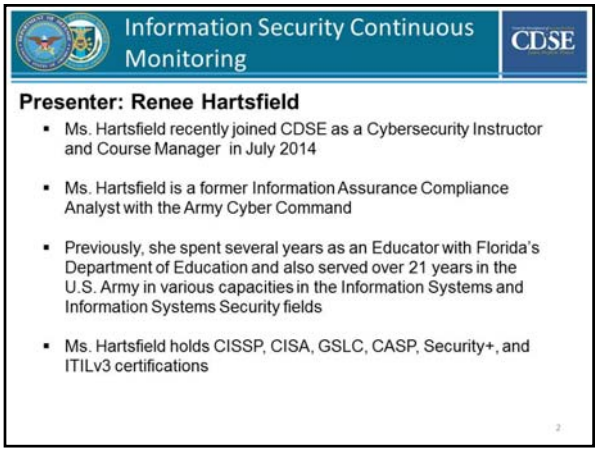

Center for Development of Security Excellence
CDSE
Learn. Perform. Protect.
Information Security Continuous Monitoring (ISCM)

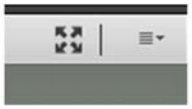

Information Security Continuous Monitoring
CDSE
Presenter: Renee Hartsfield
Ms. Hartsfield recently joined CDSE as a Cybersecurity Instructor and Course Manager in July 2014
Ms. Hartsfield is a former Information Assurance Compliance Analyst with the Army Cyber Command
Previously, she spent several years as an Educator with Florida's Department of Education and also served over 21 years in the U.S. Army in various capacities in the Information Systems and Information Systems Security fields
Ms. Hartsfield holds CISSP, CISA, GSLC, CASP, Security+, and ITILv3 certifications
2


Information Security Continuous Monitoring
CDSE
Presenter: Rebecca Morgan
Ms. Morgan is a Counterintelligence and Cybersecurity Instructor with CDSE.
Ms. Morgan has over twenty years experience in law enforcement, security, and counterintelligence.
She has served various agencies within the Department of Defense as a Special Agent, CI Analyst, Senior Intelligence Operations Planner, Senior Intelligence Advisor and Instructor.
Ms. Morgan holds a Master's Degree in Forensic Science - Corporate Espionage Investigation AND undergraduate degrees in Criminal Justice and Sociology.
3

Information Security Continuous Monitoring

CDSE

Navigation in the Meeting Room



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.

4

Information Security Continuous Monitoring

CDSE

Navigation in the Meeting Room

Q&A box for entering questions to the presenters

File share box to download resources relevant to today's presentation

5

Information Security Continuous Monitoring

CDSE

Example of a Chat Question

6

Information Security Continuous Monitoring

Overview

- Define Information Security Continuous Monitoring (ISCM)
- Identify elements of an ISCM Program
- Discuss ISCM Program Implementation
- Explain Reporting Procedures
- Integrate Counterintelligence Awareness and Security Concerns into your ISCM Program

8

Information Security Continuous Monitoring

What Is Information Security Continuous Monitoring?

NIST 800-137

Maintaining on-going awareness of information security, vulnerabilities, and threats to support organizational risk management decisions

9

Information Security Continuous Monitoring

An effective ISCM Program begins with leadership defining a strategy encompassing

- Technology
- Processes
- Procedures
- Operating Environments
- People

10

Information Security Continuous Monitoring

CDSE

- Foreign Ownership Control & Influence
- Counterintelligence
- Physical Security
- Personnel Security
- Continuity of Operations

10

Information Security Continuous Monitoring

CDSE

ISCM Strategy -

- Based on the organization's risk tolerance
- Metrics of security status indicators
- Supports the organization's core missions/business processes
- Includes change management
- Drive determinations to reject, transfer, or accept risk
- Maintains awareness of threats and vulnerabilities

12

Chat Question 1

CDSE

What resources are available to maintain awareness of threats and vulnerabilities?

Information Security Continuous Monitoring

CDSE

How to Identify Threats & Vulnerabilities

Defense Security Service
Government Contracting Agency
Intelligence Community Reporting
Your Counterintelligence Office

14

Counterintelligence Support to ISCM

CDSE

Counterintelligence is real-time threat awareness.

Counterintelligence helps to:

- Identify threats to your facilities or operations
- Focus security efforts
- Deter the foreign intelligence collection by increasing risk and cost
- Use threat-appropriate Security Countermeasures (SCM)
- Potentially save money on security

15

Threats

CDSE

Who is targeting your system?

