FEDERAL PARTNER NEWSLETTER

NATIONAL COUNTERINTELLIGENCE AND SECURITY CENTER

Volume 3 | Issue 1
April 2021

National Supply Chain Integrity Month

Rico F. and Jeanette M.,
Supply Chain & Cyber Directorate, NCSC

NCSC's Supply Chain and Cyber Directorate (SCD) is leading an aggressive messaging campaign for this year's National Supply Chain Integrity Month in April, centered upon the theme, A Call to Action. 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 (CI) and security threats.

"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," said Michael Orlando, Acting NCSC Director. "We must enhance the resilience, diversity, and security of our supply chains. The vitality of our nation depends on it."

A critical aspect of this call to action is strengthening our federal partnerships by enhancing federal supply chain risk management (SCRM) programs. For example, we are highlighting the implementation of E.O. 14017, America's Supply Chains, which is currently focused on four plans to review the supply chains of microelectronics, advanced batteries, critical minerals and materials, and pharmaceutical ingredients. In addition, this awareness campaign focuses on how enhancing federal SCRM programs improves threat information sharing, integrates risk reduction strategies, and helps build more secure and resilient supply chains.

Please read the additional articles in this newsletter for other supply chain information and visit our NCSC supply chain website for additional information.

Upcoming Events

- **April 20** – INSA Event "Securing Microelectronics Supply Chains"
- **April 21** – NITTF Talk— "Foreign Vetting"
- **April 28 –** NCSC Supply Chain Integrity Month Event for Federal Partners
- **April 29** – CDSE Event "Supply Chain Due Diligence 2021"
- **May** – Federal Partners Special Edition Newsletter
- **May 6** – National OPSEC Program Office (NOP) Orientation Briefing
- **May 6** – NITTF Tech Talk – "Trends in Insider Risk Quantification Part 3";
  By CERT, Carnegie Mellon
- **May 11** – NITTF Spring 21 Insider Threat Community Forum
- **May 14** – NITTF Talk – Interaction Between CI and Insider Threat Programs
- **May 18-19** – NITTF Hub Ops Course; Registration opens 04/01/2021
- **May 26** – Quarterly Federal Partners CI Roundtable

The White House Office of Science and Technology Policy on Bioeconomy

Paige Waterman, Executive Office of The President, Office of Science and Technology Policy

In 2019, the White House Office of Science and Technology Policy (OSTP) convened experts from across the Federal Government, private industry, non-profits, and academia to discuss potential ways in which the Federal Government could promote and protect the U.S. Bioeconomy. In conjunction with a Federal Register Request for Information, OSTP sought public input to help identify gaps, vulnerabilities, and opportunities in the U.S. Bioeconomy that may benefit from a coordinated federal response. In their 2020 "Safeguarding the Bioeconomy" consensus report, the National Academies of Sciences, Engineering, and Medicine recommended refining the concept of "bioeconomy" to focus on the economic activity driven by research and innovation in the life sciences and biotechnology that is enabled by technological advances in engineering, computing, and information sciences.

In the midst of unprecedented global mortality and economic collapse associated with SARS-CoV-2, the Biden Administration is determined to support solutions to ensure a post-pandemic society that reflect lessons learned and long-term stability of the U.S. as a global economic and innovation leader.

The bioeconomy represents a convergence of public health, economic resilience, and national security, which is why the Administration is prioritizing an iterative and continuing assessment of bioeconomic advances and vulnerabilities while strategically investing in building sustainable new economic ecosystems. These initiatives will target fundamental research, development, and manufacturing investments; leverage biological data for discovery; safeguard technological advantages; and build and sustain a diverse workforce to create economic opportunities. Prioritizing bioeconomy development will contribute to long-lasting stability for America and our allies, providing a critical foundation for American competitiveness, security, economic growth, and 21st Century leadership in research and innovation.

USDA and HHS/FDA Messaging Campaign for Food and Agriculture Sector

Carrie Moore and Timothy Owens,
USDA, Office of Homeland Security

In support of Supply Chain Integrity Month, the United States Department of Agriculture (USDA) and the Department of Health and Human Services (HHS), Food and Drug Administration (FDA) developed a four-part email messaging campaign for the Food and Agriculture Sector. USDA and HHS/FDA co-chair the Food and Agriculture Sector, one of the 16 critical infrastructure sectors establish by PPD-21.

The "farm to fork" progression from suppliers to consumers in the Agricultural Supply Chain (ASC) include activities such as farming, processing/production, packaging, warehousing, transportation, distribution, and marketing. The ASC faces a variety of risks such as climate change, availability of labor, transportation dependencies, pests and diseases, technological advances, and cyber.

