CDSE pulse
VOLUME 3 ISSUE 11
November 2022

THIS MONTH'S FOCUS

CRITICAL INFRASTRUCTURE SECURITY AND RESILIENCE

DID YOU KNOW?

The Cybersecurity and Infrastructure Security Agency is the national coordinator for critical infrastructure and resilience.

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) Outreach and Engagement 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

Pulse Staff

Adriene Brown
Chief Content Officer

Samantha Dambach
Natalie Perkins
Content Developers/ Managers

Isaiah Burwell
Content Writer

Marc Pulliam
Content Designer

PROTECTING CRITICAL INFRASTRUCTURE TOGETHER

Critical infrastructure spans everything from telecommunications and chemical facilities to healthcare, financial systems, and much more. It is interdependent with other critical infrastructure and supporting systems and encompasses all the essential services that keep our country and our economy running. Each November, the Cybersecurity and Infrastructure Security Agency (CISA) hosts Infrastructure Security Month (ISM), an effort to educate and engage all levels of Government, infrastructure owners and operators, and the American public about the vital role critical infrastructure plays in the Nation's wellbeing and the need to secure it through organizational and individual efforts. The theme for this year's ISM is **Infrastructure Security is National Security: Together We Can Drive Down Risk, Build Resilience**.

In a White House proclamation about ISM, President Biden stated, "When our critical infrastructure shows signs of wear, everyday Americans pay the price." Not only do we need to protect critical infrastructure facilities and people in and around those facilities from physical threats, but we also need to be aware of new cyber vulnerabilities that emerge as our critical infrastructure systems increasingly integrate information

and operational technologies. There are a number of steps all organizations can take, such as strengthening security plans, exercising the preparedness of those plans, reducing risk and building resilience on both the physical and cyber fronts, and embedding resilience as a foundational design feature when upgrading or building new critical infrastructure.

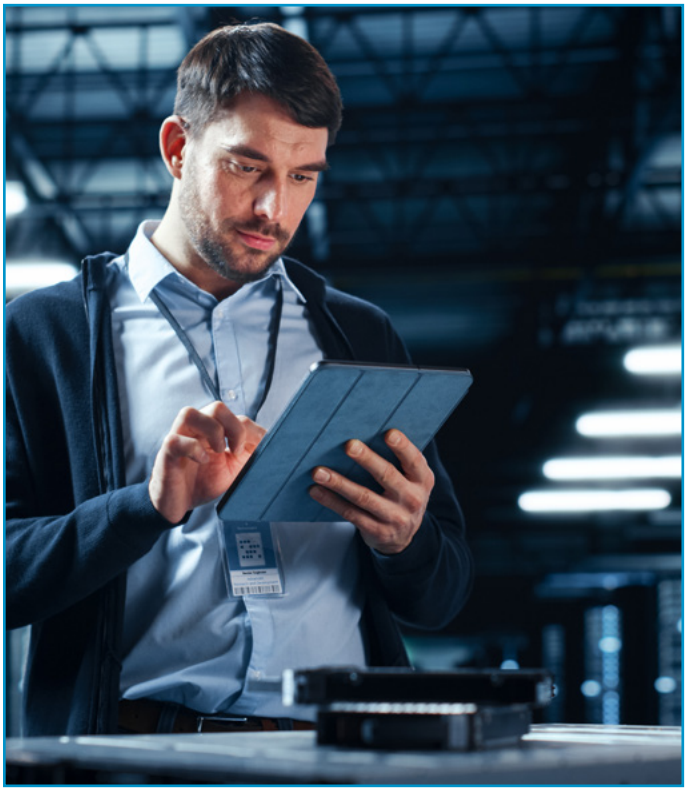
During ISM, public organizations and businesses may also promote awareness of threats and best security practices to protect critical infrastructure through social media, agency newsletters, email campaigns, fact sheets, job aids, posters, etc. Additionally, they can share information about security training and case studies with their workforce to increase their knowledge and develop enhanced security skills. Employees and individuals may participate in ISM by taking training, reviewing awareness messaging/materials, employing best security practices, and reporting security incidents/vulnerabilities/suspicious activities.

CISA provides all stakeholders with information and resources to prepare for, and respond to, various threats including active assailants, vehicular assaults, bombings, and more. Anyone can use CISA's suite of in-person and online trainings, tools, and informational materials to maintain situational awareness and prepare for and protect themselves during an incident. These resources, which can be found in this Pulse issue, help all stakeholders, including business owners, employees, and private sector security personnel better understand suspicious behaviors that may pose a threat and detail how to notify the appropriate authorities.

"CISA's mission is to lead the national effort to understand, manage, and reduce risk to the cyber and physical infrastructure Americans rely on every hour of every day—to get gas at the pump, food at the grocery store, money from the ATM, power, water, transportation, communications—effectively the backbone of networks and services that underpin our daily lives."

