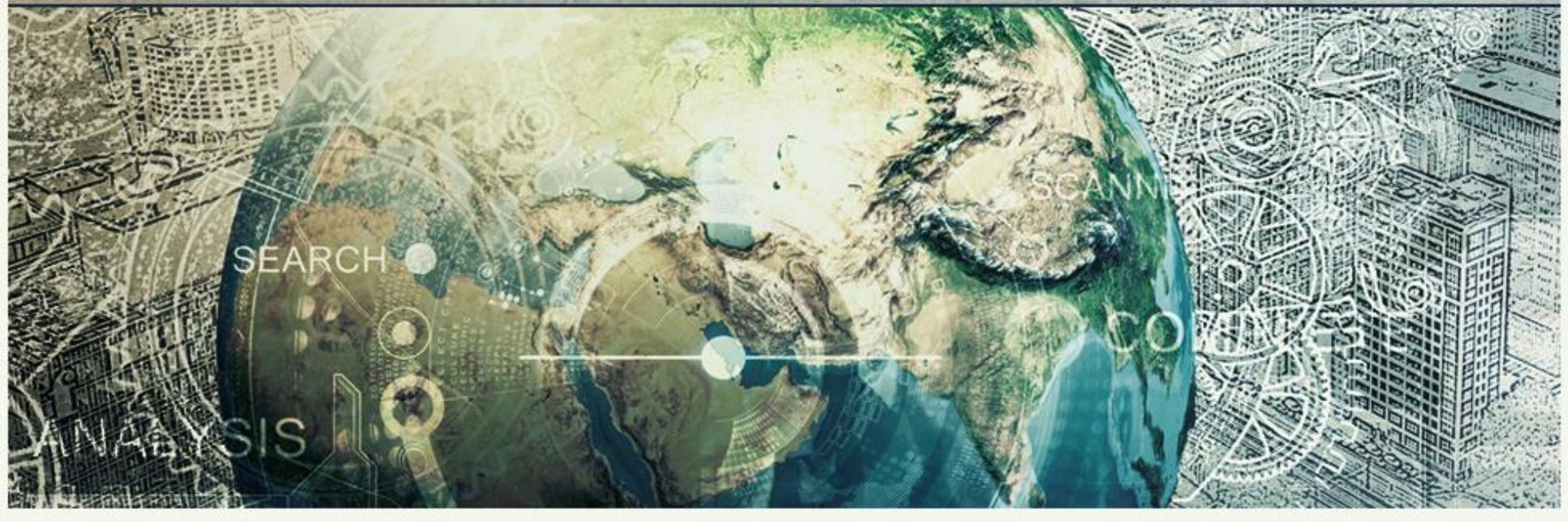


6th ANNUAL



Defense Security Service

FOCI FSO CONFERENCE





Defense Security Service
FOCI CONFERENCE



DANIEL PAYNE

Director

Defense Security Service



THE NEW NORMAL

- **Overseas Headquarters**

- Multinational corporations
- **298** FOCI facilities; **\$18B** in 2015 sales
- * Risks: illicit influence, information leaks, supply chain infiltration



- **Investment Vehicles**

- Financial organizations or individuals
- **177** facilities; **\$4.1B** in 2015 sales
- * Risks: structured acquisitions, hidden influence



- **Foreign Governments**

- Companies and sovereign wealth funds
- **28** facilities; **\$2.6B** in revenue
- * Risks: foreign intelligence targeting





