CDSE pulse VOLUME 2 ISSUE 4
April 2021

THIS MONTH'S FOCUS

NATIONAL SUPPLY CHAIN INTEGRITY MONTH

NATIONAL SUPPLY CHAIN INTEGRITY MONTH: A CALL TO ACTION

DID YOU KNOW?

One of the five pillars of the National Counterintelligence Strategy of the United States 2020-2022 is to "Reduce Threats to Key U.S. Supply Chains."

April is "National Supply Chain Integrity Month" and 2021 is the fourth year this month is nationally recognized. During the month, the Department of Defense (DOD), the Office of the Director of National Intelligence (ODNI), the Cybersecurity and Infrastructure Security Agency (CISA) and other government and industry partners have promoted a call-to-action campaign with two goals:

- Raise awareness of supply chain threats and mitigation efforts and
- Strengthen supply chains against foreign adversaries and other potential risks

The National Counterintelligence and Security Center (NCSC), located within ODNI, 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. To help industry and government stakeholders, NCSC released new supply chain risk management resources that can be found at the **NCSC supply chain website**. Additionally, throughout April, NCSC has issued sector-specific guidance on supply chain risk management for the following sectors: information and communications technology (ICT), manufacturing and production, healthcare, and energy on the same website.

CDSE – Center for Development of Security Excellence

@TheCDSE

Center for Development of Security Excellence

NATIONAL SUPPLY CHAIN INTEGRITY MONTH: A CALL TO ACTION (CONT'D)

As the nation's risk advisor, CISA, partners with the public and private sector to enhance the security and resilience of the global ICT supply chain. The agency works to ensure that supply chain risk management (SCRM) is an integrated component of their cybersecurity initiatives. Throughout April, CISA has promoted resources, tools, and information to help organizations and agencies integrate SCRM into their security programs. CISA themes for the month has included:

Week 1:	Building Collective Supply Chain Resilience
Week 2:	Assessing ICT Trustworthiness
Week 3:	Understanding Supply Chain Threats
Week 4:	Knowing the Essentials

To learn more about how CISA is enhancing supply chain resilience and to view online resources, **https://www.cisa.gov/supply-chain-integrity-month**.

The Center for Development of Security Excellence (CDSE) has scheduled two webinars to support Supply Chain Integrity. The first event "Supply Chain Risk Management 2021" kicked off the month on April 1. If you missed it, there will be another opportunity to view the Speaker Series once it is posted online. There is still time to **register** for our second event "**Supply Chain Due Diligence 2021**" on Thursday, April 29, 2021, 12:00 – 1:00 p.m. ET. Join us for this live discussion that will go in-depth on due diligence reporting for supply chain, as well as where and how to find information concerning your suppliers.

PROTECTING THE SUPPLY CHAIN ONE YEAR INTO THE COVID-19 PANDEMIC

"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.

It has been over a year since the United States went into lockdown to slow down and prevent the spread of COVID-19. With life-saving vaccines currently in production and distribution, the security of our Nation's supply chains are more important than ever. A strong supply chain leads to more efficient vaccine creation and transport, which leads to more vaccines that are available for the public, which means a quicker return to normalcy. A secure supply chain benefits everyone, and government and industry must remain vigilant against those who attempt to disrupt it.

On March 4 of this year, CISA announced a six-month extension of the Information and Communications Technology (ICT) Supply Chain Risk Management Task Force. The Task Force, chaired by CISA and the Information Technology (IT) and Communications Sector Coordinating Councils, is a public-private partnership composed of a diverse range of representatives from large and small private sector organizations charged with identifying challenges and devising workable solutions and recommendations for managing risks to the global ICT supply chain.

"The work of the Task Force over the past two years has been invaluable to the critical infrastructure community," said Bob Kolasky, CISA Assistant Director and Task Force Co-Chair. "Extending the charter for six additional months ensures the Task Force has the support and flexibility needed to function as a high-leverage, public-private partnership able to work beyond the normal governmental processes to address unique challenges impacting global ICT supply chains."

It is important to remain vigilant when it comes to securing the supply chain since there are individuals and groups that will try to sabotage it.

