Supply Chain Security *is* National Security

On April 1, to commemorate the beginning of National Supply Chain Integrity Month, INSA held its *Supply Chain Security is National Security* breakfast and panel discussion. The event started with a keynote by NCSC Director Bill Evanina, followed by a panel of senior public and private sector leaders.

Keynote

Bill Evanina
Director, National Counterintelligence and Security Center (NCSC), ODNI

Panelists

- **Kristin Baldwin,** Deputy Director, Strategic Technology Protection and Exploitation, OSD/R&E
- **Cameron Chehreh,** Chief Technology Officer, Dell EMC Federal
- **James Connelly,** Vice President and Chief Information Officer, Lockheed Martin
- **Daniel Kroese,** Associate Director, National Risk Management Center (NRMC), DHS
- **Jill Singer,** (moderator), Vice President, National Security, AT&T Global Public Sector

Key Takeaways:

- Supply chain vulnerabilities raise critical national security concerns, as they affect military preparedness, infrastructure protection, economic security, and cybersecurity.
- Three new supply chain dynamics have emerged: (1) States are attacking U.S. critical infrastructure; (2) Supply chain vulnerabilities enable adversaries to threaten all economic sectors; and (3) The difficulty of completely eliminating security threats means the United States must focus on resiliency, particularly regarding critical national functions.
- Supply chain security requires a long-term, whole-of-nation approach. Both public and private organizations of all sizes must understand their vendors and suppliers, as well as their strategic partners and subcontractors, to ensure products and services can be delivered uncompromised.
- Companies need an enterprise-wide approach to supply chain security. Executives should meet regularly with their human resources, procurement, IT, and security leaders to review current threats.
- Because microelectronics are present in all essential systems and are critical to U.S. military advantage, government and industry must work together to ensure their integrity. Through implementation of the National Semiconductor Strategy, the United States will encourage innovation and expertise in American manufacturers to secure long-term U.S. access to microelectronics and advanced technical capabilities.
- The congressionally mandated Federal Acquisition Supply Chain Security Council will foster collaboration among government agencies and private sector leaders, enabling information sharing, threat mapping, and innovative risk management.
- Security features must be included in hardware and software at the design stage and evolve to mitigate emerging risks.
- Organizations should mandate training that provides all employees a baseline understanding of supply chain threats.
- NCSC has created a robust repository of supply chain information and resources for companies to use and share with their strategic partners, available at: https://www.dni.gov/index.php/ncsc-what-we-do/ncsc-supply-chain-threats.

Thank You, Sponsors:

TRSS

LOCKHEED MARTIN

ABOUT INSA

The Intelligence and National Security Alliance (INSA) is the leading nonpartisan, nonprofit trade association for driving public-private partnerships to advance intelligence and national security priorities. A 501(c)(6) membership organization, INSA strives to identify, develop, and promote collaborative approaches to national security challenges. INSA has more than 160 organizations in its membership and enjoys extensive participation from leaders and senior executives in the public, private, and academic sectors. Learn more at www.INSAonline.org.