Center for Development of Security Excellence

CDSE

Learn. Perform. Protect.

Security Incidents Involving Special Circumstances

Information Security Webinar

CDSE

Danny Jennings

- **Physical & General Security Curriculum Manager responsible for:**
  - ✓ **Curriculum development**
  - ✓ **Course instruction**
  - ✓ **Curriculum review**
- **Retired military, over 20 years of experience in Law Enforcement and Security Operations**
- **Worked as DoD Contractor for Defense Threat Reduction Agency as onsite Program Manager for Access Control**
- **Served as Supervisor Physical Security Specialist with Pentagon Force Protection Agency**

DCO Meeting Room Navigation

CDSE

Notes box for audio information and other announcements

Use **Full Screen** (upper right corner) to maximize view of the presentation.

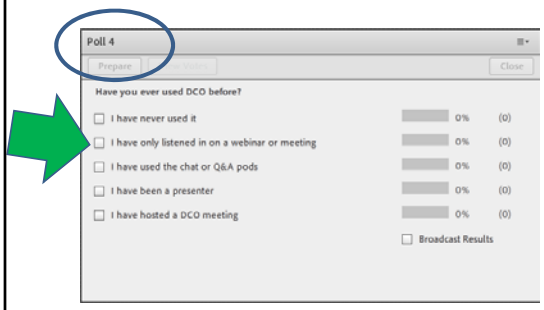
Click **Full Screen** again to switch back. You will need to be out of Full Screen view to respond to poll questions.

DCO Meeting Room Navigation

Q&A box for entering questions/feedback

File share box to download material for today's presentation

Example of a Poll Question



Webinar Objectives

By the end of this webinar, you should be able to:

- **Understand the importance of promptly reporting security incidents**
- **Identify the steps in the process**
- **Define Special Circumstances**
- **Identify the policies pertaining to special circumstances and or categories**

Poll Question 1

Why is it important to report?

It is DoD Policy that anyone who becomes aware of the loss or potential compromise of classified information shall immediately report it to the head of his or her local activity and to the Activity Security Manager.

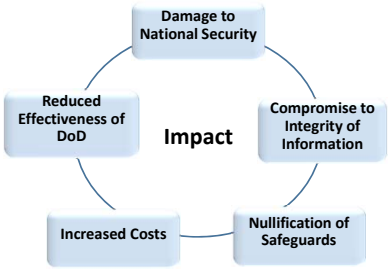
Why is it important to report?

Bradley Edward Manning

- Arrested May 2010
- Suspected of passing classified material to the website WikiLeaks.
- Charged with 22 offenses
- Largest set of restricted documents ever leaked to the public.
- Could face 136 years in prison.

What was the Impact?

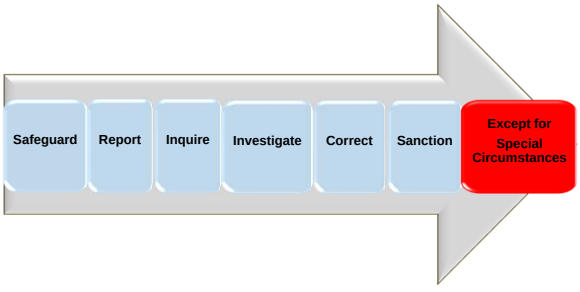
Why is it important to report?



Poll Question 2

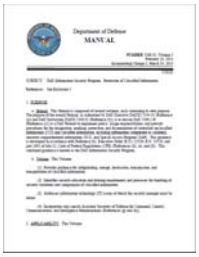
Security Incidents Involving Classified Information

Follow this process with each security incident.



Special Circumstances

Certain types of classified information or specific circumstances require unique handling or consideration of additional reporting requirements as specified in DoD Manual 5200.01-V3 Enclosure 6 paragraphs 5.a through 5.o.



