




**THIS  
MONTH'S  
FOCUS**

# INFRASTRUCTURE SECURITY AND RESILIENCE MONTH

**DID YOU KNOW?**

Most of our infrastructure was developed between the 1900s and early 2000s using climatological data from the mid-20th century, making it vulnerable to today's extreme weather and climate change. (CISA)

 CDSE – Center for Development of Security Excellence

 @TheCDSE

 Center for Development of Security Excellence

 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**

David M. Cattler     Daniel J. Lecce  
*Director, DCSA*     *Deputy Director, DCSA*

Kevin Jones     Erika Ragonese  
*Assistant Director, Security Training*     *Deputy Assistant Director, Security Training*

**CDSE Leadership**

Dr. Audrey Gutierrez     Glenn Stegall  
*Director*     *Deputy Director*

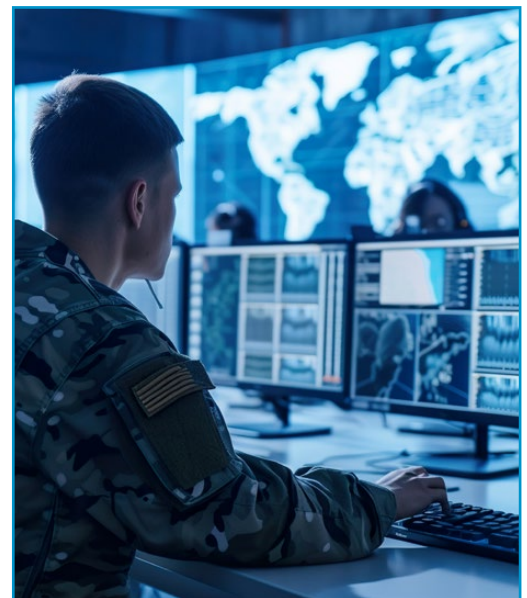
**Pulse Staff**

Cashmere He     Isaiah Burwell  
*Chief Content Officer*     *Content Writer*

Matthew Wright     Marc Pulliam  
Tammi Bush     *Content Designer*  
*Content Contributors*

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. Each November, the Cybersecurity and Infrastructure Security Agency (CISA) hosts Infrastructure Security Month (ISM), an annual 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.

Critical infrastructure spans telecommunications and chemical facilities, healthcare and financial systems, and more. It encompasses all the essential services that keep our country and our economy running. Extreme weather, as well as physical and cyberattacks, are threats to our critical infrastructure. Hurricanes Milton and Helene ravaged American cities this year, causing loss of life and property at high levels. Cyberattacks and mass shootings have become common occurrences on the evening news. Our responsibility is to strengthen critical infrastructure and protect the vital services they provide. We can do this by embracing resiliency and building it into our preparedness planning—and then continuously exercising those plans. The safety and security of the Nation depend on being adaptable to withstand and recover rapidly from disruptions. CDSE and CISA have both created resources that can help.



CDSE produced a **training video**, **job aid**, and **poster** to educate individuals about critical infrastructure threats. The video analyzes critical infrastructure from an insider threat perspective, showing how an insider's access and understanding of systems poses a unique danger. The job aid uses a counterintelligence perspective to coordinate the identification, assessment, assurance/protection, and real-time monitoring of physical and cyber infrastructures essential to the executing of the National Military Strategy.

CISA, as a leading agency, provides comprehensive **training** and resources so individuals can prepare for and respond to various threats, including active assailants, vehicular assaults, bombings, and more. These resources are designed to equip individuals and stakeholders, including



business owners, employees, and private sector security personnel, with the knowledge and skills to better understand suspicious behaviors that may pose a threat and detail how to notify the appropriate authorities.

During ISM, it's important to remember the responsibility of protecting critical infrastructure is a shared one. There are 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. However, it's not just about organizations. The public also plays a crucial role. Reevaluate your preparedness plans for securing public gatherings and make sure they are up to date with the latest techniques and tactics. Join us and take action to ensure our critical infrastructure is safe, secure, and resilient.

