Engagement and Transport Assessment Collaboration

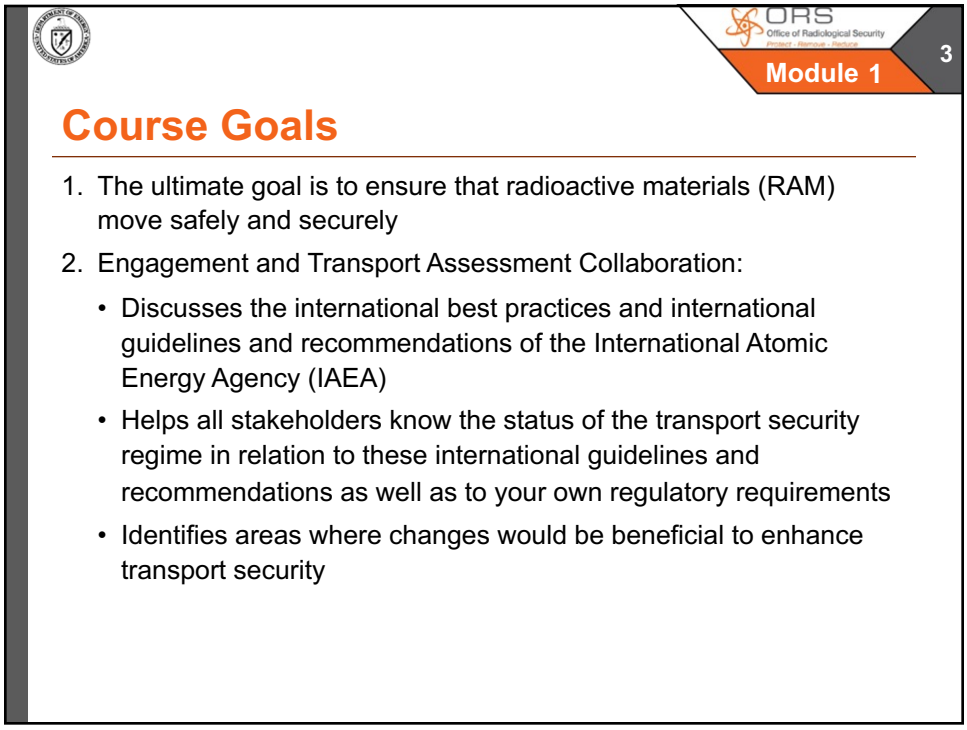
NP-FY19-50

1

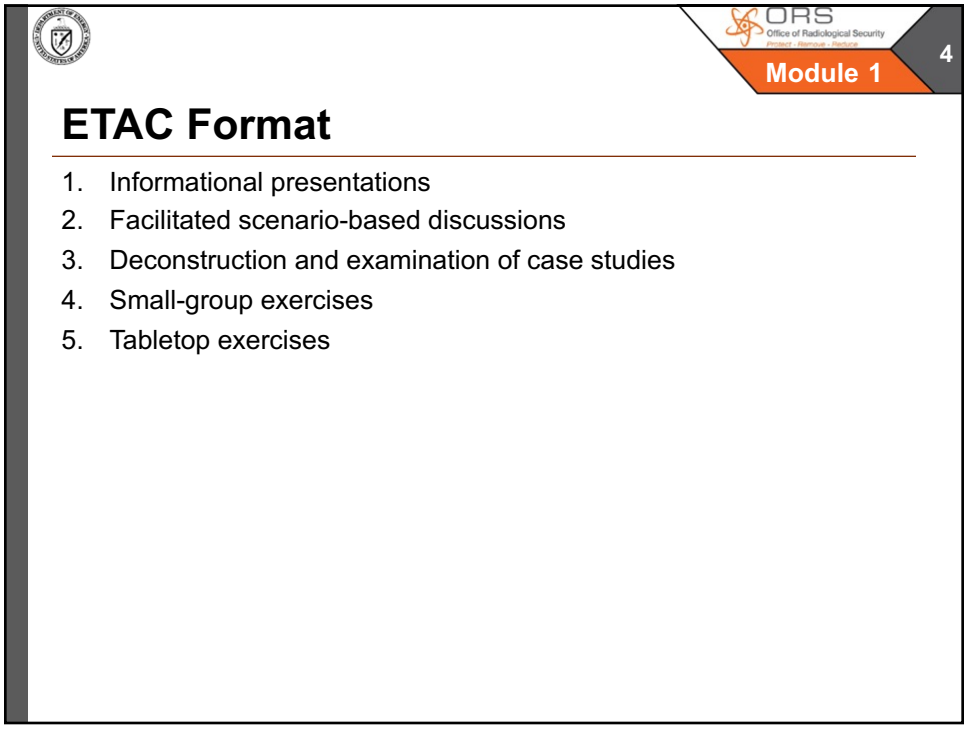
Module 1

Introduction

2


ORS
Office of Radiological Security
Module 1
3
Course Goals
1. The ultimate goal is to ensure that radioactive materials (RAM) move safely and securely
2. Engagement and Transport Assessment Collaboration:
• Discusses the international best practices and international guidelines and recommendations of the International Atomic Energy Agency (IAEA)
• Helps all stakeholders know the status of the transport security regime in relation to these international guidelines and recommendations as well as to your own regulatory requirements
• Identifies areas where changes would be beneficial to enhance transport security

3


ORS
Office of Radiological Security
Module 1
4
ETAC Format
1. Informational presentations
2. Facilitated scenario-based discussions
3. Deconstruction and examination of case studies
4. Small-group exercises
5. Tabletop exercises

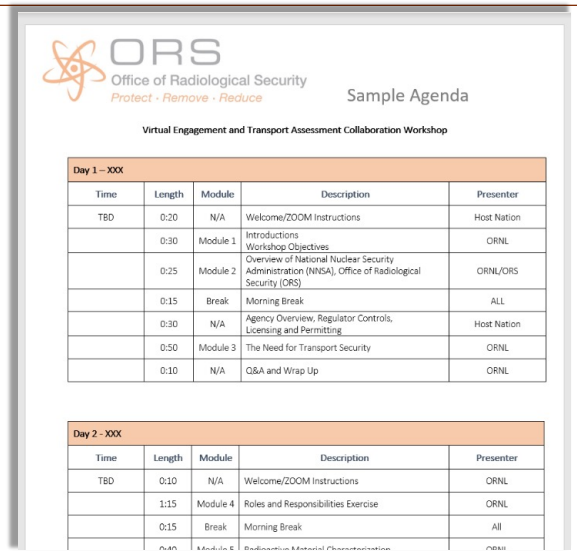
4

Suggestions for Engagement

- Interactive discussions, collaborations, and questions
- Candid and open conversations
- Communicate your organization's roles and responsibilities related to transport security

5

Review Agenda



ORS Office of Radiological Security
Protect · Remove · Reduce

Sample Agenda

Virtual Engagement and Transport Assessment Collaboration Workshop

Day 1 – XXX				
Time	Length	Module	Description	Presenter
TBD	0:20	N/A	Welcome/ZOOM Instructions	Host Nation
	0:30	Module 1	Introductions Workshop Objectives	ORNL
	0:25	Module 2	Overview of National Nuclear Security Administration (NNSA), Office of Radiological Security (ORS)	ORNL/ORS
	0:15	Break	Morning Break	ALL
	0:30	N/A	Agency Overview, Regulator Controls, Licensing and Permitting	Host Nation
	0:50	Module 3	The Need for Transport Security	ORNL
	0:10	N/A	Q&A and Wrap Up	ORNL

Day 2 - XXX				
Time	Length	Module	Description	Presenter
TBD	0:10	N/A	Welcome/ZOOM Instructions	ORNL
	1:15	Module 4	Roles and Responsibilities Exercise	ORNL
	0:15	Break	Morning Break	All

6

ORS
Office of Radiological Security
Protect · Remove · Reduce

Module 2

Office of Radiological Security

7

ORS
Office of Radiological Security
Protect · Remove · Reduce

Module 2

Learning Objectives

1. Provide an overview of the Office of Radiological Security (ORS)

2. Introduce ORS's work with partners to enhance global security by preventing high-activity radioactive materials from being used in acts of terrorism

8

ORS Office of Radiological Security
Protect · Remove · Reduce

Module 2

9

The Risk of Malicious Use of Radiological Material Requires Action

ORS works with partners to enhance global security by preventing high-activity radioactive materials from being used in acts of terrorism.

9

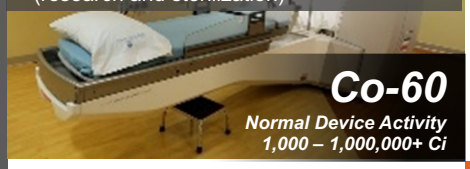
ORS Office of Radiological Security
Protect · Remove · Reduce

Module 2

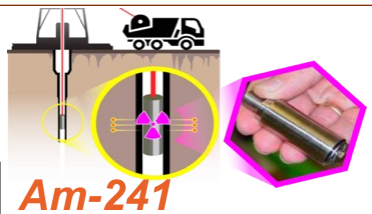
10

The "Most Attractive" Sources Come from Industry and Medicine

- Tele-therapy and Gamma Knife Units (cancer treatment)
- Self-shielded and Panoramic Irradiators (research and sterilization)



Co-60
Normal Device Activity
1,000 – 1,000,000+ Ci



Am-241
Normal Device Activity
8-20 Ci

- Oil well logging (industrial imaging)

- Radiography (industrial imaging)

Ir-192
Normal Device Activity
10-100 Ci

Cs-137
Normal Device Activity
1,000 – 50,000 Ci

- Self-shielded irradiators (i.e. blood irradiators)
- Calibrators (dosimeter and detector calibration)

10


ORS
Office of Radiological Security
Module 2
11
Threat Types and Motivations
Homegrown Violent Extremists (HVEs)
Seven Sentenced in UK Terror Plot
Non-State Actors
Insider Threats
Ex-Duke security expert charged in medical office break-ins
Lone-Wolves
Report: 'Dirty Bomb' parts found in slain man's home

11


ORS
Office of Radiological Security
Module 2
12
RDD Materials Found at Softer Targets
Hospitals
HOSPITAL
Commercial Irradiation Facilities
Universities
Materials in Transit

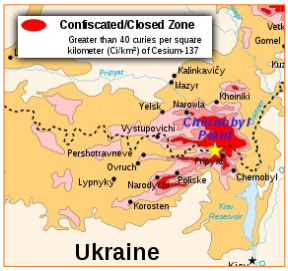
12

ORS Office of Radiological Security
Protect · Remove · Reduce

Module 2

13

Dispersed Cs-137 and Large-Scale Impacts



Chernobyl Exclusion Zone (area near plant)

Goiania Cleanup Activities

NYC Dispersion Analysis

Chernobyl: *Uninhabited area - 30 km² (approximately half the area of Manhattan)*

Goiania: *40 tons of rad-waste from a 3.3 oz. source*

NYC RDD Analysis: *Relocation area a significant portion of the island*

13

ORS Office of Radiological Security
Protect · Remove · Reduce

Module 2

14

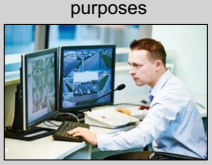
Office of Radiological Security

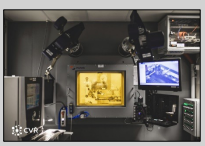
Mission: ORS enhances global security by preventing high-activity radioactive materials from use in acts of terrorism.

