CDSE Center for Development of Security Excellence

Counterintelligence Webinar Series: The Venn of Counterespionage

LEARN. PERFORM. PROTECT.

TODAY'S SESSION

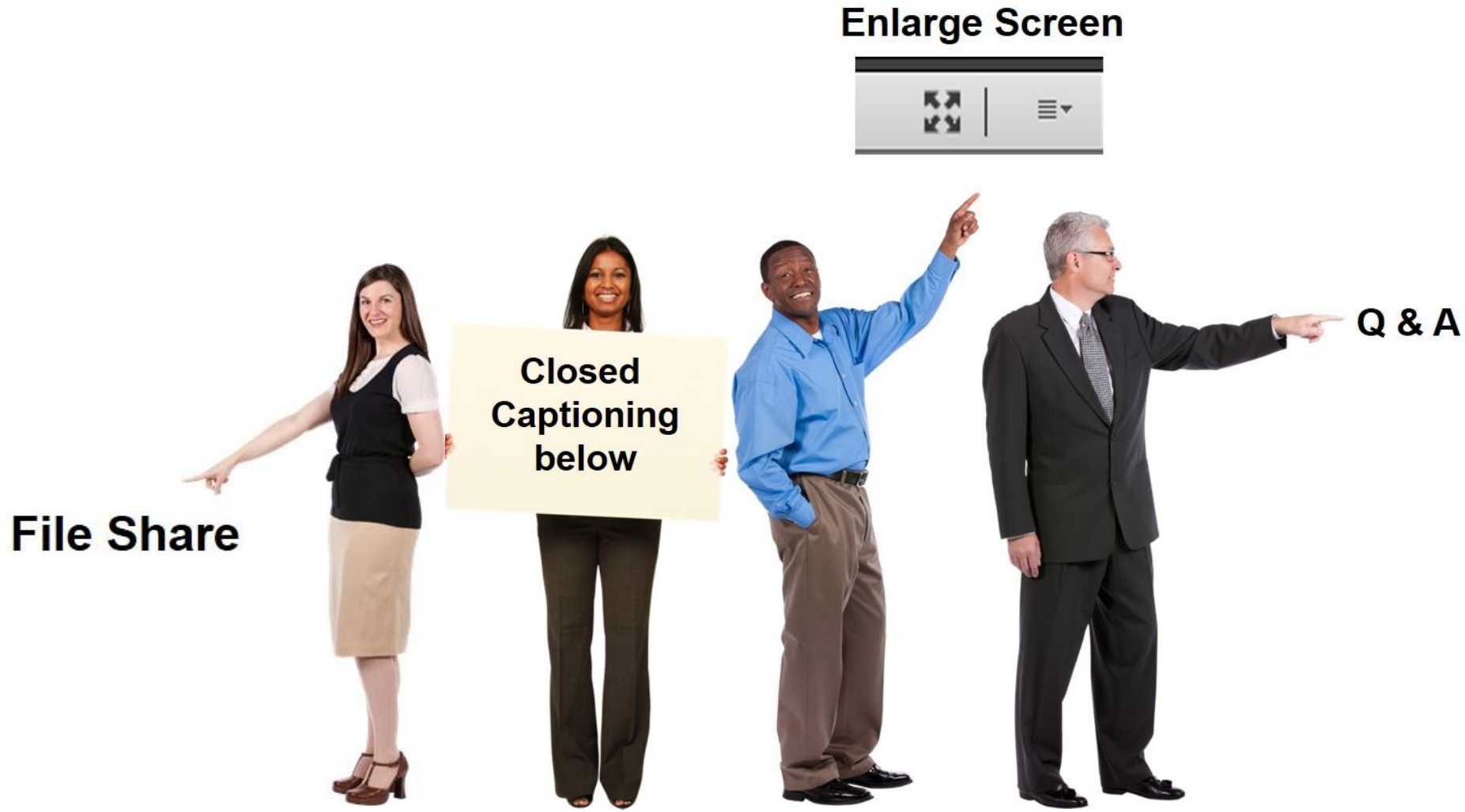
HOST:

