Network Convergence

Issue Background

Telecommunications carriers began developing cost-effective packet networks to remain competitive in the evolving telecommunications marketplace and to support wide-scale delivery of diverse advanced broadband services. Their large investments in the circuit switched network infrastructure, however, led carriers to leverage the best of both infrastructures during the transition to the next generation network (NGN), resulting in a period of network convergence. The President's National Security Telecommunications Advisory Committee (NSTAC) recognizes industry and the Government must strive to identify and remedy associated network vulnerabilities in this evolving network environment to ensure sustained critical communications capabilities of the national security and emergency preparedness (NS/EP) community.

History of NSTAC Actions

The NSTAC has established several task forces since 1999 to assess infrastructure, security, and operational vulnerabilities stemming from network convergence and to provide recommendations to mitigate those vulnerabilities. The Information Technology Progress Impact Task Force examined the potential implications for existing NS/EP services (e.g., Government Emergency Telecommunications Service and Telecommunications Service Priority) resulting from Internet protocol network and public switched telephone network (PSTN) convergence. A year later, the Convergence Task Force concluded the PSTN was increasingly vulnerable as a result of its convergence with packet networks; such vulnerabilities and possible points of failure could impact service availability and reliability essential to NS/EP operations; and the Government must remain actively engaged in the ongoing standards development efforts supporting NS/EP priority requirements. Accordingly, the NSTAC encouraged Government participation in additional exercises, assessing potential vulnerabilities in the emerging public network (PN) and subsequent NS/EP implications on a national and international basis, and use of the Telecommunications Information Sharing and Analysis Center to facilitate information sharing related to network data and vulnerabilities.

In addition to task force activity, the NSTAC co-sponsored its fourth Research & Development Exchange Symposium, focusing on network convergence issues, in September 2000. Representatives from industry, the Government, and academia met to discuss the many challenges posed by network convergence and made several recommendations to the Government and the NSTAC. As a result, the NSTAC incorporated many of these suggestions into its work on network convergence and the NGN.

Recent NSTAC Activities

In 2001, the NSTAC Industry Executive Subcommittee established the Network Security/Vulnerability Assessments Task Force (NS/VATF) to address the public network policy and technical issues associated with network disruptions and the security and vulnerability of the converged network control space. The NS/VATF stressed the importance of industry/Government efforts to devise countermeasures and strategies aimed at mitigating the impacts of physical and cyber attacks on the PN and other critical infrastructures. The NSTAC will continue to monitor network convergence and its impact on NS/EP communications.