CDSE pulse

LEARN. PERFORM. PROTECT.

This month's focus: National Supply Chain Integrity Month

Volume I, Issue 4 April 2020

April is National Supply Chain Integrity month. Throughout the month, CDSE will highlight information to raise awareness about supply chain threats and resources available to help security professionals mitigate the risks to supply chain integrity. Learn more about supply chain vulnerabilities and mitigation strategies with the CDSE resources detailed in this newsletter.

The National Counterintelligence and Security Center (NCSC) plays a lead role in education and awareness for the U.S. Department of Defense, U.S. government, and industry. They oversee Counterintelligence (CI) and security resources in the National Intelligence Program and advocate for the implementation of CI and security best practices through individual agency programs. Visit the NCSC Supply Chain Month Resource page for more information.

Combating Threats to Supply Chain Integrity During COVID-19

by Isaiah Burwell, CDSE

The Department of Defense defines supply chain management as the cross-functional approach to procuring, producing, and delivering products and services to customers. On April 1, 2019, the National Counterintelligence and Security Center (NCSC) launched National Supply Chain Integrity Month to "raise awareness about the growing threats to the supply chains of the private sector and U.S. Government and to provide resources to help mitigate these risks." A year later, there is one threat that stands above all others; COVID-19, also known as the Coronavirus.

Continued on page 3

Did you know?

A decade ago, the DSS Academy was renamed CDSE and its critical role increased in security education, training, and professional development functions, in accordance with Department of Defense policy.

CDSE – Center for Development of Security Excellence

@TheCDSE

Center for Development of Security Excellence

Enhance Your Knowledge with Job Aids and Toolkits

In a recent communications survey, performance support tools such as job aids and toolkits were some of the most requested products by CDSE students. Find the information you need to perform specific tasks in your role and gain a better understanding of Supply Chain Risk Management policies, threats, and best practices with the following job aids and toolkits:

[Job Aid: Supply Chain Risk Management]

[Job Aid: Software Supply Chain Attacks]

[Counterintelligence Toolkit: Supply Chain Risk Management]

[Cybersecurity Supply Chain Toolkit]

[Deliver Uncompromised Toolkit: Critical Technology Protection]

[Director of National intelligence Supply Chain Month Toolkit]

eLearning Opportunities

CDSE offers 105 training courses and has achieved high customer satisfaction scores for its eLearning content. The following eLearning courses are recommended for National Supply Chain Integrity Month and beyond.

[DoD Supply Chain Fundamentals]

[Life Cycle Logistics for the Rest of Us]

[Contracting for the Rest of Us]

[Thwarting the Enemy: Providing Counterintelligence & Threat Awareness to the Defense Industrial Base]

[Supply Chain Risk Management for Information and Communications Technology]

Upcoming Supply Chain Integrity Speaker Series Event

Supply Chain Resiliency, Thursday, April 23, 12:00 p.m. ET

CDSE hosts the National Counterintelligence and Security Center for a discussion on Foreign Intelligence Entity (FIE) supply chain exploitation. FIE use this method to target U.S. equipment, systems, and information used every day by government, businesses, and individual citizens. Join us and learn more about the risk and your role in recognizing and reporting suspicious activity. Register here.

Save-the-Date: Summer Webinar

2019 Targeting U.S. Technologies Report

Thursday, July 23, 12:00 p.m. ET

As part of the fight to secure the supply chain, it is important to identify what technologies are being targeted by our adversaries. Mark your calendars to join the DCSA and CDSE as we discuss the latest trends in foreign targeting of U.S. defense technologies that occurred in 2019. The webinar will focus on foreign efforts to compromise and/or exploit cleared personnel to obtain unauthorized access to sensitive and classified information. Webinar registration will open in June. You can read the report here.

What Students are Saying

Course: CI Awareness & Reporting for DoD Employees CI116

"I thought the training provided strong, real-world examples, and updated graphics. I've been in CI over 20 years, this was very good." -Anonymous

Combating Threats continued…

According to the Harvard Business Review, the COVID-19 pandemic has presented challenges to companies' supply chains unlike any other in recent memory. "Despite numerous supply-chain upheavals inflicted by disasters in the last decade — most companies still found themselves unprepared." To address these challenges, many organizations have reevaluated their efficiency and readiness; including the DoD.

Ellen M. Lord, Under Secretary of Defense for Acquisition and Sustainment (USD(A&S)), has established a Joint Acquisition Task Force to meet the supply chain challenges present by COVID-19. Secretary Lord stated that the task force will "synchronize the DoD acquisition response to this crisis, working closely with all the services and defense agencies." In addition to DoD, the Federal Emergency Management Agency (FEMA) is also taking action. Rear Admiral John Polowczyk, leader of FEMA's Supply Chain Task Force, stated that the president gave him one metric, "Get more to the hospitals and to the healthcare workers." While these organizations work to strengthen the nation's supply chain from within, there are exterior threats that security professionals need to be aware of.

In early April 2020, NCSC Director William Evanina tweeted that "#COVID19 has disrupted global supply chains and focused attention on the foreign dependence of key U.S. industries. These are areas our adversaries are likely to exploit." Since the start of 2020, there have been three cyberattacks on supply chain companies and other industry sectors by a hacker group known as Kwampirs. The FBI concluded that "Kwampirs actors gained access to a large number of global hospitals through vendor software supply chain and hardware products." Security threats show no sign of slowing down during the pandemic, so government and industry security professionals need to be prepared to identify them.

