



**Homeland
Security**

DHS NATIONAL CYBERSECURITY SUMMIT

Protecting Critical National Functions through Industry and Government Collaboration

Forging a Collective Defense in Cyberspace: The DHS National Cybersecurity Summit represents public-private partnership in action. By convening dozens of CEOs and senior executives with U.S. Cabinet secretaries and senior government officials, along with hundreds of senior risk and security officers across a wide range of critical infrastructure sectors, this Summit conveys the imperative that the evolving and increasingly sophisticated and persistent cybersecurity threat landscape compels a collective approach to defending networks and managing national risk.

This is a first-of-its kind event, providing an action-oriented forum to identify joint cybersecurity efforts across government and industry. Participants in the summit include Vice President Mike Pence, Secretary of Homeland Security Kirstjen M. Nielsen, Secretary of Energy Rick Perry, Federal Bureau of Investigation Director Christopher Wray, Commander, U.S. Cyber Command and Director, National Security Agency General Paul M. Nakasone, and top CEOs from the financial services, energy, information technology, and telecommunications sectors.

- The summit will include a series of roundtable and panel discussions with private sector executives, government leaders, and domain experts. Vice President Pence and Secretary Nielsen will deliver keynote remarks.

DHS is leading the federal government's efforts to champion a coordinated, integrated approach to protecting our nation's critical infrastructure from the growing cyber threat. As the threat to our networks and cyber infrastructure grows, managing national risk requires top-down leadership from the government and private sector alike. It is critical that federal resources are coordinated and forward-looking.

- **This summit provides an opportunity to discuss and commit to operationalizing public-private partnerships in the cyber domain.** Leaders across the federal government and companies will announce new initiatives and actions to identify, assess, prioritize, and, ultimately, reduce risk.

KEY ANNOUNCEMENTS FROM THE SUMMIT

Launching the National Risk Management Center

The Center will act as the federal hub for integrated, sector-specific and cross-sector national infrastructure risk management

- ✓ *The Center will create a structured, coordinated, and central mechanism for identifying and setting national risk management priorities for critical infrastructure while enhancing the federal government's ability to identify and mitigate systemic risks.*
- ✓ *In addition to leveraging existing DHS capabilities, resources, and authorities, the Center will integrate partners from other federal agencies, state and local governments, and the private sector.*
- ✓ *The Result: a complete systemic risk picture within and between key critical infrastructure sectors, filling the gap where no single sector has complete information to detect emerging risk conditions. This will enable all stakeholders to move beyond simply sharing threat information and instead advance efforts to manage collective risk in a targeted and prioritized manner.*

Establishing an Industry-Driven Supply-Chain Task Force

The global information and communications technology (ICT) supply chain presents a national security risk that government and industry must work together to address. Through the Critical Infrastructure Partnership Advisory Council (CIPAC), DHS, in partnership with the Information Technology (IT) and Communications Sector Coordinating Councils, will establish an "ICT Supply-Chain Risk Management Task Force" within the National Risk Management Center.

The Task Force will focus on potential near- and long-term actions to manage strategic risks through policy initiatives and opportunities for innovative public-private partnership.
