SAND2012-8990P

Contingency Planning Under INFCIRC/225/Revision 5

SAND2012-XXXXP Sandia National Laboratories is a multi-program laboratory managed and operated by Sandia Corporation, a wholly owned subsidiary of Lockheed Martin Corporation, for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-AC04-94AL85000.

Sandia National Laboratories

Course Objectives

Upon completing this course, participants should be able to:

- Identify the recommended requirements for contingency planning
- Distinguish between security plans, contingency plans, and emergency plans
- List the elements and considerations for contingency planning
- Describe the role of an event operations center

Nuclear Security Regime

- One element is the

  PLANNING AND PREPAREDNESS FOR AND RESPONSE TO NUCLEAR SECURITY EVENTS

- Fundamental Principle K: Contingency Plans
  - Contingency plans to respond to unauthorized removal of nuclear material or sabotage of nuclear facilities or nuclear material, or attempts thereof, should be prepared and appropriately exercised by all license holders and authorities concerned.
- Recommended Requirements: 3.58-2.61

Definitions

- **Security Plans** – Based on design basis threat/threat assessment and include design, evaluation, implementation and maintenance of physical protection system and contingency plans

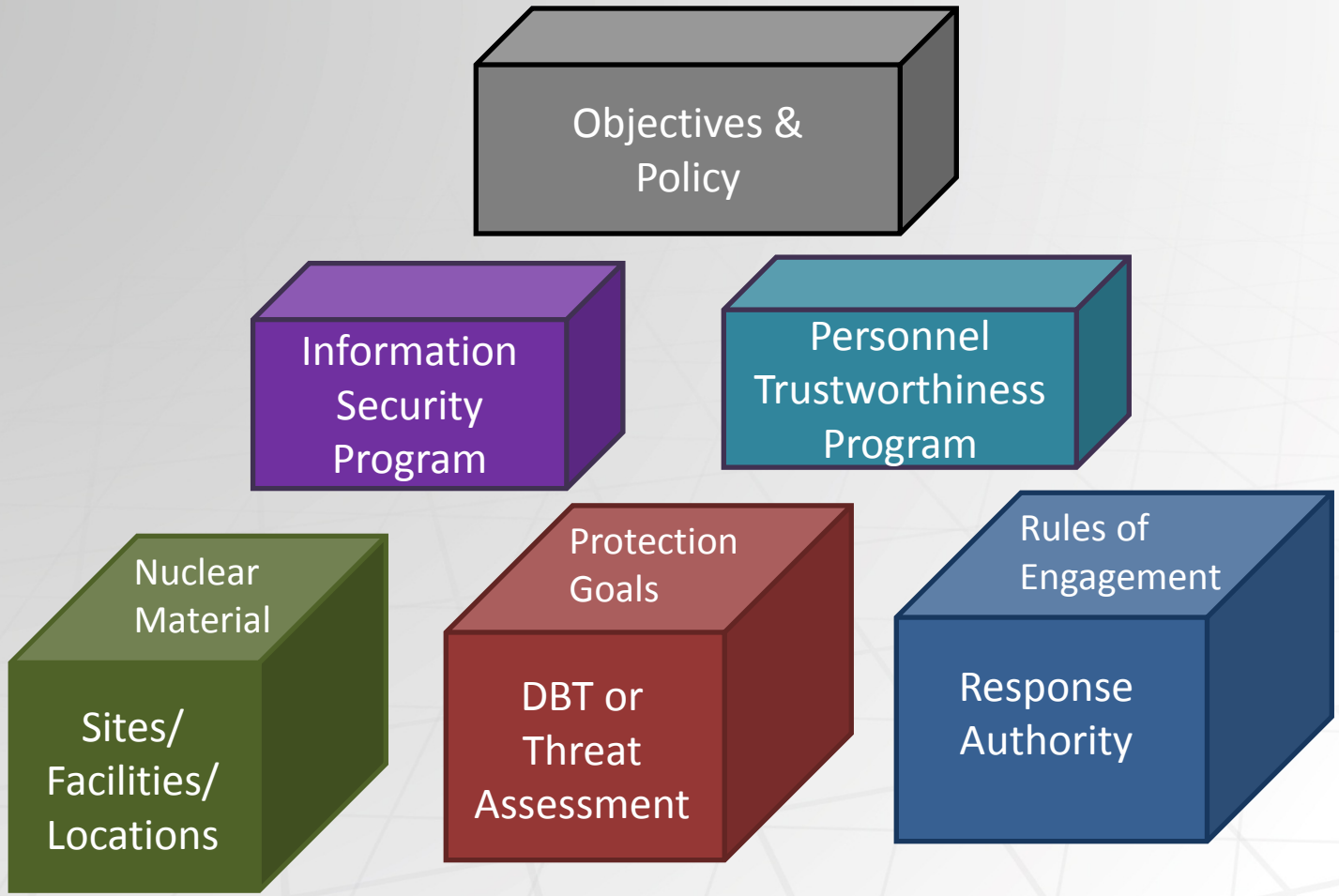
- **Contingency Plans** – Predefined sets of actions for response to unauthorized acts indicative of attempted unauthorized removal or sabotage, including threats thereof, designed to effectively counter such acts.