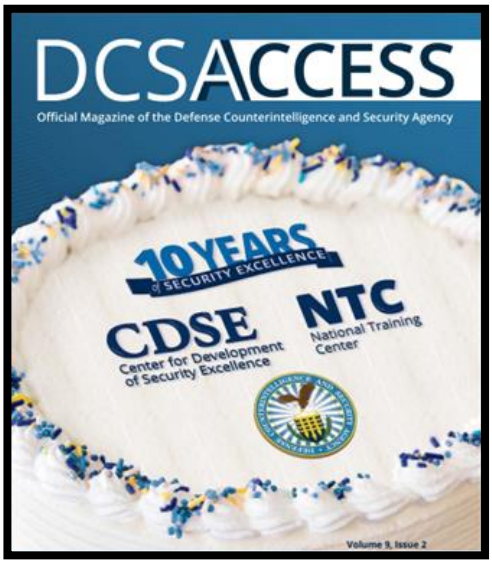
Over the past 10 years, the Center for Development of Security Excellence (CDSE) has been the premier provider and center of excellence for security education, training, and certification for the DoD and industry under the National Industrial Security Program (NISP). Our mission is to provide development, delivery, and exchange of security knowledge to ensure a high-performing workforce capable of addressing our Nation's security challenges. One of CDSE's educational tools is the Counterintelligence Awareness Toolkit. One of the categories in that toolkit is Supply Chain Risk Management (SCRM).

Continued on next page

10-Year Anniversary Milestone Featured in DCSA Access

CDSE is featured in the recently released Defense Counterintelligence and Security Agency (DCSA) Access magazine, highlighting CDSE's 10 year anniversary. Last month, CDSE celebrated a decade of security learning achievement developing security skills, increasing security knowledge, and promoting security awareness in the DoD and cleared industry workforces. CDSE has educated, trained, and certified personnel entrusted with protecting national security and has logged more than 7.5 million course completions.

From the early days of instructor-led only training and correspondence courses, CDSE's learning opportunities have evolved to include eLearning, virtual instructor-led training, and enhanced learning opportunities both domestically and internationally. To learn more about the achievements and evolution of CDSE, read the article here.



Continued from page 3

SCRM is a systematic process for managing supply chain risk by identifying susceptibilities, vulnerabilities and threats throughout the supply chain and developing mitigation strategies to combat those threats whether presented by the supplier, the supplied product and its subcomponents, or the supply chain. The "Supply Chain Risk Management" category of the counterintelligence toolkit contains job aids, supply chain risk management policy, security training videos, threat awareness, and best practices.

The SCRM job aid teaches security professionals the framework of the risk management process. The policy section outlines the specific government policies used to dictate supply chain management. The "Deliver Uncompromised" security training videos discuss both SCRM and military technology transfer. The "threat awareness" section contains resources from Computer Security Resource Center NIST, NCSC supply chain threats, U.S. Army Space & Missile Defense Command/Army Forces Strategic Command, and Software and the Supply Chain Assurance DHS U.S. CERT website. The "best practices" section contains information about the exploitation of the Global Supply Chain, a SCRM blog from the Defense Acquisition Portal, the U.S. Resiliency Project, and Interagency reports.

Foreign intelligence entities and other adversaries are continuously attempting to compromise our government and industry supply chains. Adversaries exploit supply chain vulnerabilities to steal U.S. intellectual property, corrupt software, surveil critical infrastructure, and enact other malicious activities. Trusted suppliers and vendors face infiltration which targets equipment, systems, and information used daily by the government, businesses, and individuals. Our country pays a steep price in lost innovation, jobs, economic advantage, and reduced U.S. military strength. COVID-19 has only made these threats more dangerous and impactful as the nation's health hangs in the balance. CDSE provides resources and training to enhance security professionals' knowledge of supply chain risk management to help secure the supply chain or to help achieve supply chain integrity.

Real-World Scenarios Featured in Case Studies

CDSE has 16 CI case studies available, which are analyzed accounts of real-world security activities, events, or threats designed with the DoD and industry security professional in mind. Two soon to be released Counterintelligence case studies will highlight front companies that manufacture and sell counterfeit parts. Counterfeit parts represent a tremendous risk to the supply chain and critical technology protection. Imagine a fighter jet or Mine Resistant Ambush Protected (MRAP) vehicle with counterfeit parts. One faulty part can result in loss of life and unforeseen economic losses to the U.S. Find our CI case studies here.

Threat Awareness in Cyberspace

This report from NCSC sheds light on the most pervasive nation-state threats in cyberspace. It includes a list of industrial sectors and technologies of the highest interest to malicious actors as well as disruptive threat trends to be aware of. Download the "Foreign Economic Espionage in Cyberspace" report here.

Supply Chain Posters

Security awareness posters are some of our most popular downloadable resources on the CDSE website. If your workforce is still reporting to your physical workspace, share and display them to promote supply chain awareness throughout the month.

- **Supply Chain Resiliency Month**
- **Deliver Uncompromised**