

CENTER FOR DEVELOPMENT OF SECURITY EXCELLENCE (CDSE)

NOVEMBER 2023

DEFENSE COUNTERINTELLIGENCE AND SECURITY AGENCY

Curtis Cook
Cybersecurity Curriculum Manager





MISSION

Provide the DOD with a security center of excellence for the professionalization of the security community and be the premier provider of security education and training for the DOD and industry under the National Industrial Security Program (NISP). The CDSE provides development, delivery, and exchange of security knowledge to ensure a high-performing workforce capable of addressing our Nation's security challenges.

TRAINING

Supporting today's security professionals

EDUCATION

Developing future security leaders

CERTIFICATION

Validating security professional skills and competencies

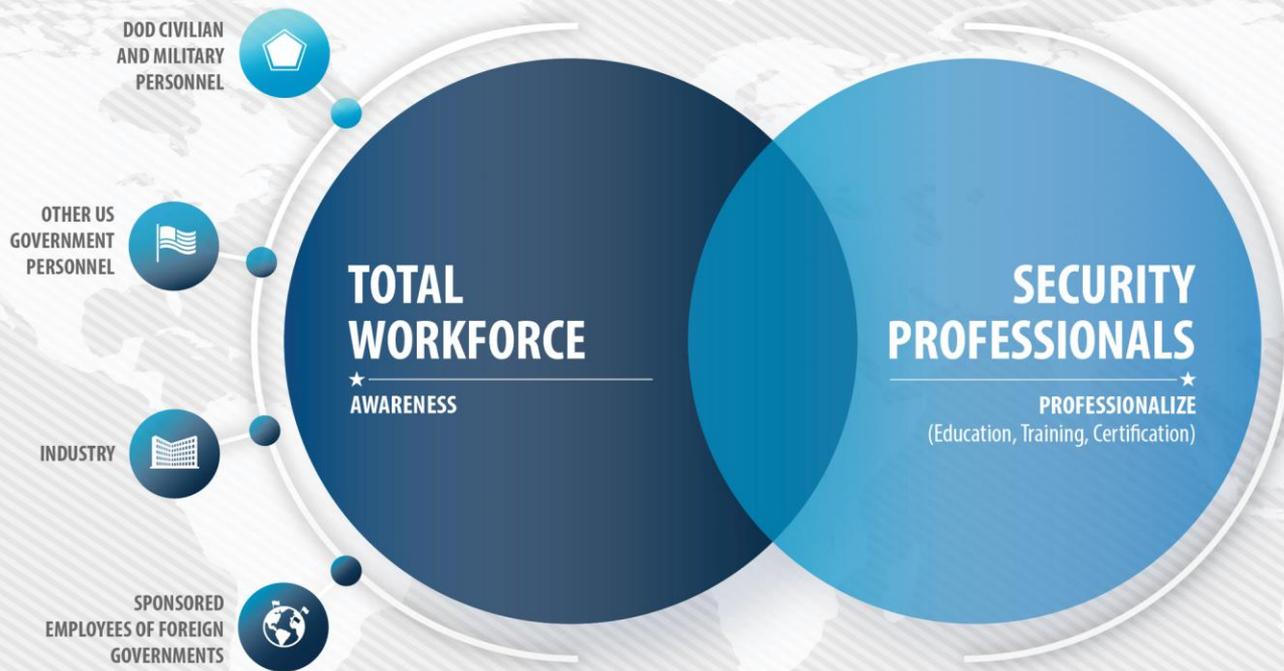
AWARENESS

Promoting security awareness to the total workforce





OUR AUDIENCE



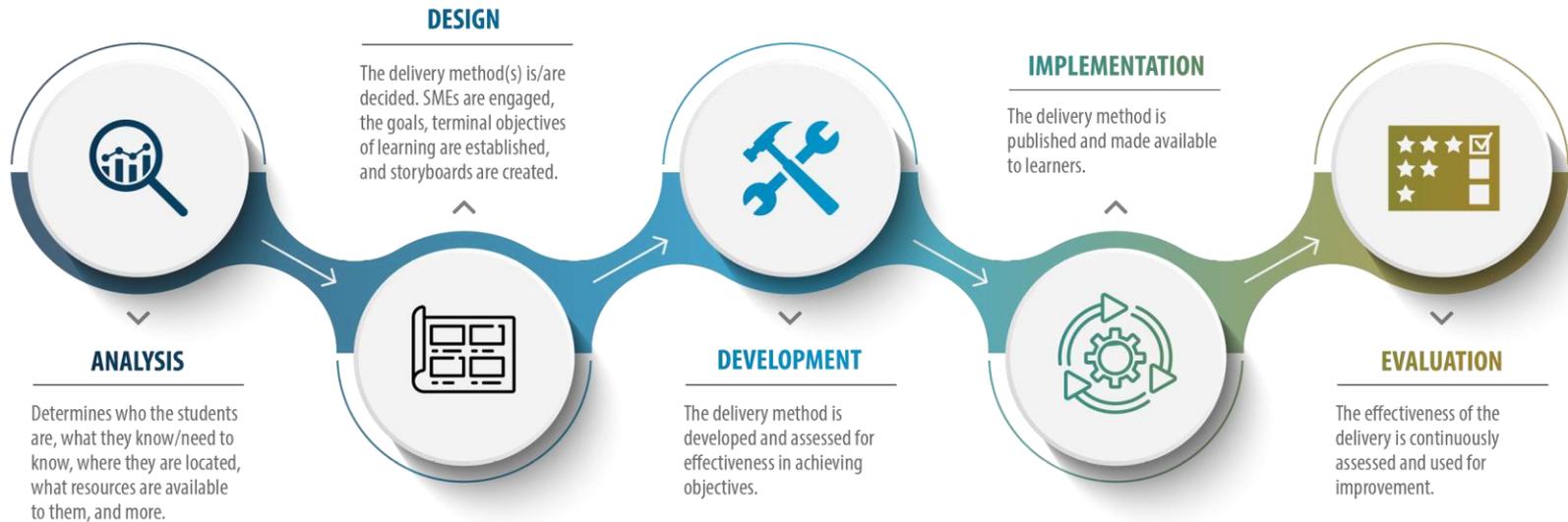


DESIGN METHODOLOGY