Additional resources:

- CDSE – CDSE's Cybersecurity **toolkit** contains critical infrastructure policy resources
- **Executive Order 13636 Improving Critical Infrastructure Cybersecurity**
- NIST Framework for Improving Critical Infrastructure Cybersecurity

#### **Critical Infrastructure Independent Study Courses**

The courses listed here are developed and maintained by the Office of Infrastructure Protection in partnership with critical infrastructure owners and operators, **Sector-Specific Agencies**, sector liaisons, **CISA regional offices**, other federal and state agencies, and the **Federal Emergency Management Agency's Emergency Management Institute (FEMA EMI)**.

#### **National Infrastructure Protection Foundational Courses**

- **IS-860.C: Introduction to the National Infrastructure Protection Plan**
- **IS-913.A: Achieving Results through Critical Infrastructure Partnership and Collaboration**

#### **Security Awareness Training Courses**

- **IS-907: Active Shooter: What You Can Do**
- **IS-912: Retail Security Awareness: Understanding the Hidden Hazards**

- **IS-914: Surveillance Awareness: What You Can Do**
- **IS-916: Critical Infrastructure Security: Theft and Diversion — What You Can Do**

These training resources and more are available via the **EMI Course Catalog**. For more information, contact [IP\\_Education@hq.dhs.gov](mailto:IP_Education@hq.dhs.gov).

#### **Sector-Specific Training**

- **Chemical Sector Training**
- **Commercial Facilities Sector Training**
- **Dams Sector Training**

#### **Critical Infrastructure Security and Resilience Training Portal**

The Office of Infrastructure Protection now hosts a collaborative **Critical Infrastructure Security and Resilience Training Portal** for members of the Homeland Security Information Network — Critical Infrastructure (HSIN-CI). This depository of links and documents serves as a central location for training courses and other resources to support critical infrastructure security and resilience activities. To learn more about HSIN-CI and to become a member, visit the HSIN-CI webpage.

#### **Interagency Security Committee Training**

**The Interagency Security Committee (ISC)** developed a **series of online and interactive training courses** to provide federal facility security professionals, engineers, building owners, construction contractors, architects, and the general public with basic information pertaining to the ISC and its facility security standards, processes, and practices.

#### **Counter-Improvised Explosive Device (IED) Training and Awareness**

The **Office for Bombing Prevention (OBP)** develops **tools to improve national preparedness for bombing threats** at all levels of Government, the public, and the private sector. **Course options** include bombing prevention workshops, soft target awareness, and surveillance detection. For more information, contact the Office for Bombing Prevention at [OBP@hq.dhs.gov](mailto:OBP@hq.dhs.gov).

#### **Active Shooter Preparedness Workshops**

The Department of Homeland Security (DHS) offers **free courses, materials, and workshops** to better prepare you to deal with an active shooter situation and to raise



awareness of behaviors that represent pre-incident indicators and characteristics of active shooters.

## AUTHORIZED USER TRAINING

### Protected Critical Infrastructure Information (PCII) Program

**Protected Critical Infrastructure Information (PCII) authorized user training** is available in a self-paced, electronic module for qualifying individuals with a need-to-know. For more information, visit the [PCII Program webpage](#) or contact the PCII Program Office at [pcii-assist@hq.dhs.gov](mailto:pcii-assist@hq.dhs.gov).

### Chemical-Terrorism Vulnerability Information

**Chemical-terrorism Vulnerability Information (CVI) training** provides an overview of the Sensitive but Unclassified designation “Chemical-terrorism Vulnerability Information.” CVI protects information developed under the **Chemical Facility Anti-Terrorism Standards (CFATS)** regulation regarding vulnerabilities of high-risk chemical facilities manufacturing, using, storing, or possessing certain explosive, reactive, flammable, or toxic chemicals of interest. Completion of this training will prepare you to successfully handle and safeguard CVI. For more information, contact [CSAT@hq.dhs.gov](mailto:CSAT@hq.dhs.gov).