One such supply chain attack was the SolarWinds Orion Code compromise of December 2020. In an emergency directive released on December 21, 2020, Department of Homeland Security (DHS) stated that malicious actors were exploiting SolarWinds Orion products. "This tactic permits an attacker to gain access to network traffic management systems." CISA determined that this exploitation of SolarWinds products posed an unacceptable risk to Federal Civilian Executive Branch agencies and required emergency action. They based this determination on the

"As supply chain attacks on our global ICT infrastructure become more frequent, aggressive – and increasingly consequential – now is the time for our Task Force to double down on its critical work," said Robert Mayer, Senior Vice President, Cybersecurity and Innovation, and Task Force Co-Chair. "Over the last two years, we've engaged a dozen government agencies and IT and communications stakeholders to make the global supply chain less vulnerable to a broad spectrum of supply chain attacks."

PROTECTING THE SUPPLY CHAIN ONE YEAR INTO THE COVID-19 PANDEMIC (CONT'D)

exploitation of affected products and their widespread use to monitor traffic on major federal network systems, which created a high potential for a compromise of agency information systems. The SolarWinds compromise emphasized the need to protect our supply chain, and the White House released two new executive orders to solidify its stance on supply chain security.

The first Executive Order, released on January 21 of this year, secured the supplies necessary for responding to the pandemic, so that those supplies are available, and remain available, to the Federal Government and state, local, tribal, and territorial authorities, as well as the healthcare sector. It also called for the Secretary of State, Secretary of Defense, Secretary of Health and Human Services, and the Secretary of Homeland Security to immediately review the availability of critical materials, treatments, and supplies needed to combat COVID-19 (pandemic response supplies), including personal protective equipment (PPE) and the resources necessary to effectively produce and distribute tests and vaccines at scale. (**Executive Order 14001**, January 21, 2021)

The next Executive Order, released on February 24, 2021 consisted of two main points. First, the order directs an immediate 100-day review across federal agencies to address vulnerabilities in the supply chains of four key products: APIs (the part of a pharmaceutical product that contains the active drug), critical minerals, semiconductors and advanced packaging, and large capacity batteries. Second, the order calls for a more in-depth one-year review of a broader set of U.S. supply chains. These two Executive Orders acknowledge that the United States needs resilient, diverse, and secure supply chains to ensure our economic prosperity and national security. (**Executive Order 14017**, February 24, 2021)

CDSE supports the call-to-action campaign to raise awareness of supply chain threats and strengthening them by providing supply chain integrity training and resources to DOD and cleared industry. Personnel are introduced to supply chain risk management, supply chain vulnerabilities, mitigation strategies, and reporting threats or incidents. This newsletter highlights CDSE's supply chain integrity eLearning, webinars, job aids, and toolkits as well as resources from CISA and NCSC.

One of our newest toolkits was developed in response to the pandemic. CDSE helped develop the Operation Warp Speed (OWS) and Beyond Toolkit for cleared and uncleared industry partners working on OWS. This toolkit provides information and resources to protect the important work performed by OWS partners.

The global COVID-19 pandemic continues to present challenges to the security of our Nation's supply chain, which can best be overcome through training, awareness, and vigilance. The year 2020 was about finding our footing and learning how to mitigate new vulnerabilities associated with telework and the use of new collaboration tools/technologies during the already tumultuous days of quarantine. This year, 2021, is about taking the lessons learned from the previous year and using them to ensure that we continue to secure our supply chains as we replenish our stocks of PPE, other medical equipment, and produce and distribute vaccines as quickly and efficiently as possible. We need to foster security awareness and remain vigilant to continue to meet these demands!

CDSE SUPPLY CHAIN INTEGRITY RESOURCES

CDSE has a variety of job aids and toolkits that provide information to help perform role-based tasks. These resources raise understanding and awareness of supply chain risk management policies, potential threats/vulnerabilities, and mitigation strategies:

- **Supply Chain Risk Management Job Aid**
- **Software Supply Chain Attacks Job Aid**
- **Acquisition Toolkit**
- **Counterintelligence Toolkit: Supply Chain Risk Management**
- **Cybersecurity Supply Chain Toolkit**
- **Deliver Uncompromised Toolkit: Critical Technology Protection**
- **Operation Warp Speed (OWS) and Beyond Toolkit**

UPCOMING SPEAKER SERIES AND WEBINARS

CDSE invites you to **sign up** for our upcoming Speaker Series:

Supply Chain Due Diligence 2021
Thursday, April 29, 2021
1:00 p.m. – 2:00 p.m. ET

Overview of Continuous Vetting (CV) Methodology
Wednesday, June 16, 2021
12:00 p.m. – 1:00 p.m. ET

Organizational Culture and Countering Insider Threat: Best Practice Examples from the Marine Corps Insider Threat Hub
Thursday, July 29, 2021
12:00 p.m. – 1:00 p.m. ET

ENHANCE YOUR KNOWLEDGE WITH SUPPLY CHAIN ELEARNING COURSES

The Defense Acquisition University (DAU) and CDSE have partnered to improve the security and acquisition knowledge of both their respective communities. The goal is to ensure acquisition professionals have access to training and resources necessary to improve their understanding and application of security best practices. Likewise, security professionals are provided the training and support tools required to increase their knowledge of the acquisition process, to include supply chain risk management and lifecycle logistics. The following eLearning courses are recommended to help understand the acquisition process and steps for helping to secure supply chains:

- **Contracting for the Rest of Us DAU-CLC011.16**
- **Counterfeit Prevention Awareness DAU-CLL062.16**
- **Counterintelligence Awareness and Security Brief CI112.16**
- **DOD Supply Chain Fundamentals DAU-CLL037.16**
- **Preventing Counterfeit Electronic Parts from Entering the DOD Supply System DAU-CLL032**
- **Program Manager Introduction to Anti-tamper DAU-CLE022.16**
- **Program Protection Planning Awareness DAU-ACQ160.16c**
- **Protecting Assets in the NISP CI117.16**
- **Counter-Proliferation CI118.16**
- **Supply Chain Risk Management for Information and Communications CLE080**

DVSCI RECORDINGS NOW AVAILABLE

The recordings from the 2021 DOD Virtual Security Conference for Industry (DVSCI) are available now until August 28, 2021 at **https://cdse.acms.com/dvsci-2021-recordings/event/login.html**.

CDSE WINS THREE HORIZON AWARDS

The Horizon Interactive Awards, a leading international interactive media awards competition, has announced the 2020 award winners to highlight this year's "best of the best" in interactive media production. CDSE was awarded three awards:

Product	Category	Award
Insider Threat Awareness Month Website	Websites - Government Agency	Bronze
Insider Threat App Sentry Mobile App	Mobile Apps - Education	Silver
Insider Threat Resilience Animation Video	Video - Instructional	Gold

The Horizon Interactive Awards holds the competition each year with the winners announced the following April. An international panel of judges, consisting of industry professionals with diverse backgrounds evaluated over 50 categories spanning multiple media types. The 2020 winning entries showcase the industry's best interactive media solutions from some of the top designers, producers, and developers all over the globe.

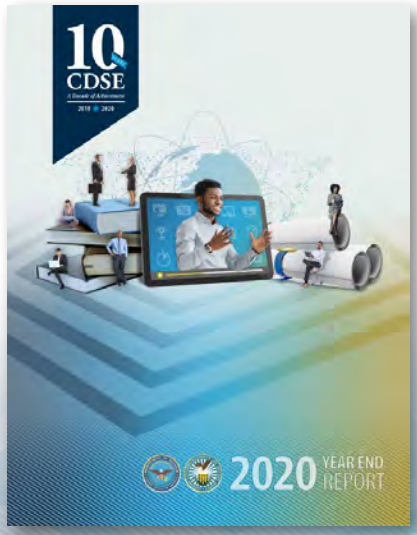
WHAT STUDENTS ARE SAYING

Course: Thwarting the Enemy: Providing Counterintelligence & Threat Awareness to the Defense Industrial Base CI111.16

"For an online course, this training is about the best I have encountered. Its [sic] direct, timing is right (not too long or short), and fluid through each section."

– Student

CDSE YEAR END REPORT NOW AVAILABLE



The CDSE Fiscal Year 2020 (FY20) Year End Report is now available on the CDSE website (**https://www.cdse.edu/annualreport/index.html**) and covers FY20 new products, accomplishments, awards, and more!

Download a copy

NEW TOPIC ON EMAIL SUBSCRIPTION SERVICE

CDSE subscribers can now sign up to receive product updates each quarter! This publication includes a list of new and changed products with descriptions and links for each.

To subscribe, visit **https://www.cdse.edu/news/index.html**