



Issue Background

The private sector owns and operates the vast majority of critical infrastructures in the United States. Protecting these infrastructures from natural and man-made disasters therefore requires a mutual commitment between industry and Government to freely exchange critical information in a timely manner. This free flow of information helps industry and the Government better determine where infrastructure vulnerabilities exist and prevent damage to key infrastructure assets. The President's National Security Telecommunications Advisory Committee (NSTAC) has closely studied public and private sector information sharing and has itself served as a model for information sharing for 25 years.

History of NSTAC Actions

As a direct result of an NSTAC recommendation, President Ronald Reagan established the National Coordinating Center (NCC) for Telecommunications in 1984 to facilitate the coordination of national security and emergency preparedness (NS/EP) telecommunications restoration and provisioning. In 2000, the National Security Council (NSC) concurred with another NSTAC recommendation to designate the NCC as the Telecommunications Information Sharing and Analysis Center (ISAC), which has been a key function of the NCC since 2001. NSTAC's information sharing proposals also extended to network security, and in 1990, the NSC requested National Communications System (NCS) identify ways Government and industry could protect critical national security telecommunications from the "hacker" threat. In response to the NSC tasking, the NCS and the NSTAC established separate, but closely coordinated Network Security Information Exchanges, which provide participants access to information resources within the intelligence, international, law enforcement and academic communities, and the ISACs.

A number of NSTAC efforts have centered on assessing legal and regulatory obstacles to sharing critical infrastructure information (CII) and monitoring the evolution of the NCC as the Telecommunications ISAC. In 1999, the NSTAC examined legal and regulatory obstacles to sharing telecommunications outage and intrusion information and the success of the *Year 2000 (Y2K) Readiness and Disclosure Act* as a catalyst for information sharing within industry. After an evaluation of the NCC's Y2K preparedness efforts, the NSTAC recommended the President support legislation that would protect CII voluntarily shared with the Government from disclosure under the *Freedom of Information Act (FOIA)*. Congress granted statutory FOIA exemptions for CII and liability protection for CII providers in the *Homeland Security Act of 2002*, and the NSTAC has continued to monitor the implementation of that provision by the Department of Homeland Security. In 2003, the NSTAC's *Barriers to Information Sharing Report* recommended the Federal Government establish similar CII sharing arrangements between industry and other Federal departments and agencies.

Recent NSTAC Activities

The NSTAC continues to promote a trusted environment for sharing information as threats and technology evolve in an increasingly interdependent global network. In 2006, NSTAC recommended ways to address various communications issues that arose during the response to Hurricane Katrina and ways the NCC should evolve in the changing technological environment. It also called for more comprehensive international NS/EP communications policies that address information sharing in next generation networks.