-CISA Director Jen Easterly

Homeland Security Presidential Directive-7 (HSPD-7) is a directive that assigns critical infrastructure protection responsibilities to the DOD and other organizations. As a federal department, DOD has both departmental and



national responsibilities. Departmental responsibilities include the identification, prioritization, assessment, remediation, and protection of defense critical infrastructure. Additionally, HSPD-7 directs all Federal departments and agencies to work together at a national level to "prevent, deter, and mitigate the effects of deliberate efforts to destroy, incapacitate, or exploit" critical infrastructure and key resources. DOD and the broader Federal Government will work with state and local governments and the private sector to accomplish this objective.

The Center for Development of Security Excellence (CDSE) offers a variety of cybersecurity, insider threat, industrial security, counterintelligence, general security training and security awareness resources (job aids/case studies/posters/videos) to help organizations educate their workforces about infrastructure security and how to promote it. Training is provided online and in-person. Security professionals and individuals can visit the CDSE website and sign up for emails to learn about and stay informed concerning the multitude of existing and new security products, and upcoming and archived events. A list of CDSE training and resources is available in this issue for quick access to pertinent products support raising awareness and protecting critical infrastructure.

WHAT'S NEW IN CRITICAL INFRASTRUCTURE SECURITY

In March 2022, President Biden signed the Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA) into law. CIRCIA creates legal protections and provides guidance to companies that operate in critical infrastructure sectors, including a requirement to report cyber incidents within 72 hours, and report ransom payments within 24 hours.

"The Cyber Incident Reporting for Critical Infrastructure Act of 2022 is a game changer for the whole cybersecurity community and everyone invested in protecting our Nation's critical infrastructure. It will allow us to better understand the threats we are facing, to spot adversary campaigns earlier, and to take more coordinated action with our public and private sector partners in response," said CISA Director Jen Easterly.

CIRCIA is a crucial step forward in protecting critical infrastructure, along with the training and resources other organizations already provide. Learn more by visiting **https://www.cisa.gov/circia**.

CDSE/CISA TRAINING AND RESOURCES

Establishing and maintaining a secure and resilient infrastructure protection program requires a multidisciplinary approach to include the following content areas:

Counterintelligence. The Counterintelligence (CI) Awareness Program's purpose is to make DOD and Industry Security personnel aware of their responsibility to report unusual activities or behaviors and various threats from foreign intelligence entities, other illicit collectors of U.S. defense information, and terrorists. CDSE provides **training and awareness resources** to help target workforces understand the threat and implement their reporting duties.

Cybersecurity. Cybersecurity is the ability to protect or defend the use of cyberspace from attacks. CDSE offers a wide range of **training and awareness products** to increase awareness of cyber threats and develop the skills your workforce needs to combat and mitigate those threats.

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 has **training and awareness products** on subjects ranging from the safeguarding of classified information to transmission and transportation for industry.

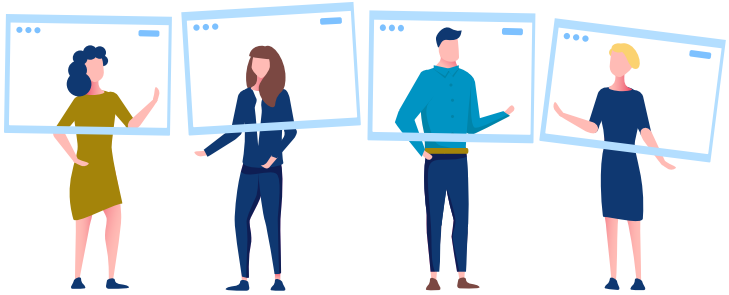
Insider Threat. Insider Threat Programs are designed to deter, detect, and mitigate actions by insiders who represent a threat to national security. CDSE supplies **multiple products** to help personnel or organizations learn how to identify and mitigate insider threats.

Physical Security. The Physical Security (PHYSEC) Program is that part of security concerned with active and passive measures, designed to prevent the unauthorized access to personnel, equipment, installations, materials, and information and to safeguard them against espionage, sabotage, terrorism, damage, and criminal activity. CDSE delivers numerous physical security **training and resource products** useful to our different stakeholders. *(Continued on next page)*

