CDSE pulse
VOLUME 1 ISSUE 11
November 2020

THIS MONTH'S FOCUS

CRITICAL INFRASTRUCTURE SECURITY AND RESILIENCE MONTH

PROTECTING CRITICAL INFRASTRUCTURE

Critical infrastructure is the power we use in our homes, transportation systems, farms that grow and raise our food, and the internet and communication systems we rely on to stay in touch with each other. Since these infrastructures benefit all Americans, it is everyone's responsibility to protect them. November is Critical Infrastructure Security and Resilience (CISR) Month, an effort led by the Department of Homeland Security's Cybersecurity and Infrastructure Security Agency (CISA) to raise awareness about protecting those essential systems from physical and virtual threats. This year's theme is "Critical Infrastructure in a Time of Transformation," in recognition of the rapid changes in technology and the impact of working/living in a pandemic.

Cybersecurity attacks are one of the primary threats critical infrastructure sectors face every day. In October 2020, a federal grand jury in Pittsburgh **charged** six Russian computer hackers, all of whom work for the Russian Main Intelligence Directorate. The charges were in response to destructive malware attacks in 2017 that infected computers worldwide, including hospitals and other medical facilities in the Western District of Pennsylvania; a FedEx Corporation subsidiary called TNT Express B.V.; and a large U.S. pharmaceutical manufacturer. The organizations suffered nearly $1 billion in losses from the attacks.

The Center for Development of Security Excellence (CDSE) supports one of the 16 sectors, the Defense Industrial Base (DIB), with security training and resources to provide security knowledge and awareness to help combat man-made threats, such as cyber and criminal incidents, as well as supply supply chain and terrorist attacks.

DID YOU KNOW?

The USA PATRIOT ACT of 2001 defined Critical Infrastructure as "systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety."

CDSE – Center for Development of Security Excellence

@TheCDSE

Center for Development of Security Excellence

PROTECTING CRITICAL INFRASTRUCTURE (CONT'D)

The DIB sector is the worldwide industrial complex that enables research and development, design, production, delivery, and maintenance of military weapons systems and subsystems to meet U.S. military requirements. It consists of more than 100,000 companies and their subcontractors who provide products and services for the DoD. The DIB is under attack from adversaries stealing critical technologies that jeopardize our mission readiness, the safety and security of our warfighters, and the security of our citizens.

CDSE provides a wide variety of security training and awareness products to support the protection of the DIB. The security training and awareness resources CDSE produces range from **Insider Threat training**, that teaches security professionals how to develop an Insider Threat Program, to games and crossword puzzles that teach the workforce cybersecurity terminology.

These training products and resources are crucial to providing the workforce with the security knowledge and tools needed to ensure the technologies developed and produced by the DIB are delivered to the warfighter uncompromised.

Physical, cyber, and insider threats will continue to attempt to disrupt, weaken, steal from, and destroy our productivity and technological advantages. Vigilance, resilience, enhanced security knowledge, and awareness will be the keys to combating those threats and protecting our technologies and capabilities. Explore this issue of the Pulse for more information on CDSE's Insider Threat, Cybersecurity, Counterintelligence, and Insider Threat training and resources which support the DIB workforce in the fight to protect their sector of critical infrastructure.

In 2020, a White House proclamation addressed the growing presence of cyber threats to critical infrastructure. "While advances in technology have enhanced the safety, security, and comprhensive integration of our Nation's critical infrastructure, vulnerabilities still exist, particularly those that can be exploited by cyber adversaries."

INSIDER THREAT

The COVID-19 pandemic has pushed many Americans to their financial and mental health limits. National Counterintelligence and Security Center (NCSC) Director William Evanina recently stated that "There are deeply personal human struggles related to healthcare, child care, financial insecurity, and political and cultural fissures. The risks for espionage, unauthorized disclosure, fraud, theft and even unwitting Insider Threat actions are higher than ever."

