

Agenda to Advance the Nation's Cybersecurity Defenses: Building on the Past, Looking Toward the Future

Policymakers should clarify and streamline the role of government in cybersecurity, strengthen existing public-private partnerships, address international cybersecurity challenges, and drive adoption of new technologies to enhance cyber resiliency.

Strengthening Public-Private Partnerships

Given the evolving nature of cyber threats, cybersecurity does not lend itself to prescriptive regulatory solutions. Public-private partnerships are better at finding flexible and evolving solutions that businesses can tailor to their needs commensurate with their risks. The government should remain committed to this model and approaches such as the existing NIST cybersecurity framework which focus on risk management vs. prescriptive solutions.

Policymakers should also implement a strategy to coordinate activities across currently siloed agencies. Today, the wide variety of government initiatives spanning many agencies make it challenging for industry to engage efficiently and effectively.

Ecosystem Wide Participation

Cybersecurity also requires solutions from across the Internet ecosystem. No one sector can address these complex issues on their own. Effectively managing cyber risk will require each participant in the ecosystem to play their part.

“Cybersecurity is a complex issue that requires industry and government to partner in finding innovative ways to stay ahead of threats.”

Bill O'Hern
Senior Vice President and
Chief Security Officer, AT&T

Improving International Cooperation

Many cyber threats emerge from overseas. Policymakers should prioritize efforts to develop a set of global norms and improve international collaboration to prevent and respond to cyber threats. The U.S. should include deterrence as part of its overall cyber strategy.

Encouraging New Technology

The government should prioritize cybersecurity in federal procurement plans to protect government networks and help drive further production and adoption of these technologies in the private sector.

Adoption of technologies like virtual security and Software Defined Networks, which are inherently more resilient to cyber-attacks, could drastically improve the security and resiliency of our country's networks.