Ed Kobeski, CDSE Counterintelligence

GUEST:

Ms. Rebecca Morgan

Attendee Participation & Feedback

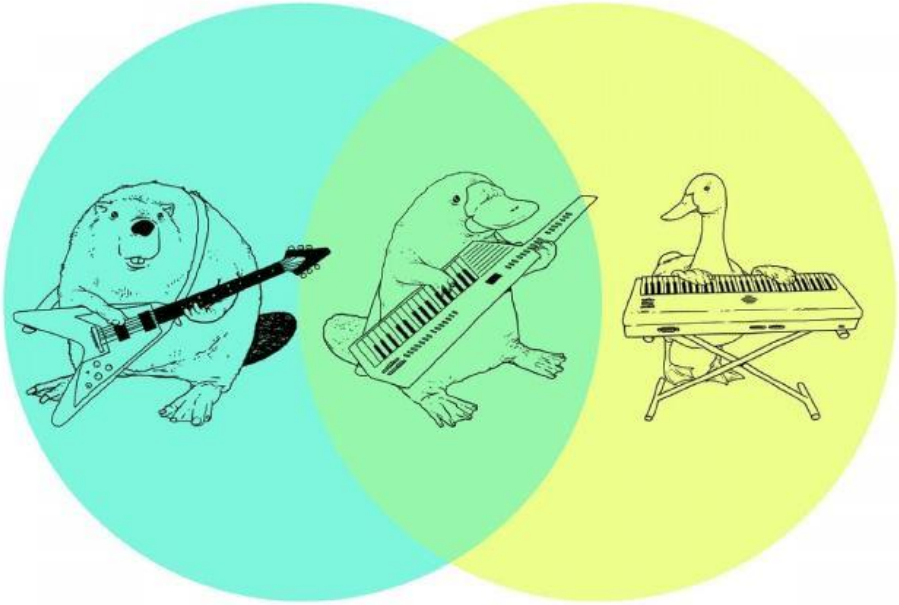


Agenda

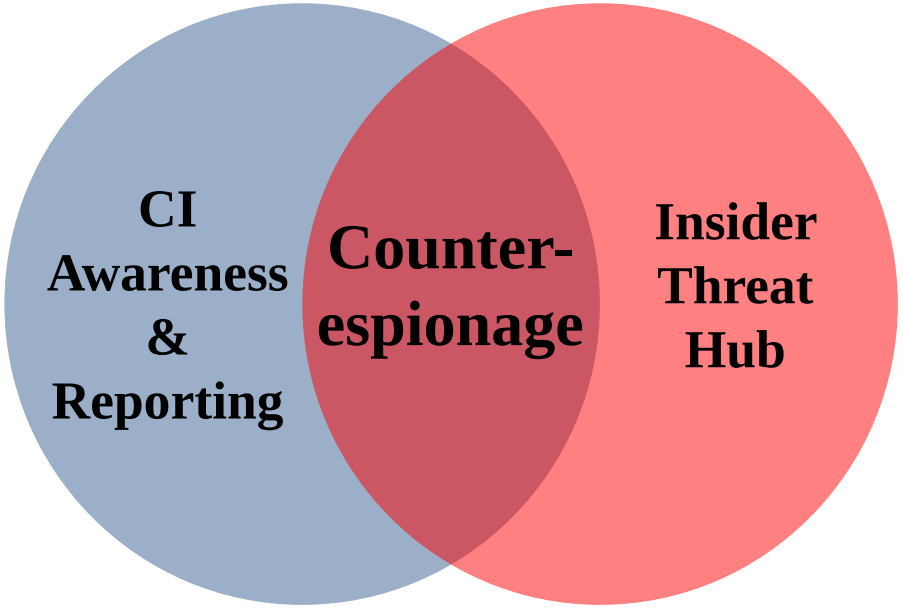
- The Venn of Counterespionage
- CI Definitions
- Insider Threat Definitions
- The Divergence
- The Mergence
- Defense
- Lightning Round!

