NATIONAL COUNTERINTELLIGENCE AND SECURITY CENTER

For Immediate Release:
1 April 2022

Contact: 301-243-0408
DNI_NCSC_OUTREACH@dni.gov

NCSC and Partners Launch "National Supply Chain Integrity Month" in April

Fortifying the U.S. Information and Communications Technology Supply Chain

WASHINGTON, D.C. -- The National Counterintelligence and Security Center (NCSC) and its partners in government and industry today launched the 5th annual "National Supply Chain Integrity Month" awareness campaign for organizations across the country to "fortify the chain" against foreign adversaries and other potential threats.

"This year's campaign is focused on fortifying the U.S. Information and Communications Technology (ICT) supply chain, which powers America's national security missions, critical infrastructure sectors, and private sector innovations," said Michael Orlando, Senior Official Performing the Duties of NCSC Director. "Foreign adversaries often target the ICT supply chain to gain access to U.S. systems for espionage, information theft, or sabotage. In doing so, they are compromising the products and services that underpin government and industry, resulting in lost intellectual property, jobs, economic advantage, and reduced military strength."

According to one private security report, software supply chain attacks more than tripled in 2021 compared to 2020. In recent years, U.S. Government attribution of software supply chain attacks to nation-state actors has increased as foreign adversaries have taken advantage of supply chain vulnerabilities found in several software applications. The exploitation of these vulnerabilities has raised the bar for software security and the need for more public-private partnerships to stem the tide.

The 2022 National Supply Chain Integrity Month campaign will focus on securing the ICT supply chain and on Executive Branch efforts to address this critical issue. Senior stakeholder commitment, exemplified by the depth and breadth of events scheduled throughout the month, is designed to bring the needed awareness to address software supply chain attack vectors such as the compromise of Microsoft Exchange servers, Log4j software, SolarWinds software, and Pulse Secure products.

On February 24, 2022, the Executive Branch issued six supply chain sector reports as required under Executive Order 14017. Throughout each report, the ICT supply chain was identified as an essential part of these critical sectors. Thus, protecting the ICT supply chain becomes a supply chain security force-multiplier for all other critical supply chains.

This year's campaign will include events sponsored or supported by participants from government, academia, and the private sector. Activities will range from small, classified briefings to large, unclassified public functions. The broad scope of events is designed to raise awareness of threats to the ICT supply chain and to share best practices on risk mitigation.

To help stakeholders in industry and government, NCSC has posted new supply chain risk management resources at the NCSC supply chain website. Among other things, the webpage provides information on supply chain threats and best practices, as well as links to resources of partner agencies.

While there is no single, silver-bullet solution to immunize America against supply chain threats, NCSC encourages organizations at a minimum to consider the following basic principles to enhance the resilience of their supply chains:

- Diversify Supply Chains: A single source of goods or services is a single point of failure. Diversify supply chains to ensure resilience in the event a supplier suffers a compromise, shortages, or other disruptions.

- Mitigate Third-Party Risks: Conduct robust due diligence on suppliers, understand their security practices, and set and enforce minimum standards for them. Incorporate security requirements into third-party contracts and monitor compliance throughout the lifecycle of a product or service.

- Identify and Protect Crown Jewels: Map the location and status of essential assets and prioritize their protection. Monitor systems and network performance to minimize impact of disruptions.

- Ensure Executive-level Commitment: Name a senior executive as owner of supply chain risk and include stakeholders across the enterprise in the risk mitigation program. Communicate across the organization to ensure buy-in and establish training and awareness programs.

- Strengthen Partnerships: Information exchange between government and industry on current threat information and security best practices is paramount.

A center within the Office of the Director of National Intelligence, NCSC is the nation's premier source for counterintelligence and security expertise and is a trusted mission partner in protecting America against foreign and other adversarial threats.

# # #