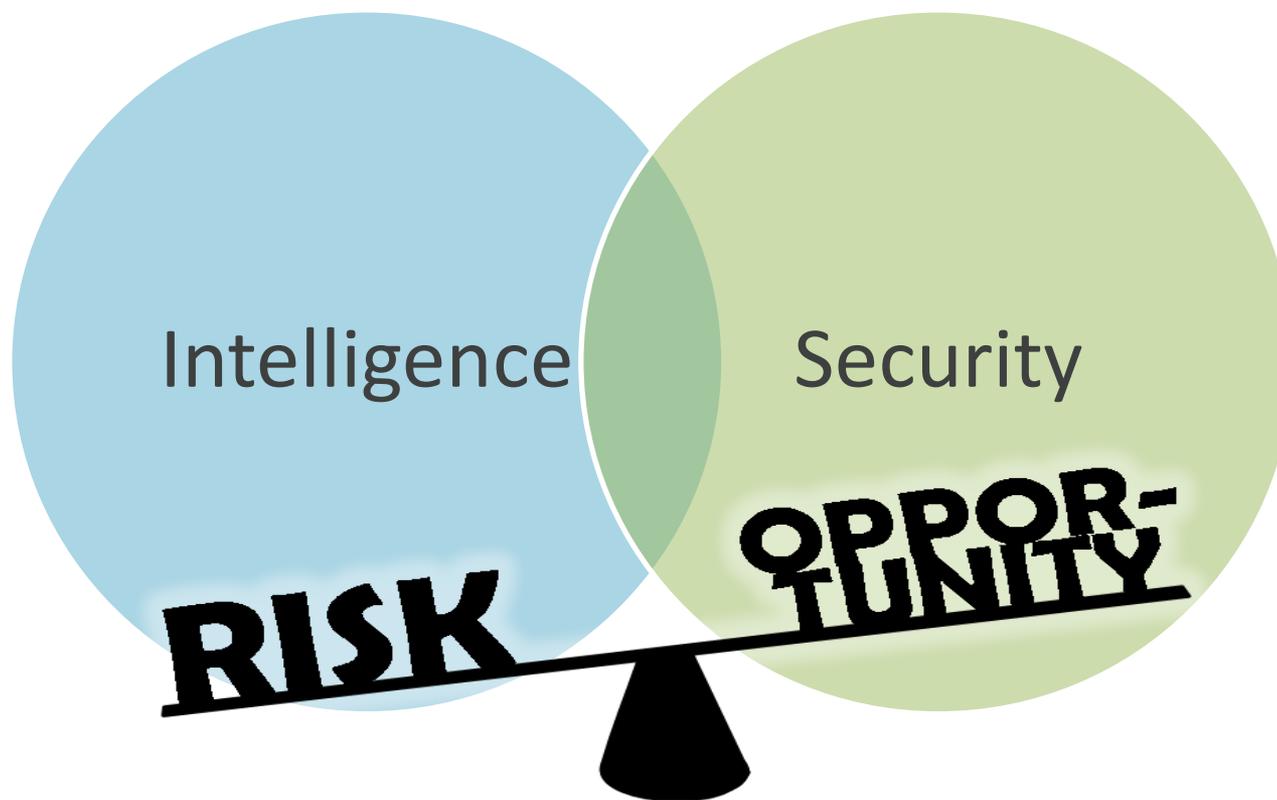
RISK BASED ANALYSIS AND MITIGATION



- 1 • Identify what we need to protect
- 2 • Determine plausible threat scenarios
• Rate impact of loss
• Use threat, impact of loss and vulnerability
- 3 • Determine if risk can be mitigated
• Re-evaluate impact of loss, and vulnerability
- 4 • Engage with stakeholders and partners to implement mitigation strategy
- 5 • Continuously evaluate results of risk mitigation

$$\text{Risk} = f\{\text{Threat, Vulnerability, Impact}\}$$

INTEGRATING INTELLIGENCE & SECURITY



CYBER THREAT



NBC NEWS HOME TOP VIDEOS DECISION 2016 ONGOING: EUROPE
U.S. WORLD LOCAL POLITICS HEALTH TECH SCIENCE POP CULTURE BUSINESS INVESTIGATION

TECH
APR 12 2016, 8:54 AM ET

Cyber Threats Are Getting Smarter: FBI

by HERB WEISBAUM

Rafe Swan / Getty Images

SHARE

Share

Tweet

Share

Email

Print

Comment

The technology you use is being targeted, every hour of every day. These digital attacks are growing in number and sophistication, according to the Internet Security Threat Report released by the FBI and Symantec on Tuesday. The data lost, the money stolen, and the damage caused by cybercriminals is worse than ever.

"We see a higher level of professionalization in cyberattacks, not just nation states where you expect that sophisticated actors, but also cybercriminals," said Kevin Haley, director of the FBI's Cyber Division.

Cybercrime is now such a part of everyday life that the staggering numbers being reported are no longer surprising. More than 430 million new and unique pieces of malware were reported from the year before.