DRIVERS:

Policy, events, analysis, and the Defense Security Skill Standards (DS3).

ADDIE is a five step, non-linear instructional design methodology CDSE uses to design and develop content for our Training and Education programs.

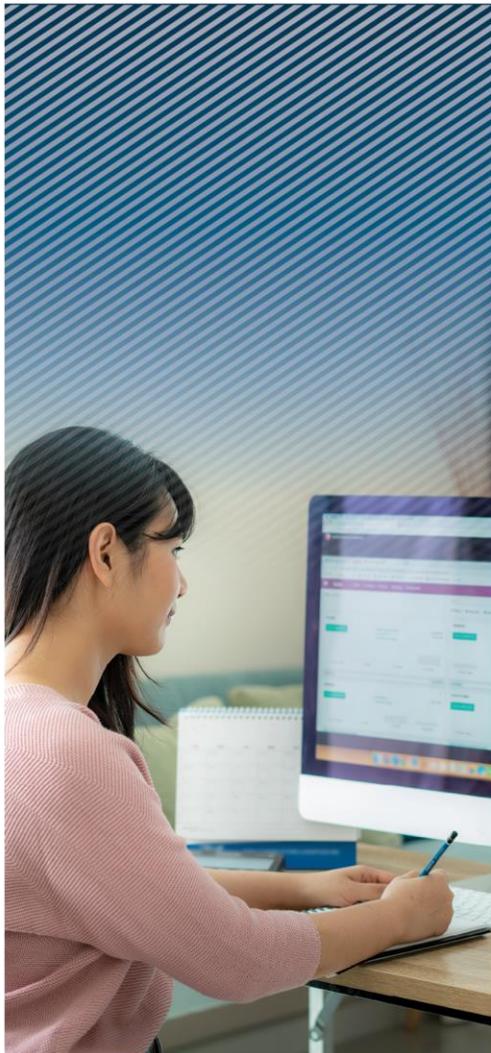


DELIVERY METHODS

Instructor-Led	Virtual Instructor-led	Job Aids	Shorts	Case Studies
eLearning	Toolkits	Webinars	Videos	Awareness Games



TRAINING



AUDIENCE

DOD Workforce
 Security Specialists
 Security Assistants
 Other Federal Agencies Personnel
 Cleared Industry Personnel
 DCSA Consolidated Adjudication Services (CAS) Personnel

DCSA Background Investigative Personnel
 DCSA Industrial Security Representatives
 DOD Personnel Security Specialists
 Facility Security Officers
 Information System Security Managers

Insider Threat Practitioners
 Special Access Programs Personnel
 Critical Infrastructure Sector Personnel
 Sponsored Foreign Government Personnel