- **Emergency Plans** - Predefined sets of actions for response to safety events or other emergency events. Measures to ensure the mitigation or minimization of the radiological consequences of sabotage as well as human errors, equipment failures and natural disasters.

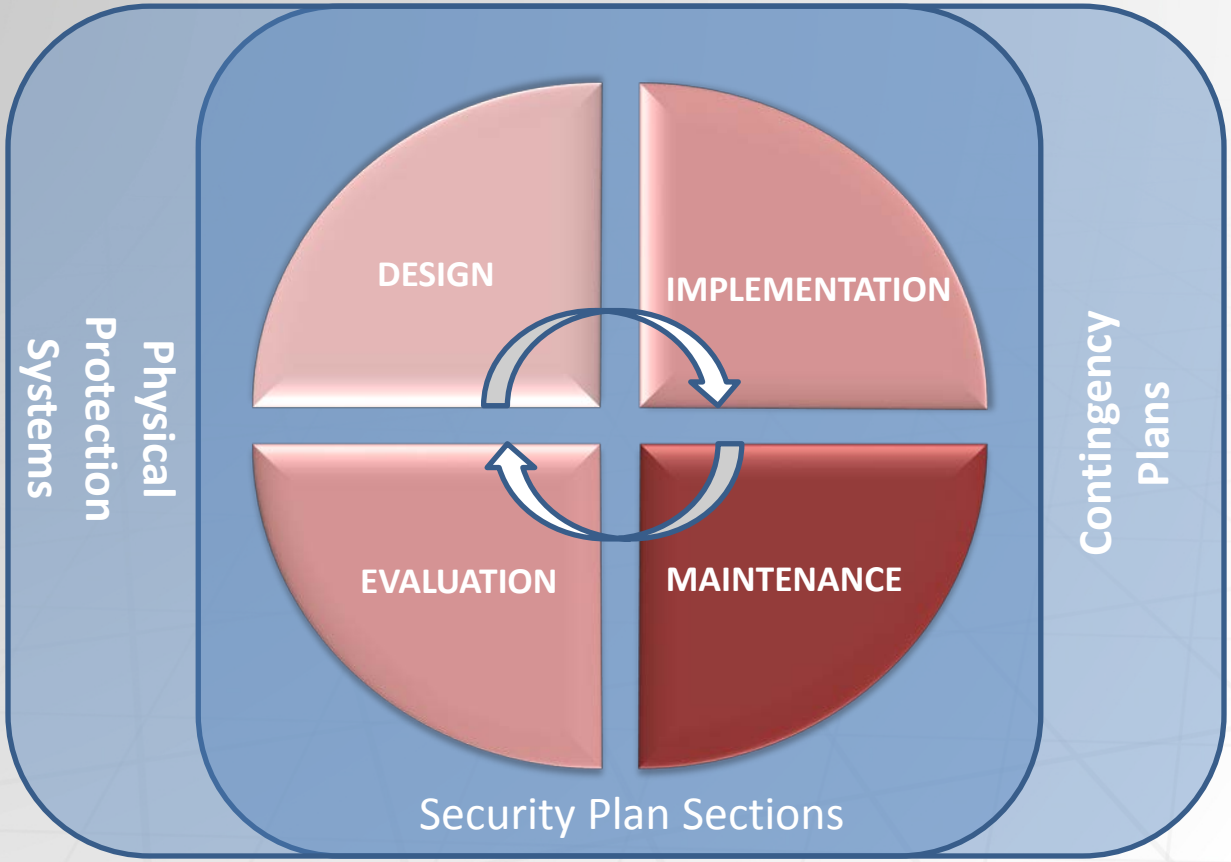
Examples

Contingency Plan Response to Security Events	Emergency Plan Response to Safety/ Emergency Event
Protestors at the facility	Fire on site
Criminal activity at the facility	Flooding
Hostage situation	Extreme weather with impacts to the site
Unauthorized removal of nuclear material	Loss of power
Sabotage of vital equipment	Loss of communications
Possible insider threat	Medical emergency

