



PRESIDENT'S NATIONAL SECURITY TELECOMMUNICATIONS ADVISORY COMMITTEE



FACT SHEET

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 is authorized to be composed of up to 30 presidentially appointed senior executives who represent various elements of the telecommunications industry. The committee advises the president on a wide range of issues related to telecommunications, information systems, information assurance, infrastructure protection, and other NS/EP concerns. The NSTAC meets quarterly to discuss its activities.

BACKGROUND

In September 1982, President Ronald Reagan created the NSTAC by 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.

PAST NSTAC ACCOMPLISHMENTS

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

- **National Coordinating Center (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 the Cybersecurity and Infrastructure Security Agency (CISA) Central hub.
- **Telecommunications Service Priority System:** The regulatory, administrative, and operational authority that enables priority provisioning and restoration of telecommunications services.
- **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.
- **Information and Communications Technology (ICT) Supply Chain Risk Management Task Force:** 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.



PRESIDENT'S NATIONAL SECURITY TELECOMMUNICATIONS ADVISORY COMMITTEE



FACT SHEET

RECENT NSTAC ACTIVITIES

In May 2021, the EOP 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 (OT); and a strategy for increasing trust in the ICT and services ecosystem.

- Phase I (November 2021): Offers recommendations to secure software development lifecycle processes and deploy supply chain risk management best practices for mission-critical networks.
- Phase II (February 2022): Offers guidance and recommendations that recognize the U.S. government’s broad opportunity and responsibility to help catalyze cybersecurity transformation through ZT adoption.
- Phase III (August 2022): Identifies opportunities for the federal government to aid in a secure convergence of OT cybersecurity within all relevant stakeholder communities.
- Phase IV (February 2023): Refines and builds upon the key findings of phases I, II, and III, and also addresses challenges that organizations encounter in providing security assurance in response to increasing government security requirements to address cybersecurity risks.

Additionally, 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 NSTAC approved the letter which includes key findings and recommendations with actionable steps for the White House and government agencies.

RECENT NSTAC PUBLICATIONS

[*NSTAC Report to the President on a Strategy for Increasing Trust in the Information and Communications Technology and Services Ecosystem*](#) (February 2023)

[*NSTAC Report to the President on Information Technology and Operational Technology Convergence*](#) (August 2022)

[*NSTAC Letter to the President on Enhancing U.S. Leadership in International Communications Technology Standards*](#) (May 2022)

[*NSTAC Report to the President on Zero Trust and Trusted Identity Management*](#) (February 2022)

[*NSTAC Report to the President on Software Assurance in the ICTS Supply Chain*](#) (November 2021)

[*NSTAC Report to the President on Communications Resiliency*](#) (May 2021)

[*NSTAC Letter to the President on NS/EP Communications Priorities*](#) (February 2021)

[*NSTAC Letter to the President on Communications Resiliency*](#) (October 2020)

[*NSTAC Report to the President on Software-Defined Networking*](#) (August 2020)

[*NSTAC Report to the President on Advancing Resiliency and Fostering Innovation in the ICT Ecosystem*](#) (September 2019)

[*NSTAC Letter to the President on Advancing Resiliency and Fostering Innovation in the ICT Ecosystem*](#) (April 2019)

[*NSTAC Report to the President on a Cybersecurity Moonshot*](#) (November 2018)



PRESIDENT'S NATIONAL SECURITY TELECOMMUNICATIONS ADVISORY COMMITTEE



FACT SHEET

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. The NSTAC is supported by the Secretary of Homeland Security, who is the Executive Agent for the NSTAC. CISA and the NSTAC's Designated Federal Officer work closely with the EOP to coordinate the committee's daily operations.

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

Mr. Peter Altabef

Chair and CEO
Unisys

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

Mr. David DeWalt

Founder and Managing Director
NightDragon Management Company

Mr. Raymond Dolan

Chair and CEO
Cohere Technologies

Mr. John Donovan

Lead Independent Director
Palo Alto Networks

Dr. Joseph Fergus

Founder, President, and CEO
Communication Technologies, Inc.

Mr. Patrick Gelsinger

CEO and Member of the Board
Intel

Ms. Lisa Hook

Managing Partner
Two Island Partners

Mr. Jack Huffard

Co-Founder and Member of the
Board
Tenable

Ms. Barbara Humpton

President and CEO
Siemens

Ms. Renée James

Founder, Chair, and CEO
Ampere Computing

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. Jeff McElfresh

COO
AT&T

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

Mr. Corey Thomas

CEO and Chair
Rapid7