The Venn of Counterespionage

The greatest
Venn diagram ever



The second greatest
Venn diagram ever



Counterintelligence

- **Counterintelligence:** Information gathered and activities conducted to identify, deceive, exploit, disrupt, or protect against espionage, other intelligence activities, sabotage, or assassinations conducted for or on behalf of foreign powers, organizations or persons or their agents, or international terrorist organizations or activities.

- **Counterespionage:** That aspect of counterintelligence designed to detect, destroy, neutralize, exploit, or prevent espionage activities through identification, penetration, manipulation, deception, and repression of individuals, groups, or organizations conducting or suspected of conducting espionage activities.

Insider Threat

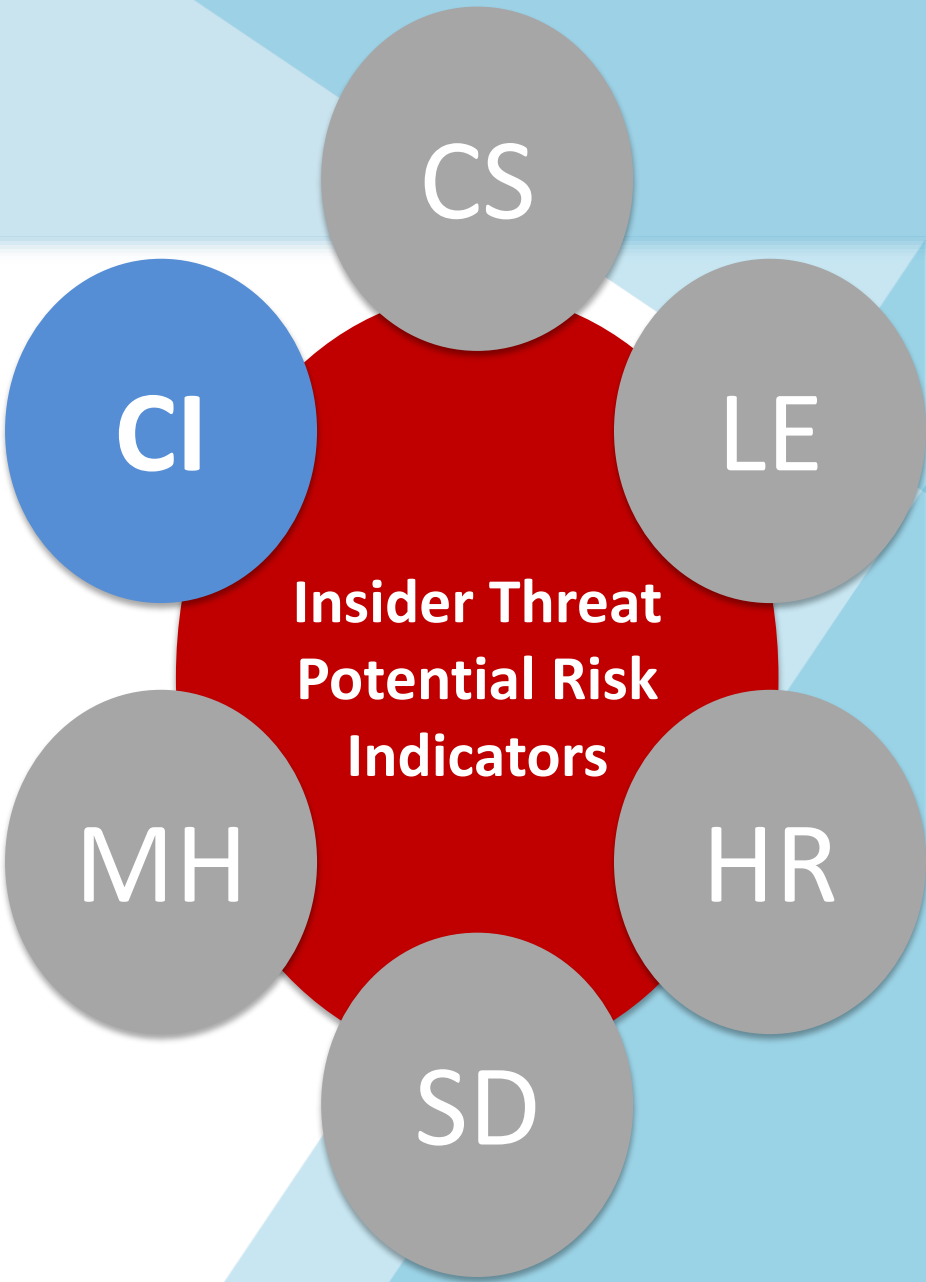
- **Insider Threat (NISPOM DoD 5220.22-M):** The likelihood, risk, or potential that an insider will use his or her authorized access, wittingly or unwittingly, to do harm to the national security of the United States. Insider threats may include harm to contractor or program information, to the extent that the information impacts the contractor or agency's obligations to protect classified national security information.