State Security Plans

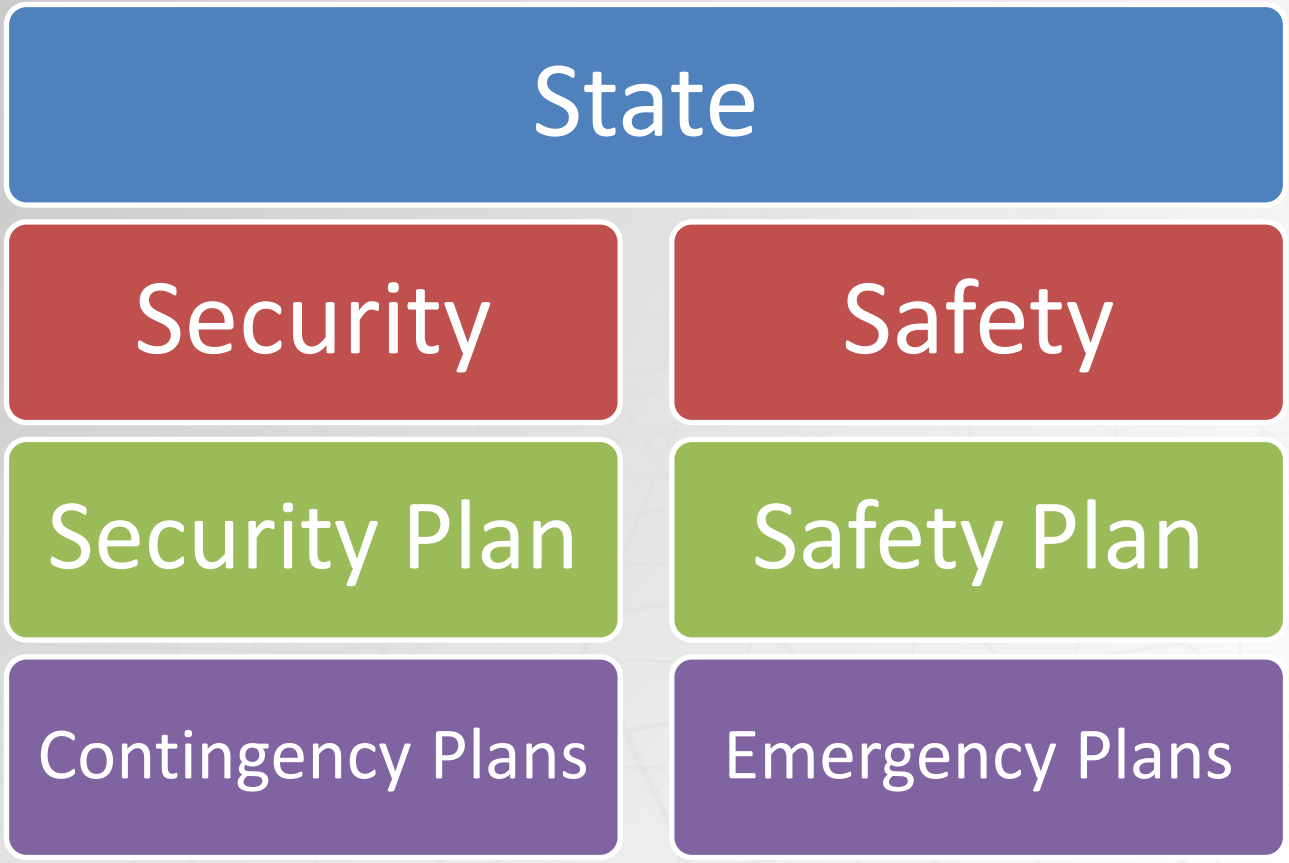


License Holder Security Plans Operators



- Part of an application to obtain a license
- Approved and verified by the competent authority
- Regularly reviewed and updated for changes approved by the competent authority

Contingency Plan Responsibilities



State Contingency Plan

Fixed Sites and Transportation

Locate and Recovery

- Defines the roles and responsibilities of appropriate State response organizations and operators
  - National Police
  - Hazmat Teams
  - Border Control
- Goal of rapid recovery and appropriate re-securing of material

State Contingency Plan

Fixed Sites and Transportation

Minimization/Mitigation of Sabotage Radiological Consequences

- Includes objectives, policy and concept of operation for all the response agencies
- Structure authorities, and responsibilities for a systematic, coordinated, and effective response
- Based on arrangements and protocols for coordinated implementation of measures for
  - Preventing further damage
  - Protecting emergency equipment and personnel
  - Onsite radiation protection for response personnel

