Federal Partner Newsletter

NATIONAL COUNTERINTELLIGENCE AND SECURITY CENTER

Volume 1 | Issue 1
April 2019

It's National Supply Chain Integrity Month

Joyce Corell, Assistant Director for NCSC's SCD

NCSC's Supply Chain and Cyber Directorate (SCD) declared April as "National Supply Chain Integrity Month" in 2018, and the call to focus on Supply Chain this April continues. Activities underway to accentuate the focus on Supply Chain Integrity include dedicating the inaugural issue of this newsletter to Supply Chain as well as significantly increasing awareness and outreach efforts using multimedia platforms and venues to promote Supply Chain Risk Management (SCRM) both inside and outside the US Government. An SCRM Forum was held at the Intelligence Community Campus in Bethesda, Maryland (ICC-B) on April 5th and there are several other events scheduled at ICC-B that our Federal Partners will be invited to via email, including:

April 18th	SCRM 101 Workshop
April 23rd	Federal Senior Intelligence Coordinators Advisory Board Meeting
May 2nd	National Insider Threat Task Force (NITTF) Spring Forum

President Signs SECURE Technology Act

Jeanette McMillian, Strategic Program Director for NCSC's SCD

On December 21, 2018, President Trump signed into law the SECURE Technology Act, which establishes the Federal Acquisition Security Council (FASC). The OMB-led council replaces the outdated piecemeal approach to addressing supply chain threats to our critical information and communication technologies (ICT). The Act completely reshapes the US Government's (USG's) current patchwork approach to SCRM by requiring departments and agencies to conduct SCRM assessments in accordance with FASC-approved criteria. Further, the Council will develop criteria for sharing SCRM information with other federal departments and agencies, state and local governments, and the private sector. Each department and agency may request the FASC to remove or excluded risky vendors. If the FASC recommends that such an exclusion will protect the ICT supply chain, then the vendor proposed for exclusion will be notified and will have an opportunity to seek judicial review of such an order.

In summary, the FASC's authorities empower the USG to determine the risk, appropriately share SCRM information, and exclude risky vendors from the ICT supply chain.

SCRM for Federal Partners

Ariana KWW DiMeo, Federal Deposit Insurance Corporation (FDIC)

We don't know what SCRM looks like for Federal Partners yet. Unfortunately, at this point, there is no "supply chain in a box," through which Departments and Agencies can plug-and-play pre-conceived and pre-approved policy, implementation, analysis, and risk-based standards. What we do have is pretty special and exciting though. We have an opportunity to create Federal-wide SCRM—together.

SCRM for Federal Partners revolves around information sharing like no other national security topic. We must share fully, freely, and frequently with each other to ensure that we identify, assess, and mitigate risks with a unified, confident voice. If we build SCRM programs disjointedly, then we may protect the Federal Supply Chain unevenly, and end up perhaps only marginally improved from our current posture. Combine our information resources, however, and we grow stronger together. *E pluribus unum.*

I invite everyone to join the FDIC on i-Space. Search for the "SCRM for Federal Partners" community and start posting! As we draft our artifacts, map our processes, celebrate successes, learn new lessons, let's share these assets and become more resilient together.

SCRM: *It Takes All of Us*

Jane H., Assistant Director NCSC's Mission Integration Directorate

SCRM requires a "whole-of-industry" and a "whole-of-government" approach that recognizes, promotes, educates, and helps mitigate the asymmetric attacks on our supply chain from adversaries. Our increasingly connected world and technologies make us more vulnerable today than ever before. For example, the Internet of Things (IOT), proliferation of software and network technologies, and increasing reliance on foreign-owned, -manufactured, or -controlled hardware, software, and services present significant opportunities for attack. Making this problem even more challenging is that the multi-tiered nature of supply chains obfuscates the security, resilience, quality, and delivery of products and technical services used in homes, cars, air transportation, and critically important, in government weapons systems and critical infrastructure.

It is important to recognize that even small companies are vulnerable, especially when they serve as secondary suppliers to or otherwise support larger companies. At almost any stage (i.e., production, fielding, and sustainment) during the supply chain cycle, our adversaries can insert malicious microelectronics that might create persistent and hard to detect vulnerabilities. Mitigating these attacks includes sharing SCRM best practices and threat information. And importantly, departments/agencies, private sector, and academia need to establish and mature comprehensive SCRM programs. NCSC has several products available on its website to provide program-building guidance and will make additional aids available in the future.

> *"The US Government is dangerously vulnerable to Chinese espionage or cyberattack because of its dependence on electronics and software made in China, a risk that threatens to grow as Beijing seeks global technological dominance."*
>
> **Congressionally Chartered Advisory Commission**

> *"Russian Government Cyber Activity Targeting Energy and Other Critical Infrastructure Sectors….They often leverage third-party suppliers with less secure networks as vectors to reach more highly valued targets such as ICT systems associated with our critical infrastructure."*
>
> **US CERT**

Security as the Critical 4th Pillar

Lourdes A., NCSC Federal Partner Liaison

Asymmetric Warfare is here. DoD's report, "*Deliver Uncompromised*," outlines the need to react with the same intensity and determination in investment, planning, and execution as when reacting to a conventional attack.

A key factor of the "*Deliver Uncompromised"* strategy is to combat adversaries' manipulation of the supply chain by reforming our acquisition policies and authorities, and adding security as the critical 4th pillar, paralleling cost, schedule, and performance. Part of the new strategy must be to transform security concerns from a cost center to a profit center. The goal is to eliminate the

need for costly, unplanned upgrades or replacements resulting from adversary-induced compromises. Existing contract authorities should be leveraged to require demonstration of system integrity, and mission assurance should be a deliverable, to the best extent reasonably possible.

From the Director

William R. Evanina
NCSC Director

NCSC leads the counterintelligence and security activities across the Intelligence Community and Executive Branch departments and agencies because it is uniquely positioned to integrate the assets of CI and security communities to understand and counter foreign intelligence threats through collaboration and partnerships. It is fostering these partnerships through efforts like this newsletter that help us stay united in our efforts to deter and defeat any adversary that threatens our national and economic security.

Federal partners are essential to the CI and security activities that underpin our national security. I ask that you find a way to emphasize Supply Chain Integrity within your departments and agencies during April and continue those efforts in partnership with NCSC going forward.

We hope you find this newsletter to be a valuable source of information and another way for us to remain connected. If you have any suggestions for improving it, have articles you would like to submit, or have other thoughts on how we can enhance our engagement with federal partners, please let us know at ***NCSC_FEDS@dni.gov.***

For more information on NCSC and counterintelligence and security topics, including the supply chain, please visit our website at **https://www.*NCSC.gov*** or follow us ***@NCSCgov on Twitter.***

> *"We will continue to foster broad partnerships in the public and private sectors and strengthen information exchange to more effectively neutralize or mitigate compromise of critical supply chains."*
>
> **NCSC Strategic Plan 2018-2022**