Industrial Security **Webinar Series**

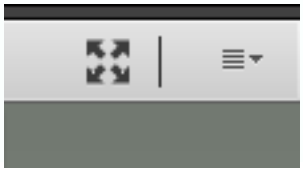
Learn @ Lunch

Security Vulnerabilities and DSS Assessments

Learn @ Lunch

CDSE

Meeting Room Navigation



Notes box for audio information and other announcements

To enlarge the slide, click on the Full Screen button. To get out of Full Screen view, select Full Screen again. You will need to be out of Full Screen view to enter question responses.

2

Learn @ Lunch CDSE

Meeting Room Navigation

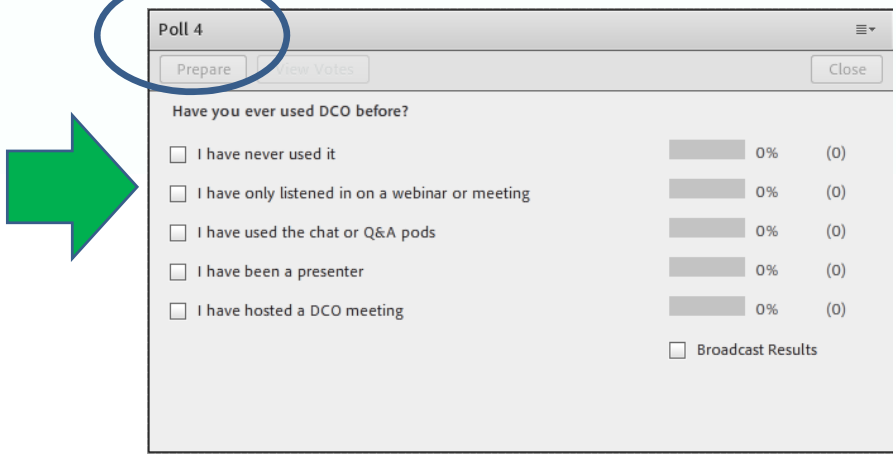
Q&A box for entering questions/feedback

File share box to download material for today's presentation

3

Learn @ Lunch CDSE

Example of a Poll Question

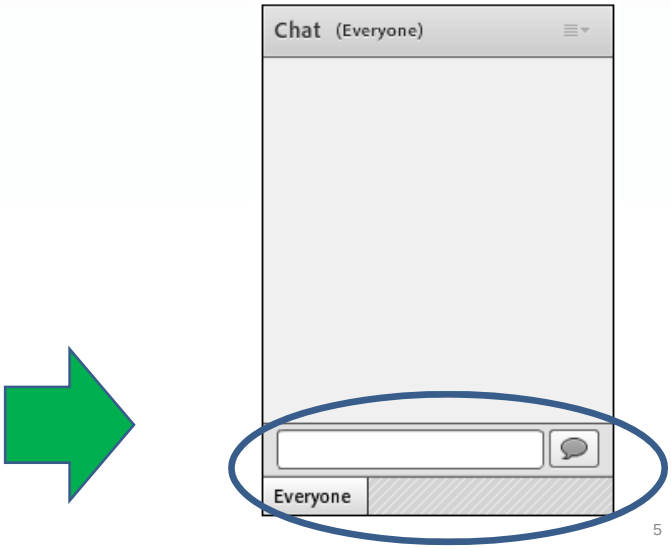


4

Learn @ Lunch

CDSE

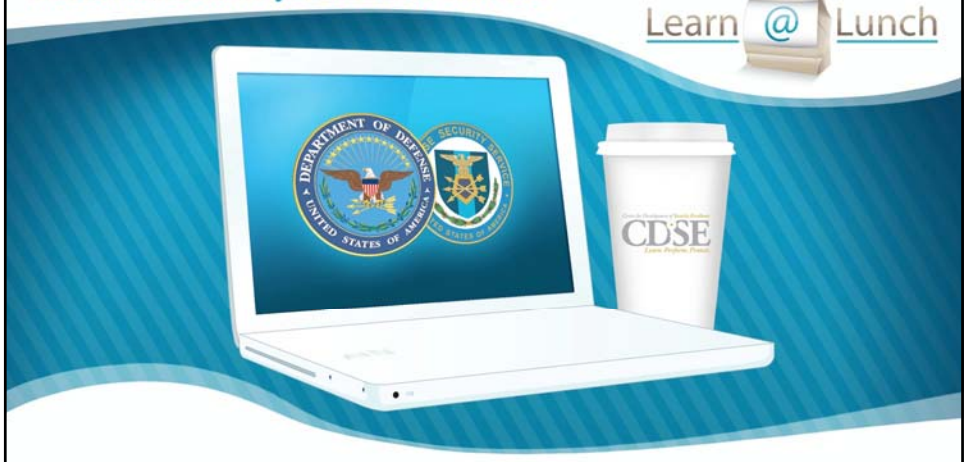
Chat Box



5

Industrial Security **Webinar Series**

Learn @ Lunch

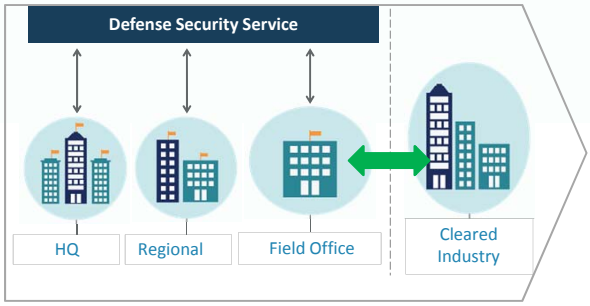


Security Vulnerabilities and DSS Assessments

Learn @ Lunch CDSE

Partnership: Defining & Refining

Partnership… key to continued success



Pathway to Optimized Operational Impact

Learn @ Lunch CDSE

Risk-based Oversight

Risk = *f* {Threat, Vulnerability, Consequence Value}

National Cleared Industrial Base

Threat

- Suspicious Contact Reports
- IIRs
- Referrals for Action
- Threat Products
- Insider Threat
- Cyber\Threat Notifications

Vulnerability

- Vulnerability Assessments
- IT Accreditations\CCRIs
- Security Clearance Process
- Technology Control Plans
- Security Violations
- Key Management Changes
- Physical Security
- Security\FOCI Mitigation
- Security Training\Education
- Operations Analysis Group

Consequence Value

- Facilities of Interest List
- "Trends" Product
- Company Assessments
- Program Assessments
- Partnership with Industry
- Finished Intelligence Industrial Base Analysis
- FOCI Analysis
- CFIUS Reviews

