CDSE pulse
VOLUME 3 ISSUE 4
April 2022

THIS MONTH'S FOCUS

NATIONAL SUPPLY CHAIN INTEGRITY MONTH

DID YOU KNOW?

Protecting the ICT supply chain is a supply chain security force-multiplier for all other critical supply chains.

CDSE – Center for Development of Security Excellence

@TheCDSE

Center for Development of Security Excellence

CDSE Pulse

Published by the Defense Counterintelligence and Security Agency (DCSA) Center for Development of Security Excellence (CDSE) Marketing and Communications Office.

DCSA Leadership

William K. Lietzau
Director, DCSA

Daniel Lecce
Deputy Director, DCSA

Kevin Jones
Assistant Director, Training

Erika Ragonese
Deputy Assistant Director, Training

CDSE Leadership

Heather Mardaga
Director

Zinethia Clemmons
Chief, Shared Services

Pulse Staff

Adriene Brown
Chief Content Officer

Samantha Dambach

Natalie Perkins
Content Developers/ Managers

Isaiah Burwell
Content Writer

Marc Pulliam
Content Designer

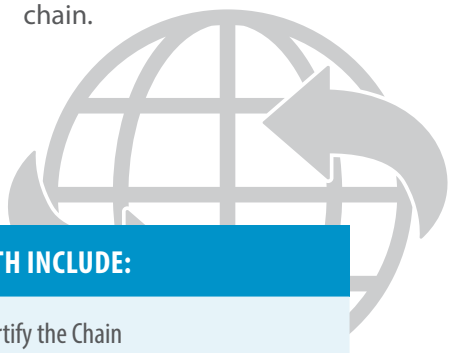
NATIONAL SUPPLY CHAIN INTEGRITY MONTH: A CALL-TO-ACTION CAMPAIGN

This April marks the fifth annual National Supply Chain Integrity Month for organizations across the country. 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 will promote a call-to-action campaign to "Fortify the Chain."

For this month, the National Counterintelligence and Security Center (NCSC), located within ODNI, has released new supply chain risk management resources to help industry and government stakeholders. Visit the **NCSC supply chain website** to find information on supply chain threats, best practices, and links to other partner agency resources.

As the Nation's risk advisor, one of CISA's top priorities is to help secure the global information and communications technology (ICT) supply chain from emerging threats. Throughout April, CISA is promoting resources, tools, and information to help organizations and agencies protect their ICT supply chains. To access CISA's online resources visit their **Supply Chain Integrity Month webpage**.

The Center for Development of Security Excellence (CDSE) scheduled two webinars to support Supply Chain Integrity month. The first event "Supply Chain Past, Present, and Future" was held on April 7. If you missed it, there will be another opportunity to view the webinar once it is posted online. There is still time to register for our second event **"Microelectronics and Supply Chain 2022"** on Thursday, April 28, 2022, 12:00 – 1:00 p.m. ET. Join us for this live discussion that will go in-depth on microelectronics issues and concerns, practical steps the security community can take, and what we need to be aware of to secure the microelectronics supply chain.



CISA THEMES FOR THE MONTH INCLUDE:
Week 1: Power in Partnership – Fortify the Chain
Week 2: No Shortages of Threats – Educate to Mitigate
Week 3: Question, Confirm, and Trust – Be Supplier Smart
Week 4: Plan for the Future – Anticipate Change

A JOINT EFFORT: SECURING THE ICT SUPPLY CHAIN

This year's National Supply Chain Integrity Month theme focuses on securing the information and communications technology (ICT) supply chain and Executive Branch efforts to address this critical issue. Every company, organization, and individual that uses ICT products and services, such as cell phone devices, online banking, and cloud computing, is part of a globally connected supply chain.

"This year's campaign is focused on fortifying the U.S. Information and Communications Technology (ICT) supply chain, which powers America's national security missions, critical infrastructure sectors, and private sector innovations," said Michael Orlando, Senior Official Performing the Duties of NCSC Director."