FOX NEWS Politics

Politics Home Elections 2016 Executive Senate House Defense Judiciary Fox News Poll

FBI warns of cyber threat to electric grid

By Bill Gertz · Published April 11, 2016 · Washington Free Beacon

Three months after a Department of Homeland Security intelligence report downplayed the threat of a cyber attack against the U.S. electrical grid, DHS and the FBI began a nationwide program warning of the dangers faced by U.S. utilities from damaging cyber attacks like the recent hacking against Ukraine's power grid.

The nationwide campaign by DHS and the FBI began March 31 and includes 12 briefings and online webinars for electrical power infrastructure companies and others involved in security, with sessions in eight U.S. cities over the next week in Washington.

Trending in Politics

1 Fresh document trove sheds light on Clinton-Trump ties

cy·ber·threat
/'sīber, THret/

noun
noun: cyber-threat

the possibility of a malicious attempt to damage or disrupt a computer network or system.
"the FBI has opened an investigation to address the potential cyberthreat"



INTEGRATING DOD AND THE INTEL COMMUNITY



Plus 31 executive branch agencies



QUESTIONS & COMMENTS



Defense Security Service
FOCI CONFERENCE



2016 FOCI FSO CONFERENCE

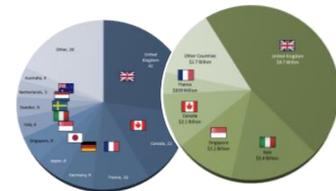
Fred Gortler
Industrial Security
Integration and
Application



UNPRECEDENTED INNOVATION AND RIGOR

- **DSS is modernizing its business analysis capabilities**

- Using financial models to understand FOCl
- Deploying new tools and methods



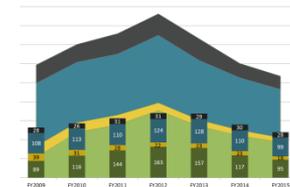
- **FOCl mitigation balances risk and opportunity**

- Risks of compromise or loss
- Opportunities for U.S. military advantage



- **In an era of consolidation, DSS must be agile**

- Not all FOCl is created equal
- Mitigation must match the risk





GLOBALIZATION IMPACT ON NISP IN 2016



QUICK FACTS:

- 31 Countries
- 240 Agreements
- 535 Facilities
- \$25B Revenues
- 95 Board Resolutions
- 18 Security Control Agreements
- 99 Special Security Agreements
- 28 Proxy Agreements



AGENDA

0830 – 0900	Welcome	Dan Payne, DSS Director
0900 – 0915	Conference Overview	Fred Gortler, Director Industrial Security Integration and Application
0915 – 1015	Risk & Competition in the Global Marketplace	Nicoletta Giordani, Assistant Director Industrial Security and Application Business Analysis and Mitigation Strategy
		Panel: Sarah Barnhart Carmine Mele Nate Millsap James Snodgrass
1015 – 1030	Break	
1030 – 1100	FOCI Year in Review	Peter Jackson
1100 – 1200	Risk Based Analysis & Mitigation	Fred Gortler Mike Halter, Deputy Director, Industrial Operations Brian Miller, Director, DSS Academy William Stephens, Director, Counterintelligence
1200 – 1315	Lunch	

AGENDA



1315 – 1415	Affiliated Operations Plan	Allyson Renzella, Branch Chief Business Analysis and Mitigation Strategy
1415 – 1430	CDSE Training Product & Resources	Glenn Stegall, Industrial-Cyber Security Branch Chief, CDSE
1430 – 1445	Break	
1445 – 1515	Behaviors in the Cyber Domain Impacting the NISP	Donald Reese, Deputy Director, CI Cyber Operations
1515 – 1600	Operations Update	George Goodwin NISP Administration and Policy Analysis Micah Komp, Quality Assurance Manager



FOR WANT OF A NAIL





QUESTIONS & COMMENTS



Defense Security Service
FOCI CONFERENCE



RISK & ANALYSIS
COMPETITION IN
THE GLOBAL
MARKETPLACE



RISK & COMPETITION IN THE GLOBAL MARKETPLACE

- Moderator:
 - Nicoletta Giordani
- Panel Members:
 - Sarah Barnhart
 - Carmine Mele
 - Nate Millsap
 - James Snodgrass