ORS is a First Line of Defense program to keep radioactive material safe and secure, thus an adequate response is key to security

- Terrorist organizations want radioactive materials
- An RDD could cause severe economic impacts
- Not all radioactive materials at any level of activity pose a concern

PROTECT	REMOVE	REDUCE
PROTECT radioactive sources used for vital medical, research, and commercial purposes	REMOVE and dispose of disused radioactive sources	REDUCE the global reliance on radioactive sources through replacement with viable non-isotopic alternative technologies



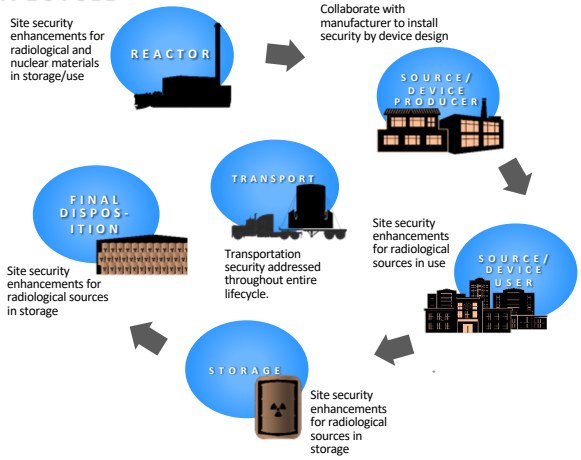


14

ORS Office of Radiological Security
Protect · Remove · Reduce

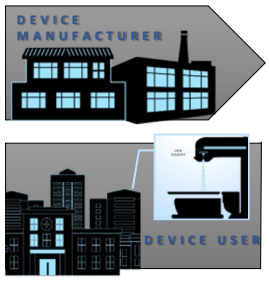
Holistic Approach to Source Security

SECURITY THROUGHOUT RADIOLOGICAL SOURCE LIFECYCLE



ALTERNATIVE NON-RADIOISOTOPIC TECHNOLOGIES

The use of non-isotopic technologies negates the need for security and disposal requirements and eliminates the risk that radioactive sources will become orphaned



NNSA National Nuclear Security Administration
Global Material Security

15

15

ORS Office of Radiological Security
Protect · Remove · Reduce
Module 2
16

International Transportation Security

- The international community recognizes that transport of radioactive sources is especially vulnerable
- A core component of the ORS mission and protection strategy involves the protection of sources in use as well as during transport
- ORS is committed to be a partner in transport security
  - ORS works with international partners and the IAEA to deter and prevent theft, sabotage, and malicious acts during transport
  - ORS strives to enhance protection through:
    - The establishment or enhancement of legislative and regulatory infrastructure
    - Creation of training capabilities and curriculum to achieve a knowledgeable and skilled workforce
    - Effective design and implementation of physical security features and security technologies to aid in protection and response to events

16

Transport Security Summary

1. Our goal is to work together to increase the security of high-priority radiological materials
2. Recognizing the need for transport security is an important first step
3. A good security culture is essential.
4. Essential elements of an effective Transportation Security Program include:
   - Laws and regulations
   - National oversight and inspections
   - Physical protection
   - Training
   - Response
   - Reliable and skilled workforce

17

ORS Office of Radiological Security
Protect · Remove · Reduce

Module 3

The Need for Transport Security

18

Learning Objectives

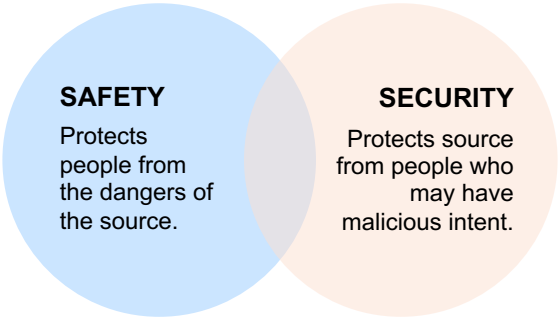
1. Discuss the risks involved in the transport of radioactive material and the critical need for transport security
2. Identify the elements of radiological threat and give examples of potential threats to these materials during transport
3. Describe how these materials can be used in malicious acts, the typical mechanisms used for those acts, and the consequences resulting from those acts

19

The Need (1 of 2)

While in the past, safety has been the central concern for transporting RAM, the need for security has now become a major focus.

Safety and Security measures differ but sometimes overlap, so they must be compatible*:*



20

The Need (2 of 2)

What adversaries know:

- RAM is most vulnerable during transport because it is in the public domain, on a conveyance, and packaged for movement
- Shipments provide an opportunity to access the material outside a secure, fixed site
- If the conveyance is seized, the material can be quickly moved to high consequence locations for dispersal or coercion

21

Adversary Intent

The Nuclear Option Holds No Fear for ISIS, August 5, 2015 (Syria)

"…The question being posed by western intelligence services is: what will ISIS do next ? It may be partly answered by an article on dirty bombs in a recent issue of the group's glossy magazine Dabiq. Such a bomb isn't particularly ingenious, it's not even a nuclear device – it packs high explosive together with radioactive material. Flown in a light plane and crashed into a western transport hub, it would be unlikely to cause mass casualties, but it would paralyze cities, spread fear and distract from actions planned elsewhere…"

http://www.thetimes.co.uk/tto/opinion/columnists/article4517360.ece (Times Online – United Kingdom)

22

Complexity of Transport Operations

Transport security is complex and frequently involves multiple:

- State and international agencies
- Customs and border control
- Licensing and authorization agencies
- Shipment control requirements
- Multiple law enforcement and emergency response forces for international operations

23

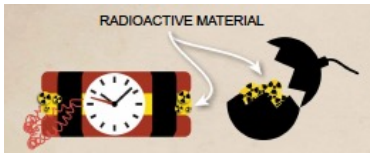
Potential Malicious Acts

Radiation exposure device (RED)

- Public economic and social impact

Radiological dispersal device (RDD)

- Coupled with explosive to cause dispersal of radioactivity ("dirty bomb")
- Non-explosive dispersion
- Potentially significant economic and social impact



24

Risk Defined

"Risk is the probability (likelihood) that an undesirable event will occur, multiplied by its consequence."

- Risks to human life
- Risks to reputation
- Risks to health and safety
- Risks to economics and financing
- Risks to the environment

25

Potential Events Related to Vehicle Transport

- Vehicle breakdown, accident
- Equipment or property damage
- Shipment or equipment sabotage
- RM cargo theft or attack
- Violence against driver or crew
- Kidnapping

26

Potential Consequences of Transport Event

- Environmental contamination (denial of use)
- Economic impacts (cleanup costs, disruption of commerce, property damage)
- Health impacts
- Psychological effects and social disruption
- Waste remediation
- Fatalities

27

The Security System Goal

The GOAL of a transport security system:

- Protect the materials from unauthorized removal and sabotage!

Accomplish this using security measures to:

- Deter the adversary
- Detect and assess access attempts
- Delay the adversary to enable apprehension
- Respond in a timely manner to interrupt the malicious acts and protect the materials

28

Summary

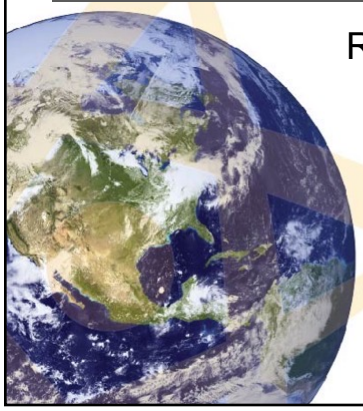
1. Discussed the risks involved in the transport of radioactive material and the critical need for transport security.
2. Identified the elements of radiological threat and provided examples of potential threats to these materials during transport.
3. Described how these materials could be used in malicious acts, the typical mechanisms used for those acts, and the consequences resulting from those acts.

29

ORS Office of Radiological Security
Protect · Remove · Reduce

Module 4

Roles and Responsibility Exercise



30

Learning Objective

1. Using a facilitated exercise, be able to explain the basic plan of ensuring security for a radioactive material transport
2. Better understand the roles and responsibilities of those involved with securing a transport shipment

31

Roles and Responsibilities Exercise

- This exercise places you in your role as a member of your organization or agency to conduct the planning and implementation of a shipment of radiological material
- Your role is based entirely on what your organization's responsibility is in the shipment process
- For the purpose of this exercise, we have structured the organizations into five (5) roles:
  - Consignor - Get the packages to the destination with minimal cost
  - Carrier - Perform the transport
  - Consignee - Take delivery of the package with radioactive material
  - Response Force - Protect the shipment
  - Regulator - Give permission to the operator or carrier to start planning

32

Scenario Information

Organize the transport of one (1) package Cobalt-60 Tele-therapy Unit
- **Category 1 RAM**
- Enhanced Security Level
- Weight: 1,100kg per package
- One package on truck

- The threat level is stated as normal. However, there is some indication of criminal activity in Province A but not sufficient to raise the threat level
- The transport will take 12 hours and will need to stop every 5-6 hours for fuel and subsistence breaks
- The escorts (if any) have limited firearms (i.e., handguns)
- The initial response force is 12-15 minutes away from the convoy at any time

33

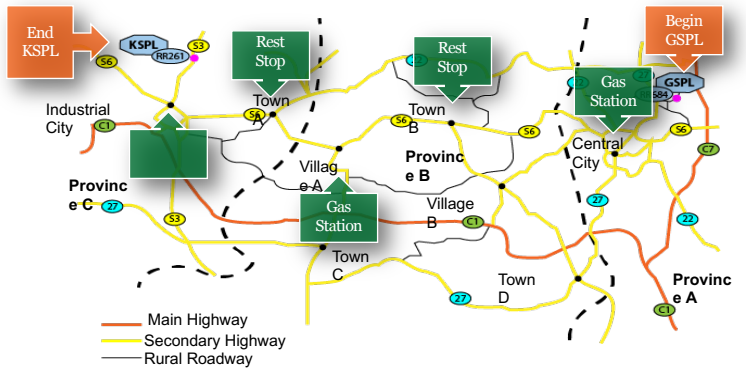
Exercise Guidelines

- You will be divided into virtual breakout rooms by your role: consignor, carrier, consignee, response force, and regulator
- Using the information provided below, your group will have 30 - 40 minutes to discuss and plan the transportation of radioactive material from the perspective of your assigned role
- Then your group will discuss the possible outcomes and actions that might occur using your transportation plan
- You should strive to answer and address the questions found in your handout, “Points to Consider”

34

Exercise Map

Assumed Geography for Shipment



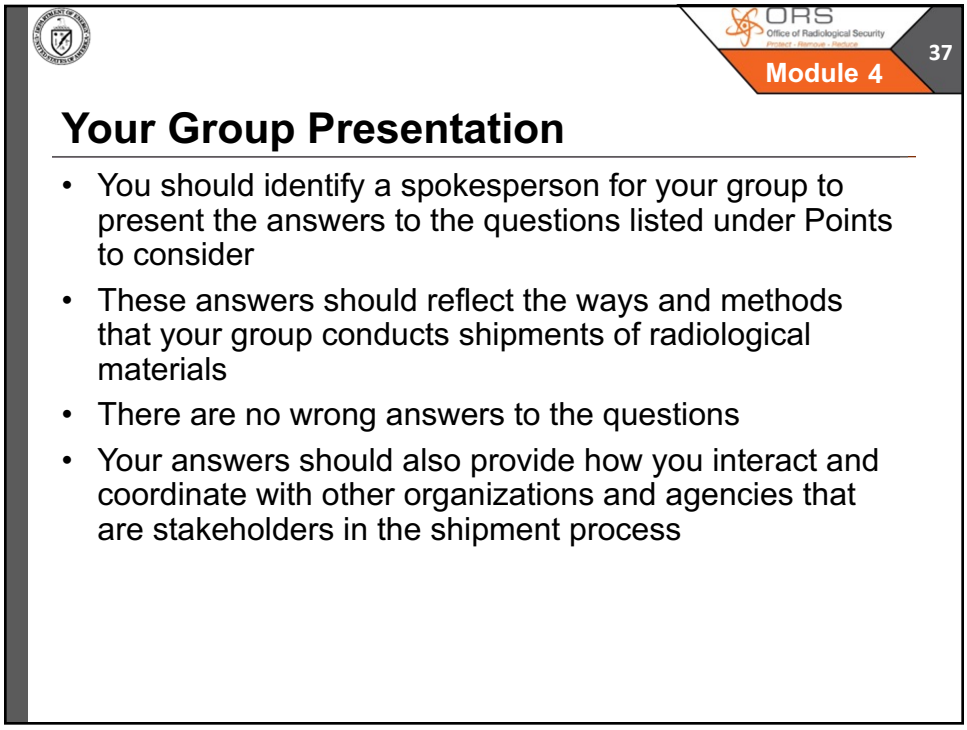
35

Assumptions for Choosing Route

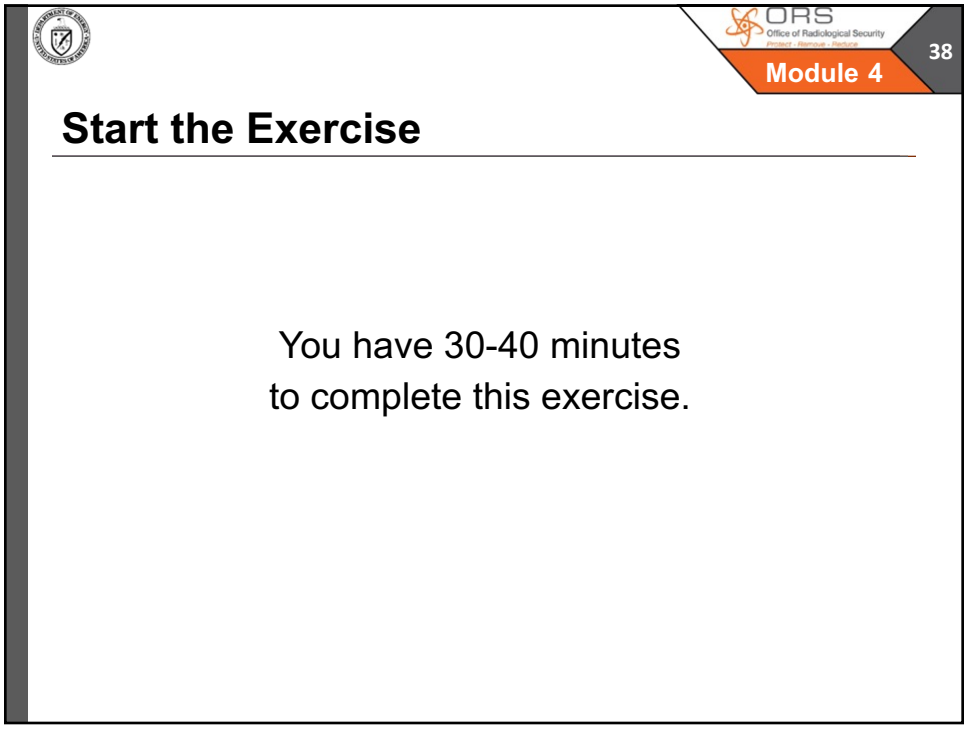
Transport from GSPL to KSPL

- Journey time: 12 hours with a two-hour stopover
- There are no resting places on C7
- There is one resting area two hours from GSPL at C1/27 intersection
- There are resting places/gas stations on S6 at
  - Central City/gas station
  - Town A
  - Village A/gas station
  - Town B
  - Industrial City/gas station