CONTENT AREAS

Background Investigations
 General Security
 Industrial Security
 Information Security

Insider Threat
 Personnel Vetting
 Physical Security
 Special Access Programs

Counterintelligence
 Cybersecurity
 Operations Security

**Content areas in this section are awareness-level*



CDSE Cybersecurity Team Members

Curtis Cook

Cybersecurity Curriculum Manager

Evelyn Okoro

Cybersecurity Course Manager

Victor Adekoya

Cybersecurity Course Manager

Rodney Poindexter

Cybersecurity Instructional Designer

CDSE Training Cybersecurity Update FY23



- **Assessing Risk and Applying Security Controls to NISP Systems CS 301.01**
 - FY 23 Courses: December, March, June, and August.
 - Next FY 24 Course December 11-15, 2023 at CDSE

- **Risk Management Framework eLearning CS 100**
 - RMF Steps 1-6 CS 100 to conform to NIST-800-37 Rev2

- **Updated DISA courses on STEPP**
 - Using Mobile Devices in a DoD Environment DS-IA109.06
 - Phishing and Social Engineering: Virtual Communications Awareness Training DS-IA103.06
 - Cyber Awareness Challenge CAC DS-IA106.06
 - DISA Privilege User Responsibilities DS-IA112.06



CDSE Training Cybersecurity Update FY24

- STEPP Courses Currently under Maintenance
- Protected Distribution Systems CS140.16
- Technical Implementation of A&A in the NISP CS300.06
- Continuous Monitoring CS 200.16

- **Updated** – 24 Cyber Awareness Challenge CAC DS-IA106.06

- **CompTIA CPEs**
- https://www.comptia.org/docs/default-source/continuing-ed/cdse.pdf?sfvrsn=6ba3faf6_8

Cybersecurity – FY 24 Priorities



- CS 301 ILT to VILT
- eLearning
 - Maintenance
 - CS160.01 – Cybersecurity for Security Personnel
 - CS130.01 – Cyber Awareness
 - New
 - Android / Apple App Permissions short
 - Zero Trust
- Update Social Media Job Aids
- ISSP Course Training Needs Analysis (TNA)





CDSE Training ISSM Course

- <https://www.cdse.edu/Training/Instructor-led/CS301/>

CENTER FOR DEVELOPMENT OF SECURITY EXCELLENCE
DEFENSE COUNTERINTELLIGENCE AND SECURITY AGENCY

[STEPP Login](#)

[I'm interested in...](#) | [I'm looking for...](#) | [I'm in need of...](#)

[HOME](#) > [TRAINING](#) > [INSTRUCTOR-LED COURSES](#) > [ASSESSING RISK AND APPLYING SECURITY CONTROLS TO NISP SYSTEMS CS301.01](#)

Assessing Risk and Applying Security Controls to NISP Systems CS301.01

Description: This course provides students with guidance on applying policies and standards used throughout the U.S. Government to protect information within computer systems, as delineated by the Risk Management Framework (RMF) process. This course will also provide a comprehensive understanding of contractor requirements under the National Industrial Security Program (NISP).

The course is administered through eLearning prerequisites and instructor-led training.

Course Resources: N/A

Learning Objectives: This course is designed to teach participants how to:

- Develop and maintain a comprehensive risk assessment report based on an ongoing risk assessment of the system environment.
- Apply organizational resources to execute a robust information system (IS) security program in alignment with RMF requirements.
- Select, implement, and assess appropriate security controls that protect the IS based on the identified risk to the system.
- Implement and oversee procedures and measures for IS incident handling, response, and reporting.
 - Ensure insider threat awareness is addressed within the cleared contractor's IS programs.
 - Ensure user activity monitoring data is analyzed, stored, and protected in accordance with established policies and procedures.
- Develop and submit system security packages and supporting artifacts using the Enterprise Mission Assurance Support Service (eMASS), appropriately documenting and justifying all selected system controls.
 - Develop and maintain Plan of Action and Milestones (POA&Ms) in order to identify IS weaknesses, mitigating actions, resources, and timelines for corrective actions.
 - Submit the system security plan (SSP) and supporting artifacts to the Information Systems Security Professional (ISSP) using eMASS for the Authorizing Official's (AO) review and consideration.
- Implement continuous monitoring procedures and tools to identify and report system vulnerabilities, threats, and anomalies as necessary.
 - Collect and analyze audit records in accordance with the SSP.
 - Develop, maintain, and execute the Continuous Monitoring Strategy.