- **Counterintelligence Insider Threat (CI InT):** A person, known or suspected, who uses their authorized access to DoD facilities, personnel, systems, equipment, information, or infrastructure to damage and disrupt operations, compromise DoD information, or commit espionage on behalf of an FIE (Foreign Intelligence Entity).

- **The Insider Threat Program:** A multidisciplinary capability designed to detect, deter and mitigate risk from an insider threat.

The Divergence

- **CI: Strictly Foreign intelligence Nexus**
- **CI examples generally NOT Insider Threat:**
  - **Solicitation at a conference**
  - **Surveillance/ search seizures during foreign travel**
  - **Brute Force attack by APT1 against your network**
- **Insider Threat examples generally NOT CI:**
  - **Workplace Violence event**
  - **Unsafe practices due to drug/ alcohol abuse in work place**

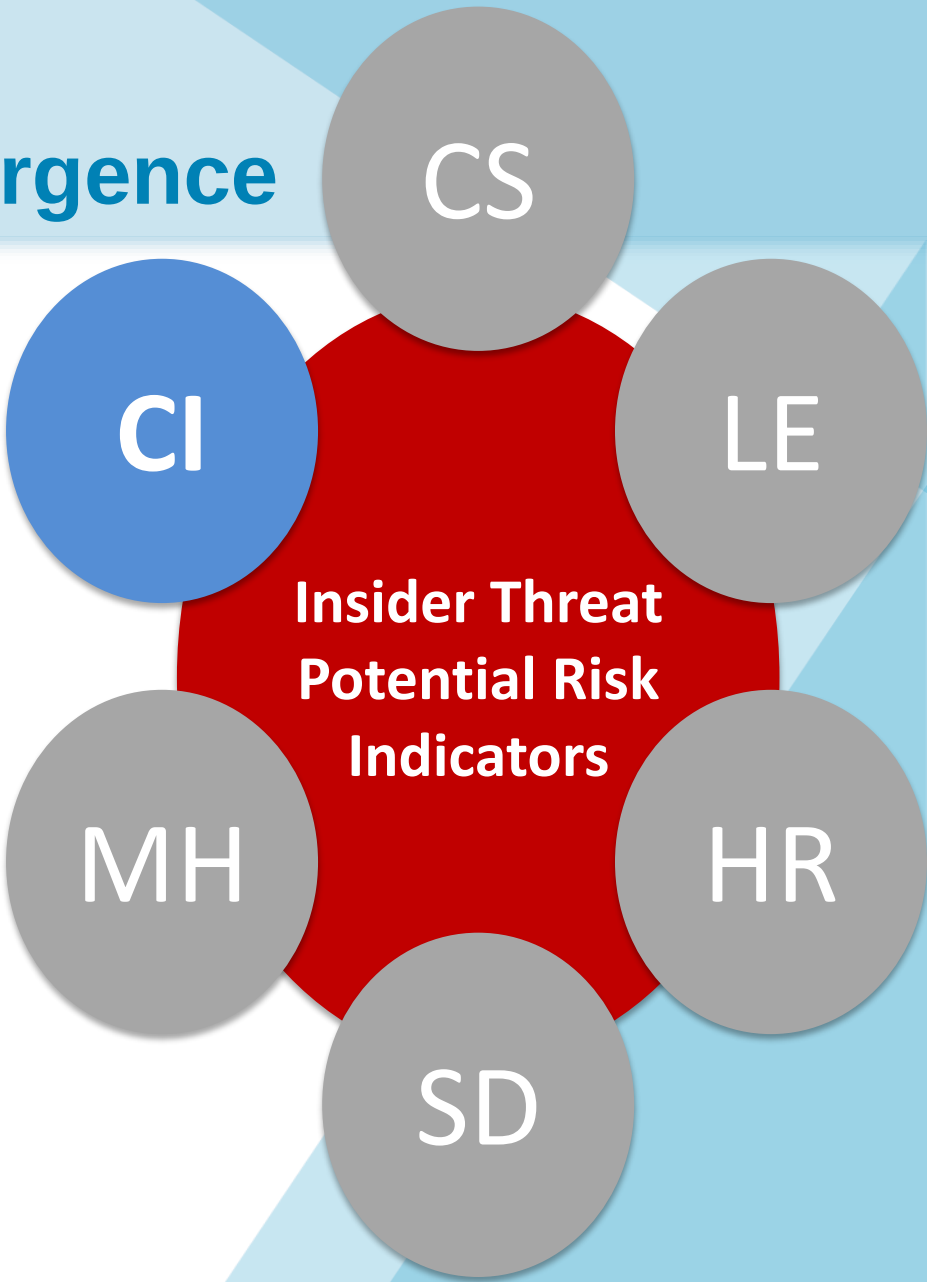


Legend

CI: Counterintelligence
CS: Cyber Security
LE: Law Enforcement
HR: Human Resources
SD: Security Department
MH: Medical/ Mental Health

The ~~Mergence?~~ Convergence

- **Supply chain, Foreign Intelligence Entities (FIE), insider enabled cyber, and poor security practices are areas of overlap**
- **Insider threat and CI convergence examples:**
  - **Employee clicking link to a malicious spear phishing email**
  - **Colluding with a competitor or foreign power**
  - **Surfing adult content on work computer**
  - **Knowingly or unknowingly purchasing sub-par or tampered with components**



Legend

CI: Counterintelligence
CS: Cyber Security
LE: Law Enforcement
HR: Human Resources
SD: Security Department
MH: Medical/ Mental Health

Defense!

Strategy	What can you do
Detect	- Enhance awareness of the unintentional insider threat - Improve usability of security tools - Report - Continuously re-evaluate your security procedures
