NSTAC FACT SHEET

OVERVIEW

The President's National Security Telecommunications Advisory Committee (NSTAC) provides industry-based analyses and recommendations to the Executive Office of the President (EOP) on how the government can enact policy for, or take actions to, enhance national security and emergency preparedness (NS/EP) telecommunications.

The NSTAC comprises up to 30 presidentially appointed senior executives representing diverse sectors of the telecommunications industry. This committee provides recommendations to the president on matters encompassing telecommunications, information systems, cybersecurity, infrastructure protection, and other NS/EP considerations. The NSTAC meets four times per year to deliberate on its endeavors.

HISTORY AND AUTHORIZATION

In September 1982, President Ronald Reagan created the NSTAC through Executive Order 12382, *President's National Security Telecommunications Advisory Committee*, to advise the president on matters regarding NS/EP telecommunications. Four issues prompted the establishment of the NSTAC: (1) the divestiture of AT&T, Inc.; (2) increased government reliance on commercial communications; (3) potential impact of new technologies on NS/EP telecommunications; and (4) the growing importance of command, control, and communications to military and disaster response modernization.

NOTABLE ACCOMPLISHMENTS

The NSTAC's work serves as the foundation for numerous technical reports, presidential recommendations, and NS/EP operational initiatives. Throughout its existence, the NSTAC has explored topics such as network and communication resiliency, security through zero-trust architecture, and the safe and effective integration of information and operational technologies. Many of the NSTAC's recommendations have led to government actions, including:

- **National Coordinating Center for Communication (NCC):** A public-private coordination center for day-to-day operational NS/EP communications support, NCC continuously monitors national and international incidents and events that may impact emergency communications.
- **Telecommunications Service Priority System:** The regulatory, administrative, and operational authority that enables priority provisioning and restoration of telecommunications services of NS/EP related organizations.
- **Network Security Information Exchanges (NSIE):** Through the NSIE, government and industry members meet bimonthly to voluntarily share information related to threats against critical telecommunications networks. Based on the United States' success with the NSIE model, and its value as an information sharing forum, Australia, Canada, New Zealand, and the United Kingdom have established NSIE-like groups of their own.
- **Information and Communications Technology (ICT) Supply Chain Risk Management Task Force:** The government's highest profile public-private partnership addressing ICT supply chain security issues, the task force identifies actionable steps for risk management within the global ICT supply chain.

THE NSTAC AT WORK

CYBERSECURITY BEST PRACTICES

In March 2024, the NSTAC voted to approve the _NSTAC Report to the President on Measuring and Incentivizing the Adoption of Cybersecurity Best Practices_. This report provided the Executive Office of the President 12 key findings and 30 recommendations aimed at narrowing the gap between critical infrastructure's current preparedness against cyberattacks and evolving threats through economic incentives, liability reforms, regulatory simplification, and effective cybersecurity measurements.

DYNAMIC SPECTRUM SHARING

In March 2024, the NSTAC voted to approve the _NSTAC Letter to the President on Dynamic Spectrum Sharing_. In this letter, the NSTAC provided findings and recommendations to guide the administration as the National Spectrum Strategy is implemented. The letter advised on a whole-of-nation approach to advance the national dynamic spectrum framework, including through the establishment of a transparent implementation plan with an aggressive timeline that accommodates both commercial and national security interests.

ABUSE OF DOMESTIC INFRASTRUCTURE

In September 2023, the NSTAC voted to approve the _NSTAC Report to the President on Addressing the Abuse of Domestic Infrastructure by Foreign Malicious Actors_. The report identified six actionable recommendations and eleven key findings to aid in mitigating the abuse of domestic infrastructure by foreign malicious actors. Through the NSTAC's recommendations, government and industry stakeholders can improve the shared public-private effort to collaborate and combat abuse of domestic infrastructure while maintaining a voluntary, private sector-driven operational model.

SECURING NEXT-GENERATION WIRELESS

In September 2023, the NSTAC voted to approve the _NSTAC Letter to the President on Securing Next Generation Wireless Telecommunications_. In this letter, the NSTAC issued recommendations and insights to improve U.S. competitiveness and maintain leadership in next-generation wireless telecommunications. Recommendations included developing a wireless spectrum strategy to deploy next-generation networks, supporting Open Radio Access Networks, and supporting industry led standards models.

For more information on the NSTAC's completed studies, visit our publications page.

MEMBERS AND LEADERSHIP

The NSTAC chair and vice chair are appointed by the president from current NSTAC membership. Mr. Scott Charney, Vice President for Security Policy, Microsoft, serves as the NSTAC Chair, and Mr. Jeffrey Storey, Senior Advisor to the Lumen Board and Chief Executive Officer (CEO), Lumen Technologies, serves as the NSTAC Vice Chair.

NSTAC CHAIR
Mr. Scott Charney
Vice President for Security Policy
Microsoft

NSTAC VICE CHAIR
Mr. Jeffrey Storey
Senior Advisor to the Lumen Board
and the CEO
Lumen Technologies, Inc.

Mr. Peter Altabef
Chair and CEO
Unisys Corp.

Mr. Johnathon Caldwell
Vice President and General
Manager, Military Space
Lockheed Martin Space

Mr. Mark Dankberg
Chair, CEO, and Co-Founder
Viasat

Ms. Noopur Davis
Executive Vice President and Chief
Information Security and Product
Privacy Officer
Comcast and Comcast Cable

Mr. Matthew Desch
CEO and Member of the Board
Iridium Communications, Inc.

Mr. David DeWalt
Founder and Managing Director
NightDragon Management
Company

Mr. Raymond Dolan
Chair and CEO
Cohere Technologies, Inc.

Mr. John Donovan
Lead Independent Director
Palo Alto Networks, Inc.

Dr. Joseph Fergus
Founder, President, and CEO
Communication Technologies, Inc.

Mr. Patrick Gelsinger
CEO and Member of the Board
Intel Corporation

Ms. Lisa Hook
Managing Partner
Two Island Partners, LLC

Mr. Jack Huffard
Co-Founder and Member of the
Board
Tenable Holdings, Inc.

Ms. Barbara Humpton
President and CEO
Siemens USA

Ms. Renée James
Founder, Chair, and CEO
Ampere Computing, LLC

Ms. Kimberly Keever
Chief Information Security Officer
Cox Communications

Mr. Kyle Malady
CEO
Verizon Business

Mr. Kevin Mandia
CEO
Mandiant

Ms. Maria Martinez
Chief Operating Officer (COO)
Cisco

Mr. Jeffery McElfresh
COO
AT&T Communications

Mr. Bryan Palma
CEO and Member of the Board
Trellix

Mr. Neville Ray
President of Technology
T-Mobile

Mr. Angel Ruiz
Chair, MediaKind
Director, Nsight

Mr. Stephen Schmidt
Chief Security Officer
Amazon

Mr. Hock Tan
President, CEO, and Director
Broadcom, Inc.

Mr. Corey Thomas
CEO and Chair
Rapid7