Contingency Plan Responsibilities

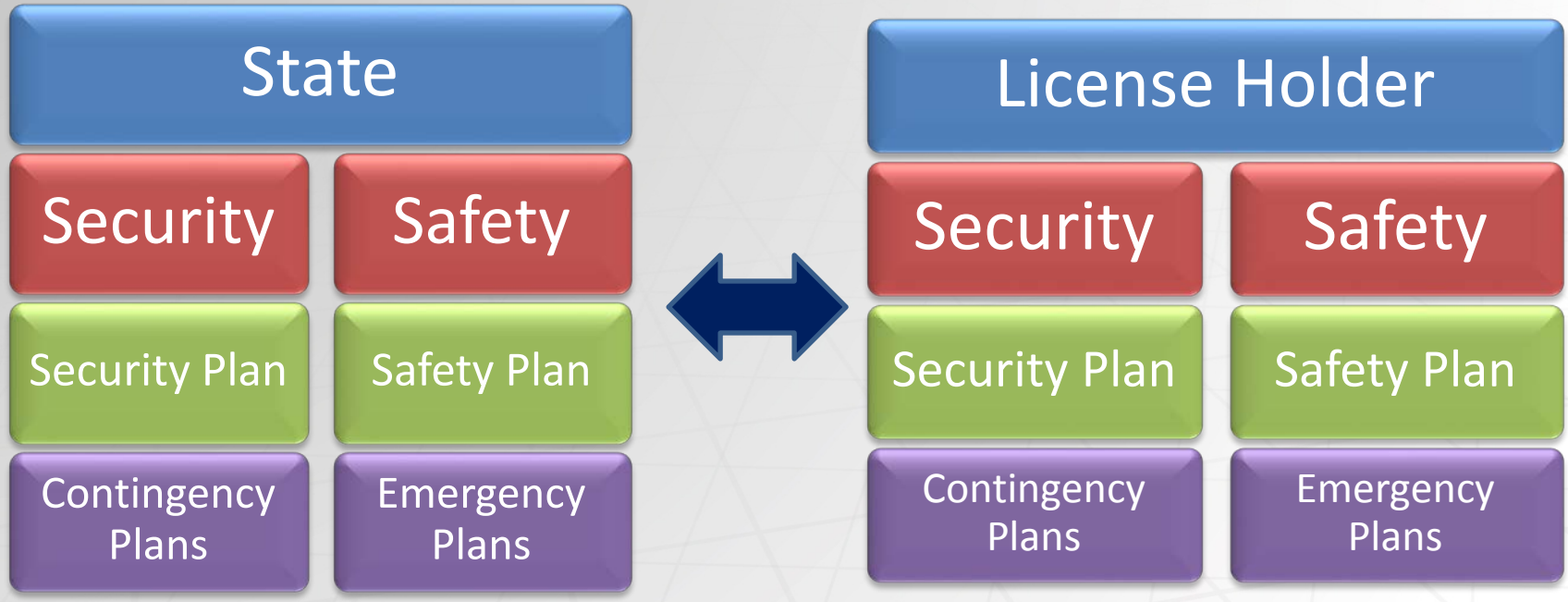
License Holder

Security	Safety
Security Plan	Safety Plan
Contingency Plans	Emergency Plans

License Holder Contingency Plan

- Implemented:
  - To protect against unauthorized removal
  - To locate and recover missing nuclear material
  - To protect against sabotage
  - To mitigate or minimize effect of sabotage
- Implemented after detection and assessment of a malicious act
- Should include the objectives, policy and concept of operation for response to a security incident
- Other requirements similar to those listed for State

State and License Holder Plans Should Be Consistent



Summary

- The Nuclear Security Regime includes contingency planning as part of a State's and Licence Holders Security Plan
- The Security Plan contains elements that pertain to the design, implementation, evaluation, and maintenance of contingency plans
- The Contingency Plan includes predefined sets of actions, including tactical contingency plans, for response to malicious acts during a security incident

Tactical Contingency Plans

Learning Objectives

Upon completing this section, participants should be able to:

- Identify the elements of a tactical contingency plan
- List the necessary topics of a communication protocol
- Describe important aids needed in a tactical approach

Tactical Contingency Plans

- Based on event type and prepared to counter or mitigate the event consequences.
- Includes – who, when, where, and what
- Should be well understood by all response forces
- Should include interfaces with safety (emergency plan)
- Should be periodically drilled/exercised such as
  - Security exercises
  - Fire drills
  - Evacuation drills
  - Shelter in place

Tactical Contingency Plans

- Should include concept of operations for the response to a security event or attempted security event
  - Guard and Response Force
  - Communication Protocols
  - Operational Considerations
  - Critical Paths
  - Tactical Approach Aids
- Incident Dependent

Tactical Contingency Plans

Response Forces

- Are they:
  - On-site
  - Off-site
  - Both
  - Off-site pursuit options
- Should understand:
  - Rules of Engagement
  - Use of deadly force and arrest authority
  - Knowledge of the targets
  - Coordination with off-site personnel
  - Transition from site to state level for recovery operations

Tactical Contingency Plans - Who

- Response Personnel Duties
  - Central Alarm Station personnel or other recipient of alarm
  - Guards
  - On-site Response Force
  - Off-site Response Forces
- Incident Response Personnel – Safety, Emergency, and Operations personnel
- Site Personnel

Tactical Contingency Plans - When

- When to respond
- When to change tactics
- When to escalate use of force
- When to notify other agencies
- When to communicate to the public

Tactical Contingency Plans - Where

- Where are mustering/coordination points
  - Onsite?
  - Off-site coming onsite?
- Where are response locations such as tactical positions for the situation?
- Where should response move to as the situation progresses?

Tactical Contingency Plans - What

Concept of operations for response

- Target consequence based response strategy (containment or denial)
- CAS operator duties
- For each type response personnel involved:
  - Procedures for what they must do including response area location, response time requirement, deployment tactics, rules of engagement
  - Communication protocols
  - Required Equipment (weapons, ammo, support equipment, vehicles, radios)
  - Facility recapture procedures

Other Decisions

- Can this malicious act lead to radiological consequences?
- What equipment or emergency personnel must be protected to minimize consequences?
- What are the overlaps between safety and security and which has priority?
- When is the incident over?

Communication Protocol

- Normal operations
- Duress
- Chain of command
- During an incident
- Phase response (dependent on type of alarm)
- Response force identifications (friend or foe)
- Situation reports
  - CAS to forces
  - Forces to CAS
- Emergency operations center

Operational & Adversary Considerations

- Site safety hazard areas
- No-shooting zones
- Likely site entry and escape routes
- Likely facility breach points
  - List of access points with descriptions (windows, doors, roof)
- Potential adversary vantage points

Critical Paths

- Critical path diagrams (with photos/video)
- Critical path elements
  - Interior/exterior
  - Glass size (wire)
  - Width/Height/Thickness
  - Lock type and door opening direction
  - Construction material
  - Keys and key control
  - Breaching means and tools

Tactical Approach Aids

- Selective shutoff and/or bypassing security/radiological/fire alarms
  - Sensor types and locations
  - Light types and locations
  - Activated barriers types and locations
  - Methods of turnoff
  - Personnel with access/control
  - Methods of bypass
- Ventilation shutoff/bypass
- Special breaching assist information
- Knowledgeable facility personnel

Summary

- A tactical contingency plan is based on an event type and prepared to counter or mitigate the event consequences.
- Communication protocol should be in place around numerous operational procedures.