36


ORS
Office of Radiological Security
Module 4
37
Your Group Presentation
• You should identify a spokesperson for your group to present the answers to the questions listed under Points to consider
• These answers should reflect the ways and methods that your group conducts shipments of radiological materials
• There are no wrong answers to the questions
• Your answers should also provide how you interact and coordinate with other organizations and agencies that are stakeholders in the shipment process

37


ORS
Office of Radiological Security
Module 4
38
Start the Exercise
You have 30-40 minutes
to complete this exercise.

38

Presentation – Regulator

Points to consider:

For what are you responsible?

How does your organization license a shipment? Shipper? Carrier?

What might be some information that you would need?

When do you get involved in this shipment, if ever?

Who do you interact with, coordinate, or work with for this shipment?

What are your threat and security concerns?

If the shipment is involved in a malicious attack what is your role?

What else do you need to know? From whom?

Who needs to know what I know, when do they need to know and how will we communicate this information?

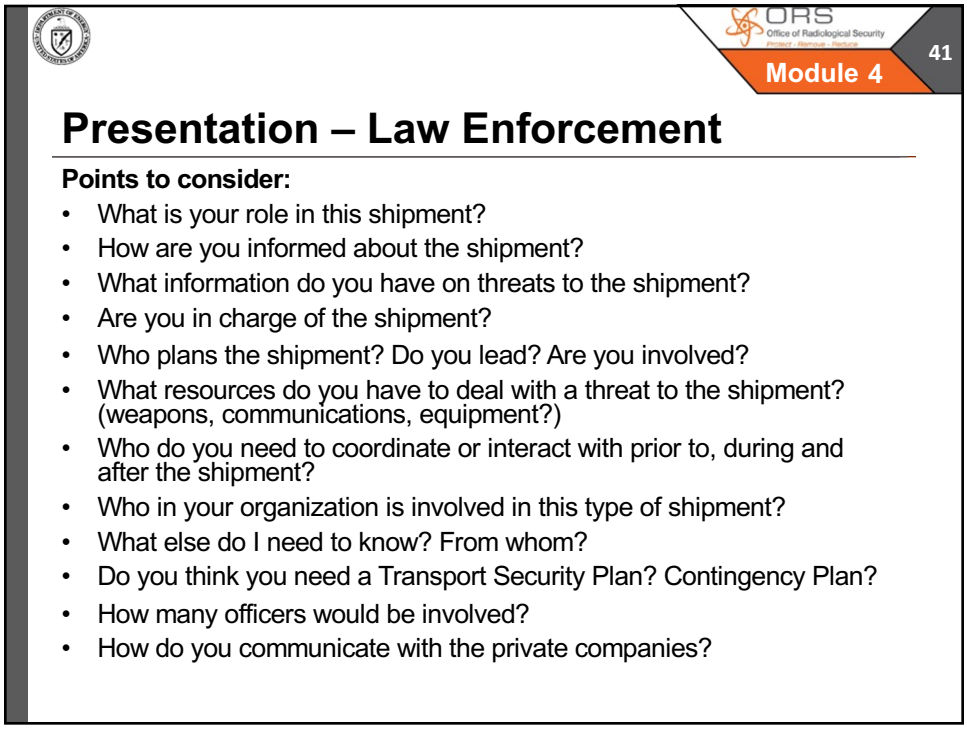
39

Presentation – Carrier

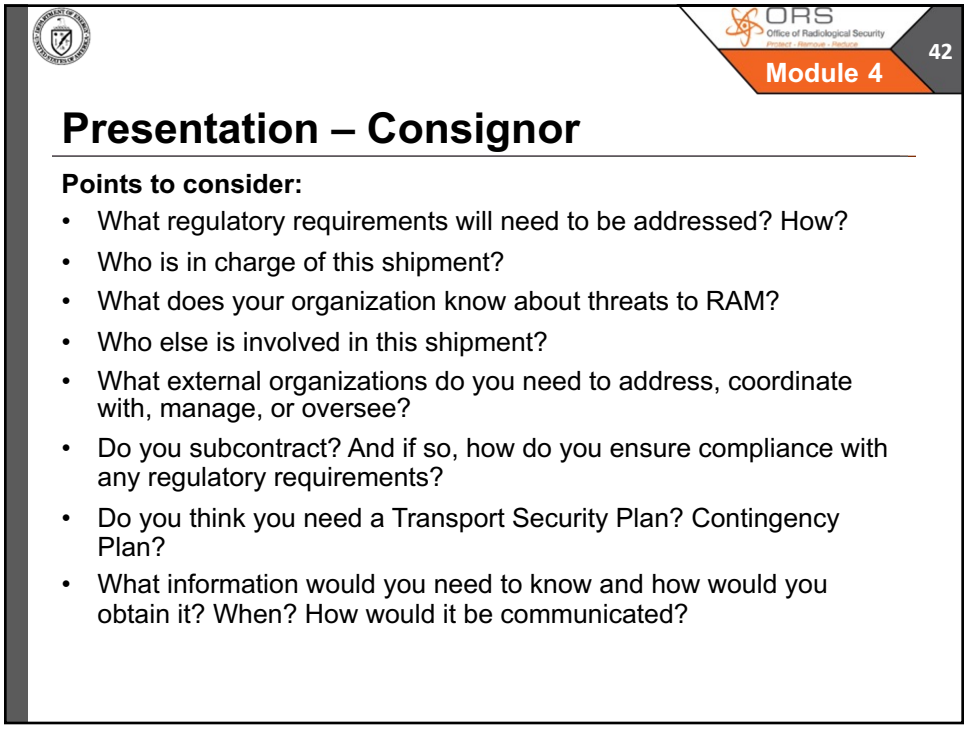
Points to consider:

- Vehicles used?
- What planning or preparations would the carrier company have to do?
- Who plans the shipment?
- Who plans the technical and security aspect of the shipment?
- Who is in charge of the shipment?
- With whom do you need to coordinate or interact with prior to, during and after the shipment?
- Who in your organization is involved in this type of shipment?
- What else do I need to know? From whom?
- Do you think you need a Transport Security Plan?

40


ORS
Office of Radiological Security
Module 4
41
Presentation – Law Enforcement
Points to consider:
• What is your role in this shipment?
• How are you informed about the shipment?
• What information do you have on threats to the shipment?
• Are you in charge of the shipment?
• Who plans the shipment? Do you lead? Are you involved?
• What resources do you have to deal with a threat to the shipment? (weapons, communications, equipment?)
• Who do you need to coordinate or interact with prior to, during and after the shipment?
• Who in your organization is involved in this type of shipment?
• What else do I need to know? From whom?
• Do you think you need a Transport Security Plan? Contingency Plan?
• How many officers would be involved?
• How do you communicate with the private companies?

41


ORS
Office of Radiological Security
Module 4
42
Presentation – Consignor
Points to consider:
• What regulatory requirements will need to be addressed? How?
• Who is in charge of this shipment?
• What does your organization know about threats to RAM?
• Who else is involved in this shipment?
• What external organizations do you need to address, coordinate with, manage, or oversee?
• Do you subcontract? And if so, how do you ensure compliance with any regulatory requirements?
• Do you think you need a Transport Security Plan? Contingency Plan?
• What information would you need to know and how would you obtain it? When? How would it be communicated?

42

Presentation – Consignee

Points to consider:

- What is your role in this shipment?
- What planning or actions are you responsible for?
- Who plans the shipment? Are you involved?
- Who is in charge of the shipment? Do you own it?
- Who do you need to coordinate or interact with prior to, during and after the shipment?
- Who in your organization is involved in this type of shipment?
- What else do I need to know? From whom?
- Do you think you need a Transport Security Plan? Contingency Plan?

43

Summary

This exercise was developed to enable an open conversation between the various agencies and organizations that have a role and responsibility in the security of radiological materials in transport.

- Did the exercise provide a better understanding of the process of transport?
- Did coordination between the organizations identify areas that could be accomplished more efficiently?
- Do you believe this exercise benefitted your relationship with the other stakeholder?

44

ORS
Office of Radiological Security
Protect · Remove · Reduce

Module 5

Radioactive Material Characterization

45

Learning Objectives

1. Discuss radioactive materials with respect to consequences, attractiveness, and security requirements
2. Describe the process and resources used to characterize radioactive materials
3. Explain how security threshold levels are determined for the transport of radioactive materials and the resources used to do so

46

Radioactive Material Definition

IAEA definition of radioactive materials:

- Any material designated in national law, regulation, or by a regulatory body as being subject to regulatory control because of its radioactivity (NSS No. 14); in the absence of such a designation by a State, radioactive material is any material for which protection is required by the current version of the International Basic Safety Standards
- A commonly used IAEA definition is also found in SSR-6 Rev.1, "Regulations for the Safe Transport of Radioactive Material"

47

Graded Approach

- Graded approach – specifying requirements commensurate with some measure of hazard or undesirable potential consequence
  - Transport safety regulations (excepted, industrial, Type A, Type B, etc., packages)
  - RAM transport security (basic and enhanced transport security levels based on radioactivity)
- Security measures suitable for each level (or category) of material can be specified to provide an appropriate level of protection

48

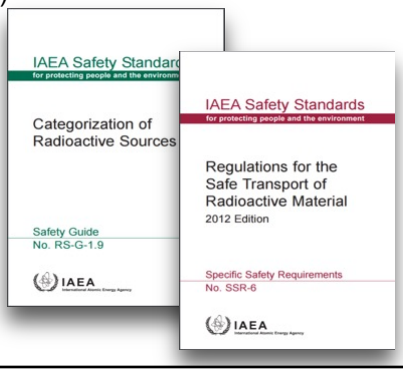
Categorization of Radioactive Material

- RAM transport security measures are determined by using radioactivity thresholds to identify the level of security required for a given shipment
- IAEA NSS-9G, Rev.1 uses a graded approach
- Packages are assigned to a transport security level based on:
  - The radionuclide contained in the package
  - The activity of the radioactive material in the package
- Determinations as to types, amounts and categorization of radiological material being shipped

Basis for Security Level Activity Thresholds

Security activity thresholds are derived from:

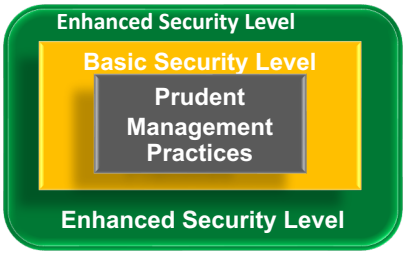
- D-Values – "Dangerous source" thresholds in the IAEA's safety document "Categorization of Radioactive Sources" (RS-G-1.9)
- A-Values – radioactivity values as specified in the IAEA's "Regulations for the Safe Transport of Radioactive Material" (SSR-6, 2012)



Establishing Security Levels

- RAM transport security levels correspond to the UN Model Regulations categories for dangerous goods:
  - Basic Security Level
  - Enhanced Security Level
- For RAM posing low potential radiological consequences, use Prudent Management Practices
- Security levels are additive (each level incorporates the security measures from the next lowest level)

If the threat is elevated, a State may apply any Additional Security Measures deemed necessary.