## OTHER TRAINING RESOURCES

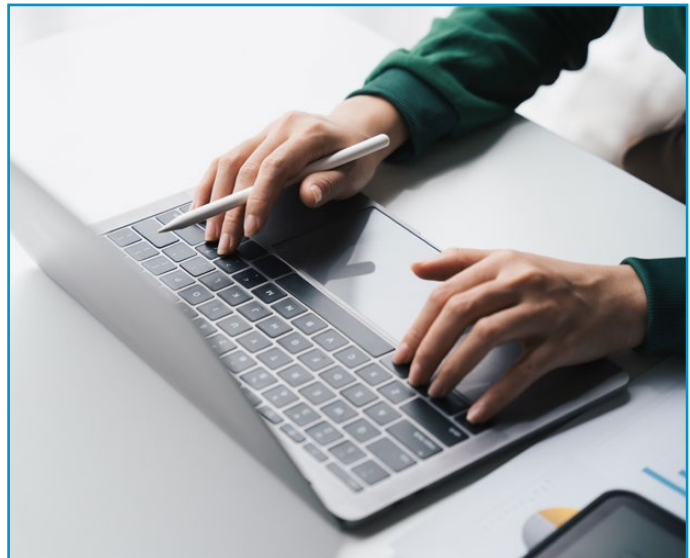
### Critical Infrastructure Learning Series

Critical infrastructure experts conduct **these one-hour webinars** that focus on the tools, trends, issues, and best practices for infrastructure security and resilience. Series offerings are available at no-cost and are highly recommended for private sector and Government partners, including critical infrastructure owners and operators and officials responsible for risk, security, and emergency management functions.

### Cybersecurity Training

The **Industrial Control Systems Cyber Emergency Response Team (ICS-CERT)** works to reduce risks within and across all critical infrastructure sectors. **The Virtual Learning Portal (VLP)** provides online training for those involved in the security of Industrial Control Systems (ICS) for no cost.

The National Initiative for Cybersecurity Careers and Studies (**NICCS**) **Education and Training Catalog** is a central location where cybersecurity professionals across



the Nation can find over 3,000 cybersecurity courses. Use the interactive map and filters to search for courses offered in your local area. All of the courses are aligned to the specialty areas of the **National Cybersecurity Workforce Framework**.

### FEMA's National Training and Education Division

The Office of Infrastructure Protection has partnered with the **Federal Emergency Management Agency's (FEMA) National Training and Education Division** to offer training programs to critical infrastructure partners. These courses provide essential knowledge and awareness for understanding and following the principles, roles, and responsibilities that enhance critical infrastructure security and resilience. Find course schedules and complete descriptions for these courses in the **Federal Emergency Management Agency's First Responder Course Catalog**.

### CISA Resources

[2022 Infrastructure Security Month Webpage](#)

[2022 Infrastructure Security Month Toolkit](#)

[Securing Public Gatherings Resources: Everyone Webpage](#)

[Securing Public Gatherings Resources: Businesses and Critical Infrastructure Webpage](#)

[Critical Infrastructure Training Webpage](#)

[Critical Infrastructure Sectors Webpage](#)

[Office for Bombing Prevention Webpage](#)

[Stop Ransomware Webpage](#)



## ESTABLISHMENT OF DCSA ACADEMY OCTOBER 1

On October 1, Central Services (CS) was formally established as a part of the overarching **Security Training (ST) Reorganization** effort. Resources to support the integration of CS can be found on the **CS (SharePoint)**. To keep you informed about CS, we've prepared a fact sheet, frequently asked questions, and a presentation outlining the changes and their impact on your division and the broader workforce. Please review the attached resources and consider the following guidance to support your transition, accessible via the **Security Training (SharePoint) site**.

Effective October 1, ST transitioned from two learning centers to three – the National Center for Credibility Assessment (NCCA), the Center for Development of Security Excellence (CDSE), and the newly created DCSA Security Academy. NCCA and CDSE will continue to provide the same high-quality training and education that the community has come to expect. The DCSA Security Academy will provide security education and training for our DCSA security professionals across the mission sets.



To be known as the premiere provider of integrated security services, we must be the best at what we do. This initiative shows a commitment to training our workforce across mission areas to a common set of standards that will help integrate the agency. We are also committed to the professional development of the workforce that will move the agency to full performance.