Classes of Events

Learning Objective

At the end of this section, participants should be able to:

- Describe classes of events for consideration in developing contingency plans

Types of Events

- Malevolent
  - Nuclear security
  - Criminal
- Abnormal, Non-malevolent
  - Safety
  - Emergency
  - Off-site events
- Planned
- Other unplanned

General Considerations

- Different classes of events may require a different protocol in the contingency plan
- Priority of events as they relate to threat to
  - National security,
  - People (onsite and off-site)
  - Environment
- Chain of command for incident
- Chain of custody for prosecution
- Protection of forensics evidence

Nuclear Security Considerations

Theft of Nuclear Material

- Operator - Off-site pursuit to maintain line-of-sight of stolen nuclear material
- Carrier – Continued pursuit to maintain line-of-sight of stolen nuclear material
- State – Coordination with local law enforcement, national police/forces, border control

Nuclear Security Considerations

Sabotage of Vital Equipment

- If no radiological release
  - Continued security of the vital areas
  - Access control for recovery/repair of vital equipment
  - Access control for validation of operations
- If there is a radiological release
  - Access control to the area at a distance to meet radiation safety standards
  - Protection of safety and nuclear personnel

Other Malicious Acts

- Theft of other assets
  - Equipment
  - Proprietary Information
  - Money
- Sabotage of mission
  - Nuclear Power Plant Example
    - Power cannot get out
    - Power cannot be generated
    - Power cannot be accounted for

Other Malicious Acts

- Hostage Taking
- Active Shooter
- Trespassers such as protestors
  - Single
  - Several
  - Mob

Safety Events

- Events causing mass evacuations
  - Radiological release
  - Earthquake
  - Floods
  - Fires

- Events causing shelter in place
  - Extreme weather (high winds)
  - Off-site chemical release

- Hazardous Material

Emergency Events

Requires access to site and secure areas

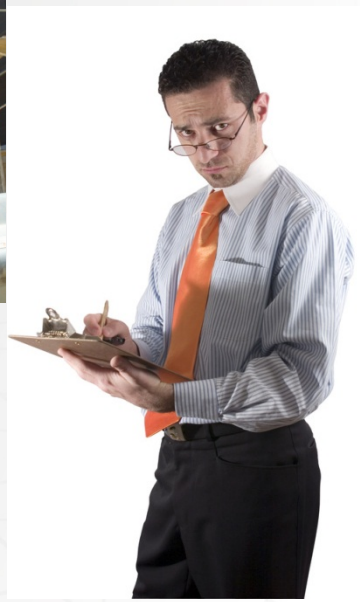
- By ambulance or medical staff for medical emergencies
- By fire trucks and firemen for fires near or on-site

Off-site Events

- Man-made or natural disaster
- Includes
  - Loss of power
  - Loss of communications (hardline, wireless, internet)
  - Loss of off-site water
  - Loss of heating/cooling
  - Loss of control systems due to malfunction
- Air, rail, water, or ground transportation incidents

Planned Events

- Official Visits
- Maintenance Visits
- Vendor Visits
- Regulatory Inspector Visits
- Grounds and Cleaning Crews



Other Unplanned Events

- Work Stoppages – Sickouts, Strikes, etc.
- No-notice inspections

Summary

- Different classes of events require different protocols for contingency plans.
- Each event requires a chain of command and a chain of custody.
- There should be a contingency plan for not just unplanned events but planned ones as well.



Incident Management

A Suggested Incident Management Methodology for Implementing Contingency Plans

Learning Objectives

Upon completing this section, participants should be able to:

- Describe the utility of an incident management system
- Identify organizations involved in incident response
- Match responsibilities to roles associated with incident management

Incident Response

- Incident response operations are not "business as usual"
- Anyone may be called to respond in an incident
- Incident response may require participation by multiple agencies and organizations

Definitions

- Incident Management System (IMS)
  - A model for command, control and coordination of a response.
  - Provides a means to coordinate the efforts of individual agencies as they work together towards the common goal of protecting life, property and the environment.
  - Provides a consistent framework for incident management at all jurisdictional levels regardless of the cause, size, or complexity of the incident.
- Emergency Operations Center (EOC)
  - A central location that supports Incident Command by making executive/policy decisions, coordinating interagency relations, dispatching and tracking requested resources, and collecting, analyzing, and disseminating information.
- Central Alarm Station (CAS) – Used to
  - Annunciate and assess security alarms
  - Initiate and coordinate security response forces
  - Coordinate with EOC as needed

Purpose of IMS

- Provide structure and coordination for incident stability
  - Standardized for all organizations involved
  - Common terminology, less jargon
- Provide for safety and health
  - Life safety
  - Property conservation
  - Environment protection