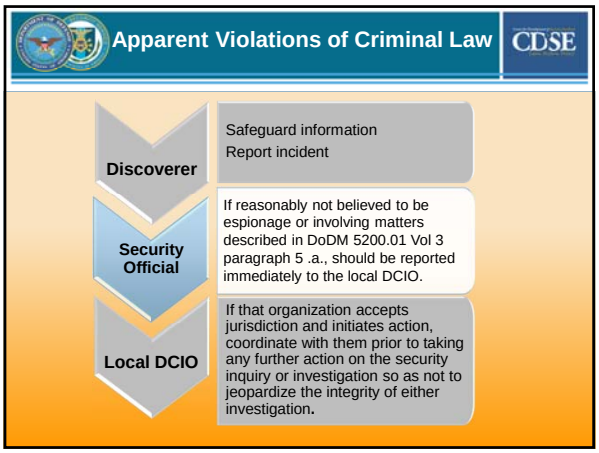
Special Circumstances Examples

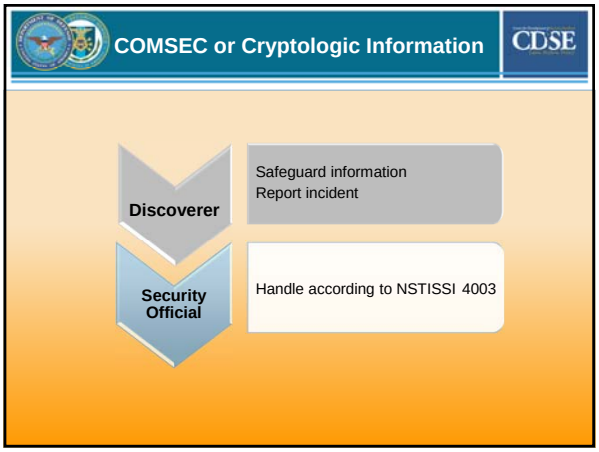
Notify required officials based on information type.

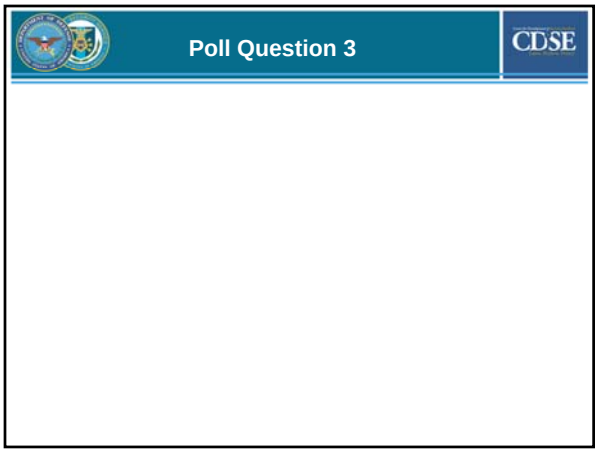
- Foreign Intelligence Service
- Violation of Criminal Law
- COMSEC
- SCI
- RD/FRD
- IT
- FGI and NATO
- Classified Info to Foreign Govs.
- SAP
- Improper Transfer
- CPI
- On-Site Contractors

Incidents involving Deliberate Compromise, a Foreign Intel Service, or a Terrorist Org.

Discoverer	Safeguard information Report incident
Security Official	Must report immediately to the cognizant Defense CI component, in accordance with DoDD 5240.06
Cognizant Defense CI Component	Security officials shall **not** initiate or continue an inquiry or investigation of the incident unless it is fully coordinated with the cognizant Defense CI component.


Apparent Violations of Criminal Law
CDSE
Discoverer
Safeguard information
Report incident
Security Official
If reasonably not believed to be espionage or involving matters described in DoDM 5200.01 Vol 3 paragraph 5 .a., should be reported immediately to the local DCIO.
Local DCIO
If that organization accepts jurisdiction and initiates action, coordinate with them prior to taking any further action on the security inquiry or investigation so as not to jeopardize the integrity of either investigation.


COMSEC or Cryptologic Information
CDSE
Discoverer
Safeguard information
Report incident
Security Official
Handle according to NSTISSI 4003


Poll Question 3
CDSE

Special Circumstances Examples

Notify required officials based on information type.

- Foreign Intelligence Service
- Violation of Criminal Law
- COMSEC
- SCI
- RD/FRD
- IT
- FGI and NATO
- Classified Info to Foreign Govs.
- SAP
- Improper Transfer
- CPI
- On-Site Contractors

Sensitive Compartmented Information

Discoverer	Safeguard information Report incident
Security Official	Actual or potential compromises involving SCI shall be reported to the activity SSO and handled in accordance with DoD5105.21-M-1 and ICD 701.
SSO	Incidents involving SCI that may become public shall also be reported to the Director of Security, OUSD(I).
Director of Security, OUSD(I)	If a DoD Component believes a disclosure may contain classified SCI information under the control of an(other) Intelligence Community agency, the DoD Component shall notify NCIX. NCIX shall coordinate notification to the affected agency.

Restricted Data (RD) and/or Formerly Restricted Data (FRD)

Discoverer	Safeguard information Report incident
Component	Components shall notify the Department of Energy as necessary and provide a copy of the notification to the Deputy Assistant Secretary of Defense for Nuclear Matters and the Director of Security, OUSD(I).
Department of Energy	
Congress	In accordance with the provisions of section 3161 of Public Law 105-261 and its implementing plan, the Secretary of Energy must report to Congress inadvertent disclosure of RD or FRD occurring pursuant to automatic declassification processes.