Defense Security Service
FOCI CONFERENCE



2015 FOCI SNAPSHOT

Foreign Investment in
the U.S. Defense
Industrial Base

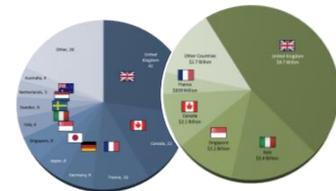
Peter Jackson



BUSINESS INTELLIGENCE AT DSS

- **DSS is modernizing its business analysis capabilities**

- Using financial models to understand FOCl
- Deploying new tools and methods



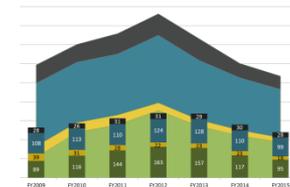
- **FOCl mitigation balances risk and opportunity**

- Risks of compromise or loss
- Opportunities for U.S. military advantage



- **In an era of consolidation, DSS must be agile**

- Not all FOCl is created equal
- Mitigation must match the risk



MITIGATION MUST MATCH THE RISK



- Mature business intelligence allows DSS to see both where risk exists—and where it does not
- Awareness of DoD buying power, the competitive landscape, and supply chains enables DSS to intelligently balance risk and opportunity
- DSS is posturing to respond to the changing business needs of its defense partners at home and abroad



QUESTIONS & COMMENTS



Defense Security Service
FOCI CONFERENCE



RISK BASED ANALYSIS & MITIGATION

Fred Gortler
Michael Halter
Brian Miller
William Stephens

RISK BASED ANALYSIS AND MITIGATION



$$\text{Risk} = f\{\text{Threat, Vulnerability, Impact}\}$$

*(Terrorists,
Criminals,
Spies)*

*(People,
Process,
Systems)*

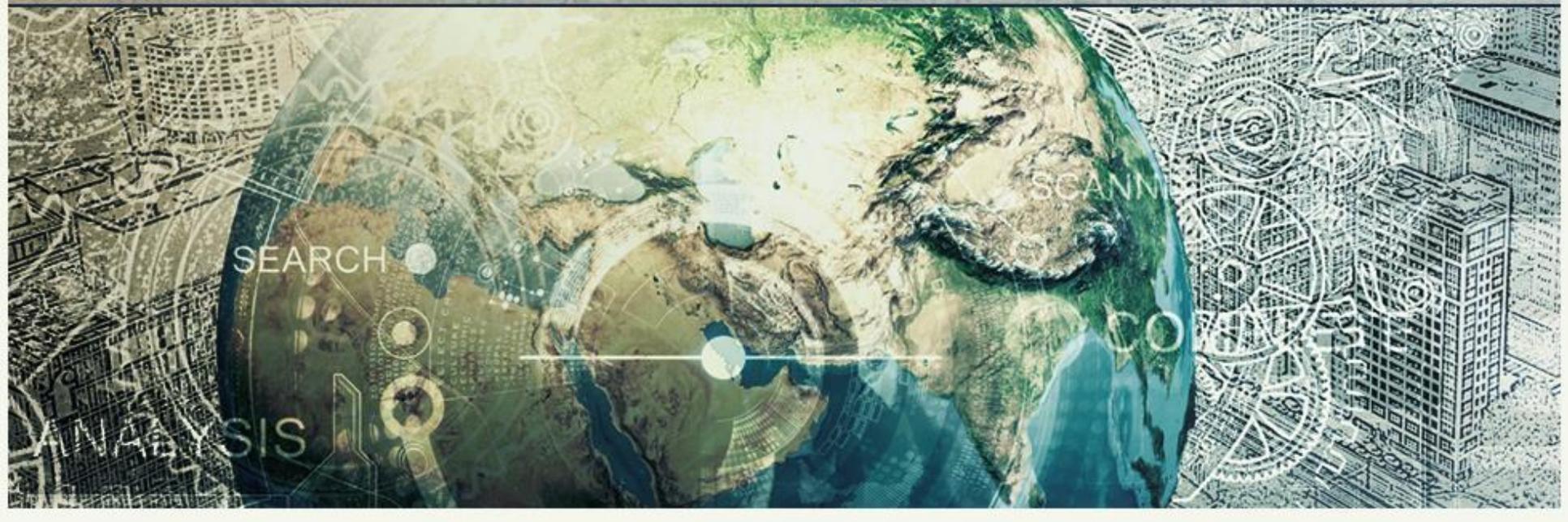
*(Lives,
Cost,
Time)*

6th ANNUAL



Defense Security Service

FOCI FSO CONFERENCE





Defense Security Service
FOCI CONFERENCE



**AFFILIATED ANALYSIS
OPERATIONS PLAN**

Allyson Renzella



AGENDA

1. AOP Guide for Industry
2. Identification of Affiliated Operations
3. AOP Submission and Acceptable/Unacceptable Examples
4. AOP Compliance and Best Practices
5. FOCI Training Update
6. Questions