Goals of Incident Management

- General
  - Establishing command
  - Ensuring responder safety
  - Assessing incident priorities
- Developing an appropriate organizational structure
- Developing an Incident Action Plan and Safety Plan
- Maintaining an effective span of control by coordinating activities of all responding agencies
- Managing incident resources including costs
- Authorizing the release of information to the media

IMS Structure

- System Structure
  - Roles and Responsibilities under one incident commander or unified command
  - Implementation
  - Interagency Coordination
  - Command Structure
  - Training & Qualifications
- Builds as required for specific incident for facilities designated by name and description

Major Components

- Common terminology
- Modular organization
- Integrated communications
- Unity of command
- A unified command structure
- Single Incident Action Plan (IAP) and Safety Plan

Communication

- Common language and terminology
- Common communications plan
- Common frequencies
- Use of cellular phones is not recommended
- Ensure sensitive or secure information is not broadcast over radios or cell phones

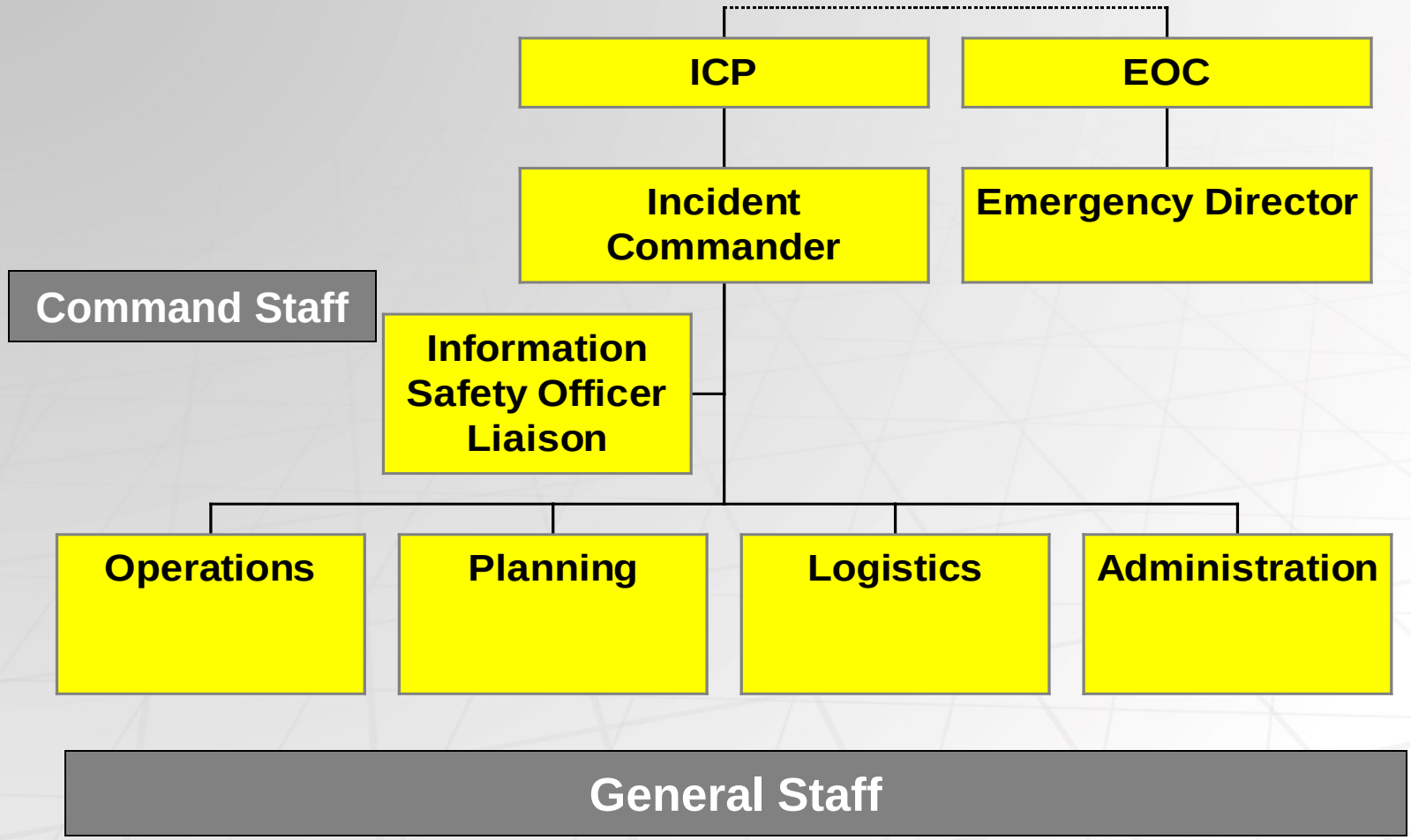
Span of Control

- How many people can be effectively managed?
  - Normally
  - Under incident conditions
- Three to seven subordinates

Modular Organization

- 95% of all incidents involved a command element and a single resource
- Special units can be added to address special needs
- Units no longer needed can be systematically released during different phases of the operations

Organizational Model



Position Titles

- Incident Commander
- Command Staff – support the incident commander
  - Safety Officer
  - Liaison Officer
  - Information Officer
- General Staff
  - Operations Section Chief
  - Planning Section Chief
  - Logistics Section Chief
  - Administration/ Finance Section Chief
- EOC supports the Incident Commander