Threats exist from insiders, foreign state and non-state actors, and any other adversary aimed at compromising our supply chain, to include our research and development. An insider threat action could include food tampering, insertion of malicious code, or theft of trade secrets and other proprietary information.

The case involving Wengui Yan and Weiqiang Zhang is one example of an insider threat case where employees worked with a visiting foreign delegation to steal proprietary rice seeds that contained proteins for use in medicines and pharmaceutical products. The case involving Mo Hailong, and the theft of inbred corn seeds, is one example of the importance of protecting agricultural trade secrets, costing billions annually, from agro-espionage.

We recently implemented the distribution of a weekly newsletter on threat information to the Sector. We remain engaged in sharing threat information to the Sector that may affect the food and agriculture industry to build awareness and enable risk-informed decision making.

NCSC Designates Insider Threat As New Directorate

Rebecca M., Deputy Director, Insider Threat Directorate, NCSC

In 2021, the National Counterintelligence and Security Center (NCSC) designated Insider Threat as its newest directorate. NCSC Insider Threat Directorate (ITD) leads the Nation's efforts to counter the insider threat by enabling federal agencies and private sector organizations to mitigate threats from insiders that would adversely affect public health and safety, national security, and the economic well-being of the U.S. NCSC ITD executes ODNI responsibilities under Executive Order (EO) 13587 to lead the National Insider Threat Task Force (NITTF) and under ICD 701 for Unauthorized Disclosure.

NITTF continues efforts to establish a U.S. Government-wide insider threat program for deterring, detecting, and mitigating insider threats, including the safeguarding of classified information from exploitation and compromise. The creation of the NCSC ITD strengthens the role of insider threat, enables integration with other national security disciplines, and fosters a more holistic response to mitigate insider risk. The NCSC ITD conducts liaison activities; develops training and professionalization opportunities; provides outreach to public and private sector partners; supports research and technological advancement; and provides mission integration, governance, and advocacy.

"The creation of the NCSC ITD strengthens the role of insider threat, enables integration with other national security disciplines, and fosters a more holistic response to mitigate insider risk."

Our outreach efforts include a number of events open to federal community members from the DOD, IC, and NT-50 including monthly "NITTF Talks" and quarterly "NITTF Tech Talks" - one hour unclassified virtual events highlighting current insider threat issues and technological capabilities for mitigating insider risk. Join us and be part of the conversation.

To learn more, reach out to your NCSC POC or visit our website.

The National Operations Security Program

Michelle A., EdD, NOP Office Group Chief, NCSC/MID
Gardenia Jackson, Chief, Interagency Operations Security Staff

The National Operations Security (OPSEC) Program (NOP) is moving to the National Counterintelligence and Security Center (NCSC)! On January 13, 2021, the President signed National Security Presidential Memorandum (NSPM) 28, the National Operations Security Program (NOP), which updates the previous policy issued in 1988. The program was originally led by the National Security Agency (NSA) through their Interagency OPSEC Support Staff (IOSS). As part of the updates to the NOP, IOSS activities and resources "shall be incorporated into the NOP office to ensure unity of effort and resource efficiency while preserving, to the extent possible,

existing OPSEC training expertise." Over the last 33 years, the IOSS has supported the OPSEC community across the U.S. Government (USG) and provided national OPSEC program development and guidance, developed and delivered OPSEC curriculum and professional training, and conducted OPSEC assessments across the world.

IOSS training and information may be found at www.iad.gov/ioss/. The revisions to the NOP will expand the OPSEC program requirements across Federal Departments and Agencies (D/As) to promote a whole-of-government approach. The IOSS will continue its operations and OPSEC community support as it is integrated into the new NOP. Over the next year, the NOP will be reaching out to D/As to provide new requirement guidelines for all organizations and OPSEC program development direction.

The updated OPSEC program is focused on systematically helping enhance risk management efforts by drawing on the strengths of NCSC at large, and providing an opportunity for additional federal D/As to be represented in the OPSEC program. Detailed information on NOP transition activities will be provided on May 6th during a special orientation for Federal Partners. For more information, inquiries should be directed to the IOSS or NCSC at NCSC_Feds@dni.gov.

Mission Integration Directorate New Initiative: Assistance Visits

James Burdock,
Mission Integration Directorate, NCSC

The Mission Integration Directorate (MID) has launched a new initiative. We have established a Non-Title-50 (NT-50) mission support team that will be offering focused Assistance Visits exclusively for NT-50 Agencies with the goal of briefing National Counterintelligence and Security Center (NCSC) capabilities, identifying counterintelligence (CI) program gaps, and providing solutions to enhance their programs, consistent with their legal authorities and policy guidelines.