CDSE/CISA TRAINING AND RESOURCES *(CONTINUED)*

COURSES

COURSES	URL
Antiterrorism Officer (ATO) Level II (eLearning)	**https://www.cdse.edu/Training/eLearning/GS109/**
Assessing Risk and Applying Security Controls to NISP Systems (Instructor-led)	**https://www.cdse.edu/Training/Instructor-led/CS301/**
Counterintelligence Awareness and Reporting for DOD (eLearning)	**https://dl.dod.cyber.mil/wp-content/uploads/covid19/pdf/unclass-top_telework_tools-PUBLIC.pdf**
Cybersecurity Awareness (eLearning)	**https://www.cdse.edu/Training/eLearning/CS130/**
Introduction to Physical Security (eLearning)	**https://www.cdse.edu/Training/eLearning/PY011/**
NISP Reporting Requirements (eLearning)	**https://www.cdse.edu/Training/eLearning/PY011/**
Physical Security and Asset Protection (Instructor-led)	**https://www.cdse.edu/Training/Instructor-led/PY201/**
Physical Security Measures (eLearning)	**https://www.cdse.edu/Training/eLearning/PY103/**
Physical Security Planning and Implementation (eLearning)	**https://www.cdse.edu/Training/eLearning/PY106/**
Protecting Assets in the NISP (eLearning)	**https://www.cdse.edu/Training/eLearning/CI117/**
Suspicious Emails (eLearning)	**https://www.cdse.edu/Training/eLearning/CI021/**
Thwarting the Enemy: Providing Counterintelligence & Threat Awareness to the Defense Industrial Base (eLearning)	**https://www.cdse.edu/Training/eLearning/CI111/**



JOB AIDS

TITLE	URL
Counterintelligence Awareness for Defense Critical Infrastructure	**https://www.cdse.edu/Portals/124/Documents/jobaids/ci/CDSE_CIP__Job_Aid.pdf**
Insider Threat Programs for the Critical Manufacturing Sector	**https://www.cdse.edu/Portals/124/Documents/jobaids/insider/insider-threat-implem-guide-critical-man-job-aid.pdf**
Insider Risk Programs For the Healthcare and Public Health Sector	**https://www.cdse.edu/Portals/124/Documents/jobaids/insider/insider-risk-jobaid.pdf**
Security-in-Depth (SID) vs. Crime Prevention Through Environmental Design (CPTED)	**https://www.cdse.edu/Portals/124/Documents/jobaids/physical/PYJ0186-SID.pdf**
Deliver Uncompromised: Supply Chain Risk Management	**https://www.cdse.edu/Portals/124/Documents/jobaids/ci/deliver-uncom-supply-chain-risk-management-job-aid.pdf**
Understanding Espionage and National Security Crimes	**https://www.cdse.edu/Portals/124/Documents/jobaids/ci/ci-jobaidseries-understandingespionage.pdf**

TOOLKITS

TITLE	TABS
Acquisition	• eLearning
CI Awareness Toolkit	• Training and Awareness • Reporting/Requirements • Cyber CI • Counterterrorism • Foreign Travel and Visits • Supply Chain Risk Management
Cybersecurity Toolkit	• Social Media • Supply Chain Risk Management • Training and Awareness
Deliver Uncompromised Toolkit	• No Tabs

(Continued on next page)

TOOLKITS

TITLE	TABS
Facility Security Officer (FSO) Toolkit	• Reporting • Risk Management • eLearning
Insider Threat Toolkit	• Critical Infrastructure • Kinetic Violence • Research • Training and Awareness
Physical Security Toolkit	• Physical Security Planning • Electronic Security Systems • Security Measures

CISA RESOURCES

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. Learn more by viewing these CISA training and awareness resources:

RESOURCE TITLE	URL
2022 Infrastructure Security Month Webpage	**https://www.cisa.gov/infrastructure-security-month**
2022 Infrastructure Security Month Toolkit	**https://www.cisa.gov/sites/default/files/publications/ISM_2022_Toolkit_October%202022_Final-with-Cover_508c.pdf**
Securing Public Gatherings Resources: Everyone Webpage	**https://www.cisa.gov/all-stakeholders**
Securing Public Gatherings Resources: Businesses and Critical Infrastructure Webpage	**https://www.cisa.gov/spg-resources-businesses-and-ci-partners**
Critical Infrastructure Training Webpage	**https://www.cisa.gov/critical-infrastructure-training**
Critical Infrastructure Sectors Webpage	**https://www.cisa.gov/critical-infrastructure-sectors**
Office for Bombing Prevention Webpage	**https://www.cisa.gov/office-bombing-prevention-obp**
Stop Ransomware Webpage	**https://www.cisa.gov/stopransomware**

UPCOMING ILT/VILT TRAINING COURSES

As you consider signing up for one of CDSE's instructor-led (ILT) or virtual instructor-led (VILT) training courses, keep in mind training is free and VILT eliminates travel expenses. CDSE courses earn Professional Development Units (PDUs) toward maintenance of Security Professional Education Development (SPēD) Program certifications and credentials. Select courses with American Council on Education (ACE) credit recommendations may earn transfer credits at participating universities. Additionally, the DOD Security Specialist course is approved for Continuing Education Unit (CEU) credit toward several CompTIA certification renewals. Here is a list of ILT/VILT courses available from December 2022 through February 2023:

DOD Security Specialist Course (VILT)

January 9 – February 5, 2023
This course provides students a baseline of fundamental knowledge to perform common DOD security tasks and practices. It incorporates industrial, information, personnel, and physical security disciplines to understand their interrelationships, related policies, programs, and procedures.

