CDSE pulse
VOLUME 2 ISSUE 11
November 2021

THIS MONTH'S FOCUS

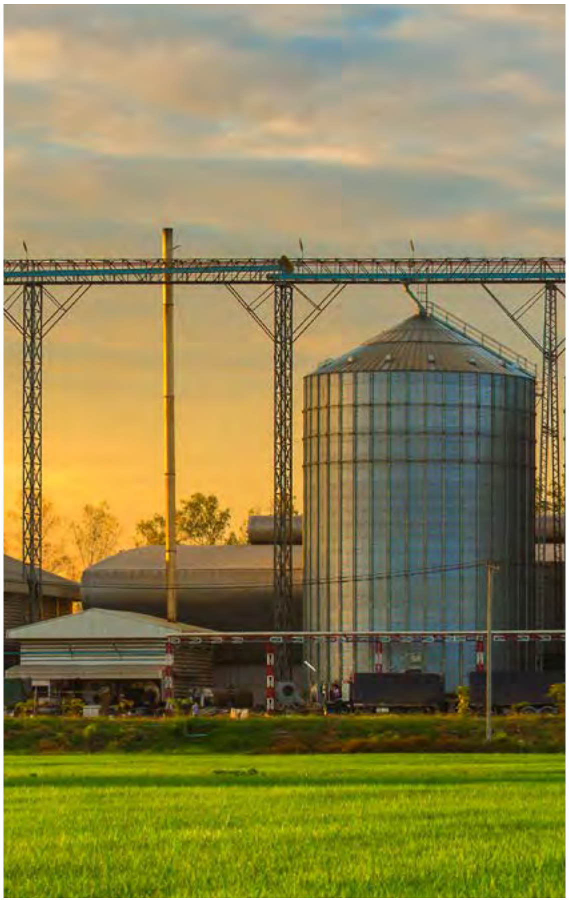
CRITICAL INFRASTRUCTURE SECURITY AND RESILIENCE

PROTECTING CRITICAL INFRASTRUCTURE: A SHARED RESPONSIBILITY

DID YOU KNOW?

The critical infrastructure community includes the owners and operators of critical infrastructure, officials across all levels of government, and all who benefit from our nation's critical infrastructure.

There are **16 critical infrastructure sectors** whose assets, systems, and networks (whether physical or virtual) are considered so vital to the United States that their incapacitation or destruction would have a debilitating effect on security, the economy, public health or safety, or any combination thereof. The Cybersecurity and Infrastructure Security Agency (CISA) promotes Infrastructure Security Month (ISM), an annual effort in November 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.



CRITICAL INFRASTRUCTURE SECTORS

Chemical	Commercial Facilities
Communications	Critical Manufacturing
Dams	Defense Industrial Base
Emergency Services	Energy
Financial Services	Food & Agriculture
Government Facilities	Healthcare & Public Health
Information Technology	Nuclear Reactors, Materials & Waste
Transportation Systems	Water & Wastewater Systems

CDSE – Center for Development of Security Excellence

@TheCDSE

Center for Development of Security Excellence

PROTECTING CRITICAL INFRASTRUCTURE: A SHARED RESPONSIBILITY (CONT'D)

The theme for ISM 2021 is "Critical Infrastructure Security and Resilience: Build it In" as a reminder to all audiences about how important it is to consider infrastructure security and resilience from design concept all the way through development and implementation. CISA also released a **toolkit** detailing how it will spotlight a different aspect of infrastructure security every week of ISM.

On October 29, 2021, the White House issued a **Presidential Proclamation** about ISM where President Joe Biden stated, "Threats to the critical infrastructure that we all depend on, which underpins our economic and national security, are among the most significant and growing concerns for our Nation, including cyber threats, physical threats, and climate threats… We must do everything we can to safeguard and strengthen the systems that protect us; provide energy to power our homes, schools, hospitals, businesses, and vehicles; maintain our ability to connect; and ensure that we have reliable access to safe drinking water."

WEEK 1

(November 1-7)
Interconnected and Independent Critical Infrastructure: Shared risk means building in shared responsibility.

WEEK 2

(November 8-14)
Planning for Soft Target Security: Build in security for mass gatherings starting with your planning.

WEEK 3

(November 15-21)
Building Resilience into Critical Infrastructure.