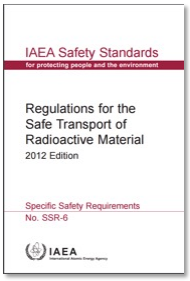


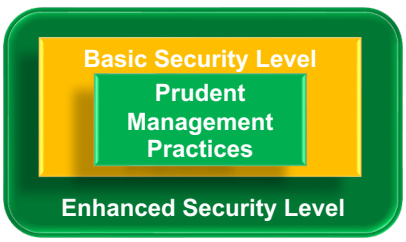
51

Prudent Management Practices

Prudent Management Practices are used for:

- RAM that present limited security concerns
- Excepted packages (as defined by SSR-6)
- Low Specific Activity material (LSA-I)
- Low-level Surface Contaminated Objects (SCO-1)

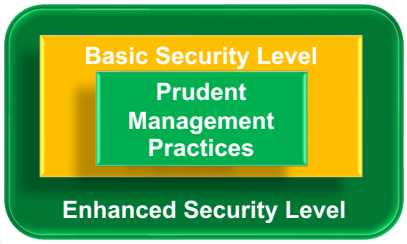




52

Basic Security Level

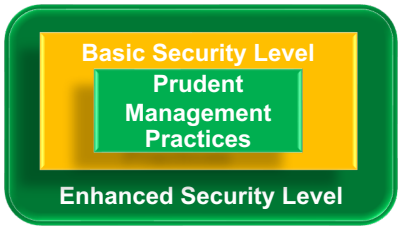
- Used for packages that are analogous to the UN "other dangerous goods" classification
- RAM shipments are subject to "general provisions" for security purposes
- All Prudent Management Practices also apply, as well as graded security systems to deter, detect, delay, and respond to malicious acts



53

Enhanced Security Level

- Used for RAM packages that are analogous to UN "high consequence dangerous goods"
- These packages have an activity the activity NSS-9G, Rev.1
- All Prudent Management Practices apply to the shipment
- All Basic Security Level measures apply to the shipment



54

Enhanced Security Level Activity Thresholds

- The value given in the table for each of the listed radionuclides (equal to 10D)
- 3000 A2 in a single package for all radionuclides not listed in the table
  - (See NSS-9G, Rev.1 Appendix.)

Radionuclide	Transport security threshold (TBq)
Am-241	0.6
Au-198	2
Cd-109	200
Cf-252	0.2
Cm-244	0.5
Co-57	7
Co-60	0.3
Cs-137	1
Fe-55	8000
Ge-68	0.7
Gd-153	10
Ir-192	0.8
Ni-63	600
Pd-103	900
Pm-147	400
Po-210	0.6
Pu-238	0.6
Pu-239	0.6
Ra-226	0.4
Ru-106	3
Se-75	2
Sr-90	10
Tl-204	200
Tm-170	200
Yb-169	3

55

Summary

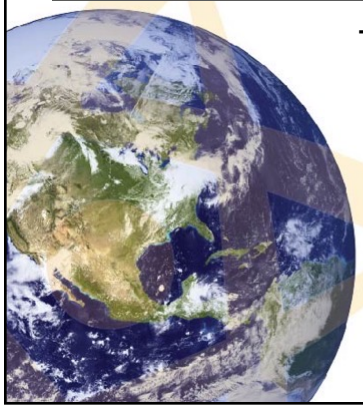
1. Discussed radioactive materials with respect to consequences, attractiveness, and security requirements
2. Described the process and resources used to characterize radioactive materials
3. Explained how security threshold levels are determined for the transport of radioactive materials and the resources used to do so

56

ORS
Office of Radiological Security
Protect · Remove · Reduce

Module 6

Threat and Capabilities Assessment



57

ORS
Office of Radiological Security
Protect · Remove · Reduce

Module 6 58

Learning Objectives

1. Describe the threats involved in radioactive material transport
2. Explain how a threat assessment can be used to design an effective physical protection system

58

How the State Evaluates Threat

Threat Assessment:

- An analysis that documents the credible motivations, intentions, and capabilities of potential adversaries that could cause undesirable consequences to RAM in transport
- Input for the Design Basis Threat (DBT)

Design Basis Threat:

- The attributes and characteristics of potential insider and/or outsider adversaries who might attempt unauthorized removal of RAM or sabotage, against which a RAM security and measurement system is designed and evaluated
  - Based on the results of threat assessments as well as other policy considerations
  - Typically, only fully developed for fixed sites and transport of nuclear material

59

Adversary Capabilities

Types of adversary capabilities addressed in a Design Basis Threat:

- Numbers
- Weapons
- Equipment
- Explosives
- Knowledge and skills
- Training and tactics
- Transportation means
- Insider assistance

60

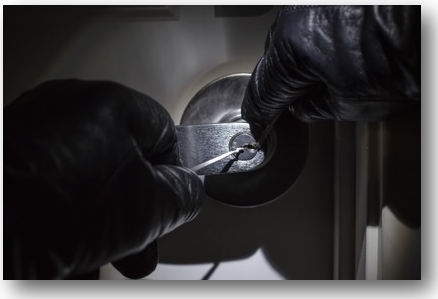
Terrorists

- **Motivation**
  - Commit violent acts to gain ideological objectives
- **Common Characteristics**
  - Expert use of explosives (military, commercial, and homemade/improvised)
  - Well funded and staffed
  - Core group may have support of a larger group
  - Military weapons (fully automatic weapons, sniper rifles, etc.)
  - Wide range of transportation options
  - Highly trained and motivated
  - Willing to kill and/or die

61

Criminals

- **Motivation**
  - Economic gain
- **Common Characteristics**
  - Small group (1 to 3)
    - Organized crime may be larger group
  - Have conventional weapons
    - Commercially available
  - Have small amounts of commercial or homemade explosives
  - Use deceit, theft, fraud, coercion, and extortion
  - Not willing to die, but may be violent to prevent capture
  - May cooperate with terrorists



62

Insider Threat Definition

Insider Threat:

Any individual with authorized access, knowledge, or authority related to radiological facilities or transport who might attempt unauthorized removal or sabotage, or who could aid outsiders to do so.

Insider Motivations:

Ideological – fanatical conviction

Financial – wants / needs money

Revenge – disgruntled employee or customer

Ego – look what I am smart enough to do

Psychotic – mentally unstable but capable

Coercion – family or self threatened

63

Insider Mitigation

- Awareness of employee activities
- Provide resources for employees to seek help with difficult circumstances
- Require that employees work together so that they are not isolated
- Provide training to management and other employees to help recognize aberrant behavior
- Strong security culture

64

Management Practices to Mitigate Risk

- Screen personnel
- Monitor employee behavior
- Implement physical, administrative controls
- Limit access to areas and information

65

Trustworthiness and Reliability

- Initial background screening
- New-hire/rehire and periodic screening--may include:
  - Financial records, check/government records disclosure
  - Substance abuse screening
  - Criminal activity
- Screening for suspected cause

66

Role of State and Competent Authority

NSS 14 and NSS-9G, Rev.1 note that the State should understand the threat and should base its transport security requirements on that threat.

Competent Authority is responsible for:

- Regulatory framework for transport security
- Coordination and development of DBT
- Incorporation of DBT within regulatory or legal framework
- Dissemination, if appropriate, of DBT to those responsible for transport security
- Maintenance and review of DBT
- Monitoring compliance and enforcement of regulations

The Competent Authority must have support from other government agencies.

67

Summary

1. Described the threats involved in radioactive material transport
2. Explained how a threat assessment can be used to design an effective physical protection system

68

ORS
Office of Radiological Security
Protect · Remove · Reduce

Module 7

Security Functions: Deterrence, Detection, Delay and Response

69

Learning Objectives

1. Describe security functions (deterrence, detection, delay, and response)
2. Describe what is meant by balance in security, defense-in-depth, and a graded approach to security
3. Identify transport security approaches for designing and implementing a transport security system recommended by international guidelines
4. Identify response strategies for security events involving the transport of radioactive material

70

Security Functions (1 of 4)

Deterrence

- Encompasses actions undertaken intended to discourage someone from doing something or to persuade someone not to do something
- May be provided by visible security measures that indicate a hardened target
- May decrease the likelihood of a potential threat by reducing the expectancy of success
- Cannot be measured
- Is not effective against a determined adversary

71

Security Functions (2 of 4)

Detection

- Encompasses actions undertaken for the discovery and assessment of unauthorized access or removal of RAM or of attempted sabotage during transport
- Can be achieved by several means:
  - Visual observation
  - Electronic sensors
  - Seals and other tamper-indicating devices
  - Monitoring systems
  - Other means

NOTE: Only a person can perform "assessment." Without assessment, there is no detection.

72

Security Functions (3 of 4)

Delay

- Encompasses actions undertaken to impede an adversary's attempt to remove RAM during transport, generally through barriers or other physical means
- These actions should:
  - Increase adversary task time
  - In whole, be equal to or greater than the response time

73

Security Functions (4 of 4)

Respond

- Actions taken following detection to prevent an adversary from accomplishing their goal
- These actions are typically performed by security or law enforcement personnel, or other State agencies
- Response actions include:
  - Interrupting
  - Preventing
  - Recovering

74

Effective and Timely Detection and Delay

Detection should include effective communications between involved personnel and good command and control center.



Delay should increase adversary task time to be equal to or greater than the response time available after assessment of the alarm.

Response time must be less than the adversary task time remaining after assessment of the alarm in order to interrupt the adversary before completing their task.

75

Adversary Advantage

Transport Information:

If an adversary obtains transport information, they can pre-set the attack time, location, and other variables.

76

Types of Response Forces

Guard Internal to Shipment

- First response comes from members of the shipment that can function as and are trained for security purposes
- Have specific mission assignment upon attack: Defend material/cargo
- Enhanced capability for defense, locate, recapture and recovery operations
- Special tactics, weapons, and tools to defend

77

Response Considerations: Guards

- Escorts
- Material custodians
- Radiation protection or health specialists
- Guards
  - Private guards
  - May have radiation safety awareness
- Varying levels of protection training and skills
  - Armed actions
  - Level of training for counter ambush/attack actions

May have coordination and communication issues with law enforcement response

78

Response Considerations: Police Escort

Police or Security Force Escorts

- Command and coordination issues with external response if from different organizations
- Level of training for counter ambush/attack actions
- Linkup with incoming forces; friendly-on-friendly issues
- Better communications
- Better training and procedures

79

Response Strategies

Overall goal is to prevent unauthorized access to radioactive material.

Two main strategies:

- Interdiction/interruption
- Containment

Keys to success:

- Planning
- Training
- Awareness of target
- Intelligence gathering
  - Know your potential adversary
- Collaboration with all stakeholders

80

Module 7

Points for Discussion: Transport Security Training Program

- Personnel having roles and responsibilities in the shipment, preparation, packaging, and escorting radiological materials should be trained, qualified and in some cases be certified to perform their functions
- Regulator, consignors, carriers and consignees should receive formal initial and periodic training respective of their role in the transportation process
- Task specific training promotes capabilities in:
  - Practical and operational knowledge
  - Improving and sustaining operational readiness
  - Strengthen interjurisdictional and international cooperation
  - Clarifying organizational roles and responsibilities
  - Awareness raising and benefits exercise and drill programs

81

Module 7

82

Defense in Depth in Security During Transport

The Concept of Defense in Depth

- Is used in designing security systems, requiring an adversary to overcome or circumvent multiple obstacles
- Consists of implementing several layers of defense that adversaries would have to overcome or circumvent to achieve their objectives, including
  - Administrative aspects (procedures, instructions, sanctions, access control rules, confidentiality rules)
  - Technical aspects (multiple layers of protection together with measures for detection and delay)

82

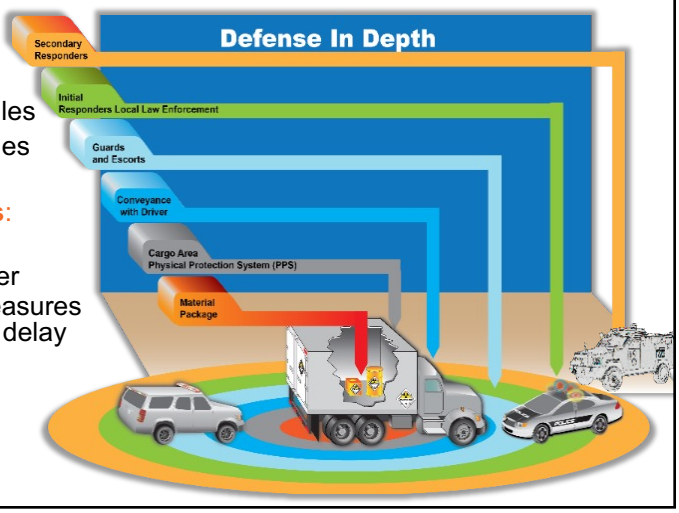
Implementing Defense in Depth

Administrative Aspects:

- Procedures
- Instructions
- Sanctions
- Access control rules
- Confidentiality rules

Technical Aspects:

- Multiple layers of protection together with technical measures for detection and delay



83

Summary

1. Described security functions (deterrence, detection, delay, and response)
2. Described what is meant by balance in security, defense-in-depth, and a graded approach to security
3. Identified transport security approaches for designing and implementing a transport security system recommended by international guidelines
4. Identified response strategies for security events involving the transport of radioactive material

84

ORS
Office of Radiological Security
Protect · Remove · Reduce

Jared Adkins Theft

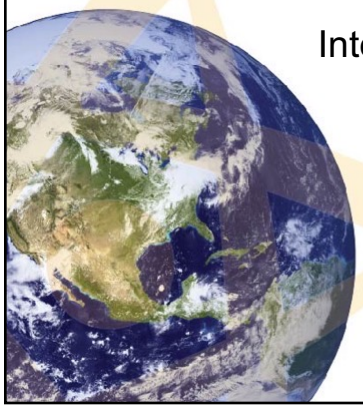
Case Studies

85

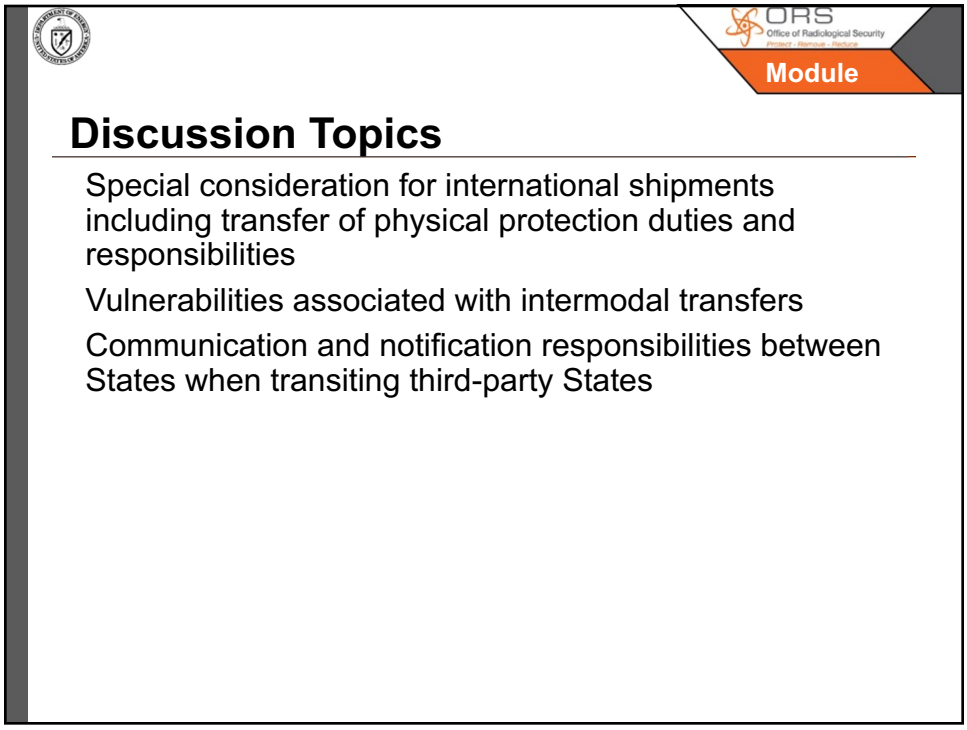
ORS
Office of Radiological Security
Protect · Remove · Reduce

Module 8

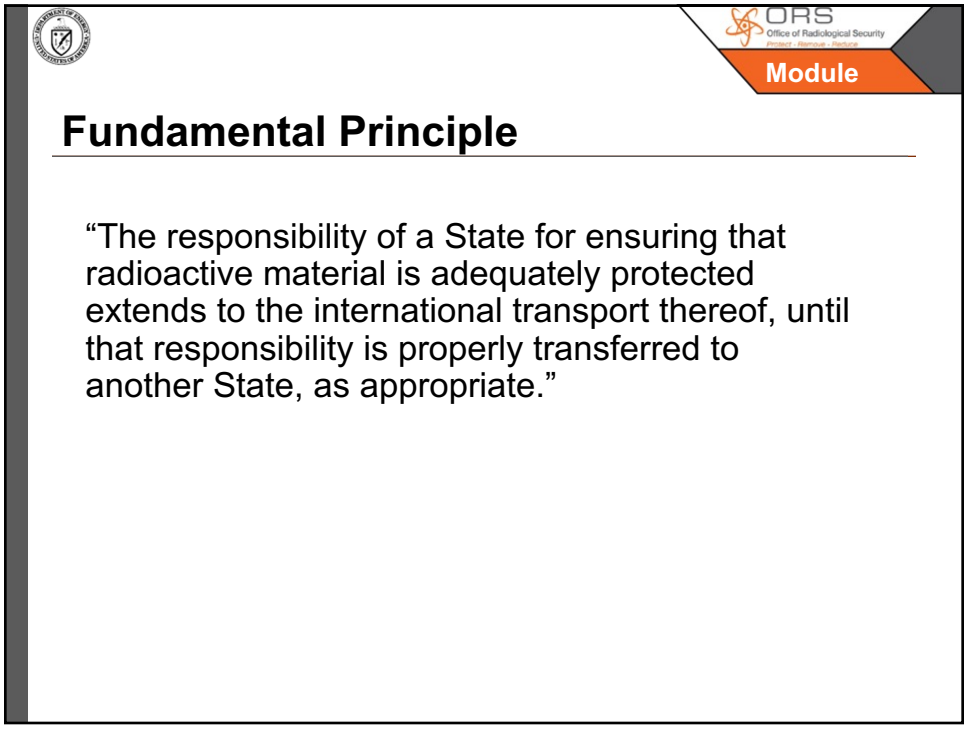
International Shipments and Intermodal Transfers



86


ORS
Office of Radiological Security
Module
Discussion Topics
Special consideration for international shipments including transfer of physical protection duties and responsibilities
Vulnerabilities associated with intermodal transfers
Communication and notification responsibilities between States when transiting third-party States

87


ORS
Office of Radiological Security
Module
Fundamental Principle
"The responsibility of a State for ensuring that radioactive material is adequately protected extends to the international transport thereof, until that responsibility is properly transferred to another State, as appropriate."

88

Module

State Responsibilities

The responsibility for physical protection within a State rests with the government of that State

The State has responsibility for physical protection of radioactive material onboard vessels and aircraft registered under its flag

For international transport there is a need for close international cooperation

89

Module

Ministry of Transportation

The shipper needs information pertaining to the following:

- Requirements or restrictions regarding Class 7 transport
- Identification of vehicle inspection requirements
- Need for driver medical examinations and all certifications and qualifications
- Driver medical exams or drug screens (if required)
- Identification of carriers licensed to transport Class 7

90

Module

Transfer of Responsibilities

For land transport the point of transfer of jurisdiction to another State is dictated by the borders of the States concerned

During intermodal transfers responsibilities for protection may change

91

Module

Radiological and Nuclear Competent Authority

Provides the following essential information to shipper or oversight entity:

- Laws and regulations of the State
- Transport Security Plan (TSP) approval process
- Responsible organization for TSP preparation
- Timelines for TSP submissions and expected approval
- Other State agencies that may need to have input from the shipper or carrier
- Requirements needed from the carrier or receiver

92

Module

TSP Preparation and Submission

In many cases the regulatory body will require the carrier to develop and submit a transport security plan (TSP) for review and approval. In this event, the shipper will review the carrier's ability to prepare a TSP that meets the information requirements mandated by the regulatory body. The TSP may be requested by other State agency competent authorities that have mandatory requirements.

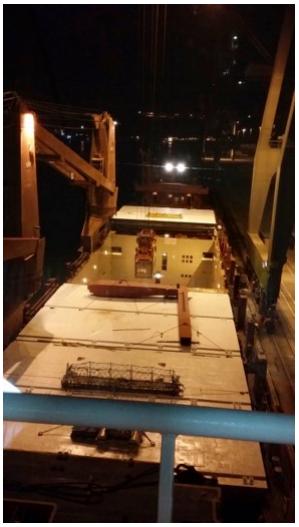
93

Module

Transfer of Responsibilities

For maritime shipments, due to the jurisdiction of the flag State of the vessel, the point of transfer may be less clearly defined, due to coexistent jurisdiction

For air transport, the point of transfer of responsibility will normally be the point at which the material is loaded/unloaded



94

Module

Identifying Class 7 Carriers

The shipper will rely primarily on two sources for identifying a carrier that is acceptable for use in the transport of radioactive materials and sources:

- The State competent authority may be asked to provide a list of carrier companies that have license or permits to transport Class 7, and provide their input on the best qualified carrier
- The shipper will conduct open-source research to determine if the carrier company can support the movement of the package selected to transport the source, equipment/vehicles, age of equipment, maintenance program and other desired qualities and capabilities

95

Module

Licensing and Permits

The shipper will ascertain the carrier's:

- Existing permits and licenses regarding Class 7 transport
- Ability to obtain needed permissions to conduct the planned shipment

96

Module

Equipment Quality and Serviceability

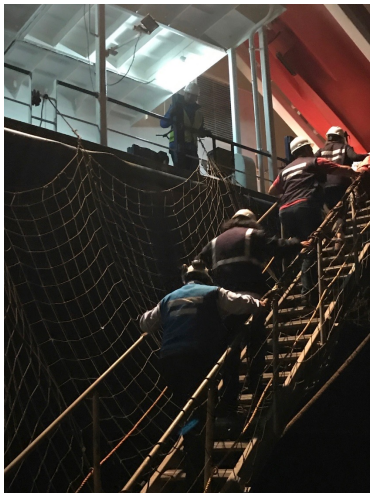
- Equipment size/carrying capacity
- Length of route
- Type of terrain

97

Module

Transfer of Security Responsibilities

- The point of transfer of responsibilities must be clearly defined and agreed
- When armed guards accompany a shipment, written arrangements for physical protection responsibilities should be prepared and accepted by the States involved
- Sensitive information should be protected appropriately



98

Module

Driver Qualifications and Trustworthiness

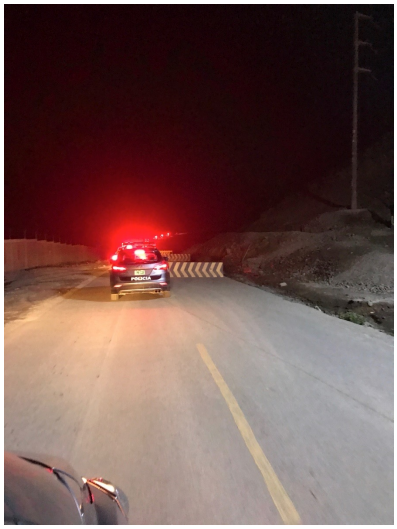
- State required background vetting
- Length of service
- Special licenses held
- Experience transporting Class 7
- Any required specialized training
- Possible medical checks or drug screening

99

Module

Ensuring Continuous State Responsibility

Before allowing international transport, the shipping State should consider if the States involved in the transport, including transit States, are willing to accept physical protection responsibilities



100

Module

Pre-Shipment Inspection

- Is a vehicle inspection required?
- Scope of required inspection
- Can the carrier meet requirements?

101

Module

Evaluate Driver Security Instructions, Plans and Briefings

This would include:

- Interactions with police/military escorts
- Actions to take in the event of an accident or mechanical breakdowns
- Needing fire, medical or security response
- Notifications and contact information
- Other needed information

102

Module

Law Enforcement

Provides information pertaining to the following shipment related topics:

- Route approval or recommended alternate routes based on internal procedures
- Number and availability of personnel for escorts
- Sources of secondary response
- Shipment dates and time of day for departure
- Local threat assessment and criminal activities
- Personnel equipment capabilities

103

Module

Carrier Responsibilities

The carrier would be required to perform the following:

- Maintain certifications and qualifications
- Conduct trustworthiness checks of drivers and persons associated with the shipment
- Prepare transport security plans and submit to appropriate entities
- Maintain vehicle maintenance
- Undergo stringent inspection requirements
- Prepare shipping documents
- Perform shipment under police escort supervision during the shipment

104

Module

Transit Shipments

When international shipments transit the territory of a State other than that of the shipping or receiving State, arrangements should be made to;

- Identify transit States
- Inform them in advance
- Obtain in advance their cooperation and assistance to ensure that the proposed arrangements are in accordance with their national law
  - Formal communication through official channels may be necessary

105

Module

Summary

States have responsibility for physical protection of radioactive material within their borders and onboard aircraft and vessels registered under their flag

Seamless and continuous physical protection should be provided during international transport, including through transit States

106

ORS
Office of Radiological Security
Protect · Remove · Reduce

Module 9

Shipment Security Planning and Verification

107

Learning Objectives

1. Discuss the steps involved in effective planning and conduct of transport operations
2. Describe the purpose of a Transport Security Plan (TSP) and identify those responsible for developing the plan
3. Explain how an effective contingency plan can help prevent and minimize the damage from malicious events and other unplanned, abnormal events
4. Discuss the measures that can be taken to prevent or minimize malicious events that could lead to a release and the mitigation actions recommended following a release
5. Discuss the need for conducting a pre-shipment security verification of shipments and the operations involved

108

What is the Purpose of a Transport Security Plan?