- Foreign Intelligence Entities
- Quasi-Governmental Entities
- Commercial Enterprises
- Individuals
- Insider Threats

16

Targets

Both classified and unclassified systems are targeted.

Targeted information includes:

- Dual-use technology
- Militarily critical technology
- Sensitive company documents
- Proprietary information
- Export controlled/classified information and technology
- Information on DoD-funded contracts

17

Vulnerabilities

Vulnerabilities

- Mobile Platform Devices
- Vendor/Business Partner Access
- Physical Environment
- Operational Requirements
- Outdated Hardware/Software
- Personnel – witting or unwitting

18

Vulnerabilities

DoD Insider Threat Program

"Leverages counterintelligence (CI), security, cybersecurity, Human Resources (HR), Law Enforcement (LE), and other relevant functions and resources to identify and counter the insider threat"

Department of Defense
DIRECTIVE

NUMBER 5205.16
September 30, 2014
USD(I)

SUBJECT: The DoD Insider Threat Program

References: See Enclosure 1

1. PURPOSE. In accordance with sections 113 and 131 through 137 of Title 10, United States Code (U.S.C.) (Reference (a)), Presidential Memorandum (Reference (b)), Executive Orders (E.O.s) 12333, 13526, and 13587 (References (c), (d), and (e)), section 922 of Public Law 112-81 (Reference (f)), National Security Directive 42 (Reference (g)), and Committee on National Security Systems Directive 504 (Reference (h)), this directive:

a. Establishes policy and assigns responsibilities within DoD to develop and maintain an insider threat program to comply with the requirements and minimum standards to prevent, deter, detect, and mitigate actions by malicious insiders who represent a threat to national security or DoD personnel, facilities, operations, and resources.

b. Identifies appropriate training, education, and awareness initiatives that may be made available to DoD personnel and contractors in accordance with Reference (b).

c. Ensures appropriate DoD policies, including but not limited to counterintelligence (CI),

19

Information Security Continuous Monitoring

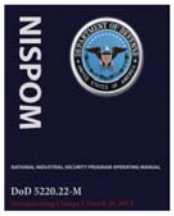
CDSE

Vulnerabilities

NISPOM Reporting Requirements

DoD 5220.22-M

1.301 and 1.302



19

Information Security Continuous Monitoring

CDSE

Process of Implementing ICMS

- **Define** an ISCM strategy
- **Establish** an ISCM program
- **Implement** the ISCM program
- **Analyze and Report** findings
- **Respond** to findings
- **Review and Update** ISCM strategy and program

21

Information Security Continuous Monitoring

CDSE

Define an ISCM strategy based on risk tolerance that maintains clear visibility into assets, awareness of vulnerabilities, up-to-date threat information, and mission/business impacts.

- Tiered Approach
  - Tier 1 – **ORGANIZATION**
  - Tier 2 – **MISSION/BUSINESS PROCESS**
  - Tier 3 – **INFORMATION SYSTEMS**

22

Information Security Continuous Monitoring

Establish an ISCM program determining metrics, status monitoring frequencies, control assessment frequencies, and an ISCM technical architecture.

- Derive from specific objectives to maintain/improve security posture
- Organize to support risk decision making/reporting requirements
- Calculate from a combination of security status data
- Determine at any tier across an organization

23

Information Security Continuous Monitoring

Implement the ISCM program and collect the security-related information required for metrics, assessments, and reporting. Automate collection, analysis, and reporting of data where possible.

Analyze and Report findings, determining the appropriate response. It may be necessary to collect additional information to clarify or supplement existing monitoring data.

- IAW with strategy
  - Collect Data
  - Conduct Assessments
  - Produce Reports
- Use automation where possible

24

Reporting Requirements

DoD Security Must:

- Identify and report illicit foreign cyber activities


Department of Defense
DIRECTIVE

25

Chat Question 2

How can an ISCM Program help identify reportable illicit cyber activity?

Reportable Cyber Activities

- Actual or attempted unauthorized access into U.S. automated information systems and unauthorized transmissions of classified or controlled unclassified information.
- Password cracking, key logging, encryption, steganography, privilege escalation, and account masquerading.
- Network spillage incidents or information compromise.
- Use of DoD account credentials by unauthorized parties.
- Tampering with or introducing unauthorized elements into information systems.