WEEK 4

(November 22-30)
Securing our Elections: Build resilience into our democratic processes.

Shining a spotlight on critical infrastructure is crucial due to modern, sophisticated cybercrimes that put the U.S. at risk. Earlier this year, major cyberattacks caused issues up and down the supply chain. Since our nation relies on critical infrastructure for health, energy, communications, and other vital services, it is equally important that everyone understand their role and take action to ensure our critical infrastructure remains strong, secure, and functional.

On October 18, 2021, CISA, the Federal Bureau of Investigation (FBI), and the National Security Agency (NSA) published a **cybersecurity advisory** regarding BlackMatter ransomware cyber intrusions targeting multiple U.S. critical infrastructure entities, including two U.S. food and agriculture sector organizations. The advisory includes technical details, analysis, and assessment of this cyber threat, as well as several mitigation actions to reduce the risk to this ransomware. "This advisory highlights the evolving and persistent nature of criminal cyber actors and the need for a collective public and private approach to reduce the impact and prevalence of ransomware attacks," said Eric Goldstein, Executive Assistant Director for Cybersecurity, CISA. "CISA, FBI and NSA are taking every step possible to try to make it harder for cyber criminals to operate. Americans can help us in this long-term endeavor by visiting **Stopransomware**.

INFORMATION FROM THE BLACKMATTER RANSOMWARE CYBERSECURITY ADVISORY:

Actions You Can Take Now to Protect Against BlackMatter Ransomware Implement and enforce backup and restoration policies and procedures.

- Use **strong, unique passwords**.
- Use **multi-factor authentication**.
- Implement network segmentation and traversal monitoring.

PROTECTING CRITICAL INFRASTRUCTURE: A SHARED RESPONSIBILITY (CONT'D)

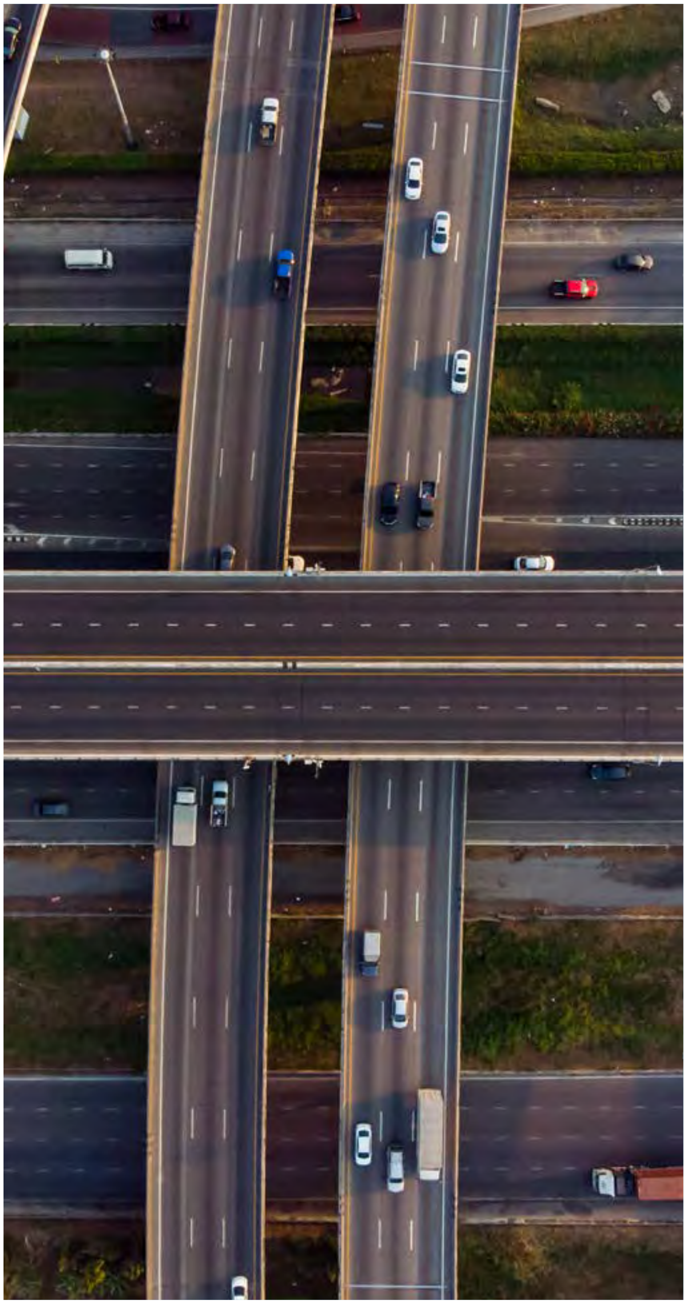
gov to learn how to reduce their risk of becoming a victim of ransomware."

