Cybersecurity

Issue Background

The Nation's increasing reliance on globally interconnected information technology systems heightens the risk of cyber threats to critical infrastructure and key resources and overall national security. Securing cyberspace and critical communications infrastructure requires a systematic, joint approach between Government and the private sector to mitigate these risks.

History of NSTAC Actions

Recognizing that the public and private sectors have engaged in efforts to address emerging cyber concerns, the President's National Security Telecommunications Advisory Committee (NSTAC) has undertaken multiple efforts to improve Government and industry collaboration to secure cyberspace. In February 1990, the NSTAC established the Network Security Task Force—renamed the Network Security Group in 1994—to examine network software security. It later sponsored the Network Security Research and Development Exchange Workshop to analyze research and development issues related to authentication, intrusion detection, and access control across the public and private sectors. In 2004, the NSTAC also created the Next Generation Networks (NGN) Task Force to identify threats to NGN and recommend areas for greater Government involvement.

In 2004, the NSTAC began to examine the key role of cybersecurity information sharing between the public and private sectors. The NSTAC created the National Coordinating Center (NCC) Task Force to study the growing role of cybersecurity in the traditional telecommunications mission of the NCC. The result of this effort was the 2006 *NSTAC Report to the President on the National Coordinating Center*, which recommended the establishment of a joint coordinating center (JCC) for round-the-clock operational collaboration and information sharing on cybersecurity between public and private sector participants.

Following on this recommendation and at the request of the Executive Office of the President, the NSTAC launched the Cybersecurity Collaboration Task Force (CCTF) in 2008 to further examine the need for and feasibility of creating a joint, public-private operational capability for cyber detection, prevention, mitigation, and response (DPMR). In 2009, the NSTAC subsequently recommended that the President direct the phased development of an integrated JCC with public and private sector representatives to promote information sharing and collaboration on cyber DPMR activities. The report further recommended that the Government fund this JCC and designate a Federal department or agency to permanently house the capability, building upon the current integration of the NCC and the United States Computer Emergency Readiness Team.

Recent NSTAC Activities

In March 2009, the Obama Administration asked the NSTAC to respond to four questions to inform its Cyberspace Policy Review. In its *NSTAC Response to the Sixty-Day Cyber Study Group*, the NSTAC reiterated several past recommendations, including those on the need for greater Federal integration of cybersecurity activities, new structures for timely and secure information sharing, a secure, responsive, and extensible identity management framework, new legal and regulatory initiatives, enhanced research and development efforts for critical cybersecurity capabilities, and the development of international cyber incident warning and response capabilities, among others.

In July 2009, as a continuation of the CCTF's efforts, the NSTAC initiated a study to identify specific information sharing, analysis, and collaboration frameworks and mechanisms that would support the creation of the previously recommended JCC. The data gathered from this study will be implemented within current private sector domains and relationships and potentially used as an information sharing, analysis, and collaboration pilot program for further consideration.