific steps to secure the commercial SATCOM infrastructure for NS/EP, the task force provided the framework of an action plan for Federal departments and agencies. To improve NS/EP policy, the task force suggested the establishment of a steering committee to examine how commercial SATCOM can best be used in operational support role to the *National Response Plan*, study satellite technology export controls and their impact on the economic stability of the domestic satellite industry, and reevaluate domestic and foreign policies on the use of commercial SATCOM in support of NS/EP missions.

To increase the robustness of Government communications through better use of commercial SATCOM, the task force suggests the following actions: (1) maintain awareness of commercial SATCOM usage within the Federal Government enabling decision makers to rapidly prioritize commercial satellite services required to support NS/EP needs; (2) extend the purview of the Telecommunications Service Priority to all fixed satellite service operators and extend the Wireless Priority Service model to mobile satellite operators; and (3) develop, in coordination with the commercial satellite industry, a strong and proactive information assurance policy to further reduce the vulnerability of command and control links.

Furthermore, the task force suggests actions to mitigate vulnerabilities in the SATCOM infrastructure. These suggestions include conducting studies on physical vulnerabilities, identifying a systemwide hierarchy of physical and cyber vulnerabilities to terrorist attack, developing a plan and process to rapidly mitigate interference, and developing security requirements commensurate with NS/EP communications needs.

TASK FORCE MEMBERS, OTHER PARTICIPANTS, GOVERNMENT PARTICIPANTS, AND BRIEFERS

Task Force Members

Mr. Bob Britton (STF Co-Chair)	Lockheed Martin
Mr. Shawn Cochran (GPS Subgroup Chair)	BellSouth
Mr. Alan Goldey	Raytheon
Ms. Joan Grewe	MCI
Mr. Peter Hadinger (STF Vice Chair)	Northrop Grumman
Mr. Ken Kato	Rockwell Collins
Mr. Hank Kluepfel (Classified Subgroup Chair)	SAIC
Mr. Ben LaPointe	Motorola
Ms. Rosemary Leffler	SBC
Mr. Jon Lofstedt (GPS Subgroup Vice Chair)	Qwest
Mr. William Reiner (STF Co-Chair)	Boeing

Other Industry and Nongovernmental Participants

Mr. Steve Adelmann	Lockheed Martin
Mr. Carson Agnew	Mobile Satellite Ventures
Mr. Bob Berry	Loral
Ms. Leslie Blaker (Use Subgroup Co-Chair)	SES Americom
Mr. Don Brown (Use Subgroup Co-Chair)	PanAmSat G2 Satellite Solutions
Mr. Richard Buenneke	The Aerospace Corporation
Mr. David Cavossa	Satellite Industry Association
Mr. D. D'Ambrosio	Loral
Mr. Richard Dalbello	Satellite Industry Association
Dr. Al Dayton (Vulnerabilities Subgroup Chair)	Lockheed Martin
Mr. Jack Deasy	Inmarsat
Mr. Amir Dehdasty	Hughes Net Systems
Mr. Robert Demers	Inmarsat
Mr. Brian Deobald	Mobile Satellite Ventures
Mr. Pat Fagan	Spacenet
Dr. Edward Jacques	MITRE
Mr. Joe Jankowski	Intelsat
Mr. Michael Kelley	Intelsat
Dr. Jack Oslund	The George Washington University
Ms. Kay Sears	Verestar
Mr. Robert Steele	Boeing
Mr. John Stern	Loral

Government Participants

LCDR R. Bronson Armstrong	National Security Space Architect
Mr. Dale Barr	National Communications System
Mr. Richard Bourdon	Defense Information Systems Agency
Ms. Sabrina Crane	General Services Administration
Mr. Tom Falvey	National Communications System
Ms. Linda Haller[1]	Federal Communications Commission
Mr. Mark LeBlanc	Office of Science and Technology Policy
Maj Robert Licciardi	U.S. Strategic Command
Mr. Gabriel Martinez	National Communications System
Ms. Hillary Morgan	Defense Information Systems Agency

[1] *Ms. Haller provided only technical expertise to the STF efforts.*

Mr. Thomas Sellers	General Services Administration
Mr. Steven Shirley	U.S. Strategic Command
Mr. Hollace Twining	Department of Transportation

Briefers

Dr. Edward Conrad	Institute of Defense Analyses
Lt Col Timothy Deaver	Office of the Undersecretary of the Air Force
Dr. Michael Frankel	Commission to Assess the Threat to the United States from an Electromagnetic Pulse Attack
Mr. John Gass	National Intelligence Council
Mr. David Jarrell	General Services Administration
Mr. Ronald Kidwell	National Security Agency
Mr. Michael Ware	The Aerospace Corporation