Supply chain risk increases when adversaries attempt to exploit ICT and their related supply chains for the purposes of espionage, sabotage, and foreign interference activity. Vulnerabilities in supply chains, either developed intentionally for malicious intent or unintentionally through poor security practices, can enable data and intellectual property theft, loss of confidence in the integrity of the system, or exploitation to cause system or network failure. Increasingly, adversaries, including foreign adversaries such as Russia, China, North Korea, and Iran, are looking at these vulnerabilities as principal attack vectors.

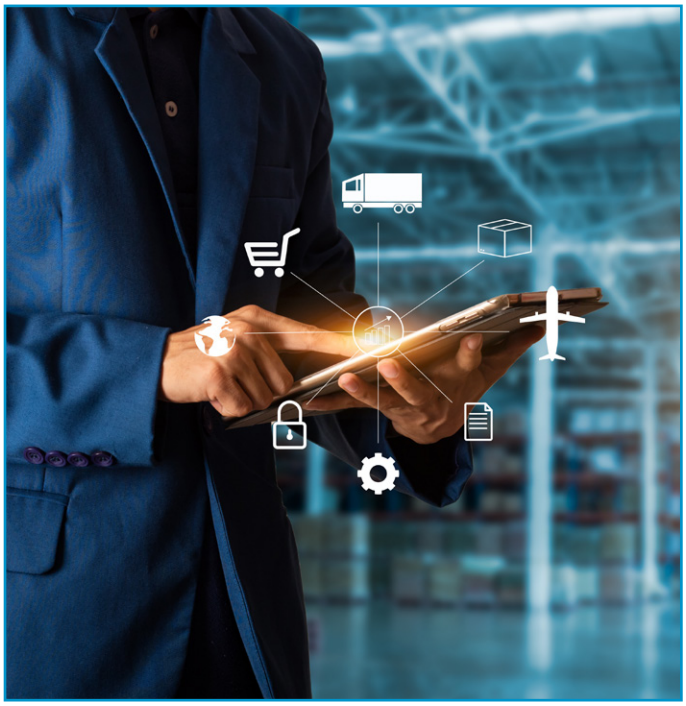
According to one private security report, software supply chain attacks more than tripled in 2021 compared to 2020. The exploitation of these vulnerabilities raised the bar for software security and the need for more public-private partnerships.

In December 2018, CISA established the ICT Supply Chain Risk Management (SCRM) Task Force. The ICT SCRM Task Force is a public-private partnership focused on global ICT supply chain security. It is composed of a diverse range of professionals within the Information Technology and Communications Sectors with representatives from large and small private sector organizations and federal agencies. This includes subject matter experts, infrastructure owners and operators, and other key stakeholders who provide recommendations and guidance to help shape trusted supply chain practices.

Over the next several months, the Task Force's efforts will include the launch of a new Hardware Bill of Materials Working Group, continuation of two current working groups, and scoping of two additional efforts related to promoting software assurance and, the utility of Software Bill of Materials.

The ongoing COVID-19 pandemic highlighted vulnerabilities in complex global supply chains in very real ways to the public, government, and industry. In order to strengthen the national industrial base during times of disruption, the President signed Executive Order (E.O.) 14017 on February 24, 2021. The E.O. calls for a comprehensive review of supply chains in critical sectors, including the defense industrial base (DIB).

In response to E.O. 14017, the Department of Commerce and Department of Homeland Security released a one-year report titled, "Assessment of the Critical Supply Chains Supporting the U.S. Information and Communications Technology Industry." The report defines the critical sectors and subsectors supporting the ICT industry, evaluates



the current supply chain conditions, identifies key risks that threaten to disrupt those supply chains, and proposes eight recommendations to mitigate risk and strengthen supply chain resiliency.