SAP Mid-Level Security Management (VILT) SA201.10

ACE CREDIT CompTIA

January 17 – February 3, 2023
This course offers an in-depth explanation of Special Access Program (SAP) security management and focuses on the student's ability to determine enhanced security requirements based on the threat and vulnerability of SAPs.

Getting Started Seminar (GSS) for New FSOs (VILT)

ACE CREDIT CompTIA

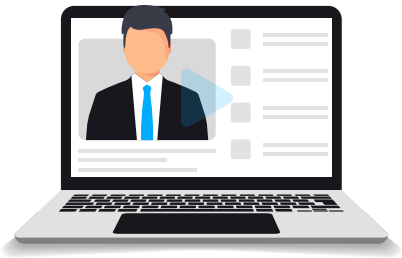
February 7 – 10, 2023
This course is not only a great way to get started as a new FSO, but also a way for experienced FSOs to learn about policy changes, procedural changes, emerging trends, threats, concerns, etc.

Orientation to SAP Security Compliance Inspections (ILT)

February 14 – 15, 2023
This course provides students with policy and direction to ensure inspections are standardized, equitable, and consistent across inspection agencies utilizing the DOD Special Access Program (SAP) Security Manuals.

NEW INDUSTRIAL SECURITY WEBCAST NOW AVAILABLE

CDSE has a new recorded webcast to improve your industrial security knowledge! This webcast "Metrics for a More Secure Industrial Security Program," provides a greater understanding of how the National Access Elsewhere Security Oversight Center (NAESOC) uses the information that you report to create tools and mitigations that support your security program. It also provides an enhanced awareness of how you can ensure effective program execution and how NAESOC resources can help you "get it right." View the recording at **https://www.cdse.edu/Training/Webinars-and-Conferences/Webinar-Archive/Metrics-for-a-More-Secure-Industrial-Security-Program/** .



2022 VIRTUAL DOD SECURITY CONFERENCE PRESENTATIONS NOW AVAILABLE

The 2022 Virtual DOD Security Conference was held on October 12-13 and drew nearly 2,000 participants! This year's conference theme was "Developing a Resilient Security Workforce in a Changing Environment" and 30% of the participants were attending for the first time. The agenda included policy change and implementation updates on topics such as security in a digital world, operations security, controlled unclassified information, personnel security policy, PERSEREC studies, and more. If you missed the conference or would like to revisit the presentations, the recordings are available now in the CDSE Conference Archive. Please note, you must have a .mil or.gov email to access the presentations.

WHAT THE SECURITY COMMUNITY IS SAYING

Thwarting the Enemy: Providing CI and Threat Awareness for the Defense Industrial Base (CI111.16)

"Everything executed flawlessly. The content was relevant, comprehensive, and, most importantly, in a highly digestible format."

CI Awareness and Reporting for DOD Employees (CI116.16)

"This training is absolutely outstanding and well informative. Lots of great information to apply to my current job or to any job out there in the field."

"This is excellent. The terms are well-explained and elaborated for someone with no experience in the field. I like how everything is worded and all the terms are defined before they are used. Everything is divided into clearly marked categories and one has the option to follow their own path in learning the content. There are also fun facts about spies that help connect the content to real-life examples."

REGISTER FOR SPRING EDUCATION CLASSES

Registration is now open for the spring semester of CDSE Education classes that run from January 23 - May 21, 2023. Classes fill quickly, so please register early to secure your spot in the spring semester. The CDSE Education Program offers:

- Tuition-free, flexible and 100% virtual instructor-led courses
- Real-world practical assignments
- Virtual networking with professionals throughout the security community
- Five Security Education Certificate programs
- Highly qualified instructors

You can learn more about the available classes and register for them by accessing the links here: **https://www.cdse.edu/education/courses.html**

To register, log into STEPP via: **https://cdse.usalearning. gov/login/index.php**

If you have any questions, or need additional information, contact the CDSE Education Program at: **dcsa.cdseeducation@mail.mil**

CDSE NEWS

CDSE offers an email subscriber news service to get the latest CDSE news, updates, and information. You may be receiving the Pulse through your subscription, but if you were forwarded this newsletter from another source and would like to subscribe to the Pulse or one of our other publications, visit our news page to sign up or update your account today - **https://www.cdse.edu/news/index.html**

Insider Threat Bulletins	Flash	Quarterly Product Report