Information Technology (IT)

Discoverer	Safeguard information Report incident
Security Official	Information Assurance (IA) Manager reports to the activity security manager.
Local IA Officials	Inquiries and resolutions involving compromise of classified information on IT systems require coordination and assistance from local IA officials.

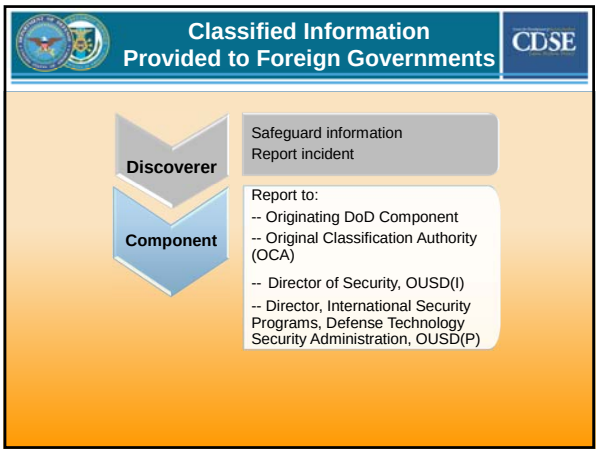
Special Circumstances Examples

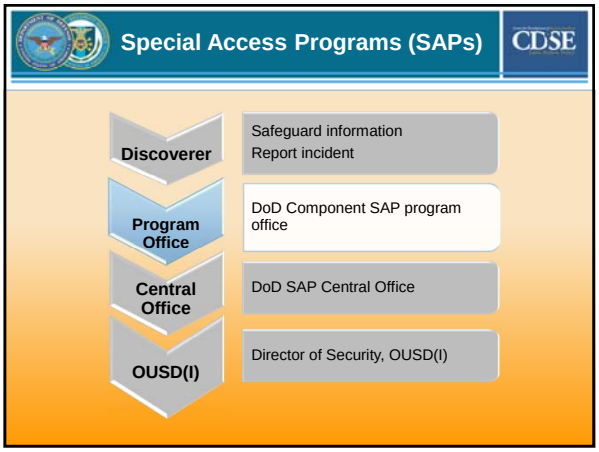
Notify required officials based on information type.

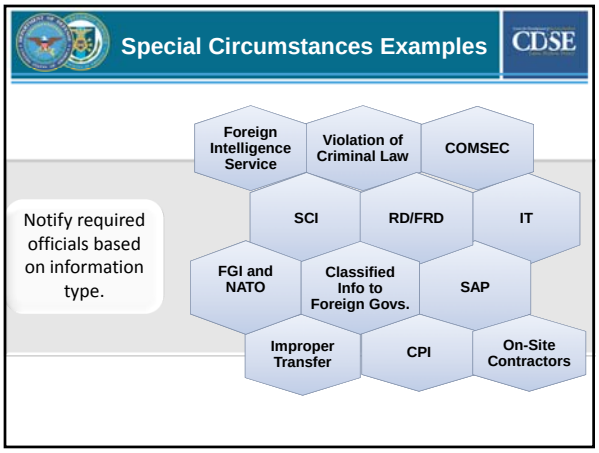
- Foreign Intelligence Service
- Violation of Criminal Law
- COMSEC
- SCI
- RD/FRD
- IT
- FGI and NATO
- Classified Info to Foreign Govs.
- SAP
- Improper Transfer
- CPI
- On-Site Contractors

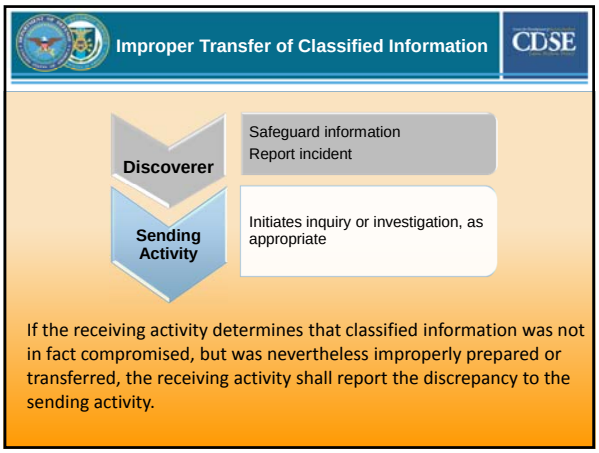
Foreign Government Information (FGI) or North Atlantic Treaty Organization (NATO) Information