---

## REGISTRATION NOW OPEN FOR SPRING 2025 SEMESTER OF CDSE TUITION-FREE EDUCATION CLASSES

Expand your knowledge with CDSE! Registration is now open for CDSE Education classes for the 2025 spring semester. The 16-week semester runs from November 4 through January 20, 2025. The courses are asynchronous online, tuition free, and allow students the flexibility to collaborate with each other and instructors. In need of professional development units? Students can earn 160 PDU's by completing these classes.

Enrollment fills quickly, so register early to secure a spot. You can learn more and register [here](#) or to register via STEPP, click [here](#).

Still have questions? Contact the **CDSE Education Division**.



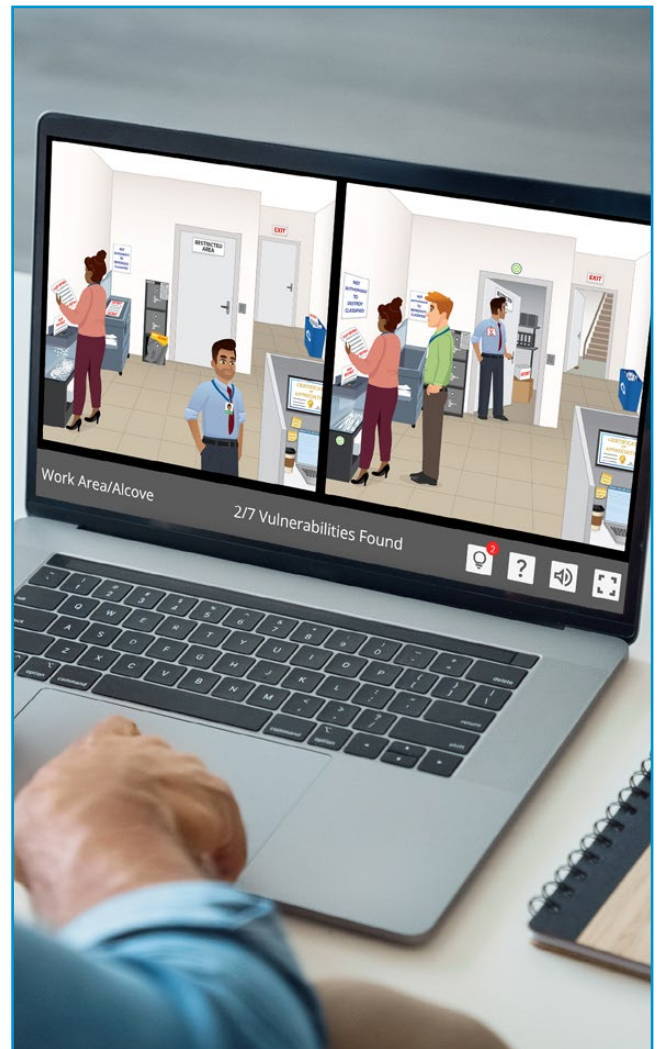


## NEW INDUSTRIAL SECURITY AWARENESS GAME

The Industrial Security team has released a new **Security Awareness Game**, “Spot the Vulnerabilities.” The game is a fun way for our stakeholders to learn how to identify and prevent security vulnerabilities within their work environments.

## NEW SHORT COURSE SERIES ON LIFE CYCLE OF CONTROLLED UNCLASSIFIED INFORMATION RELEASED

CDSE has published the CUI Life Cycle Shorts series, consisting of four short courses. The shorts provide learners with specific “how-to” guidance, aligning with current policy requirements, on common tasks they complete day-to-day that involve CUI; safeguard CUI; share CUI, and decontrol and destroy CUI in accordance with DODI 5200.48 “Controlled Unclassified Information (CUI).” Visit CDSE’s Information Security [page](#) to learn more and to access this new training.