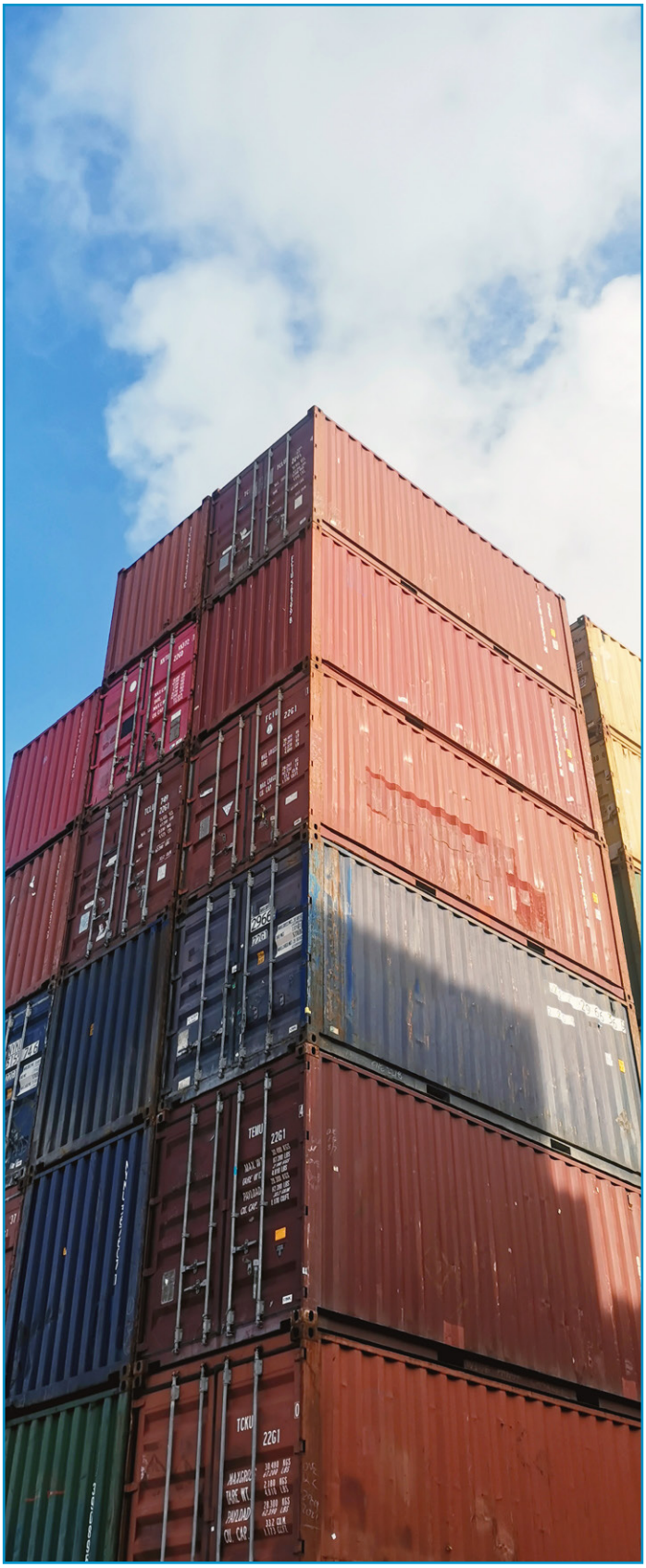
DOD also released the report "Securing Defense-Critical Supply Chains," February 24, 2022, in response to E.O. 14017. This report outlines government and national strategies for assessing and strengthening critical DIB supply chains.

> "This report is a strategic roadmap for the department to build lasting resilience in our defense industrial base." Andrew Hunter, Acting Under Secretary of Defense for Acquisition and Sustainment.

In the report, DOD highlights a set of strategic enablers that underpin overall mission success and supply chain resilience. One of those strategic enablers is cyber posture. Making Cybersecurity-Supply Chain Risk Management (C-SCRM) a priority was identified as key to enhancing supply chain cyber resilience.