- Provide a basis for developing and implementing an effective transport security system
- Specify security measures for a shipment or a multi-shipment campaign
- Base security measures on a risk-informed decision-making process to deter, detect, delay, and respond to malicious acts

109

When is a Transport Security Plan Recommended?

A security plan is recommended:

- For the shipment of any package that requires enhanced security level measures
- Also, when otherwise
  - Required by a State's competent authority
  - Deemed necessary by an operator

110

The Transport Security Plan

- Each transport consignor and carrier should have a transport security plan which can be used, as necessary
- The structure and format of the transport security plan can vary widely and should suit the needs of the operator
- All the transport security plan elements listed in NSS-9G, Rev.1 should be considered for inclusion in the plan

111

Contingency Plan

- Will be covered in next session….

112

Controlling Transport Related Information

What are information assets? Equipment or components (including media) that are used to store, process, control, or transmit information.

- Background checks
- Defining and marking classified information
- Controlling information access
  - Need-to-know system

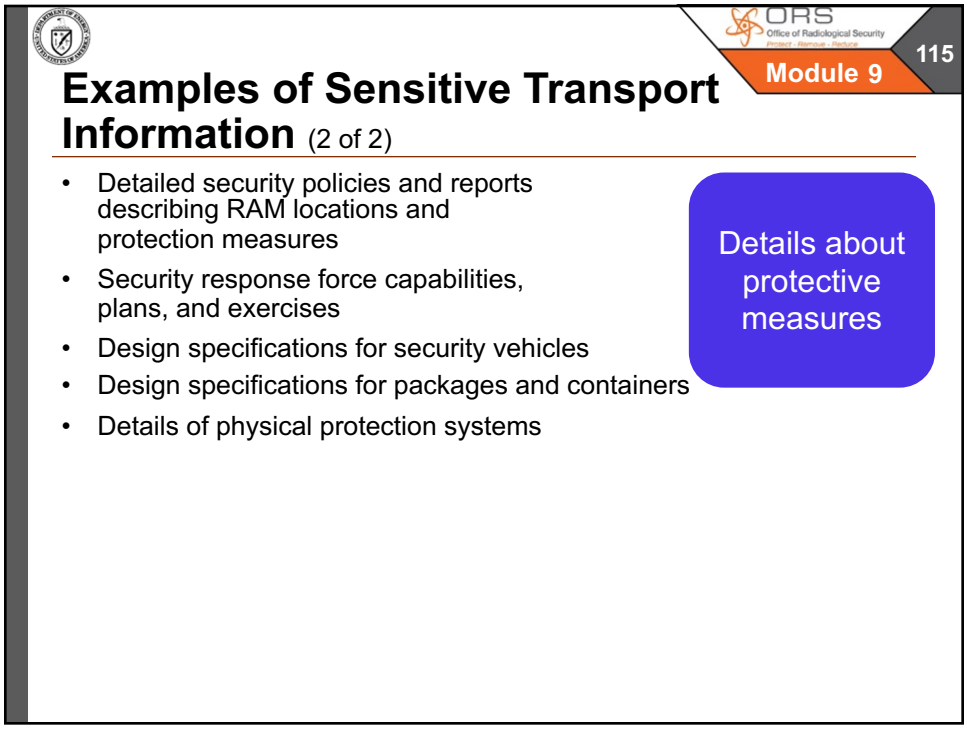
113

Examples of Sensitive Transport Information (1 of 2)

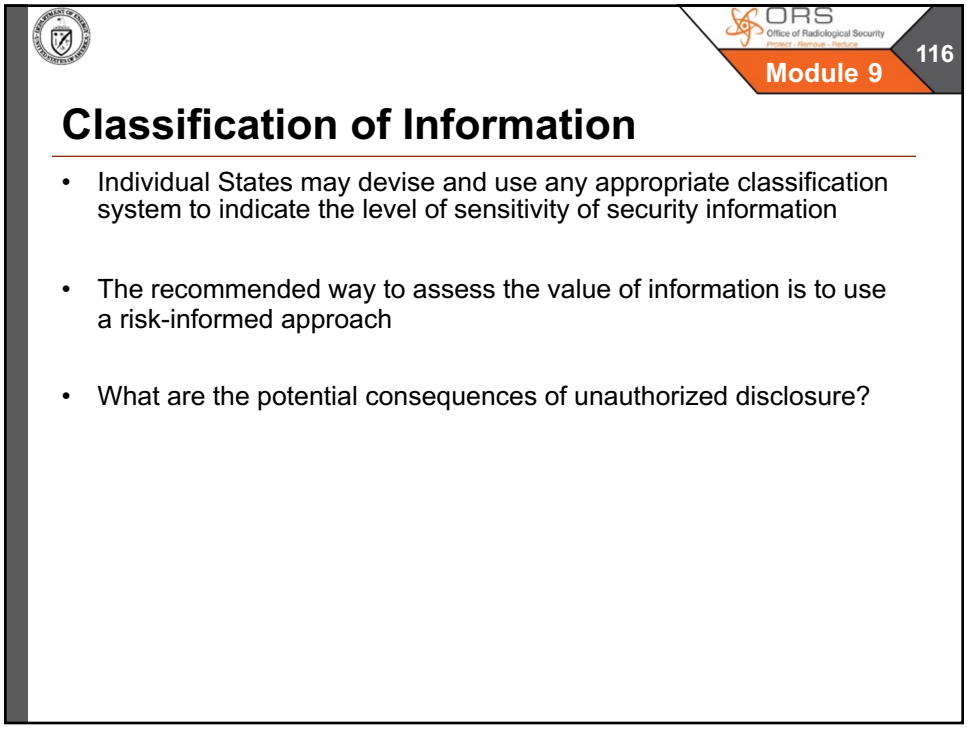
- Shipment schedules
- RAM quantities and locations, types, and forms
- Routes and RAM movements (in the Transport Security Plan)
- Personnel files and trustworthiness check results
- Physical security information

Details on transport operations for radioactive material

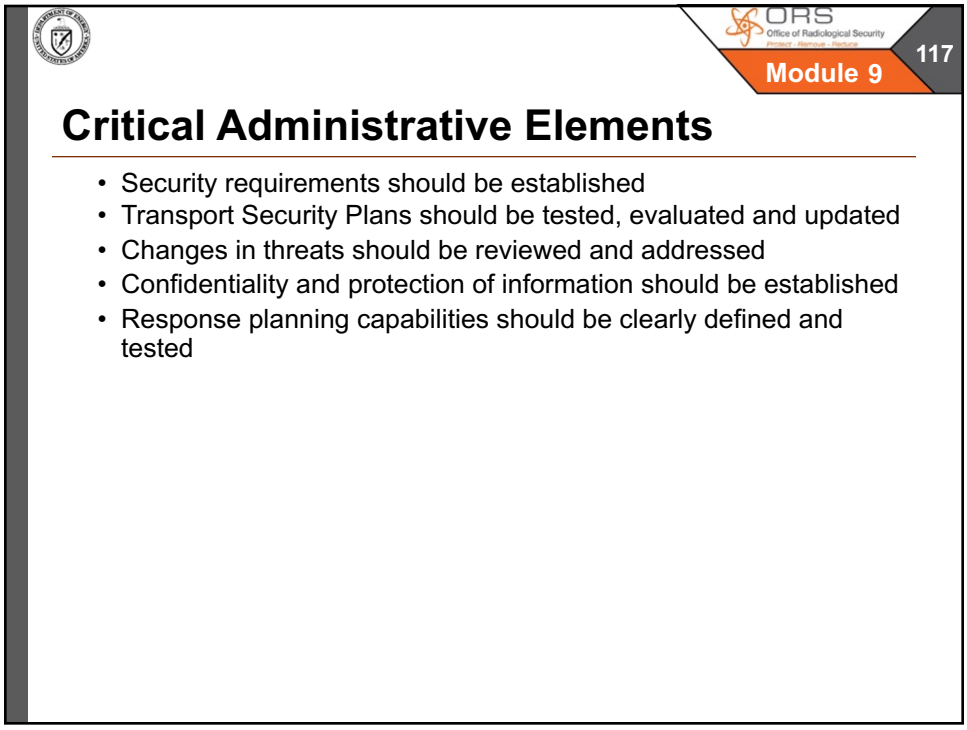
114


ORS
Office of Radiological Security
Module 9
115
Examples of Sensitive Transport Information (2 of 2)
• Detailed security policies and reports describing RAM locations and protection measures
• Security response force capabilities, plans, and exercises
• Design specifications for security vehicles
• Design specifications for packages and containers
• Details of physical protection systems
Details about protective measures

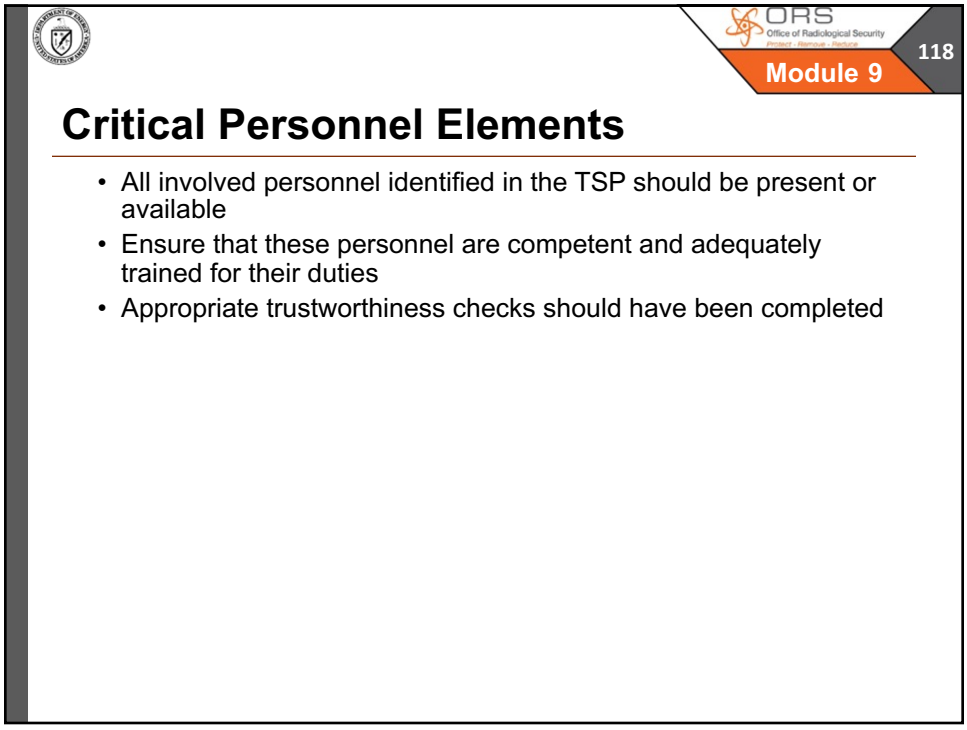
115


ORS
Office of Radiological Security
Module 9
116
Classification of Information
• Individual States may devise and use any appropriate classification system to indicate the level of sensitivity of security information
• The recommended way to assess the value of information is to use a risk-informed approach
• What are the potential consequences of unauthorized disclosure?

116


ORS
Office of Radiological Security
Module 9
117
Critical Administrative Elements
• Security requirements should be established
• Transport Security Plans should be tested, evaluated and updated
• Changes in threats should be reviewed and addressed
• Confidentiality and protection of information should be established
• Response planning capabilities should be clearly defined and tested

117


ORS
Office of Radiological Security
Module 9
118
Critical Personnel Elements
• All involved personnel identified in the TSP should be present or available
• Ensure that these personnel are competent and adequately trained for their duties
• Appropriate trustworthiness checks should have been completed

118

Critical Equipment Elements

- All personnel involved in the shipment have the necessary equipment to perform their duties
- All Physical Protection System (PPS) measures and equipment identified in the TSP are fully functional and tested
- Communications, and where appropriate tracking systems, are available and functional. Redundancy in equipment may be necessary

119

Pre-Shipment Verification

- The pre-shipment verification should be initiated with sufficient time prior to the planned start of a shipment to:
  - Allow deficiencies to be identified
  - Ensure that corrective actions are taken
  - Address any risk remaining if corrective actions can not be taken
- It may be appropriate to conduct a pre-shipment verification both well in advance, and immediately prior to the shipment
- Critical elements should be defined in detail using the TSP
- May need to rely on assurances given by other organizations, e.g., police/national response agencies
- Pre-Shipment Verification may include several categories of critical elements

120

Pre-Shipment Verification Checklist

- Checklists are recommended for use by those performing the review.
- The structure of the pre-shipment verification checklist should:
  - Follow, as much as possible, the structure of the Transport Security Plan
  - Cross-reference, using section/paragraph numbering of the Transport Security Plan, each element being reviewed
- The corrective actions identified should be detailed as the review proceeds, addressing outstanding and unsatisfactory issues.