Deter	- Training, Training, Training - Policies enforced
Deny	- Provide effective security practices (e.g. two factor authentication for access) - Maintain staff values and attitudes that align with organizational mission and ethics
Mitigate	- Insider Threat Programs can provide intervention for positive outcomes for individuals and organizations

Lightning Round! Question 1

Event	CI Only Concern	Insider threat, but not CI	Both!	Neither!
Someone clicks on a link or opens an attachment in a spear phishing email				

Lightning Round! Answer 1

Event	CI Only Concern	Insider threat, but not CI	Both!	Neither!
Someone clicks on a link or opens an attachment in a spear phishing email			X	

Lightning Round! Question 2

Event	CI Only Concern	Insider threat, but not CI	Both!	Neither!
You find a tuft of cat fur in some muffins you bought at the bake sale				

Lightning Round! Answer 2

Event	CI Only Concern	Insider threat, but not CI	Both!	Neither!
You find a tuft of cat fur in some muffins you bought at the bake sale				X

Lightning Round! Question 3

Event	CI Only Concern	Insider threat, but not CI	Both!	Neither!
State sponsored CNE actor launches SQL attack on server				

Lightning Round! Answer 3

Event	CI Only Concern	Insider threat, but not CI	Both!	Neither!
State sponsored CNE actor launches SQL attack on server	X			

Lightning Round! Question 4

Event	CI Only Concern	Insider threat, but not CI	Both!	Neither!
Disgruntled employee engages in work place violence				

Lightning Round! Answer 4

Event	CI Only Concern	Insider threat, but not CI	Both!	Neither!
Disgruntled employee engages in work place violence		X		

Lightning Round! Question 5

Event	CI Only Concern	Insider threat, but not CI	Both!	Neither!
Employee making suicidal gestures				