Learn @ Lunch CDSE

Facilities of Interest List (FIL)

- Published quarterly by DSS to prioritize vulnerability assessments and oversight in the field
- Determines the level of risk for the facilities technology threat
- Supports the National Counterintelligence Strategy and the DoD Counterintelligence Strategy

Goal:

A coordinated, integrated visit from DSS to the right facility, at the right time, with appropriate resources resulting in a more effective, meaningful assessment.

Learn @ Lunch CDSE

FIL-based Prioritization

Tier 1 = High risk → Tier 2 = Medium risk → Tiers 3 (Possessing) and 4 (Non-possessing) = Lower risk

Tier 1
Targeted by entities with malicious intent

Tier 2
Targeted by entities whose malicious intent has not been fully ascertained

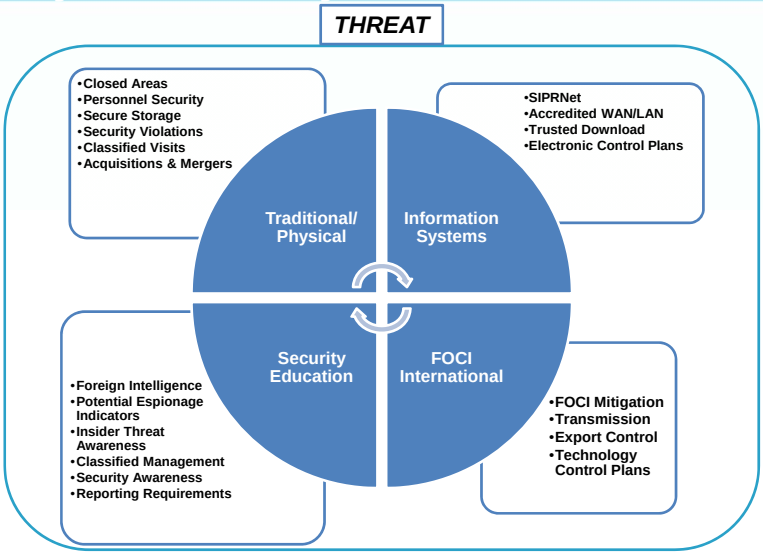
Tier 3
Facilities with no credible information that it is being, or is likely to be, targeted

Tier 4
All non-possessing facilities not meeting the criteria of other tiers

Learn @ Lunch

CDSE

Security Vulnerability Assessments



Learn @ Lunch

CDSE

Vulnerabilities Defined

ACUTE Vulnerability	CRITICAL Vulnerability	Vulnerability
• Puts classified information at imminent risk of loss or compromise, or that has already resulted in the compromise of classified information • Requires immediate corrective action • Further categorized as either "Isolated," "Systemic," or "Repeat"	• Instances of NISPOM non-compliance that are serious, or that may foreseeably place classified material at risk or in danger of loss or compromise • Will be further categorized as either "Isolated," "Systemic," or "Repeat"	• All instances of non-compliance with a NISPOM requirement that are not acute or critical

Learn @ Lunch CDSE

Let's Chat-Scenario 1

A cleared employee discloses classified information to an non cleared employee.