Example Section of a Pre-Shipment Verification Checklist

READINESS REVIEW CHECKLIST				
Ref.	**Security Requirements**	**Status * Y, N, C, NC, NA, P**	**Comments (Specify Details)**	**Corrective Action Needed? Y or N**
	Description of the Material to be Transported (Continued)			
	Has the radiological material in each package been verified to determine if the contents of each package the description in the transport security plan			
	ADMINISTRATIVE REQUIREMENTS			
	Has a transport security plan been prepared and implemented for the shipment of radiological material?			
	Does the security plan specifically allocate responsibilities?			
	Does the security plan provide for the keeping of records of radiological material being transported?			
	Does the security plan provide for review of current operations and assessment of vulnerabilities?			
	Does the security plan provide clear statements of security measures and procedures that will be followed?			

* Y – Yes, N – No, C – Completed, NC – Not Completed, NA – Not Applicable, P – Pending

Example: Section of a Corrective Action Checklist

CORRECTIVE ACTION CHECKLIST			
TSP Ref.	ISSUE	CORRECTIVE ACTION OR RESPONSE NEEDED	CORRECTIVE ACTION COMPLETED (Date/Authorizing Person)

123

Summary

1. Described the steps involved in effective planning and conduct of transport operation
2. Described the purpose of a Transport Security Plan and those responsible for developing the plan
3. Explained how an effective contingency plan can help prevent and minimize the damage from malicious events and other unplanned, abnormal events.
4. Explained the need for a security plan and a contingency plan
5. Described when a pre-shipment verification should be performed?
6. Explained what step(s) should be taken when a deficiency is identified

124

ORS
Office of Radiological Security
Protect · Remove · Reduce

Facilitated Discussion

Discussion:
Contingency Plans
and Response

125

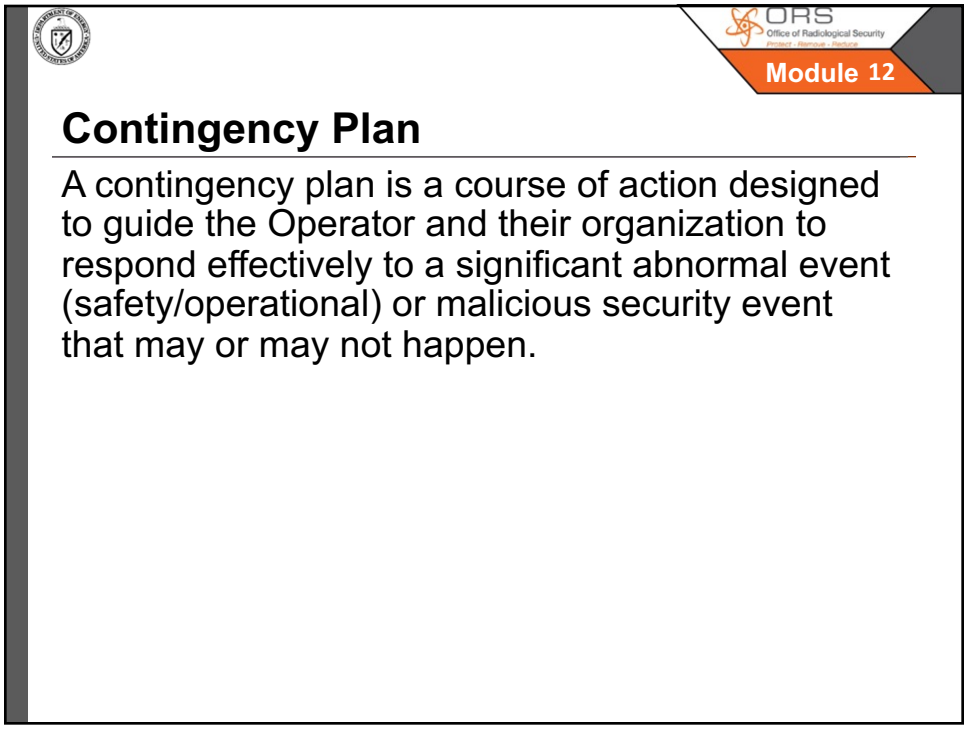
ORS
Office of Radiological Security
Protect · Remove · Reduce

Module 12

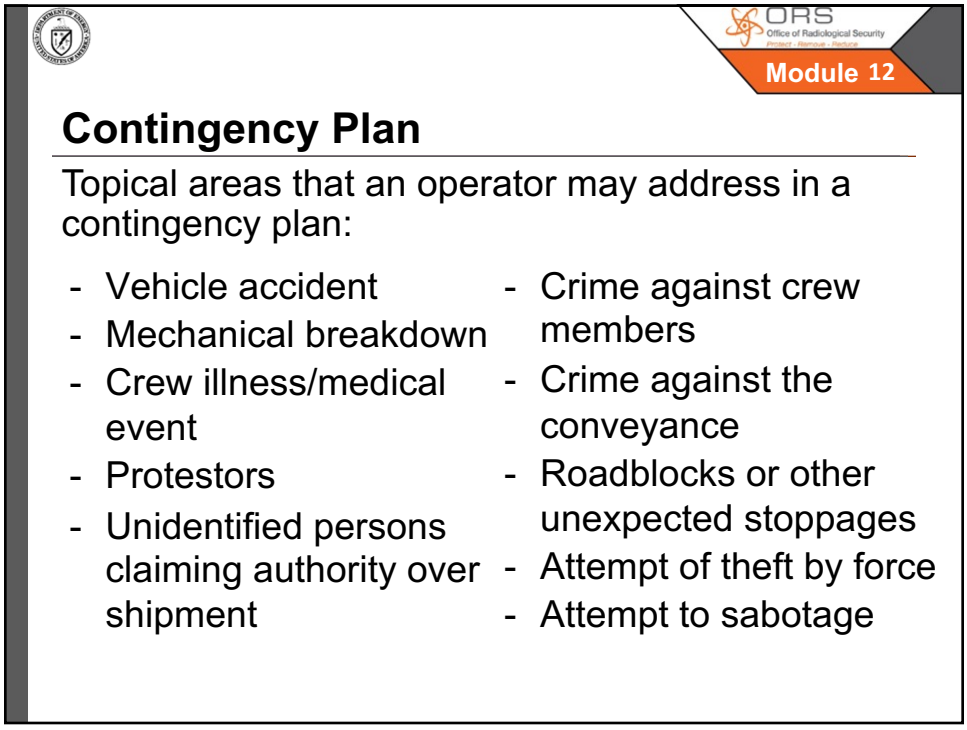
Discussion Topics

1. Explain how an effective contingency plan can help prevent and minimize the damage from malicious events and other unplanned, abnormal events
2. Discuss the measures that can be taken to prevent or minimize malicious events that could lead to a release, and the mitigation actions recommended following a release
3. Discuss the need for conducting a readiness review of shipments and the operations involved

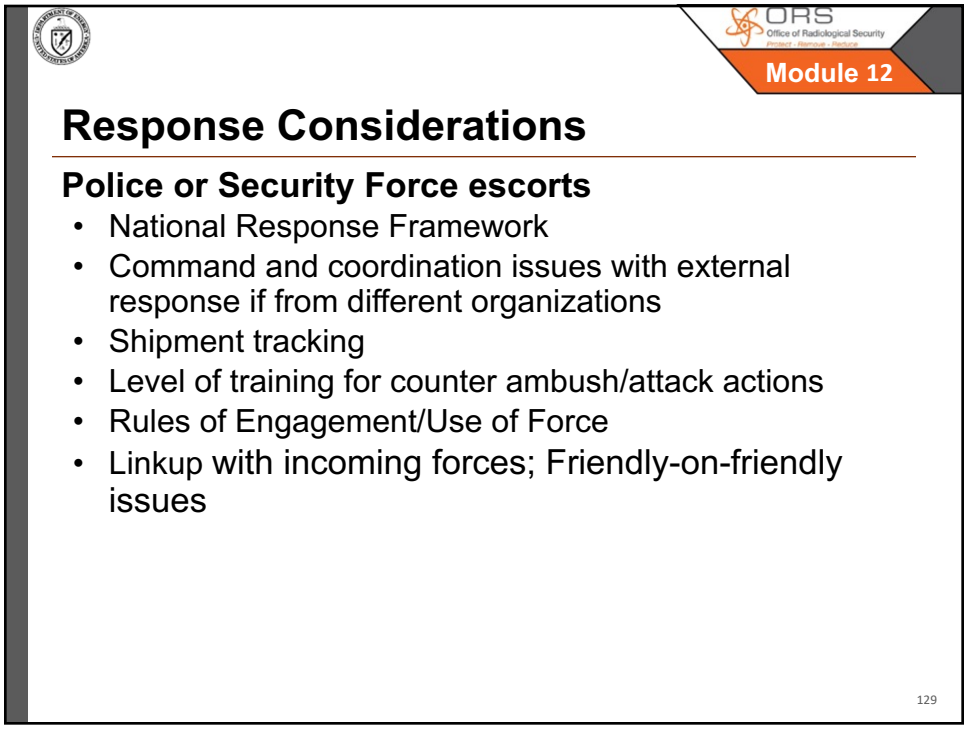
126


ORS
Office of Radiological Security
Module 12
Contingency Plan
A contingency plan is a course of action designed to guide the Operator and their organization to respond effectively to a significant abnormal event (safety/operational) or malicious security event that may or may not happen.

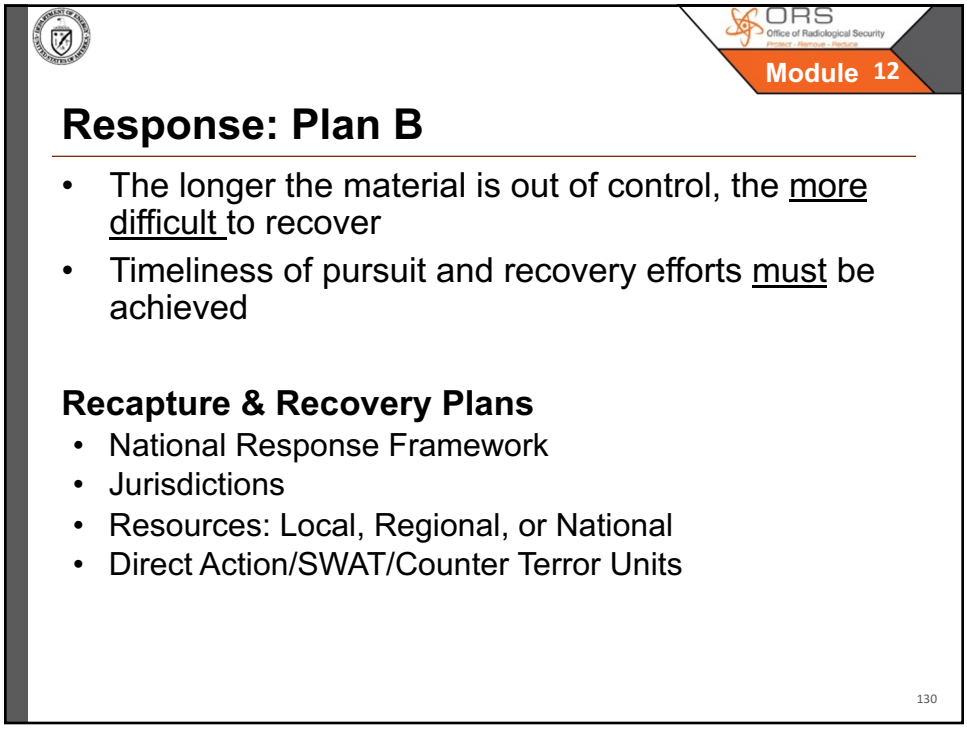
127


ORS
Office of Radiological Security
Module 12
Contingency Plan
Topical areas that an operator may address in a contingency plan:
- Vehicle accident
- Mechanical breakdown
- Crew illness/medical event
- Protestors
- Unidentified persons claiming authority over shipment
- Crime against crew members
- Crime against the conveyance
- Roadblocks or other unexpected stoppages
- Attempt of theft by force
- Attempt to sabotage

128


ORS
Office of Radiological Security
Module 12
Response Considerations
Police or Security Force escorts
• National Response Framework
• Command and coordination issues with external response if from different organizations
• Shipment tracking
• Level of training for counter ambush/attack actions
• Rules of Engagement/Use of Force
• Linkup with incoming forces; Friendly-on-friendly issues
129

129


ORS
Office of Radiological Security
Module 12
Response: Plan B
• The longer the material is out of control, the more difficult to recover
• Timeliness of pursuit and recovery efforts must be achieved
Recapture & Recovery Plans
• National Response Framework
• Jurisdictions
• Resources: Local, Regional, or National
• Direct Action/SWAT/Counter Terror Units
130

130

Readiness Review

The Readiness Review should be initiated with sufficient time prior to the planned start of a shipment to:

1. Allow deficiencies to be identified
2. Ensure that corrective actions are taken
3. Address any risk remaining if corrective actions can not be taken

It may be appropriate to conduct a Readiness Review both well in advance, and immediately prior to the shipment.