Reportable Cyber Activities

- Unauthorized downloads or uploads of sensitive data.
- Unauthorized use of Universal Serial Bus, removable media, or other transfer devices.
- Downloading or installing non-approved computer applications.
- Unauthorized network access.
- Unauthorized e-mail traffic to foreign destinations.
- Denial of service attacks or suspicious network communications failures.

Reportable Cyber Activities

- Excessive and abnormal intranet browsing, beyond the individual's duties and responsibilities, of internal file servers or other networked system contents.
- Any credible anomaly, finding, observation, or indicator associated with other activity or behavior that may also be an indicator of terrorism or espionage.
- Data exfiltrated to unauthorized domains.

29

Reportable Cyber Activities

- Unexplained storage of encrypted data.
- Unexplained user accounts.
- Hacking or cracking activities.
- Social engineering, electronic elicitation, e-mail spoofing or spear phishing.
- Malicious codes or blended threats such as viruses, worms, trojans, logic bombs, malware, spyware, or browser hijackers, especially those used for clandestine data exfiltration.

30

Information Security Continuous Monitoring

Respond to findings with technical, management, and operational mitigating activities or acceptance, transference/sharing, or avoidance/rejection.

Review and Update the monitoring program, adjusting the ISCM strategy and maturing measurement capabilities to increase visibility into assets and awareness of vulnerabilities, further enable data-driven control of the security of an organization's information infrastructure, and increase organizational resilience.

- Ensure data is current and complete
- Provide Insight into security posture
- Support informed risk management decisions
- Improve ability to respond to known and emerging threats
- Continually refined

Assessments, metrics, and monitoring frequencies change IAW organizational needs

31

Countermeasures

- Threat Awareness and Training for all Personnel
- Conduct frequent computer security audits
- Follow your organization's removable media policy
- Comply with the measures in your organization's policies, including the Technology Control Plan (TCP)
- Stay current with patches and updates
- Conduct frequent computer audits
- Do not rely on firewalls to protect against all attacks
- Report intrusion attempts

Additional Resources

- Counterintelligence & Security Countermeasures

http://www.dss.mil/ci/count_n_sec_count_meas.html

- NIST SP 800-137

http://csrc.nist.gov/publications/nistpubs/800-137/SP800-137-Final.pdf

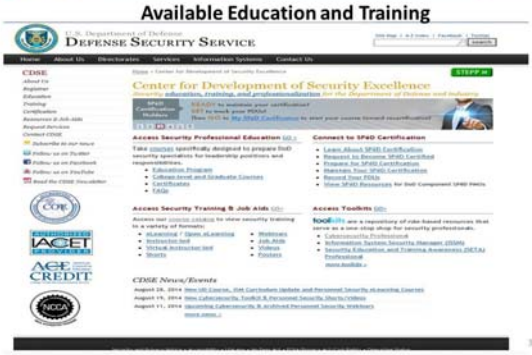
- Continuous Diagnostics and Mitigation (CDM)

https://www.us-cert.gov/cdm

ISCM Can Make a Difference

Information Security Continuous Monitoring

Available Education and Training



Information Security Continuous Monitoring

Questions

Information Security Continuous Monitoring

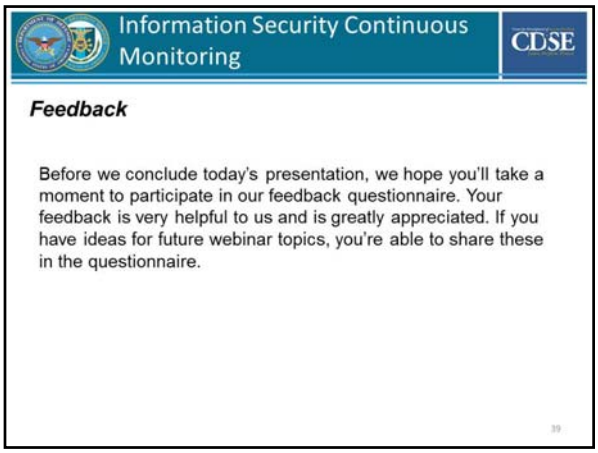
Cybersecurity Training Products and POC

Past Webinars

- Cyber Insider Threat
- Risk Management Framework
- Trusted Downloading
- Top 20 Critical Security Controls

All Other Training

- CDSE Cybersecurity


Information Security Continuous Monitoring
CDSE
Feedback
Before we conclude today's presentation, we hope you'll take a moment to participate in our feedback questionnaire. Your feedback is very helpful to us and is greatly appreciated. If you have ideas for future webinar topics, you're able to share these in the questionnaire.