Delivery Method: Instructor-led

Length: 5 days

Target Audience: The target audience for this training includes Information System Security Managers (ISSMs), Information System Security Officers (ISSOs), and Facility Security Officers (FSOs) involved in the planning, management, and execution of security programs for cleared industry.

Number of Students per Course: N/A

Requirements:

CompTIA

Course Schedule

Aug 21-25, 2023 (Linthicum, MD)
 Dec 11-15, 2023 (Linthicum, MD)
 Mar 18-22, 2024 (Linthicum, MD)
 Jun 24-28, 2024 (Linthicum, MD)
 Sep 09-13, 2024 (Linthicum, MD)

Quick Links

[Take this course](#) [↗](#)
[Technical support](#) [↗](#)
[Content related questions](#)

CDSE Training Cybersecurity Website



- <https://www.cdse.edu/Training/Cybersecurity/>

CENTER FOR DEVELOPMENT OF SECURITY EXCELLENCE
DEFENSE COUNTERINTELLIGENCE AND SECURITY AGENCY

STEPP Login

I'm interested in... ▾ I'm looking for... ▾ I'm in need of... ▾

Cybersecurity

Cybersecurity is the ability to protect or defend the use of cyberspace from attacks. If you are new to cybersecurity, we suggest you review the training products in the order listed to develop a foundation in cybersecurity concepts and principles. After reviewing these training products, additional training is available on this webpage to expand your knowledge and skills.

1. Cybersecurity Awareness CS130.16
2. Introduction to the Risk Management Framework (RMF) CS124.16

CASE STUDIES

CURRICULA

ELEARNING COURSES

- Applying Assessment & Authorization (A&A) in the National Industrial Security Program (NISP) CS250.16 CompTIA
- Continuous Monitoring CS200.16 CompTIA
- Cyber Awareness Challenge (CAC) DS-IA106.06
- Cybersecurity Awareness CS130.16
- Cybersecurity for Security Personnel CS160.16 CompTIA
- Enterprise Mission Assurance Support Service (eMASS) DISA-100.06
- Introduction to the NISP RMF A&A Process CS150.16 CompTIA
- Introduction to the Risk Management Framework (RMF) CS124.16
- Phishing and Social Engineering: Virtual Communication Awareness Training DS-IA103.06
- Protected Distribution System CS140.16
- Risk Management Framework (RMF): Prepare Step CS101.16
- Risk Management Framework (RMF) Step 1: Categorization of the System CS102.16
- Risk Management Framework (RMF) Step 2: Selecting Security Controls CS103.16
- Risk Management Framework (RMF) Step 3: Implementing Security Controls CS104.16
- Risk Management Framework (RMF) Step 4: Assessing Security Controls CS105.16
- Risk Management Framework (RMF) Step 5: Authorizing Systems CS106.16
- Risk Management Framework (RMF) Step 6: Monitor Security Controls CS107.16
- Technical Implementation of A&A in the NISP CS300.06 CompTIA
- Using Mobile Devices in a DoD Environment DS-IA109.06

JOB AIDS

INSTRUCTOR-LED COURSES

Courses taught by training staff and guest instructors at CDSE in Linthicum, MD and various mobile training sites

- Assessing Risk and Applying Security Controls to NISP Systems CS301.01 CompTIA

SECURITY AWARENESS GAMES

SECURITY POSTERS

SECURITY SHORTS

SECURITY TRAINING VIDEOS

TOOLKITS

WEBINARS



Cybersecurity Catalog

- One Instructor-Led course
- 20 eLearning courses
- Two Curricula
- Two Toolkits
- Five Security Shorts
- 11 Job Aids
- 18 Webinars
- Three Security Training Videos
- Seven Security Awareness Games
- Three Interdisciplinary collaborations
- Case Studies
- 16 Cybersecurity Posters

Cybersecurity eLearning Courses



- Introduction to the NISP RMF A&A Process CS150.16
- Applying Assessment & Authorization (A&A) in the National Industrial Security Program (NISP) CS250.16
- Technical Implementation of A&A in the NISP CS300.06
- Continuous Monitoring CS200.16
- Protected Distribution System CS140.16
- Cybersecurity Awareness CS130.16
- Cybersecurity for Security Personnel CS160.16