Cybersecurity-Supply Chain Risk Management (C-SCRM) efforts manage supply chain risk by identifying susceptibilities and vulnerabilities to cyber-threats throughout the supply chain and developing mitigation strategies to counter those threats whether presented by the supplier, the supplier's products and its subcomponents, or the supply chain (e.g., initial production, packaging, handling, storage, transport, mission operation, disposal). Several organizations provide C-SCRM training and resources for government and industry personnel. NCSC, CISA and CDSE all have a wealth of training and resources available to increase C-SCRM knowledge and raise awareness of threats, mitigations, and best practices to improve supply chain integrity. These learning and awareness resources are designed to emphasize the role that we all have in securing ICT supply chains.

ICT products and services ensure the continued operation and functionality of U.S. critical infrastructure. When a supply chain incident occurs, everyone suffers: buyers, suppliers, and users. Government and industry partners have come together to combat the threats to ICT. Securing the global ICT supply chain from the evolving risks of tomorrow through training and awareness should be a priority for industry and government personnel.



SUPPLY CHAIN INTEGRITY RESOURCES

CDSE has several toolkits that include courses to enhance supply chain knowledge and performance support tools that provide information to help perform role-based tasks and raise understanding and awareness of supply chain risk management policies, potential threats/vulnerabilities, and mitigation strategies:

- **Acquisition Toolkit**
  https://www.cdse.edu/Training/Toolkits/Acquisition-Toolkit/
- **Counterintelligence Awareness Toolkit: Supply Chain Risk Management Tab**
  https://www.cdse.edu/Training/Toolkits/Counterintelligence-Awareness-Toolkit/
- **Cybersecurity: Supply Chain Risk Management Tab**
  https://www.cdse.edu/Training/Toolkits/Cybersecurity-Toolkit/
- **Insider Threat Toolkit: Cyber Insider Threat/User Activity Monitoring Tab**
  https://www.cdse.edu/Training/Toolkits/Insider-Threat-Toolkit/
- **Deliver Uncompromised Toolkit**
  https://www.cdse.edu/Training/Toolkits/Deliver-Uncompromised-Toolkit/
- **Operation Warp Speed (OWS) and Beyond Toolkit**
  https://www.cdse.edu/Training/Toolkits/Operation-Warp-Speed-and-Beyond-Toolkit/

This includes several supply chain integrity month posters:

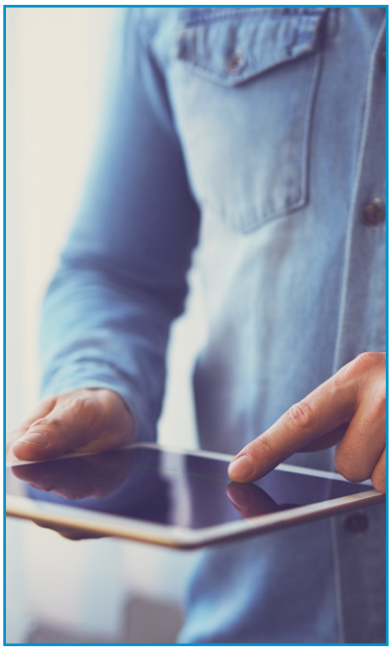
- **Insider Risk in Software Supply Chains**
  https://www.cdse.edu/Training/Security-Posters/Article/2978389/insider-risk-in-software-supply-chain/
- **Keep the Troops Safe**
  https://www.cdse.edu/Training/Security-Posters/Article/2753947/supply-chain-month/
- **Deliver Uncompromised**
  https://www.cdse.edu/Training/Security-Posters/Article/2753845/deliver-uncompromised-campaign/
- **Supply Chain Resilience Month**
  https://www.cdse.edu/Training/Security-Posters/Article/2753664/supply-chain-resilience-month/

NCSC and CISA also have resources to raise awareness and educate industry and government personnel on supply chain integrity issues and best practices:

- **NCSC Supply Chain Risk Management**
  https://www.dni.gov/index.php/ncsc-what-we-do/ncsc-supply-chain-threats
- **NCSC Awareness Materials**
  https://www.dni.gov/index.php/ncsc-how-we-work/ncsc-know-the-risk-raise-your-shield/ncsc-awareness-materials
- **CISA National Integrity Month**
  https://www.cisa.gov/supply-chain-integrity-month
- **CISA ICT Supply Chain Library**
  https://www.cisa.gov/ict-supply-chain-library
- **CISA ICT Supply Chain Toolkit**
  https://www.cisa.gov/ict-supply-chain-toolkit
- **ICT SCRM Task Force**
  https://www.cisa.gov/ict-scrm-task-force

NEW DIGITAL BADGING OPTION

CDSE recently launched the CDSE Digital Badging and Transcript Service for courses with an American Council on Education's College Credit Recommendation. The ACE College Credit Recommendation Service (CREDIT) connects CDSE courses with colleges and universities by helping employees gain access to academic credit for formal courses and examinations taken outside traditional degree programs.



ACE Credit recommendations allow students to transfer credit earned from approved courses toward completion of degree programs. Students who have completed a CDSE ACE Credit Recommended course are eligible to receive a digital badge through the Credly website. Digital badges are electronic representations of traditional paper certificates and offer several benefits:

- Provides verified digital recognition for acquiring new skills
- Allows hiring managers to easily validate acquired competencies
- Third parties can verify status of credentials in seconds online
- Easily share accomplishments and skillsets on social media
- Send official transcripts directly from Credly website

To learn more about the services offered and request a CDSE ACE digital badge or transcript, visit **My Certificates/Digital Badges/Transcripts**.

.

CDSE WINS HORIZON AWARDS

CDSE won six Horizon Interactive Awards and was recognized as a Distinguished Agency in the 2021 competition. CDSE received six bronze trophies for the following CDSE products:

Training/eLearning:
- Department of Defense (DOD) Mandatory Controlled Unclassified Information (CUI) Training/eLearning Websites (Bronze)

Videos:
- Center for Development of Security Excellence (CDSE) "Communication Products " PSA Video – Advertisement/ Commercial (Bronze)
- Center for Development of Security Excellence (CDSE) "Professional Affiliations" PSA Video – Advertisement/ Commercial (Bronze)
- Center for Development of Security Excellence (CDSE) "Industry" PSA Video – Advertisement/Commercial (Bronze)
- Center for Development of Security Excellence (CDSE) "Education vs. Training " PSA Video – Instructional (Bronze)
- Center for Development of Security Excellence (CDSE) The "Insider Threat Overview for FSOs" Video - Instructional (Bronze)

The Horizon Interactive Awards is a prestigious international competition recognizing outstanding achievement among interactive media producers. In its 20th year, the Horizon Interactive Awards recognize the best websites, videos, online advertising, print media, and mobile applications. Learn more by visiting the **Horizon Interactive Awards website**.

CDSE'S INSIDER THREAT VIGILANCE CAMPAIGN 2022

The 2022 Insider Threat Vigilance Campaign will be promoting a different theme each month and publishing/ distributing awareness materials relevant to that theme in unique ways throughout the year. Regular messaging through communication and awareness materials reinforces annual insider threat awareness training and helps ensure the workforce is prepared to recognize and respond to the insider threat.

Use this campaign or consider tailoring it to your organization with resources from our website: **https://www.cdse.edu/Training/ Toolkits/Insider-Threat-Toolkit/**

.

INSIDER THREAT SENTRY APP

Have you downloaded the Insider Threat Sentry App? This mobile addition to CDSE's insider threat portfolio expands the availability of posters, videos, security awareness games, job aids, case studies, and more. The application is available for users from the Android and iOS app stores. The app provides direct access to relevant insider threat content in one easy-to-use place. Download it today!

WHAT THE SECURITY COMMUNITY IS SAYING

Course: Protecting Assets in the NISP CI117.16

"This training was very logical & easy to follow. The exercise questions & final exam included questions (information) that was covered during the course/training."

"I thought the training was very well done in this section of the course. Material was up to date, presented in a logical manner, and easy to understand."

Cyber Insider Threat Course INT280.16

"I enjoyed this course much more than all the other courses I've taken. The format and the way the material was presented was well done."