In addition to cybersecurity incidents, critical infrastructure is under threat from a myriad of natural (climatological, meteorological, biological, geophysical, hydrological, etc.) and manmade (supply chain attacks, untrusted investment, foreign influence operations, unscheduled disruptions, criminal incidents and terror attacks, etc.) events.

Homeland Security Presidential Directive-7 (HSPD-7) is a directive that assigns critical infrastructure protection responsibilities to the Department of Defense (DOD) and other organizations. DOD is responsible for two roles for critical infrastructure protection. First, as a federal department, and second, as the Sector-Specific Agency for the Defense Industrial Base (one of the sixteen sectors previously mentioned). Within DOD, the Assistant Secretary of Defense for Homeland Defense and Americas' Security Affairs, ASD(HD&ASA), has the lead for providing policy, guidance, oversight, and resource advocacy for both roles. Visit the **Defense Critical Infrastructure Program (DCIP) web portal** to learn more about the program.

One of the key messages of ISM is that we all share in the responsibility to protect critical infrastructure. The CISA Infrastructure Security Month Toolkit lists many different ways for organizations and individuals to get involved in supporting critical infrastructure security and resilience. One of the primary actions is through promoting awareness and taking training. Training is vital to the success of a critical infrastructure security and resilience program. The training can cover general security concepts, best practices, or specific topics such as:

Physical security best practices	**Supply chain risk management**
Active shooter/ kinetic violence	**Identifying & Reporting Suspicious Activity**
Insider threat	**Cybersecurity**
Credentialing	**Antiterrorism**



The Center for Development of Security Excellence (CDSE) and CISA have a multitude of training and awareness products covering various critical infrastructure protection topics. Visit and share the training and resources from both organizations listed in this newsletter to enhance individual and agency knowledge/skills. Join us and do your part to secure our nation's critical infrastructure.

CDSE AND DOD TRAINING AND RESOURCES

Establishing and maintaining a secure and resilient infrastructure protection program requires a multidisciplinary approach. CDSE has training courses and resources in many of the disciplines needed to promote awareness and skills to protect our critical infrastructure.

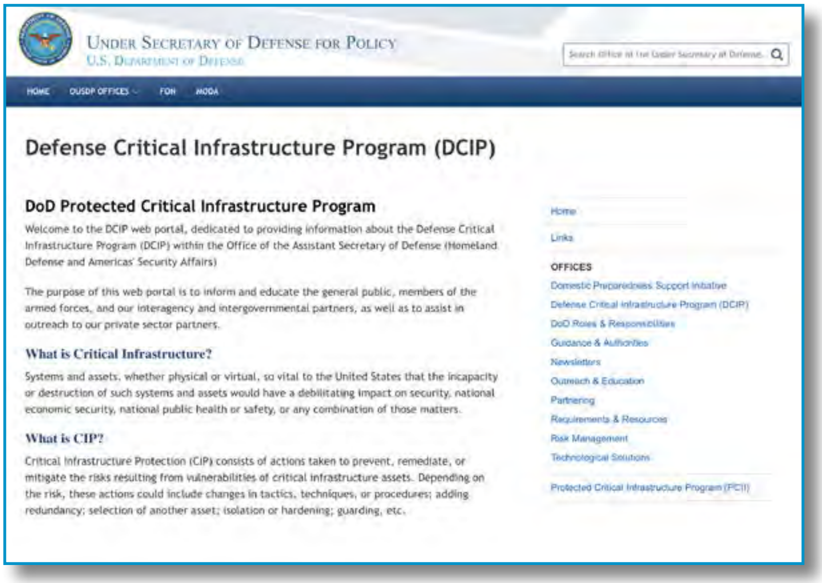
COUNTERINTELLIGENCE

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 the target workforces understand the threat and implement their reporting duties.