AOP GUIDE FOR INDUSTRY

Ensure **COMPLIANCE** with the processes outlined in the approved AOP

SURVEY administrative and operational functions to identify Affiliated Operations

DESCRIBE Affiliated Operations, risks and mitigation in an AOP for DSS approval

Identify **RISKS** presented by each Affiliated Operation

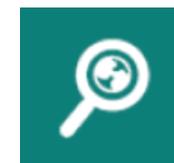
Work with relevant **EMPLOYEES** to develop risk mitigation measures



IDENTIFICATION OF AFFILIATED OPERATIONS



- The AOP provides transparency to DSS and the GSC about interactions and relationships between FOCI companies and their affiliates, to include:
 - Shared Services
 - Reversed Shared Services
 - Shared Employees
 - Shared Third-Party Services
 - Cooperative Commercial Arrangements
- From this potential risks can be identified:
 - Unauthorized access to classified or sensitive information.
 - Undue influence over the management and operations of mitigated companies.





AOP SUBMISSION

The guide describes how to develop the AOP, to include the following elements for each identified shared service:

1. Detailed description of the shared service.



2. Risks inherent in sharing the service.



3. Mitigation measures associated with shared service.



4. Review of the shared service, internally by the GSC, FSO, and TCO, and externally by DSS.



ACCEPTABLE AOP SUBMISSION: INTERNAL AUDIT



1. Service Description:



- The cleared company (Company) may work with the affiliate to scope the internal audit and receive guidance on the affiliate's standard corporate practices.
- The focus of the audit will be financial reporting, operational performance, and compliance with pertinent laws and regulations.
- Internal audits are expected to take place annually.
- Company may submit the results of the audit to the affiliate for review.
- Company's board will determine whether to accept or deny internal audit recommendations proposed by the affiliate.

ACCEPTABLE AOP SUBMISSION: INTERNAL AUDIT



2. Risks:



- Affiliate scoping, guidance, and review of audit report may result in:
 - Inadvertent disclosures of classified or other sensitive information.
 - Identification of cleared personnel and classified programs.
 - Compromise of company managerial independence.
 - Undue influence on process improvement recommendations impacting the performance of classified contracts.

ACCEPTABLE AOP SUBMISSION: INTERNAL AUDIT



3. Mitigation Measures:



- The company maintains an internal audit capability or may use a third-party internal audit provider. The affiliate will not directly participate in the company's internal audit.
- The cleared company's board will work with the affiliate to scope the internal audit and determine how to use the subject matter expertise.
- FSO/TCO will review the audit report and GSC will approve dissemination of final version to the affiliate.
- The cleared company's board will make the final decision on implementation of recommendations.

ACCEPTABLE AOP SUBMISSION: INTERNAL AUDITS



4. Review of Service:



- Documentation pertaining to the scope and standard corporate practices used for the internal audit.
- Board meeting minutes pertaining to internal audit (e.g. approval of scope, review of audit results, deliberation on improvement recommendations).
- Records pertaining to interactions related to the service (e.g. visitor requests, electronic communications)
- Copy of audit results submitted to the affiliates and records of FSO, TCO, and GSC approvals.

UNACCEPTABLE AOP SUBMISSION



1. Service Description:

- Affiliate will participate in the cleared company's internal audit.



2. Risk:

- There is no risk because classified information is not involved.
- This service presents no FOCI risks.

3. Mitigation Measures:

- The risk is mitigated by the FOCI mitigation agreement.
- The audit will be conducted by U.S. affiliate personnel

4. Review of Service:

- DSS may review any documents at any time.

AOP COMPLIANCE & BEST PRACTICES



- An AOP is a living document that requires continuous monitoring of new and existing shared services.
- When planning to integrate business functions and processes, resulting affiliated operations should be addressed before decisions are made.
- GSC should be involved in the development and maintenance of the AOP.
- Senior management should involve FSO for awareness of possible affiliated operations.
- Affiliated operations can be identified while reviewing electronic communications and visit requests.



