

Emergency Planning




Emergency Planning Webinar



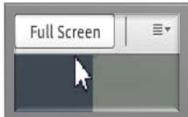
Roy Ringrose

- Information Systems Security Analyst
- 40 years of Law Enforcement and Security Program Management at the Local and Federal Levels
- CDSE Information Security Management instructor and Course Manager


2



Webinar Room Navigation



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.

3



 **Emergency Planning** 



 **Objectives** 


- Understand DoD policies and how they relate to safeguarding classified information
- Recognize how military operations affect provisions of DoD Manual 5200.01, Vol. 1, Enclosure 3
- Identify types of threats and their impact on information security
- List factors to be considered when planning for emergency handling of classified information
- Apply the planning process in the development of emergency plans

68

 **Background Information** 

Background Information



**DoD Information Security Program Manual
DoDM 5200.01 Volumes 1 and 3**



Provisions pertaining to accountability, dissemination, transmission, and storage may be modified by military commanders.

Military operations include:

- Combat
- Peacekeeping Operations
- NOT routine military deployments or exercises

 **4 Step Planning Process** 

There are four steps to developing an information security emergency plan.

- ✓ **Step 1** is to identify threats.
- ✓ **Step 2** is to assess risks.
- ✓ **Step 3** is to determine protection strategies.
- ✓ **Step 4** is to develop the plan.



0-10

 **Identify the Threats** 


Step 1: Identify Threats

				
Fire	Natural Disaster	Civil Disobedience	Terrorist Attacks	Enemy Action



0-11

 **Threats/Fire** 


- Should Continental United States (CONUS) plans differ from Outside the Continental United States (OCONUS)?
- Are there procedures in place for emergency entrance into the spaces that store classified material?
- Are there procedures in place for after the emergency?



0-12

 **Threats/Fire (cont.)** 

- Should you take time to secure classified information before evacuating?
- What should you do about emergency response personnel who may have come into contact with classified information?
- Do you require emergency response personnel to complete a non-disclosure agreement?



13

 **Threats/Natural Disasters** 



14

 **Threats/Civil Disobedience** 



15

 **Threats/Terrorist Attacks** 





13

 **Threats/Enemy Action** 



14

 **Chat Question 1** 

What type of threat is indicated in this photo?





Photo: Rex Features

Enter your response in the chat box 

15

 **Chat Question 2** 

What type of threat is indicated in this photo?



Enter your response in the chat box 

0:18



 **Chat Question 3** 



What type of threat is indicated in this photo?



Enter your response in the chat box 


0:21

 **Assess Risk** 



- ✓ Emergency Plan Contents
 - Level of Detail
 - Amount of Testing/Rehearsal
- ✓ Depth of Plan
 - Coverage based on assessment of risk factors

3:1

 **Assess Risk** CDSE

Military Operations
"Classified Information should only be introduced into combat areas, zones, or areas of potential hostile activity, when necessary to accomplish the military's mission."


CONFIDENTIAL

SECRET

TOP SECRET

"Have you completed the risk evaluation?"

0-22

 **Assess Risk** CDSE


COMSEC Material

"Destruction and Emergency Protection Procedures for COMSEC and Classified Material w/amended ANNEX B dated 9 JAN 08", August 2006.


- Committee on National Security Systems /NSA Instruction 4004.1

- No-notice emergency destruction
- Plan for emergency protection
- Hold minimum amount of COMSEC material
- Conduct routine destruction
- Dispose of excess COMSEC according to regulations


0-23

 **Poll #1** CDSE

0-24

 **Poll #2** CDSE

0-25

 **Protection Strategies** CDSE

Step 3: Determine Protection Strategies

Emergency Plan actions include:

- ✓ Protection in place
- ✓ Removal
- ✓ Destruction

 **Protection Strategies** CDSE

Protection Considerations

	Capability to secure in place <ul style="list-style-type: none">• Fire and water protection
	Transportation requirements for removal/evacuation <ul style="list-style-type: none">• Alternate safeguarding site
	Adequate high-speed destruction equipment

 **What's the Best** 



So what's the best protection against the threat of...

Natural Disaster
Terrorist Attack
Civil Disobedience
Fire
Enemy Action



"Running shoes!"

0-28

 **Develop the Plan** 

Step 4: Develop the Plan

Reduce



- Permanent transfer
- Archive
- Destruction

Store

- Off-site storage facility

Transfer


- High-density formats
- Microforms
- Removable AIS media

 **Develop the Plan** 

Emergency Planning Considerations


Have a detailed plan if...

- You possess extremely sensitive classified materials
- You are located close to hostile or potentially hostile countries
- You have limited ability to defend
- You conduct sensitive operations
- Potential for hostile action is great

 **Develop the Plan** CDSE

Emergency Planning Considerations Cont.

- Minimize risk of injury or loss of life to personnel
- Must prevent unauthorized disclosure

 **Recommendations** CDSE

Recommendations

- Make the plan as simple as possible
- Develop a checklist
- Do not list priorities on the containers – detail in plan
- Schedule periodic drills
- Practice the plan – up to a point!

 **What Next** CDSE

What is your next step?

- ✓ Develop/review your emergency plan
 - Level of detail determined by the threat and level of risk



- ✓ Keep it simple and well coordinated

DILBERT
By Scott Adams

 So 





0-31


 Summary 



Objectives Summary


- Demonstrate an understanding of DoD policies and how they relate to safeguarding classified information
- Recognize how military operations affect provisions of DoD manual 5200.01 Vol. 1, Enclosure 3
- Identify types of threats and their impact on information security
- List factors to be considered when planning for emergency handling of classified information
- Apply the planning process in the development of emergency plans

 Questions 

Why have an emergency plan?



	Questions	CDSE
What is the overall objective of the plan?		
		

	Contacts and Resources	CDSE
Handouts and frequently asked questions from this webinar will be posted at		
http://www.cdse.edu/catalog/webinars/information-security/information-security-emergency-planning.html		
You may also email Information Security training related questions to DSS at		
InformationSecurity.Training@dss.mil		