Cybersecurity eLearning Courses



- Cyber Awareness Challenge (CAC) DS-IA106.06
- Enterprise Mission Assurance Support Service (eMASS) DISA-100.06
- Phishing and Social Engineering: Virtual Communication Awareness Training DS-IA103.06
- Privileged User Responsibilities DS-IA112.06
- Using Mobile Devices in a DoD Environment DS-IA109.06
- Introduction to the Risk Management Framework (RMF) CS124.16
- Risk Management Framework (RMF): Prepare Step CS101.16
- Risk Management Framework (RMF) Categorization of the System CS102.16
- Risk Management Framework (RMF) Selecting Security Controls CS103.16
- Risk Management Framework (RMF) Implementing Security Controls CS104.16
- Risk Management Framework (RMF) Assessing Security Controls CS105.16
- Risk Management Framework (RMF) Authorizing Systems CS106.16
- Risk Management Framework (RMF) Monitor Security Controls CS107.16

Cybersecurity Security Shorts



- Assured File Transfer
- Data Spills
- Cybersecurity Attacks: The Insider Threat
- Cybersecurity: Incident Response
- Cybersecurity and the Use of New Personal Devices



18 On Demand Webinars



- Assessment and Remediation using the SCAP Tool
- Best Practices and Vulnerabilities for Privileged Accounts
- Common Scams and Frauds
- Developing an Incident Response Capability
- Greater Security in Seven Days
- Information Security Continuous Monitoring
- Cybersecurity and Teleworking: Concerns, Challenges, and Practical Solutions – Part 1
- Cybersecurity and Teleworking: Concerns, Challenges, and Practical Solutions – Part 2
- Preventing and Recovering from Ransomware
- Secure Communication for an Insecure World
- Secure Configuration for Hardware and Software
- Creating a Workplace Culture of Cybersecurity
- Top 20 Critical Security Controls
- Your Evolving Digital Life
- Your Fridge May be Spying On You: Securing the Internet of Things
- Know Your CDSE – Cybersecurity
- Cloud Computing
- Cybersecurity and Teleworking: Concerns, Challenges, and Practical Solutions – Part 3 (Collaboration Tools)



Two Toolkits commonly accessed by DOD & Industry:

Cybersecurity Toolkit

[Home](#) / [Training](#) / [Toolkits](#) / Cybersecurity Toolkit

This toolkit will quickly point you to the resources you need to help you perform your role in Cybersecurity. Do you have a question about how to do something or need more information about a topic?

Select a category below to start accessing resources.



Policy



Training/
Awareness



Assessment and
Authorization



Audit/Continuous
Monitoring



System
Management



Incident
Response



Alternate
Platform
Device



Social Media



Supply Chain
Risk Management

[Toolkit Index](#)

Information System Security Manager Toolkit

[Home](#) / [Training](#) / [Toolkits](#) / Information System Security Manager Toolkit

This toolkit will quickly point you to the resources you need to help you perform your role as an Information System Security Manager (ISSM). Do you have a question about how to do something or need more information about a topic?

Select a category below to start accessing resources.



ISSM Overview



Facility Security Program



Threats to
Cleared Facilities



Safeguarding



System &
Network Security



A&A Process



Security
Incidents



Authorization
& Auditing

[Toolkit Index](#)

Toolkit feedback/suggestions? Email dcsa.cdsetraining@mail.mil.



Cybersecurity Instruction in CDSE Security Discipline Products

- DOD Security Specialist Course (DOD SSC) 2-hour block of instruction for 0080 Security Specialists
- Special Access Programs (SAPs) Mid-Level Course 2-hour block of instruction covering SAP Cybersecurity principles
- Insider Threat Sentry App for Android / Apple devices that include Cyber focused videos and other content

Security Awareness Hub / Case Studies



CDSE

An official website of the Center for Development of Security Excellence, Defense Counterintelligence and Security Agency

LEARN. PERFORM. PROTECT.

SECURITY AWARENESS HUB

Select eLearning awareness courses for DOD and Industry

This website provides frequently assigned courses, including mandatory annual training, to DOD and other U.S. Government and defense industry personnel who do not require transcripts to fulfill training requirements for their specialty. You do not need an account or any registration or sign-in information to take a Security Awareness Hub course.

Please note end-of-course evaluations are temporarily suspended. You will still be able to save your course completion certificate. Thank you for looking to CDSE for your security training needs.



Counterintelligence

Counterintelligence Awareness and Reporting for DOD

CDSE

HOME

ABOUT THE CASES SEARCH

CDSE CASE STUDY LIBRARY

Your awareness is key to protecting our national security.

Explore a growing repository of U.S. case studies. Learn about the crimes, the sentences, the impact, and the potential risk indicators that, if identified, could have mitigated harm.