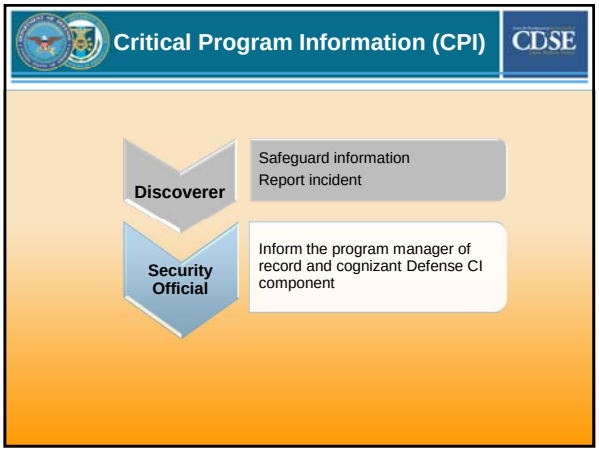
Discoverer	Safeguard information Report incident
Designated Security Authority	DoD Component senior agency official reports promptly to the USD(P), who serves as the designated security authority (DSA).
Local IA Officials	Director, International Security Programs, Defense Technology Security Administration, OUSD(P) shall notify NATO or foreign government as appropriate.

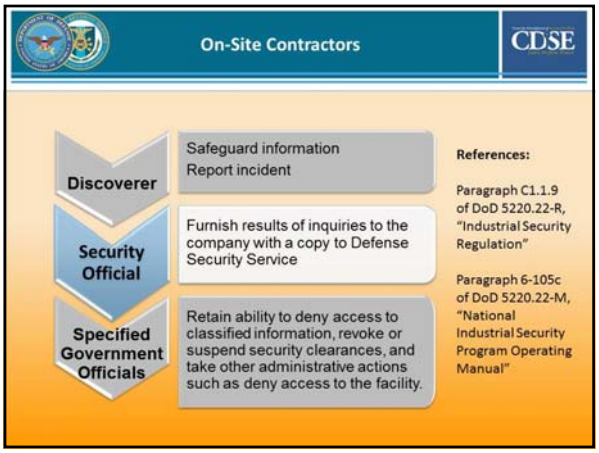

Classified Information Provided to Foreign Governments
CDSE
Discoverer
Safeguard information
Report incident
Component
Report to:
-- Originating DoD Component
-- Original Classification Authority (OCA)
-- Director of Security, OUSD(I)
-- Director, International Security Programs, Defense Technology Security Administration, OUSD(P)


Special Access Programs (SAPs)
CDSE
Discoverer
Safeguard information
Report incident
Program Office
DoD Component SAP program office
Central Office
DoD SAP Central Office
OUSD(I)
Director of Security, OUSD(I)


Special Circumstances Examples
CDSE
Notify required officials based on information type.
Foreign Intelligence Service
Violation of Criminal Law
COMSEC
SCI
RD/FRD
IT
FGI and NATO
Classified Info to Foreign Govs.
SAP
Improper Transfer
CPI
On-Site Contractors


Improper Transfer of Classified Information
CDSE
Discoverer
Safeguard information
Report incident
Sending Activity
Initiates inquiry or investigation, as appropriate
If the receiving activity determines that classified information was not in fact compromised, but was nevertheless improperly prepared or transferred, the receiving activity shall report the discrepancy to the sending activity.


Critical Program Information (CPI)
CDSE
Discoverer
Safeguard information
Report incident
Security Official
Inform the program manager of record and cognizant Defense CI component


On-Site Contractors
CDSE
Discoverer
Safeguard information
Report incident
Security Official
Furnish results of inquiries to the company with a copy to Defense Security Service
Specified Government Officials
Retain ability to deny access to classified information, revoke or suspend security clearances, and take other administrative actions such as deny access to the facility.
References:
Paragraph C1.1.9 of DoD 5220.22-R, "Industrial Security Regulation"
Paragraph 6-105c of DoD 5220.22-M, "National Industrial Security Program Operating Manual"

Poll Question 4

Poll Question 5

Questions

- Please discuss natural disaster and other emergency response situations.

Questions

- Please provide location where we can find guidance regarding when incidents will be updated in JPAS.

Summary

You should now be able to:

- Understand the importance of promptly reporting security incidents
- Identify the steps in the process
- Define Special Circumstances
- Identify the policies pertaining to special circumstances and or categories

Survey

Contacts and Resources

- Handouts and frequently asked questions from this webinar will be posted at http://www.cdse.edu/catalog/webinars/information-security/security-incidents-involving-special-circumstances.html
- Email information security training-related questions to DSS at InformationSecurity.Training@dss.mil