FOCI TRAINING UPDATE

- DSS is developing three new training modules (4, 5, & 6) for Outside Directors and Proxy Holders





FOCI - Outside Directors, Proxy Holders, and Voting Trustees Training – Module 1

Module 1 Introduction to DSS and Foreign Ownership, Control, or Influence (FOCI)

Menu Transcript

▼ Module1

Module 1: Introduction

Module 1: Objectives

DSS Overview

Define FOCI

FOCI Factors

▼ FOCI Lifecycle

Mitigation Negotiation

▼ Mitigation Implementation

ECP Definition

TCP Definition

AOP Definition

FLP Definition

Visitation Plan Definition

Mitigation Oversight

Change Condition

Identification & Assessment

▼ Mitigation Instruments

Minority Ownership

Majority Ownership

Module 1: Conclusion



< PREV

NEXT >

A large, faint, grey world map is centered in the background of the slide. The text "QUESTIONS & COMMENTS" is overlaid on the map in a dark teal color.

QUESTIONS & COMMENTS

www.cdse.edu

Center for Development of Security Excellence

CDISE

Learn. Perform. Protect.



CDSE Training Products & Resources

Information and Services

CDSE supports the security community's readiness through education, training, and certification



Take a course

Diverse security courses in a variety of formats for DoD personnel, DoD contractors, employees of other federal agencies, and selected foreign governments



Attend a webinar

Online, informative events available live, on-demand, or previously recorded and address topics and issues of interest to defense security personnel



Become certified

DoD's initiative to professionalize the security workforce via a common set of competencies that promote interoperability, facilitate professional development and training, and develop a workforce of security professionals



Resources

Toolkits, videos, posters, security shorts, job aids, brochures, and other materials to help security personnel perform their jobs



Common questions

Answers to questions about courses, registration, advanced education, certificates, certification, and more



Popular content

The most frequently searched keywords and sought after content, including Derivative Classification, JPAS, PII, and Insider Threat

Take a Course



[Home](#) / [Take a Course](#)

Awareness Courses

Open eLearning, no registration required

These eLearning courses do not require registration or sign in. Students can print a Certificate of Completion at the end of a course; however, CDSE maintains no record of course completion. Open eLearning courses cannot be used as prerequisites for instructor-led courses; they are for occasional users of select CDSE awareness courses (e.g., annual mandatory training).

Training Courses

STEPP registration required

These are instructor-led, eLearning, and virtual instructor-led training courses. Students register in our learning management system STEPP, where their transcripts and certificates are maintained for record keeping. These courses are for DoD personnel and contractors with security responsibilities.

Advanced and Graduate Courses

STEPP registration required

These semester-long, education courses are designed specifically to develop leaders for the DoD security community and are similar in scope to graduate level courses. Students are required to register in STEPP. Courses are delivered using an online collaborative learning environment and available to U.S. Government civilian personnel and U.S. military service members worldwide.

CDSE Webinars



[Home](#) / [Training](#) / [CDSE Webinars](#)

CDSE Security Speaker Series

CDSE's Security Speaker Series delivers live interviews with knowledgeable, respected leaders in the security community. Speakers discuss trending topic areas. Conversation is driven by hot topics, and the audience may ask questions. Register now!

The OPM Data Breach: How might adversaries use background investigation information against the U.S. Government?

Thursday, April 21, 2016

1:00 p.m. Eastern Time

Registration is restricted to .mil and .gov e-mail

Upcoming Webinars

These live web presentations address topics and issues of interest to defense security personnel. Presenters are able to answer audience questions.

CDSE Cybersecurity Products and Resources

Thursday, 14 April 2016

11:30 a.m. Eastern Time

2:30 p.m. Eastern Time

FSO Effectiveness

Thursday, 19 May 2016

11:30 a.m. Eastern Time

2:30 p.m. Eastern Time

Previously Recorded Webinars

- Access [On Demand webinars](#) with a CDSE Certificate of Training available for download. *Registration is required.*
- Access [webinars](#) without a CDSE Certificate of Training available for download. *No registration is required.*

What are CDSE webinars?

A series of live web events to address topics and issues of interest to defense security professionals.

Who can attend CDSE webinars?

Most CDSE webinars are open to anyone with an interest in DoD-related security issues and concerns.