You may search these case studies by various criteria including gender, type of crime, and military affiliation. Individual case studies contain information such as: plea, court (Court Martial, US District Court, and Federal), year convicted, age at time of conviction, job, employer, country of concern, method of operation, method of contact, technology, indicators, and sentencing.

Search Case Studies

NEWEST CASE STUDIES

 ALDRICH AMES Crime: Foreign Espionage View Aldrich Case	 AARON ALEXIS Crime: Targeted Violence View Alexis Case	 ALIREZA JALALY MESGAR GHOOSANI Crime: Illegal Export View Mesgar-Choobkol Case
---	---	--

View all case studies

SUSPICIOUS ACTIVITIES

Study analyzed accounts of real-world security activities, events, or threats to build awareness and help identify the impacts of subversive behavior on National Security.

- ACTIVE TERROR GROUP
- CYBER CRISIS
- ECONOMIC ESPIONAGE
- FOREIGN ESPIONAGE
- TRAVEL
- ILLEGAL EXPORT
- TECHNOLOGY CLASSIFIED INFORMATION
- SABOTAGE
- TARGETED VIOLENCE
- UNAUTHORIZED DISCLOSURE

INDICATORS

Most insider threats exhibit risky behavior prior to committing negative workplace events. Not all of these potential risk indicators will be evident in every insider threat and not everyone who exhibits these behaviors is doing something wrong. However, most of insider threats have displayed at least some of the potential risk indicators. If identified early, many risks can be mitigated before harm to the organization occurs. Select an indicator to explore some examples.



CDSE Instructor-Led Schedule



- <https://www.cdse.edu/Training/Schedule/>

CENTER FOR DEVELOPMENT OF SECURITY EXCELLENCE
DEFENSE COUNTERINTELLIGENCE AND SECURITY AGENCY

I'm interested in... ▾ I'm looking for... ▾ I'm in need of... ▾

🔍

[STPEP Login](#)

HOME > TRAINING > SCHEDULE

Training Schedule

Cybersecurity

Assessing Risk and Applying Security Controls to NISP Systems CS301.01 **CompTIA**

- Aug 21-25, 2023 (Linthicum, MD)
- Dec 11-15, 2023 (Linthicum, MD)
- Mar 18-22, 2024 (Linthicum, MD)
- Jun 24-28, 2024 (Linthicum, MD)
- Sep 09-13, 2024 (Linthicum, MD)

General Security

DOD Security Specialist GS101.01 **ACE CREDIT** **CompTIA**

- Sep 19-27, 2023 (Linthicum, MD) *Registration closed*
- Mar 05-13, 2024 (Linthicum, MD)
- Jun 04-12, 2024 (Linthicum, MD)
- Sep 17-25, 2024 (Linthicum, MD)

DOD Security Specialist VILT GS101.10 **ACE CREDIT** **CompTIA**

- Aug 21-Sep 17, 2023 (Virtual)
- Nov 06-Dec 23, 2023 (Virtual)
- Jan 08-Feb 04, 2024 (Virtual)
- May 20-Jun 16, 2024 (Virtual)
- Aug 14-Sep 15, 2024 (Virtual)

Industrial Security

Getting Started Seminar for New Facility Security Officers (FSOs) IS121.01

- October 17 - 18, 2023 (Linthicum, MD)

Getting Started Seminar for New Facility Security Officers (FSOs) VILT IS121.10

- Aug 01-04, 2023 (Virtual) *Registration Closed*
- Jan 23-26, 2024 (Virtual)
- Apr 16-19, 2024 (Virtual)
- Aug 20-23, 2024 (Virtual)