ELEARNING COURSES	JOB AIDS	TOOLKITS
Protecting Assets in the NISP **Thwarting the Enemy: Providing Counterintelligence & Threat Awareness to the Defense Industrial Base** **Counterintelligence Awareness and Reporting for DOD** **Suspicious Emails**	**Counterintelligence Awareness for Defense Critical Infrastructure** **Supply Chain Risk Management** **Understanding Espionage and National Security Crimes**	**CI Awareness Toolkit** • Training and Awareness • Reporting/Requirements • Cyber CI • Counterterrorism • Foreign Travel and Visits • Supply Chain Risk Management

DEFENSE CRITICAL INFRASTRUCTURE PROGRAM (DCIP)

The **DCIP web portal** is dedicated to providing information about the Defense Critical Infrastructure Program (DCIP). It is hosted by ASD(HD&ASA), The purpose of this web portal is to inform and educate the general public, members of the armed forces, and our interagency and intergovernmental partners, as well as to assist in outreach to our private sector partners. Visit the web portal today to learn more about DCIP.



UNDER SECRETARY OF DEFENSE FOR POLICY
U.S. DEPARTMENT OF DEFENSE
Search Office of the Under Secretary of Defense...
HOME
OUSDP OFFICES
FON
MODA

Defense Critical Infrastructure Program (DCIP)

DoD Protected Critical Infrastructure Program

Welcome to the DCIP web portal, dedicated to providing information about the Defense Critical Infrastructure Program (DCIP) within the Office of the Assistant Secretary of Defense (Homeland Defense and Americas' Security Affairs)

The purpose of this web portal is to inform and educate the general public, members of the armed forces, and our interagency and intergovernmental partners, as well as to assist in outreach to our private sector partners.

What is Critical Infrastructure?

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, or any combination of those matters.

What is CIP?

Critical Infrastructure Protection (CIP) consists of actions taken to prevent, remediate, or mitigate the risks resulting from vulnerabilities of critical infrastructure assets. Depending on the risk, these actions could include changes in tactics, techniques, or procedures; adding redundancy; selection of another asset; isolation or hardening; guarding, etc.

Home
Links
OFFICES
Domestic Preparedness Support Initiative
Defense Critical Infrastructure Program (DCIP)
DoD Roles & Responsibilities
Guidance & Authorities
Newsletters
Outreach & Education
Partnering
Requirements & Resources
Risk Management
Technological Solutions
Protected Critical Infrastructure Program (PCII)

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.

ELEARNING/ INSTRUCTOR-LED (ILT) COURSES	WEBINARS	TOOLKITS
Cybersecurity Awareness **Assessing Risk and Applying Security Controls to NISP Systems (ILT)**	Cybersecurity and Telework: Concerns, Challenges and Practical Solutions: **Part 1** **Part 2** **Part 3 (Collaboration Tool)**	**Cybersecurity** • Social Media • Supply Chain Risk Management • Training and Awareness

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 classified information to transmission and transportation for industry.

ELEARNING COURSES	TOOLKITS	
NISP Reporting Requirements	**Facility Security Officer (FSO)** • Reporting • Risk Management	**Acquisition** • eLearning **Deliver Uncompromised**
VIDEO		
Insider Threat Overview for FSOs		

INSIDER THREAT

Insider Threat Programs are designed to deter, detect, and mitigate actions by insiders who represent a threat to national security. CDSE provides **multiple products** to help personnel/organizations learn how to identify and mitigate insider threats. These products are located in the Insider Threat Toolkit tabs listed below along with two sector specific job aids developed last year:

ELEARNING COURSES	JOB AIDS	TOOLKITS
Insider Threat Awareness **Establishing an Insider Threat Awareness Program for Your Organization** **Insider Threat Mitigation Responses**	**Insider Threat Programs for the Critical Manufacturing Sector** **Insider Risk Programs for the Healthcare and Public Health Sector** **Insider Risk Mitigation Programs: Food and Agriculture Sector**	**Insider Threat** • Critical Infrastructure • Kinetic Violence • Research • Training and Awareness

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. Here is an abbreviated list of CDSE's PHYSEC training and resources:

ELEARNING COURSES	JOB AIDS	TOOLKITS
Antiterrorism Officer (ATO) Level II **Introduction to Physical Security** **Physical Security Measures** **Physical Security Planning and Implementation** **Physical Security and Asset Protection (ILT)**	**Security-in-Depth (SID) vs. Crime Prevention Through Environmental Design (CPTED)**	**Physical Security Toolkit** • Physical Security Planning • Electronic Security System • Security Measures