## THE SECURITY TRIANGLE COURSE

CDSE’s Education Program released its newest virtual instructor-led course, ED402, “**The Security Triangle: Security, Law Enforcement (LE), and Intelligence.**” It focuses on the three components of the security triangle. Through the review of case studies, this course explores how the DOD security professional collaborates with and supports LE and intelligence communities to prevent future security failures. This new eight-week course runs between October 14 and December 15 and is open to all federal civilians and military personnel (active and reserve) with or without an undergraduate degree. The course is unavailable to contractors. Students will receive 80 professional development units (PDUs) upon successful completion. Visit the course webpage to learn more and the Security Training, Education, and Professionalization (STEPP) Portal to [register](#).



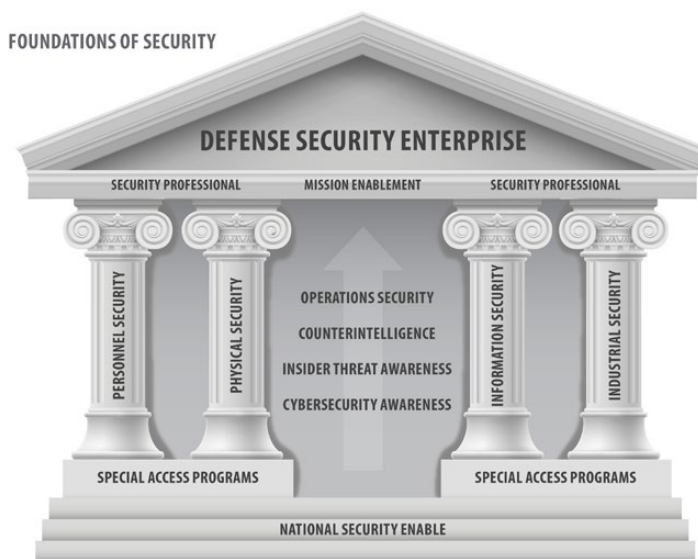
## CDSE EDUCATION COURSE - “THE DEFENSE SECURITY ENTERPRISE: A NATIONAL SECURITY ENABLER”

The CDSE Education Division’s new eight-week virtual instructor-led education course, “ED401, The Defense Security Enterprise: A National Security Enabler,” opened for registration on November 1. ED401 is a distance-learning asynchronous course delivered in the STEPP in a collaborative learning environment by experienced security professionals with decades of experience in the security management field.

ED401 will run in the Spring 2025 Semester starting January 20, 2025. This course will be open to all DOD and U.S. Government civilian and military personnel on active duty and reserve. ED401 is the second new college equivalent level eight-week course CDSE has launched. The first course, ED402, “The Security Triangle: Security, Law Enforcement, and Intelligence,” started on October 14, 2024. Students do not require a bachelor’s degree to enroll in these courses.

The ED401, “The Defense Security Enterprise: A National Security Enabler” course, provides students with a foundational understanding of the core tenets of security and the role of security as a mission enabler in achieving the broader goals of the U.S. Department of Defense. It treats Security Management as a doctrine and discusses

examples of how security successes and failures have historically bolstered and undermined the DOD mission. The course explores how the core defense security disciplines serve as critical enablers to the missions of DOD commands and agencies. The course is designed to help mid-career security professionals understand their critical role in supporting national security.



## ACTIVITY SECURITY MANAGER COURSE

Don’t miss CDSE’s upcoming “Activity Security Manager” course. This mid-level, virtual instructor-led course provides students with a comprehensive understanding of how to apply and implement specific DOD Information Security policies and procedures to mitigate and manage risks associated with developing, managing, and evaluating a DOD Information Security Program (ISP). Students are anticipated to invest 40-60 hours over four weeks in a primarily asynchronous environment. The course is tailored for DOD civilian, military, and contractor personnel with primary duties as an activity security manager, information security program specialist, or manager within a DOD Component ISP. Students should have a functional working knowledge of the DOD ISP.

After taking this course, students can expect to implement the fundamental policies and requirements of the ISP, implement risk management to protect DOD assets, determine fundamental cybersecurity and information technology principles, and so much more. The first iteration takes place February 2, 2025, through March 3, 2025. For more dates and information, check out the [CDSE website](https://www.cdse.edu).