Personnel Security

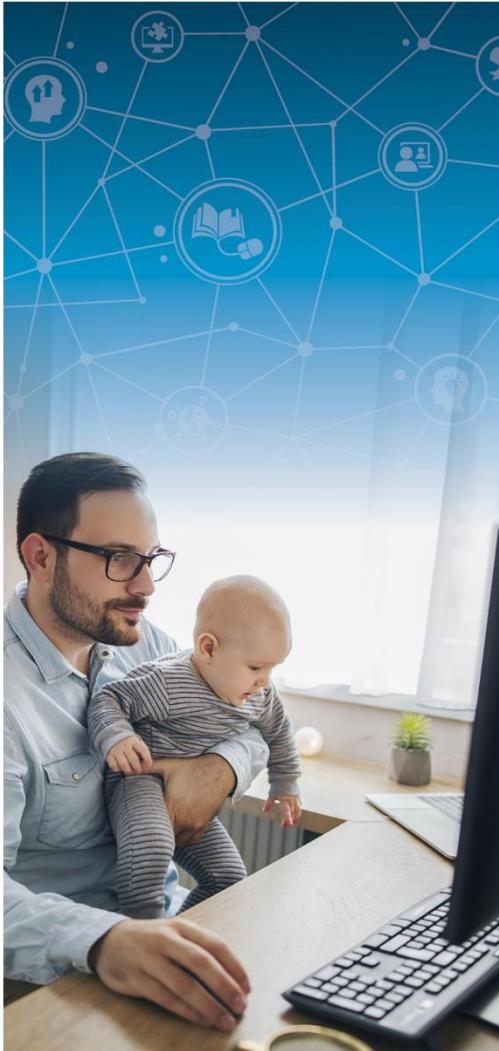
Advanced National Security Adjudication VILT PS301.10 **CompTIA**

- Sep 11-21, 2023 (Virtual)
- Dec 04-14, 2023 (Virtual)
- Mar 18-28, 2024 (Virtual)
- Jun 03-13, 2024 (Virtual)
- Sep 16-26, 2024 (Virtual)

Fundamentals of National Security Adjudications PS101.10 **ACE CREDIT**

- Oct 24-Nov 03, 2023 (Linthicum, MD)
- Jan 23-Feb 02, 2024 (Linthicum, MD)
- Apr 16-26, 2024 (Linthicum, MD)
- Jul 09-19, 2024 (Linthicum, MD)

CDSE Instructor-Led Schedule



AUDIENCE

U.S. Government civilian and military personnel

18 COLLEGIATE-LEVEL COURSES

Advanced Education courses to broaden understanding of security programs, operations, and policy development

Delivered as Virtual Instructor-led

Highly qualified professors

Students can transfer credits to participating universities and institutions

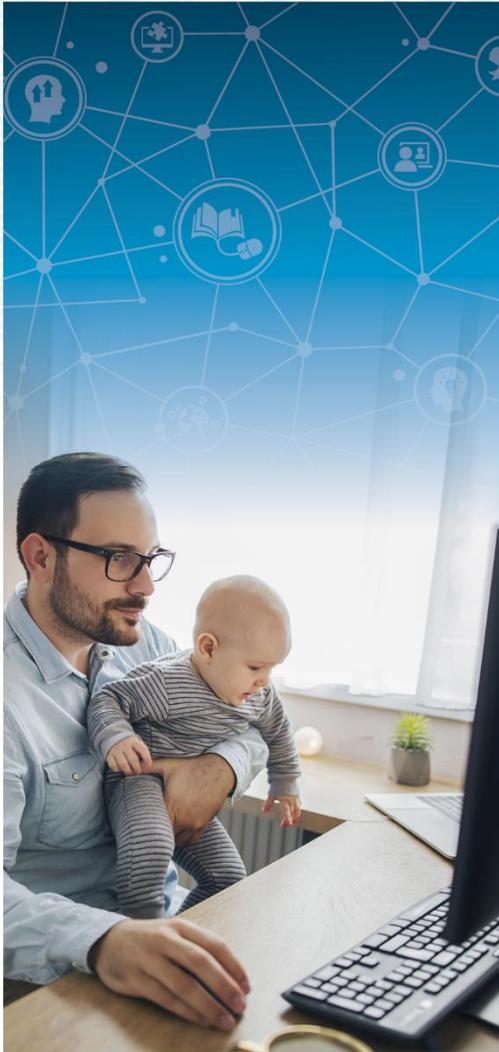
CONTENT AREAS

Five Concentrations:

- Risk Management
- Security Leadership
- Security Management
- Security (Generalist)
- Systems and Operations

Attained by successful completion of four Education courses

EDUCATION



AUDIENCE

U.S. Government civilian and military personnel

18 COLLEGIATE-LEVEL COURSES

Advanced Education courses to broaden understanding of security programs, operations, and policy development

Delivered as Virtual Instructor-led

Highly qualified professors

Students can transfer credits to participating universities and institutions

CONTENT AREAS

Five Concentrations:

- Risk Management
- Security Leadership
- Security Management
- Security (Generalist)
- Systems and Operations

Attained by successful completion of four Education courses



CERTIFICATION

AUDIENCE | DOD Security practitioners, military, and contractors assigned to a DOD security function