Many NT-50s face numerous CI challenges, such as exposure resulting from foreign visitors to their facilities or employee travel. These partnerships are important to NCSC as we all employ a whole-of-government CI and security approach called for in the National CI Strategy.

Mission support is a priority in building, refining, and enhancing our relationships with NT-50 agencies. We will achieve our coordinated objectives by leveraging the subject matter experts (SME) across the NCSC before, during, and after these assistance visits; James Burdock will lead the integrated team of SME's from across the NCSC. This new initiative is in the planning stage MID will begin scheduling visits as early as May/June 2021. We look forward to working with you! For more information, please contact James Burdock at (301) 243-0525.

A Public-Private Approach to Protecting Global ICT Supply Chains

Cybersecurity and Infrastructure Security Agency (CISA)

Information and communications technology (ICT) have accelerated digital transformations in almost every part of society including in healthcare, manufacturing, and education. Through ICT, millions of people across the globe can remotely access work and school environments, conduct mobile banking, set virtual medical consultations, and more. However, recent software compromises and other incidents have revealed how new and inherent vulnerabilities in ICT supply chains can have globally cascading impacts on our daily lives, economic growth, national security, and public safety.

As the Nation's risk advisor, supply chain security is a top priority for the Cybersecurity and Infrastructure Security Agency (CISA)—a priority it achieves largely through the ICT Supply Chain Risk Management (SCRM) Task Force. Co-chaired by CISA's National Risk Management Center and the Information Technology and Communications Sector Coordinating Councils (SCC), the Task Force is a public-private partnership that embodies the Agency's collective approach to enhancing global supply chain resilience.

With April being National Supply Chain Integrity Month, CISA is partnering with government and industry partners to promote a call to action for a unified effort to strengthen global supply chains. CISA will release resources, tools, and information to help organizations integrate SCRM into their overall security, including:

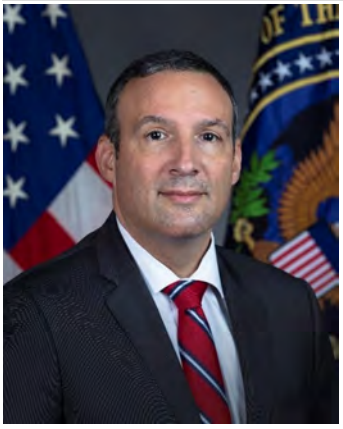
- Two new Task Force tools (the report on Mitigating ICT Supply Chain Risks and Qualified Bidder and Manufacturer Lists and the Vendor SCRM Template);
- The use of a common supply chain threats lexicon;
- Step-by-step guidance for leaders and staff on how to build a SCRM program; and
- A social media toolkit with sample messaging for stakeholders to utilize.

To learn more, visit CISA.gov/supply-chain-integrity-month.

LINKING TO NCSC

- **Insider Threat Mitigation for U.S. Critical Infrastructure Entities: Guidelines from an Intelligence Perspective**
- **2018 Foreign Economic Espionage in Cyberspace Report**
- **Supply Chain Risk Management Resources**
- **IOSS Website Account Registration and Available Training**

From the Acting Director



Michael J. Orlando
Acting NCSC Director

On April 1st, 2021, the National Counterintelligence and Security Center (NCSC) and its partners in government and industry 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.

While there is no single, silver-bullet solution to immunize America against supply chain threats, NCSC encourages organizations, at a minimum, to diversify their supply chains to ensure resilience, mitigate third-party risks by conducting due diligence on suppliers, identify and protect essential assets, ensure executive-level commitment for a supply chain risk mitigation program, and strengthen partnerships and information sharing.

To help stakeholders in industry and government, NCSC has disseminated new supply chain risk management (SCRM) 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 SCRM for the information and communications technology (ICT) sector, the manufacturing and production sector, the health care sector, and the energy sector.

> *"NCSC has disseminated new supply chain risk management resources …[and] is issuing sector-specific guidance throughout April on supply chain risk management"*

Throughout the month of April, NCSC is hosting a social media campaign on Twitter and LinkedIn to share supply chain related information and resources. For more information on National Supply Chain Integrity Month, NCSC, and counterintelligence and security topics, please visit our website at **https://www.NCSC.gov**, follow us on **Twitter @NCSCgov**, or follow our **NCSC page on LinkedIn**.

Michael J. Orlando