Lightning Round! Answer 5

Event	CI Only Concern	Insider threat, but not CI	Both!	Neither!
Employee making suicidal gestures		X		

Lightning Round! Question 6

Event	CI Only Concern	Insider threat, but not CI	Both!	Neither!
Reporting that you were surveilled at an overseas tradeshow				

Lightning Round! Answer 6

Event	CI Only Concern	Insider threat, but not CI	Both!	Neither!
Reporting that you were surveilled at an overseas tradeshow	X			

Lightning Round! Question 7

Event	CI Only Concern	Insider threat, but not CI	Both!	Neither!
Failing to report that you were surveilled and solicited at an overseas tradeshow				

Lightning Round! Answer 7

Event	CI Only Concern	Insider threat, but not CI	Both!	Neither!
Failing to report that you were surveilled and solicited at an overseas tradeshow			X	

Lightning Round! Question 8

Event	CI Only Concern	Insider threat, but not CI	Both!	Neither!
Selling your programming job to a foreign actor that you don't know is a spy				

Lightning Round! Answer 8

Event	CI Only Concern	Insider threat, but not CI	Both!	Neither!
Selling your programming job to a foreign actor that you don't know is a spy			X	

Lightning Round! Question 9

Event	CI Only Concern	Insider threat, but not CI	Both!	Neither!
Staying late at work and working weekends, unexplained affluence, high use of copy machine, several security infractions				

Lightning Round! Question 9

Event	CI Only Concern	Insider threat, but not CI	Both!	Neither!
Staying late at work and working weekends, unexplained affluence, high use of copy machine, several security infractions			X	