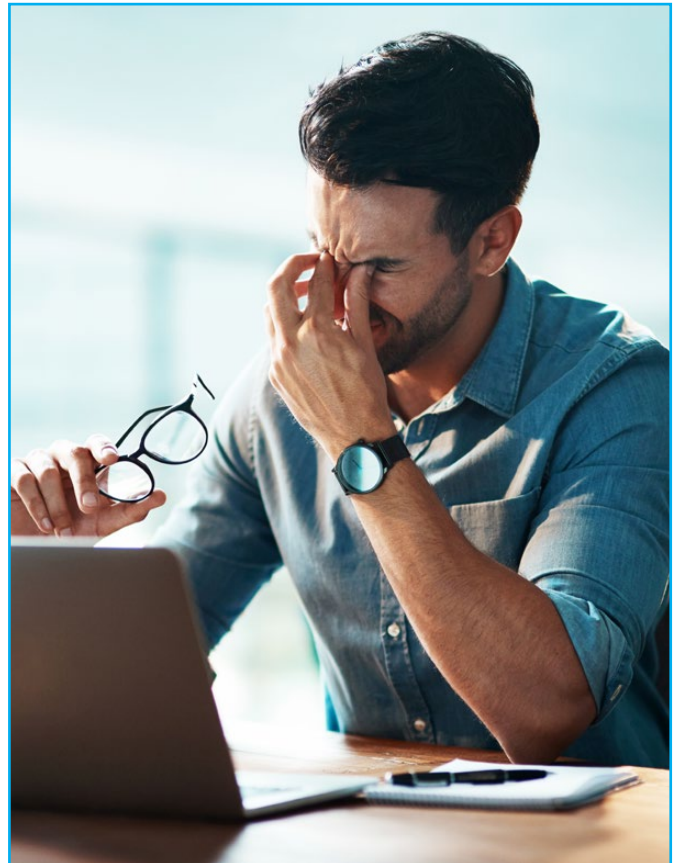


## INSIDER THREAT DETECTION AND ANALYSIS COURSE

Insider threats are one of the biggest risks to national security. Learn the latest analytic techniques with CDSE's virtual instructor-led "Insider Threat Detection Analysis Course" (ITDAC) training. During this five-day course, attendees will apply critical thinking skills and applicable structured analytic techniques to potential insider threat indicators.

This course also allows learners to obtain and use holistic data in conjunction with the application of critical pathway theory. Some prerequisites apply. Register for courses [here](#). Below is the 2024 and 2025 course schedule:

Nov. 18-22, 2024 (Virtual)	May 12-16, 2025 (Virtual)
Dec. 2-6, 2024 (Virtual)	June 23-27, 2025 (Virtual)
Jan. 13-17, 2025 (Virtual)	July 21-25, 2025 (Virtual)
Feb. 10-14, 2025 (Virtual)	Aug. 18-22, 2025 (Virtual)
March 17-21, 2025 (Virtual)	Sept. 22-26, 2025 (Virtual)
April 7-11, 2025 (Virtual)	



## PERSONNEL VETTING SEMINAR

CDSE is presenting the virtual-led "Personnel Vetting Seminar" on November 19-21. This seminar will address the requirements associated with the reform of the Federal Government's personnel vetting system, which is known as Trusted Workforce 2.0 (TW 2.0). Its purpose is to aid personnel vetting practitioners in DOD, federal agencies, and private industry to understand TW 2.0 requirements, identify gaps between current and future procedures, and provide support through the implementation process. The seminar covers topics such as end-to-end personnel vetting operations, including the federal background investigations program, National Security Adjudications, Continuous Vetting, and Insider Threat analysis in a collaborative environment.

This 3.5-day course is intended for U.S. Government security professionals, military personnel, cleared industry FSOs, and other federal personnel performing personnel vetting security-related duties, as well as personnel executing security programs for cleared industry. Visit the [course page](#) to learn more and register.

## 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, Insider Threat Bulletins, or the Weekly Flash, visit our [news page](#) and sign up or update your account today.