Sign up for the webinar you are interested in to receive an invite with access information.

How do I access CDSE webinars?

CDSE webinars are hosted on CDSE.AdobeConnect.com and can be accessed from any computer with an Internet connection and Adobe's Flash Player. For detailed access information see [CDSE Webinars on AdobeConnect](#).

AskPSMO-I Webinars [GO»](#)

PSMO-I webinars discuss topics that currently effect Industry personnel security clearances, initiatives and procedural updates.

Certification



[Home](#) / [Certification](#)

About SPeD Certification

Get an overview of the SPeD Certification Program and learn about our certifications.

Become Certified

Learn the 10 steps to becoming SPeD certified and register for a SPeD assessment.

Prepare for Certification

Support your security knowledge and skills with the help of CDSE's Competency Preparatory Tools (CPTs).

Maintain Your Certification

You need 100 Professional Development Units (PDUs) to maintain your SPeD certification.

SPeD Resources

Resources for Candidates, Certificants, and DoD SPeD Components.

Our Certifications



Security Fundamentals Professional Certification (SFPC)



Security Asset Protection Professional Certification (SAPPC)



Security Program Integration Professional Certification (SPIPC)



Special Program Security Certification (SPSC)



Industrial Security Oversight Certification (ISOC)



Physical Security Certification (PSC)



Adjudicator Professional Certification (APC)



Due Process Adjudicator Professional Credential (DPAPC)

Resources



[Home](#) / [Resources](#)



Registrar

Information for current and prospective students.



Security Shorts

Training shorts are usually ten minutes or less and allow security personnel to refresh their knowledge of a critical topic or quickly access information needed to complete a job.



Toolkits

A repository of role-based resources that serve as a one-stop shop for security essentials.



Job Aids

Security products designed to provide guidance and information to perform specific tasks.



Security Training Videos

Training videos provide information and demonstrate various security procedures.



Security Posters

Our posters are available for you to download and promote security awareness in the workplace.

Common Questions and answers



[Home](#) / [Common Questions](#)

Choose a category below to find the help you need.



Accessibility



Certification



Certification
Maintenance



Course Offerings



Exams



Logging In



Open eLearning
Questions



PDUs, CEUs, and
ACE Credits



Pending/Waiting Lists



Printing Course
Certificates



Reference Materials



Registration



Security Education &
Training



STEPP



System Requirements



Technical Issues/
Error Messages



Test Scores



Transcripts
(ACE/STEPP)



Virtual Training

Popular Content



[Home](#) / [Popular Content](#)

- [Counterintelligence \(CI\) Awareness and Reporting](#)
- [Derivative Classification](#)
- [Insider Threat](#)
- [Joint Personnel Adjudicative System \(JPAS\)](#)
- [Marking Classified Information](#)
- [Personally Identifiable Information \(PII\)](#)
- [OPSEC](#)
- [Unauthorized Disclosure](#)

Information and Services

CDSE supports the security community's readiness through education, training, and certification



Take a course

Diverse security courses in a variety of formats for DoD personnel, DoD contractors, employees of other federal agencies, and selected foreign governments



Attend a webinar

Online, informative events available live, on-demand, or previously recorded and address topics and issues of interest to defense security personnel



Become certified

DoD's initiative to professionalize the security workforce via a common set of competencies that promote interoperability, facilitate professional development and training, and develop a workforce of security professionals



Resources

Toolkits, videos, posters, security shorts, job aids, brochures, and other materials to help security personnel perform their jobs



Common questions

Answers to questions about courses, registration, advanced education, certificates, certification, and more



Popular content

The most frequently searched keywords and sought after content, including Derivative Classification, JPAS, PII, and Insider Threat



Defense Security Service
FOCI CONFERENCE



OPERATIONS UPDATE

George Goodwin
Micah Komp

OPERATIONS UPDATE



- NISPOM Change 2 (General Overview)
- Risk Management Framework (System Accreditation)
- Insider Threat Program Implementation and Management

NISPOM CHANGE 2, INSIDER THREAT



- What will be required?
- How do I implement my program?
- Company vs. Corporate Program
- DSS Resources and Tools
- The oversight question?

A large, faint, light gray world map is centered in the background of the slide. The text "QUESTIONS & COMMENTS" is overlaid on the map in a dark teal color.

QUESTIONS & COMMENTS