For Immediate Release:
1 April 2021

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

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

A Call-to-Action Campaign to Raise Awareness of Supply Chain Threats and Mitigation

WASHINGTON, D.C. -- The National Counterintelligence and Security Center (NCSC) and its partners in government and industry today launched the 4th annual "National Supply Chain Integrity Month" with a call to action for organizations across the country to strengthen their supply chains against foreign adversaries and other potential risks.

Throughout April, NCSC is teaming up with the Department of Homeland Security's Cybersecurity and Infrastructure Security Agency (CISA), the Federal Communications Commission (FCC), the Department of Defense's Center for the Development of Security Excellence (CDSE), the National Association of State Procurement Officials (NASPO), the National Association of Counties (NACo), and other partners to raise awareness of threats to U.S. supply chains and share information on risk mitigation. A host of public and non-public events with stakeholders in government, industry, and academia are planned to enhance supply chain risk management efforts.

"If the Covid-19 pandemic and resulting product shortages were not a sufficient wake-up call, the recent software supply chain attacks on U.S. industry and government should serve as a resounding call to action. We must enhance the resilience, diversity, and security of our supply chains. The vitality of our nation depends on it," said Michael Orlando, Acting NCSC Director.

To help stakeholders in industry and government, NCSC today is disseminating new supply chain risk management resources that can be found at the NCSC supply chain website. Among other things, the webpage provides extensive information on supply chain threats and best practices, as well as links to resources of partner agencies. In addition, NCSC is issuing sector-specific guidance throughout April on supply chain risk management for the information and communications technology (ICT) sector, the manufacturing and production sector, the health care sector, and the energy sector.

Foreign Adversary Exploitation of U.S. Supply Chains

While production shortages, trade disruptions, natural disasters, and other unforeseen events can all stress America's global supply chains, actions by foreign adversaries to exploit vulnerabilities in U.S. supply chains pose unique counterintelligence and security threats.

Foreign adversaries are increasingly using companies and trusted suppliers as attack vectors against us for espionage, information theft, and sabotage. In doing so, they are compromising the products and services that underpin America's government and industry – resulting in lost intellectual property, jobs, economic advantage, and reduced military strength.

Over the past decade, for example, state-sponsored hackers have compromised software and Information Technology service supply chains to steal intellectual property, conduct espionage, and

carry out sabotage. While the recent SolarWinds compromise has brought greater public attention to software supply chain attacks, it is only the latest in a long line of such attacks in recent years.

- In February, U.S. charges were unsealed against North Korean military hackers for cyber-crimes that included cryptocurrency schemes supported by software supply chain attacks.

- Last October, six members of Russian military intelligence were indicted for multiple cybercrimes, including the 2017 NotPetya software supply chain attack that crippled banks, commerce, utilities, and logistics worldwide, causing billions of dollars in damages.

- Last September, U.S. charges were unsealed against Chinese hackers for targeting more than 100 companies worldwide, including software providers. The hackers modified providers' software code for further cyber intrusions against the providers' customers worldwide to steal data and business information.

As detailed in NCSC's new materials, software supply chain attacks are particularly insidious because they erode the basic trust between consumers and software providers. Consumers are correctly conditioned to use software only from trusted sources through authorized vendors and urged to promptly install security updates from developers. Customers must now be wary of performing even these basic, cyber-hygiene tasks because authorized resources may be compromised.

The Basics of Supply Chain Risk Management

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 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, the NCSC is the nation's premier source for counterintelligence and security expertise and a trusted mission partner in protecting America against foreign and other adversarial threats.

# # #