Incident Commander

- Develops an appropriate organizational structure
- Maintains an effective span of control
- Manages Incident Resources

Safety Officer

- Has overall responsibility for Incident Safety
- Minimizes risks to personnel
- Reviews the Incident Action Plan
- Writes the Safety Plan

Liaison Officer

- Point of contact for assisting agencies
- This may include, local fire and police departments, and other organizations
- Usually not required for on site emergencies

Information Officer

- Compiles information for release to the news media
- Usually Public Affairs Personnel
- Information must be cleared through IC/ EOC

General Staff

- Support the Incident Commander
  - Operations Section Chief
    - Responsible for all tactical operations concerned with the IAP; the primary mission of the Incident Command System
    - May have Fire, EMS, and Facility Branches
  - Planning Section Chief - Collects and analyzes information used in developing the current, probable and alternative plans for the incident
  - Logistics Section Chief - Provides materials, resources, and facilities to support the incident
  - Finance/Administration Section Chief - Analyzes the financial and cost aspects of the incident and supervises the finance section, especially for incidents that may require State assistance

Other Positions

- Staging Area Manager
  - Reports to the Operations Section Chief
  - Stages equipment, personnel and other resources at an suitable area

- Facility Manager
  - Known as the Facility Command Leader
  - Responsible for providing information on incident, actions, and site specific hazards

Potential Response Agencies

- Law Enforcement
- Military
- Fire Department
- Ambulance
- Utility companies
- Public Works/Highway Department
- Emergency Management
- Specialty Teams

Resources & Specialized Teams

- Hazardous Devices Team (HDT)
  - Response for explosive or potentially explosive materials, packages, or chemicals
- Hazardous Materials Team (HAZMAT)
  - Response to any loss of control of hazardous materials
- Special Response Team (SRT)
  - Provides offensive special weapons and tactics
- Crisis Negotiations Team (CNT)
  - Perform negotiations with hostage-takers, barricaded subjects, terrorists or distraught personnel
- Critical Incident Stress Management Team (CISM)
  - Provides “psychological first aid” for personnel exposed to a critical or traumatic situation
- Radiological Emergency Medical Support (REMS)
  - Provides wound monitoring and decontamination assistance
- Emergency Technical Support Center (ETSC)
  - Provides Environment, Safety, & Health assessment expertise in the EOC

National Resources & Specialized Teams

- Accident Response Group (ARG)
  - To manage or support the successful resolution of a U.S. nuclear weapons accident anywhere in the world
- Aerial Monitoring System (AMS) NTS
  - Detects, measures and tracks radioactive material in an emergency to determine contamination levels
- Atmospheric Release Advisory Capability (ARAC)
  - Develops predictive plots generated by sophisticated computer models
- Federal Radiological Monitoring and Assessment Center (FRMAC)
  - Coordinates Federal radiological monitoring and assessment activities with State and local agencies
- Joint Tactical Operations Team (JTOT)
  - Specialized technical expertise to the Federal response in resolving nuclear/radiological terrorist incidents and other specialized capabilities
- Radiation Emergency Assistance Center/Training Site (REAC/TS)
  - Provides treatment and medical consultation for radiation injuries, also a training facility
- Radiological Assistance Program (RAP)
  - Usually the first responder for assessing the situation in a radiological emergency

Indicators of Poor IMS

- Lack of Overall Command Structure
- Nonstandard Terminology
- Nonstandard and Nonintegrated Communications
- Poor Resource Management
- Lack of Consolidated Action Plans
- Lack of Designated Facilities
- Lack of ability to expand or contract
- Freelancing

Summary

- Important to provide structure and coordination in order to maintain stability during the incident.
- Requires numerous staff members with different responsibilities to ensure structure is present.
- Response agencies should also be included as part of the organizational model.

Emergency Operations Center

In Support of the Contingency Plan

Learning Objectives

Upon completing this section, participants should be able to:

- Define the role of the emergency operations center
- Describe when incidents transition to emergency response
- Describe the role of the CAS during an incident response

Incident Commander Role

- Knows when to activate the EOC
  - Under what conditions
  - Based on resource requirements
  - Based on staffing requirements
  - Based on reporting, categorization requirements
- Understands role with the EOC
- Knows how to activate the EOC
  - Triggering factors
  - Request procedures
  - Alerting considerations

EOC Role

- Provides resources, planning and support to the Incident Commander
- Assists the Incident Commander with
  - additional information
  - support as the strategic objectives and goals are defined for the incident
- Networks through other organizations' EOCs for support and notification requirements

EOC Communications Role

- Key to providing accurate information between the Emergency Operations Center (EOC) primary room Emergency Director position and to the Incident Commander in the field
- Tasked to make notifications, transmit emergency information and gather information
- Communication Coordinators must keep the flow of information available so that decision makers can properly do their jobs

Role of the CAS

- Annunciate and assess security alarms
- During a security incident, serves as tactical operations commander
  - Gathering information about the incident
  - Coordinating communication with response personnel
  - Providing tactical options for incident resolutions
  - Ensuring that all tactical options comply with use of force policy
  - Maintaining written records and logs
- Initiate and coordinate with off-site security response forces
- Coordinate with EOC

Coordination with EOC During an Incident

- Getting any incomplete building information
- Communication of hazardous material
- Safety considerations
- Coordination with off-site agencies as needed
- Locating resources to assist in the incident
- Notifications to on-site and off-site
- Classification guidance

Summary

- The emergency operations center provides information, planning and support to the incident commander.
- The EOC plays a vital role when it comes to communicating during the incident.
- The CAS serves as a tactical operations commander during a security incident and insures that information is gathered, communicated, and documented for records and logs.