CORE CERTIFICATIONS



Security Fundamentals Professional Certification



Security Asset Protection Professional Certification



Security Program Integration Professional Certification

SPECIALTY CERTIFICATIONS AND CREDENTIALS



Physical Security Certification



Industrial Security Oversight Certification



Adjudicator Professional Certification



Due Process Adjudicator Professional Credential



Special Program Security Credential



Antiterrorism Credential



Accredited by the National Commission for Certifying Agencies (NCCA)



CERTIFICATION AND CREDENTIALING BENEFITS

- Demonstrates success and mastery of knowledge, skills, and abilities by a security professional
- Provides a recognized credential for security professionals
- Provides a common set of standards to measure requirements for a position
- Supports seamless transfer of security professionals among DoD components and agencies
- Facilitates interoperability among DOD security practitioners



SECURITY AWARENESS



AUDIENCE

DOD General Population
Defense Industrial Base

Other Government
Organizations
Critical Infrastructure

General Public

OFFERINGS

eLearning Courses on the
Security Awareness Hub

Awareness Products

 Job Aids

 Case Studies

 Videos

 Posters

 Awareness Games

Events - Conferences, Webinars

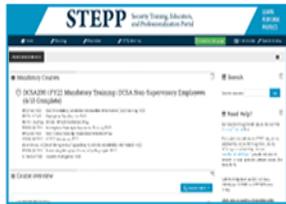
Pulse Newsletter

Public Service Announcements



CDSE PLATFORMS

STEPP



The Security, Training, Education and Professionalization Portal (STEPP) is the LMS that delivers eLearning training and is also used to facilitate Virtual Instructor-led training and education courses.

SECURITY AWARENESS HUB



The Security Awareness Hub provides frequently-assigned courses, including mandatory annual training, to DOD and other U.S. Government and defense industry personnel who do not require transcripts to fulfill training requirements for their specialty.

Insider Threat Sentry App

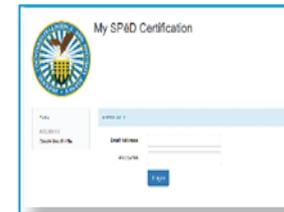
<https://securityawareness.usalearning.gov/cdse/nitam/sentry.html>

BI ONLINE



BI Online is the LMS for the background investigation (BI) mission. It hosts BI Courses and course components along with the capability for users to interact with instructors either synchronously or asynchronously.

MY SP&D CERTIFICATION



My SP&D Certification (MSC) is the system of record for the SP&D Certification Program. The MSC is where candidates manage SP&D certification activities.

NATIONAL AWARDS



Recipient of the Defense Intelligence Agency (DIA) DOD Counterintelligence and HUMINT Awards "CI Team of the Year."



Recipient of Government Distance Learning Association Five-Star Award for excellence in providing enterprise-wide distance learning solutions for the Federal Government.



From 2016 - 2020, CDSE was recognized at the Learning! 100 Awards.



Since 2008, won over 100 Horizon and Omni awards for outstanding achievement in media production for training courses, security shorts, practical exercises and virtual environments.



Finalist for Chief Learning Officer (CLO) magazine's LearningElite award for the past three years.

For the full list of awards, visit our website:

<https://www.cdse.edu/About-CDSE/Awards/>



STAY CONNECTED WITH CDSE

Keep up to date on the latest CDSE offerings by subscribing to one of our publications and sharing this information with your workforce.

Weekly
Flash

Monthly
Pulse

Quarterly Product
Update

Sign up at

<https://www.cdse.edu/CDSE-News/>

FOLLOW US ON SOCIAL MEDIA



<https://www.facebook.com/TheCDSE>



<https://twitter.com/TheCDSE>



<https://www.linkedin.com/showcase/cdse>



<https://www.youtube.com/user/dsscde#p/u>



CDSE BY THE NUMBERS

1
CDSE

2
LOCATIONS

6 CERTIFICATIONS WITH NATIONAL-LEVEL ACCREDITATION

7 AWARDS RECEIVED

37 CDSE COURSES WITH ACE CREDIT™ RECOMMENDATIONS

178
EDUCATION COURSE COMPLETIONS IN FY2022



1,706
CERTIFICATION AND CREDENTIAL CONFERRALS

2,374
DIGITAL BADGES ISSUED IN FY2022

24,492
LIVE WEBINAR ATTENDEES IN FY2022

23,763
RECORDED WEBINAR ATTENDEES IN FY2022



4,294,695
COURSE COMPLETIONS IN FY2022