Learn @ Lunch CDSE

Let's Chat-Scenario 2

A facility did not provide annual training to its five cleared employees:

Helen Smith, Roger Banks, Mary Jones, James Cook, Bill Owens

The same vulnerability (no annual training provided to the same five cleared employees) was cited during the last vulnerability assessment.

Learn @ Lunch CDSE

Let's Chat-Scenario 3

The FSO did not destroy a new employee's SF86 after the employee's personnel clearance was granted.

Learn @ Lunch CDSE

Poll Question

Learn @ Lunch CDSE

Top Ten Common Vulnerabilities

- **Inadequate security education, training, awareness** 15.9%
- Persons without proper eligibility accessing classified 15.8%
- *Not auditing & reviewing audit results for classified systems* 6.5%
- Failure to provide written notification that review of the SF-86 is for adequacy and completeness or destroy when eligibility has been granted or denied 5.7%
- **Failure to perform self-inspection of security program** 2.9%
- **Not reporting classified compromises** 2.4%
- *Classified IS configuration and connectivity management* 2.3%
- Personnel clearance re-investigations out-of-scope 2.2%
- *Processing classified on a unaccredited system* 2.1%
- **Unreported facility clearance change conditions (foreign buyout, merger, key mgt. personnel changes, etc.)** 1.8%

Italicized = IT systems
Underlined = Personnel Security Clearance
Bold = Other process/procedures

Learn @ Lunch CDSE

Vulnerability Assessments

Focus Areas:

- Personnel Security Clearance Validation/Reduction
- Incident and Adverse Information Reporting
- Information Technology Security
- Security, Education, Training, & Awareness (SETA)

Learn @ Lunch CDSE

IT Vulnerabilities

Top 5 deficiencies in System Security Plans (SSP):

- Incomplete or missing attachments
- Inaccurate or incomplete diagram
- General procedures contradict protection profile
- Integrity & availability not properly addressed
- SSP was not tailored to the system

Top 5 vulnerabilities during visits:

- Inadequate auditing controls
- Security Relevant Objects not protected
- Inadequate configuration management
- Improper session controls
- Identification & authentication controls

Learn @ Lunch CDSE

NISP Enhancements…

- Enhance protection of classified information beyond baseline NISPOM standards
- Are validated as having an effective impact on the overall security program, through employee interviews and review of process/procedures
- DSS established NISP enhancement categories, based on practical areas, to simplify and ensure field consistency
- Full credit for a NISP enhancement will be given to facilities that complete any action/item in a given category
- Will granted to facilities that meet the baseline NISPOM requirements in that area

Learn @ Lunch CDSE

Your SVA

- Uses a numerical-based rating system
- All facilities start with the same score (700)
- Points are added for identified NISP Enhancements by Category
- Points are subtracted for vulnerabilities by NISPOM reference
- Acute/Critical and Non-Acute/Non-Critical vulnerabilities are weighed separately
- Points subtracted for vulnerabilities by NISPOM reference, not by number of occurrences
- Accounts for size and complexity of a facility

Learn @ Lunch CDSE

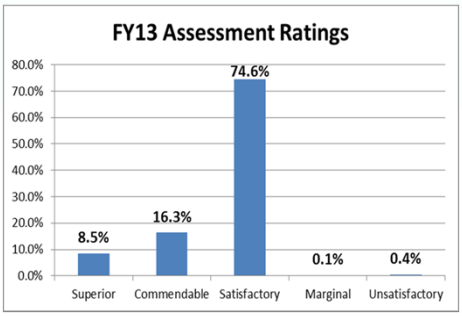
Security Ratings

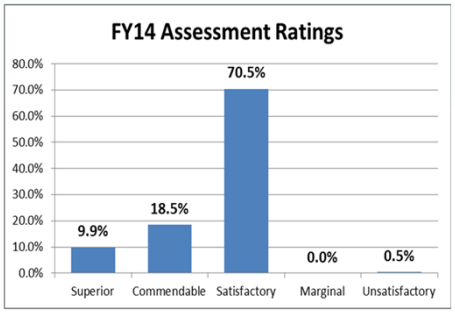
Superior	**Highest Caliber** Contractor has consistently and fully implemented requirements of NISPOM
Commendable	**Exemplary** Contractor has implemented requirements of NISPOM
Satisfactory	**Most Common** Security program is in general conformity with basic requirements of NISPOM
Marginal	**Not in Conformity** Basic requirements of NISPOM not met
Unsatisfactory	**Most serious** Contractor has lost, or is in imminent danger of losing, its ability to adequately safeguard classified information

Learn @ Lunch CDSE

National SVA Ratings

Assessment Ratings for FY13 and FY14





Learn @ Lunch CDSE

Questions?