For Immediate Release:
1 April 2024

Contact: (301) 243-0403
DNI_NCSC_OUTREACH@dni.gov

NCSC and Partners Launch National Supply Chain Integrity Month 2024

WASHINGTON, D.C. — The National Counterintelligence and Security Center (NCSC) and its partners in government and industry today launched the “National Supply Chain Integrity Month” awareness campaign in April to encourage organizations across the country not to gamble with supply chain security against foreign adversaries and other potential threats.

“Hostile nation states and other threat actors exploit supply chain vulnerabilities to steal American intellectual property, target our critical infrastructure, and compromise our cybersecurity,” said Michael Casey, NCSC Director. “While these incidents have increased in number and severity, so has our resolve to build resilience in the supply chains we all rely upon.”

Throughout 2023, threat actors — ranging from criminal elements and ransomware gangs to sophisticated hackers sponsored by nation states — conducted high-profile cyber campaigns that resulted in costly supply chain consequences. In June 2023, the “Clop” ransomware gang conducted large-scale data-theft operations that victimized thousands of U.S. organizations and impacted tens of millions of people.[i] In addition, People’s Republic of China (PRC) state-sponsored cyber actors known as “Volt Typhoon” conducted extensive cyber intrusions that breached U.S. critical infrastructure.[ii] Organizations must prepare now to deal with these threats and keep ahead of potential risks.

Supply chain security has been a priority focus for public and private sector organizations seeking to enhance their resilience in the face of unpredictable supply chain shocks in recent years. These shocks are not only increasing in number but also in severity. Recent examples include the Microsoft cloud 365 breach by China-based actors identified as “Storm-0558,” which accessed the email servers of 25 organizations, including U.S. government agencies and consumer accounts in the public cloud.[iii]

For 2024, NCSC and its partners, including the U.S. Departments of Homeland Security, Defense, Energy, and Commerce, are asking organizations to bolster their Supply Chain Risk Management (SCRM) programs with an “A.C.E.” — Acquisition Security, Cyber Security, and Enterprise Security.

Incorporating A.C.E. into SCRM programs will help organizations make risk decisions that last throughout the supply chain lifecycle. When a contract partner fails to deliver on time; when a cyber breach threatens data integrity; or when an insider compromises corporate or customer information, having effective A.C.E. principles in place can help organizations better mitigate and withstand such incidents.

Throughout April, NCSC and its partners in government and industry will conduct multiple outreach events to promote supply chain integrity by spotlighting adversarial activity, sectors at risk, and ways organizations can enhance SCRM with A.C.E. principles. The events will include classified discussions within the Intelligence Community, multi-national engagements with international partners, and events with industry and public participation. NCSC also plans to publish advisories and other materials related to SCRM on its website at www.ncsc.gov and on social media platforms.

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.

# # #

[i] https://www.cisa.gov/news-events/alerts/2023/06/07/cisa-and-fbi-release-stopransomware-cl0p-ransomware-gang-exploits-moveit-vulnerability

[ii] https://media.defense.gov/2024/Feb/07/2003389935/-1/-1/0/CSA-PRC-COMPROMISE-US-CRITICAL-INFRASTRUCTURE.PDF

[iii] CISA and FBI Release Cybersecurity Advisory on Enhanced Monitoring to Detect APT Activity Targeting Outlook Online | CISA, Microsoft mitigates China-based threat actor Storm-0558 targeting of customer email | MSRC Blog | Microsoft Security Response Center