REGISTRATION NOW OPEN FOR THE GETTING STARTED SEMINAR

The next Getting Started Seminar(GSS) for FSOs is scheduled to start February 8, 2022 and it is entirely virtual! This course is not only a great way to get started as a new FSO, but also a way for experienced FSOs to stay informed about policy changes, procedural changes, emerging trends, threats, concerns, etc. Students work in collaboration with other security professionals, exploring security topics through practical exercises. To learn more and register today, visit **https://www.cdse.edu/Training/Virtual-Instructor-led-Courses/IS121/**

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:

Infrastructure Security Month

A Guide to Critical Infrastructure Security and Resilience

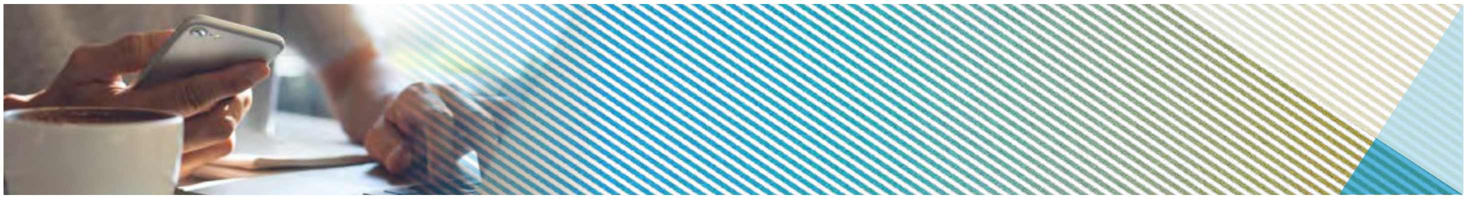
2021 Infrastructure Security Month Toolkit

Business Resources

Critical Infrastructure Training

Critical Infrastructure Sectors

Stop Ransomware



CDSE WEBSITE MIGRATION

The CDSE website has recently migrated to a new server and is working to resolve some issues users are experiencing when accessing the site. These may be resolved by entering in the full site URL: **https://www.cdse.edu** in your browser, but some of the issues may be related to site certificates. Additional updates to follow.

2021 INSIDER THREAT VIRTUAL CONFERENCE PRESENTATIONS NOW AVAILABLE

The 2021 Insider Threat Virtual Conference was held on September 2, 2021. The conference was open to security professionals in Government and industry and was jointly hosted by Defense Counterintelligence and Security Agency (DCSA) and Office of the Under Secretary of Defense for Intelligence & Security OUSD(I&S). The event brought security professionals and policy makers from across the U.S. Government and industry together to kick off the National Insider Threat Awareness Month (NITAM) campaign. The theme for this year's conference and campaign was "Workplace Culture and Insider Threat." If you missed the conference, or would like to revisit the presentations, the recordings are now available in our webinar archive under Insider Threat.

★★★★★ WHAT STUDENTS ARE SAYING

Cybersecurity Awareness and Reporting for DOD Employees (CI116.16) eLearning Course

“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.”

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

“Very interesting, practical presentation of the material. One of the best online trainings I’ve done.”

Physical Security and Asset Protection (PY201.01) Instructor-led Course

“The hands-on opportunity and peer interactions to process the information were invaluable to get insight and understand how to implement the information. Resources given were also vital to let me be able to independently adjust my own protocols and correct errors and gaps in our security practices and setups.”

“I have 100 building’s I need to protect and this course gave me the tools needed to do so.”

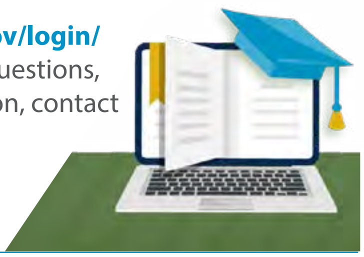
REGISTER FOR SPRING EDUCATION CLASSES

Registration is now open for the spring semester of CDSE Education classes that run from January 10 to May 6, 2022. Classes fill quickly, so please register early to secure your spot in the spring semester.

CDSE Education Program offers:

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

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: **dss.ncr.dss-cdse.mbx.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**