Contingency Performance Testing

Learning Objectives

Upon completing this section, participants should be able to:

- State the definition and purpose of performance testing of contingency plans
- List testing options
- Describe the use of performance testing results

Definition and Purpose of Performance Testing

- Definition: "Testing of the physical protection measures and the physical protection system to determine whether or not they are implemented as designed; adequate for the proposed natural, industrial and threat environments; and in compliance with established performance requirements." INFCIRC/225/Revision 5
- Applies to PPS and contingency plans
- Purpose: Performance testing programs provide:
  - Assurance that the contingency plans and supporting systems are functioning at the appropriate level
  - Provides data for evaluation and contingency plan improvement

Performance Testing Options

- Tabletop Exercises
- Limited Scope Performance Tests
- Whole system exercises including Force-on-Force exercises

All provide training to their participants

Performance Testing - State

- State responsibility for competent authority to perform periodic or annual testing of site or carrier contingency plans
- Regular testing of contingency plans ensure the development, evaluation, maintenance and implementation of contingency plans (State and License Holder) are adequate

Performance Testing – License Holder

- Includes administrative and technical measures of the contingency plan as it relates to:
  - Detection
  - Assessment
  - Delay
  - Communications
  - Response
  - Implementation of procedures
- Validated by competent authority
- Check for compensatory measures/corrective actions for any previously identified deficiencies in the contingency plan
- Check for any physical protection system weaknesses discovered during the testing of the contingency plan
- Maintained by the site/carrier, consistent with State contingency plans
- Should prepare facility personnel to act in full coordination with guards, response forces, law enforcement, and safety response

Performance Testing - Transportation

- Assessed and validated by the competent authority
- Test State response organizations, carrier response and response of other relevant entities
- Regularly reviewed and updated
- Include interfaces with safety responders

Using Results to Understand Effectiveness

- Did the contingency plan response successfully address the event tested?
- Was the information gained in the performance test sufficient to properly assess and determine effectiveness?
- Were weaknesses in the contingency plan elements or response identified?
- Were weaknesses in the physical protection system identified?
- Were there any unintended consequences?

Using Results – Lessons Learned

- What worked
- What didn't work
- What can be done better to improve
  - Response times (various entities)
  - Response effectiveness
  - Communications between response entities

Impact of Training and Exercises

- Before incident
  - Provides understanding of roles and responsibilities
  - Provides familiarization with procedures and tactics to be used
  - Provides familiarization of the site and facilities
  - Provides guidance to operations personnel on how to react in these situations
- During incident
  - Everyone knows what to do and how to do it in an efficient and effective manner
- After incident
  - Provides the basis for evaluation and improvement
  - Incorporates and tests changes made due to lessons learned from previous training or exercises

Summary

- Contingency plans should be tested by the state, license holder, and the competent authority.
- Performance testing programs should provide:
  - Assurance that the contingency plans and supporting systems are functioning at the appropriate level
  - Provides data for evaluation and contingency plan improvement

Security Regime and Contingency Plan Exercise

1. The requirement for a Contingency Plan is listed in which Fundamental Principle?

2. What is the difference between a contingency plan and an emergency plan?

3. List four elements of a License Holder security plan.

4. List the four reasons a License Holder contingency plan is implemented.

5. True or False, State and License Holder Plans should **NOT** be consistent?

Tactical Plan Exercise

1. Describe the four components that should be present in a tactical plan.

2. True or False, Tactical plans should be practiced on a regular basis and be well understood by all response forces.

3. Name three areas that should be covered in a Communication Protocol.

4. Name one operational and one adversary consideration and explain its importance.

Classes of Events Exercises

1) Define the 4 types of events that should be planned for.

    1. _____
    2. _____
    3. _____
    4. _____

2) Provide 2 examples of each type of event

Incident Management Exercise

Identify who is responsible for each duty in the chart below.

(**IC**) – Incident Commander
(**SO**) – Safety Officer
(**IO**) – Information Officer
(**LO**) – Liaison Officer
(**GS**) – General Staff

Responsible Party	Responsibility
	Clearing information prior to the release of information to the media
	Develops overall organizational structure
	Analyzes financial and cost of the incident
	Manages incident resources
	Responsible for overall safety
	Maintains span of control
	Assisting agency point of contact
	Releases information to the news media
	Reduces personnel risk
	Provides materials, resources, and facilities to support the incident
	All operations concerned with the IAP

Emergency Operations Center Exercises

1) Describe the role of the emergency operations center.

2) List 4 ways that the CAS supports the EOC during an incident.

   1. _____
   2. _____
   3. _____
   4. _____

System Performance Testing Exercises

List 3 options for performance testing.

1. _____
2. _____
3. _____

List two things a performance testing program provides.

Name 2 things that performance testing should answer about how effective your system is.

1.

2.