CDSE provides multiple products to help identify and mitigate insider threats with the ultimate goal of getting people the help they need. These products can be found in the **Insider Threat Toolkit** in the following tabs: Awareness & Training, Reporting, Resilience, and Research. CDSE also offers the following Critical Infrastructure resources:

Insider Threat Critical Infrastructure Toolkit

Insider Threat Programs for the Critical Manufacturing Sector

Insider Risk Programs for the Healthcare and Public Health Sector

Insider Threat in Critical Infrastructure

CYBERSECURITY

Cybersecurity was always a priority for the U.S., but with so many activities going virtual due to the pandemic, it has become even more important. In a press release promoting the 17th annual National Cybersecurity Awareness Month (NCSAM), CISA Director Christopher Krebs stated that "Gone are the days when individuals could think about cybersecurity casually. Our homes, schools, and businesses are now more connected than ever, introducing a whole new set of potential vulnerabilities."
CDSE has met this challenge head on with a variety of cybersecurity training and awareness content. The following are a few products recommended to enhance workforce cybersecurity awareness and knowledge:

Cybersecurity Awareness

Phishing Awareness

Cybersecurity and Telework: Concerns, Challenges, and Practical Solutions Pt 1 and Pt 2

Staying Protected While Connected

Find additional resources on the **Cybersecurity Content site**.

COUNTERINTELLIGENCE AWARENESS

"Exploitation of our supply chains by foreign adversaries – especially when executed in concert with cyber intrusions and insider threat activities – represents a direct and growing threat to strategically important U.S. economic sectors and critical infrastructure," added NCSC Director Evanina.

The purpose of CDSE's Counterintelligence (CI) Awareness is to make DoD and industry security personnel aware of their responsibility to report unusual activities or behaviors. CDSE's CI Awareness Program helps Americans identify various threats from foreign intelligence entities, other illicit collectors of U.S. defense information, or terrorists. The following resources are recommended to increase CI knowledge and awareness for the DIB workforce:

Counterintelligence Awareness for Defense Critical Infrastructure Job Aid

CI Awareness and Training Toolkit

Deliver Uncompromised Toolkit

INDUSTRIAL SECURITY

CDSE's Industrial Security Program is a multi-disciplinary security program focused on the protection of classified information developed by, or entrusted to, U.S. industry operating under the National Industrial Security Program (NISP). CDSE provides training and awareness products on subjects ranging from the safeguarding of classified information to transmission and transportation for industry. **The Facility Security Officer (FSO) Toolkit**: FSO and Safeguarding tabs contain resources to enhance the knowledge and awareness of the workforce to protect critical information and technology.

CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENCY (CISA)

CISA works with businesses, communities, and government at every level to help make the nation's critical infrastructure more resilient to cyber and physical threats. Everyone has a role in securing our Nation's critical infrastructure. Learn more by viewing these CISA resources:

Infrastructure Security Month

A Guide to Critical Infrastructure Security and Resilience

Infrastructure Security Toolkit

Critical Infrastructure Training

STEPP • SUPPORT •

NAVIGATION BUTTONS MISSING WHEN COURSE LAUNCHES?

If you are launching STEPP from a new tab on an existing browser session, STEPP will inherit the previous session's zoom level. If the zoom setting is above 130%, the eLearning navigation buttons will not be visible at the bottom of the page.

To fix this, press and hold the control (ctrl) key while clicking the minus (-) key until the navigation buttons are visible at the bottom. This will work on all browsers. To return to previous zoom level, press and hold ctrl while clicking the plus (+) key.

★★★★★ WHAT STUDENTS ARE SAYING

About: Cybersecurity Awareness Course CS130.16

" It was excellent and I think will help many of our users grasp the gravity of this subject matter."
– Anonymous

"One of the best Cyber Awareness courses I have ever completed."
– Anonymous

"This is one of the best training courses I have taken. It moves smoothly and has very good information. The format and image of each page make it interesting to participate."
– Anonymous