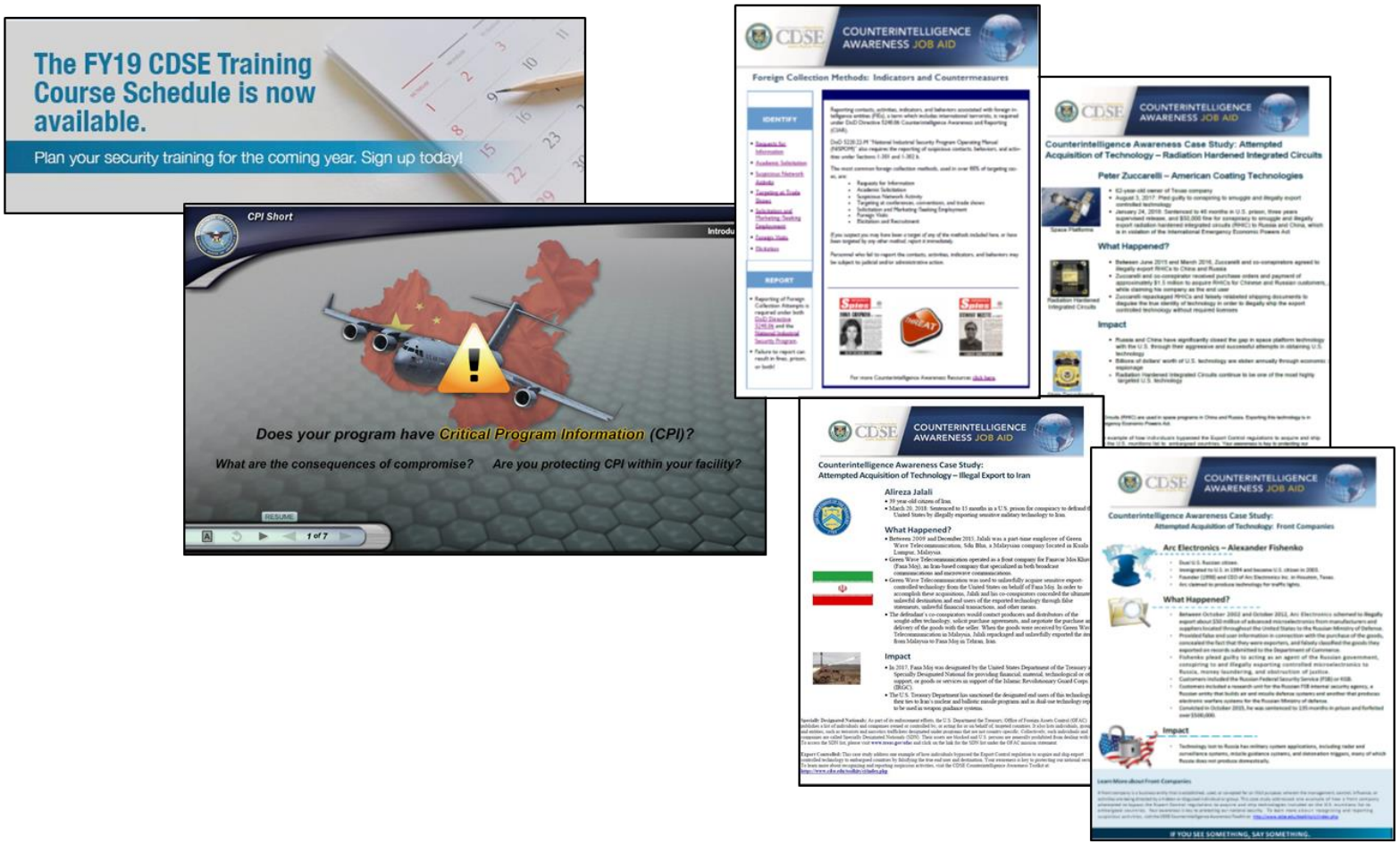
Lightning Round! Question 10

Event	CI Only Concern	Insider threat, but not CI	Both!	Neither!
Whistleblower using proper procedures				

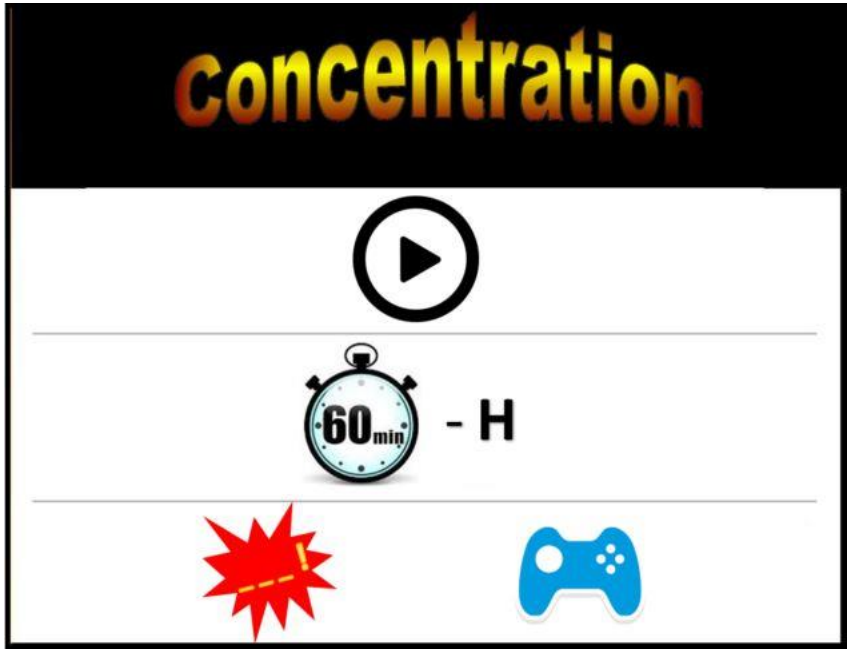
Lightning Round! Answer 10

Event	CI Only Concern	Insider threat, but not CI	Both!	Neither!
Whistleblower using proper procedures				X

CDSE CI Training and Job Aids



NEW VIGILANCE CAMPAIGN MATERIAL



VIEW MORE MATERIAL HERE:
https://www.cdse.edu/toolkits/insider/vigilance.html

CDSE WANTS TO HEAR FROM YOU!

CDSE Counterintelligence POC:

Ed Kobeski

410-689-7842

EMAIL: Edwin.f.Kobeski.civ@mail.mil