NSTAC: Forty Years of Service

For forty years (1982-2022), the President's National Security Telecommunications Advisory Committee (NSTAC) has provided industry-based advice and expertise to the president of the United States on the reliability, security, and preparedness of vital communications and information infrastructure. Due to the advanced industry knowledge of its members—and the government officials who partner with them—the NSTAC provides national security and emergency preparedness (NS/EP) solutions by providing innovative policy advice backed by unique industry perspective. This creates a more secure and resilient communications infrastructure for the American people. The NSTAC's partnership with government is facilitated through the Cybersecurity and Infrastructure Security Agency's (CISA) Stakeholder Engagement Division (SED), a government-industry coordination center for day-to-day operational NS/EP communications support. SED coordinates stakeholder engagements and partnerships to manage key relationships and support CISA's efforts to reduce national risk.

Since its inception, the NSTAC has advised seven presidents and eleven administrations and has proven itself vital to responding to challenges affecting the Nation. The NSTAC's public-private partnership has proven effective over the course of the past 40 years as a model for fostering cooperation and trust, not only among industry participants, but also between industry and the government. Its record of accomplishments includes substantive recommendations to the president that have led to enhancements of the Nation's NS/EP communications, critical infrastructure policies, and related information systems security posture. Enhancements in the form of operational programs and policy solutions benefit both industry and government as security requirements of the future become increasingly more important and more difficult to achieve.

NSTAC Member Meeting at the Eisenhower Executive Office Building, Indian Treaty Room in November 2019.

In this time of increased awareness of the criticality of and nexus between communications, technology, and national security, the NSTAC's work over the past 40 years highlights the importance of its advice to administrations and response to incidents affecting national security. As threats to the Nation's critical information infrastructure increase, the NSTAC is well positioned to continue to serve the Nation's interests and safeguard the American people. The NSTAC, in keeping with its long, supportive history, will continue to be a fundamental building block and model for public-private collaboration, and provide essential national security guidance to the government now and in the future.

RECENT ACCOMPLISHMENTS

In May 2021, the Executive Office of the President tasked the NSTAC with a study on "Enhancing Internet Resilience [EIR] in 2021 and Beyond" to examine: software assurance; zero trust (ZT) networking and trusted identity management; the convergence of information technology and operational technology (IT/OT); and a strategy for increasing trust in the information and communications technology (ICT) and services ecosystem.

- In November 2021, the NSTAC approved the phase I *NSTAC Report to the President on Software Assurance in the Information and Communications Technology and Services Supply Chain*, which offers recommendations to secure software development lifecycle processes and deploy supply chain risk management best practices for mission-critical networks.
- In February 2022, the NSTAC approved the phase II *NSTAC Report to the President on Zero Trust and Trusted Identity Management* which offers guidance and recommendations that recognize the U.S. government's broad opportunity and responsibility to help catalyze cybersecurity transformation through ZT adoption.
- In August 2022, the NSTAC approved the phase III *NSTAC Report to the President on Information Technology and Operational Technology Convergence* on which identifies opportunities for the federal government to aid in a secure IT/OT convergence within all relevant stakeholder communities.

Furthermore, in November 2021, the EOP tasked the NSTAC with developing a letter to outline recommendations on how government and industry can work together to preserve the widespread use of the industry-driven standards development model and enhance U.S. competitiveness through effective participation in global standards bodies. In May 2022, the committee approved the letter which outlines the NSTAC's key observations regarding the current state-of-play of ICT standards development. Additionally, the letter includes the NSTAC's key takeaways and recommendations on how to preserve and enhance U.S. competitiveness through participation in standards bodies and the appropriate role for government.

NOTABLE ACCOMPLISHMENTS

NSTAC activities are the genesis for many technical reports, presidential level recommendations, and NS/EP operational programs. Since its inception, the NSTAC has examined a multitude of issues, including network resilience and convergence; commercial satellite survivability; cybersecurity; intrusion detection; emergency communications and interoperability; and information system, network, and wireless services security. The government has acted on many of the NSTAC's recommendations, which have culminated in successes such as:

National Coordinating Council (NCC)

- Acting as a government-industry coordination center for day-to-day operational NS/EP communications support, the NCC was officially recognized as the Communications Sector Information Sharing and Analysis Center in January 2000, and later integrated into the National Cybersecurity and Communications Integration Center (NCCIC), a 24-hour coordinated information sharing and incident response capability designed to protect and secure the Nation's cyber infrastructure. The NCCIC and NCC are now implemented as part of CISA's Central hub.

Cybersecurity Moonshot Report

- A call to action from NSTAC to the government with a goal to "make the Internet safe and secure for the functioning of government and critical services for the American people by 2028." This plan recommended a whole-of-nation cybersecurity strategy to promote national cyber resilience and restructure the cyber ecosystem to make it safer and more secure. Parts of this report were adopted by The Foundation for Defense of Democracies (FDD) in their 2022 Annual Report. FDD is a non-profit that was formed out of the U.S. Cyberspace Solarium Commission.

NSTAC Report to the President on Emerging Technologies Strategic Vision

- A strategic plan presented to the president to modernize ICT networks with an emphasis on leveraging specific technologies including 5G, the Internet of Things, quantum computing, artificial intelligence, and software-defined networking.

ICT Supply Chain Risk Management Task Force

- As the government's highest profile public-private group addressing ICT supply chain security issues, the task force identifies actionable steps for risk management within the global ICT supply chain.

Telecommunications Service Priority System

- The regulatory, administrative, and operational authority that enables priority provisioning and restoration of telecommunications services.
- Adopted by CISA to provide end-to-end communications priority via three services: Government Emergency Telecommunications Service, Wireless Priority Service, and Telecommunications Service Priority.

Network Security Information Exchanges

- Government and industry meet bimonthly to voluntarily share information on related to threats posed to the public network when system vulnerabilities are exploited.