131

Readiness Review Checklist

Checklists are recommended for use by those performing the review.

The structure of the Readiness Review checklist should:

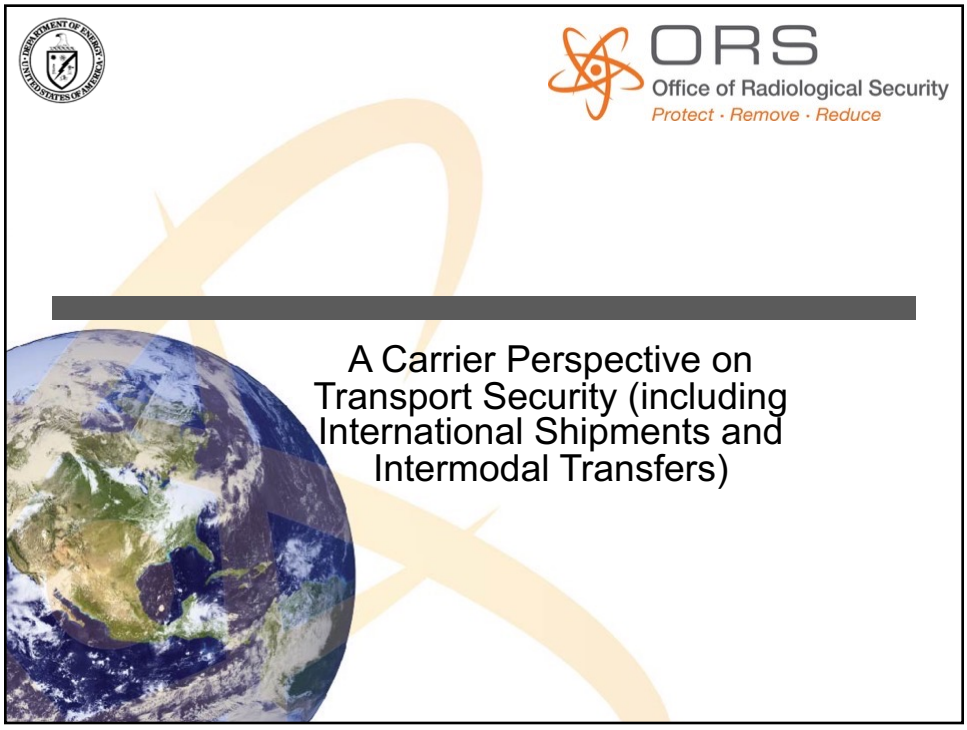
- Follow, as much as possible, the structure of the Transport Security Plan
- Cross-reference, using section/paragraph numbering of the Transport Security Plan, each element being reviewed

The corrective actions identified should be detailed as the review proceeds, addressing outstanding, unsatisfactory issues

132


ORS
Office of Radiological Security
Protect · Remove · Reduce
Facilitated Discussion: Regulators Role in Security Planning and verification

133

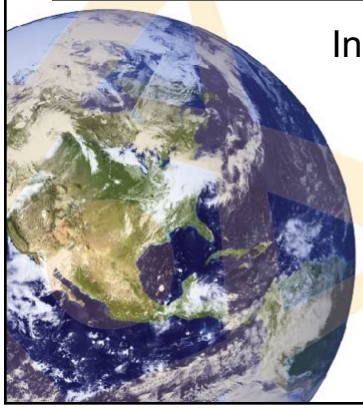

ORS
Office of Radiological Security
Protect · Remove · Reduce
A Carrier Perspective on Transport Security (including International Shipments and Intermodal Transfers)

134

ORS
Office of Radiological Security
Protect · Remove · Reduce

Module 10

Introduction to Battleboard Exercises



135

ORS Office of Radiological Security
Protect · Remove · Reduce

Module 10 136

Learning Objectives

1. Detail the functionality and benefits of a battleboard exercise
2. Understand how a battleboard exercise can be utilized to validate adequacy of security for a transport shipment
3. Identify methods to strengthen security and reevaluate through replay

136

Battleboard Tabletop Defined

- A Battleboard tabletop is a turn-based (adversary then protective force) simulation designed to evaluate the system's capability in response to an attack by an adversary force
- A Battleboard is a 3-dimentional scale model with as much detail as practical to assure accuracy of the results
  - Terrain features
  - Moveable units (people and vehicles)
  - Vegetation
  - Buildings

137

Typical Uses of the Battleboard

- Evaluation of a current system (baseline)
- Evaluation of an upgraded or changed system
- Development of tactical plans
- Training of protective forces
- Evaluate procedural changes in the safeguards and security program
- Contingency planning

138

Overview of the Methodology (1 of 3)

- Concept is like combat-oriented board games
- Participants are divided into two groups
  - Adversaries
  - Protective Forces
- The two groups are separated to create plans of attack and defense
- When planning is complete the two groups meet around the battle board that represents the system that will be evaluated
- Each team has **five minutes** to complete a turn

139

Overview of the Methodology (2 of 3)

- Adversaries begin the "battle" with the first move (turn)
- Protective force has the second move
- Each move reflects a unit of time on a clock (typically 30 seconds)
  - One adversary move and the subsequent protective force move reflects one 30-second unit of time
  - This allows for more detailed analysis of critical events

	Time					
	30 Second Move	60 Second Move	90 Second Move	120 Second Move	180 Second Move	210 Second Move
Adversary						
Protective Force						

140

Overview of the Methodology (3 of 3)

The battle continues until one of the following conditions is met:

- Adversaries have met their objective
- Adversaries are no longer capable of meeting objective. Typical reasons:
  - Attrition: Not enough people to complete remaining tasks
  - Loss of essential capability such as explosives, vehicle, or tools

141

Roles and Responsibilities (1 of 2)

- **Senior Controller** – person responsible for an accurate and unbiased outcome of the simulation
  - Assures all parties act in accordance with the agreed upon rules
  - Has final decision-making authority when parties do not agree on an issue
- **Adversary Controller** – unbiased person responsible for assuring that adversary team makes plans in accordance with agreed threat and capabilities
- **Protective Force Controller** – unbiased person responsible for assuring that the protective force acts according to approved defense plans, training, and tactics

142

Roles and Responsibilities (2 of 2)

- **Adversary Team Lead** – is the person who strives without personal compromise to achieve the adversary objective
- **Protective Force Team Lead** – person who strives without personal compromise to achieve system success
- **Team Members** – assists in the development of plans, suggests tactical moves, provides technical input in area of expertise
- **Recorder** – person recording all movements and engagement outcomes

143

Engagements of Forces (1 of 3)

- Tokens represent people. Each token is uniquely identified for documentation and tracking purposes (i.e., PF 1 for Protective Force number 1)
- Adversary plans that include hidden traps, explosives, snipers, etc. must be announced to the controllers prior to the simulation beginning

144

Engagements of Forces (2 of 3)

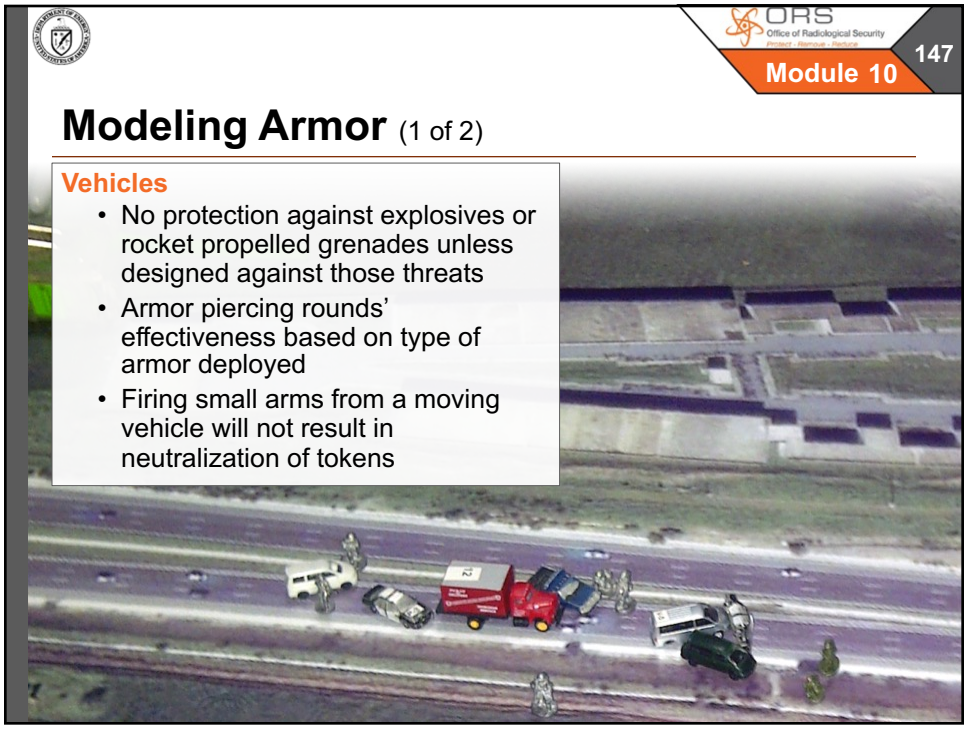
- A token may engage only one other token per turn
- A token firing from a hidden position becomes visible to those in line of sight and may be engaged in that same turn

145

Engagements of Forces (3 of 3)

- Multiple tokens may engage a single token during the same turn
- Variation of success of firearm engagements is determined by the roll of two six-sided dice
- Possible outcomes of an engagement:
  - Miss
  - Wound
  - Kill
- Outcomes are determined by weapon tables based on:
  - Type of weapon
  - Observation capability
  - Distance from target

146

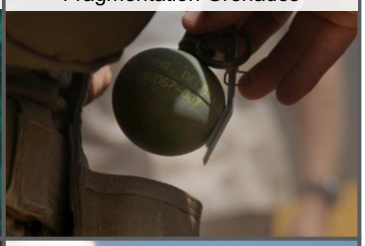

ORS
Office of Radiological Security
Module 10
147
Modeling Armor (1 of 2)
Vehicles
• No protection against explosives or rocket propelled grenades unless designed against those threats
• Armor piercing rounds' effectiveness based on type of armor deployed
• Firing small arms from a moving vehicle will not result in neutralization of tokens

147


ORS
Office of Radiological Security
Module 10
148
Modeling Armor (2 of 2)
Personnel
• No protection achieved with body armor
Hardened Fighting Positions
• No protection against explosives or rocket propelled grenades unless designed against those threats
• Armor piercing rounds' effectiveness based on type of armor deployed
POLICE

148

Special Weapons and Equipment

Distraction/Disorientation Devices	Fragmentation Grenades
	
	
Bulk Explosives	Rocket Propelled Grenades

149

Movement of Tokens (1 of 2)

- Tokens may not shoot and move at the same time and achieve engagement success (suppression only)
- Tokens cannot travel full distance allowed and fire on another token
- Tokens may move ½ distance and engage a token in the same turn

150

Movement of Tokens (2 of 2)

Movement distances are based on:

- Walking
- Running—defensive standard
- Running—offensive standard
- Tokens encumbered with weight (>20 kg), or awkward items will be slowed to at least half of maximum

151

Summary

- The battleboard methodology allows for a disciplined and systematic approach to evaluate the effectiveness of a system or program
- It is an integrating tool for all safeguards and security functions and can aid in developing plans and the training to implement those plans
- The exercise is limited only by the imagination of the user and provides a low-cost and sustainable analytical tool.

152


ORS
Office of Radiological Security
Module 10
153
Questions
Comments
Discussion

153