Suspicious Activity Detection and Reporting

Security Threats and Suspicious Behavior

Security Threats and Suspicious Behavior

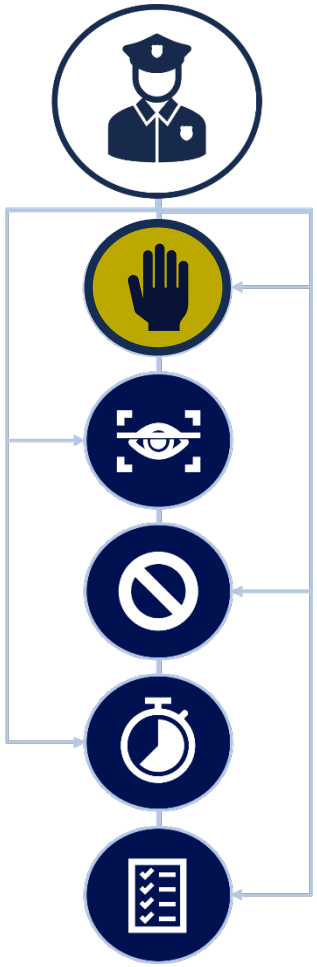


June 2024

V1.0

Agenda

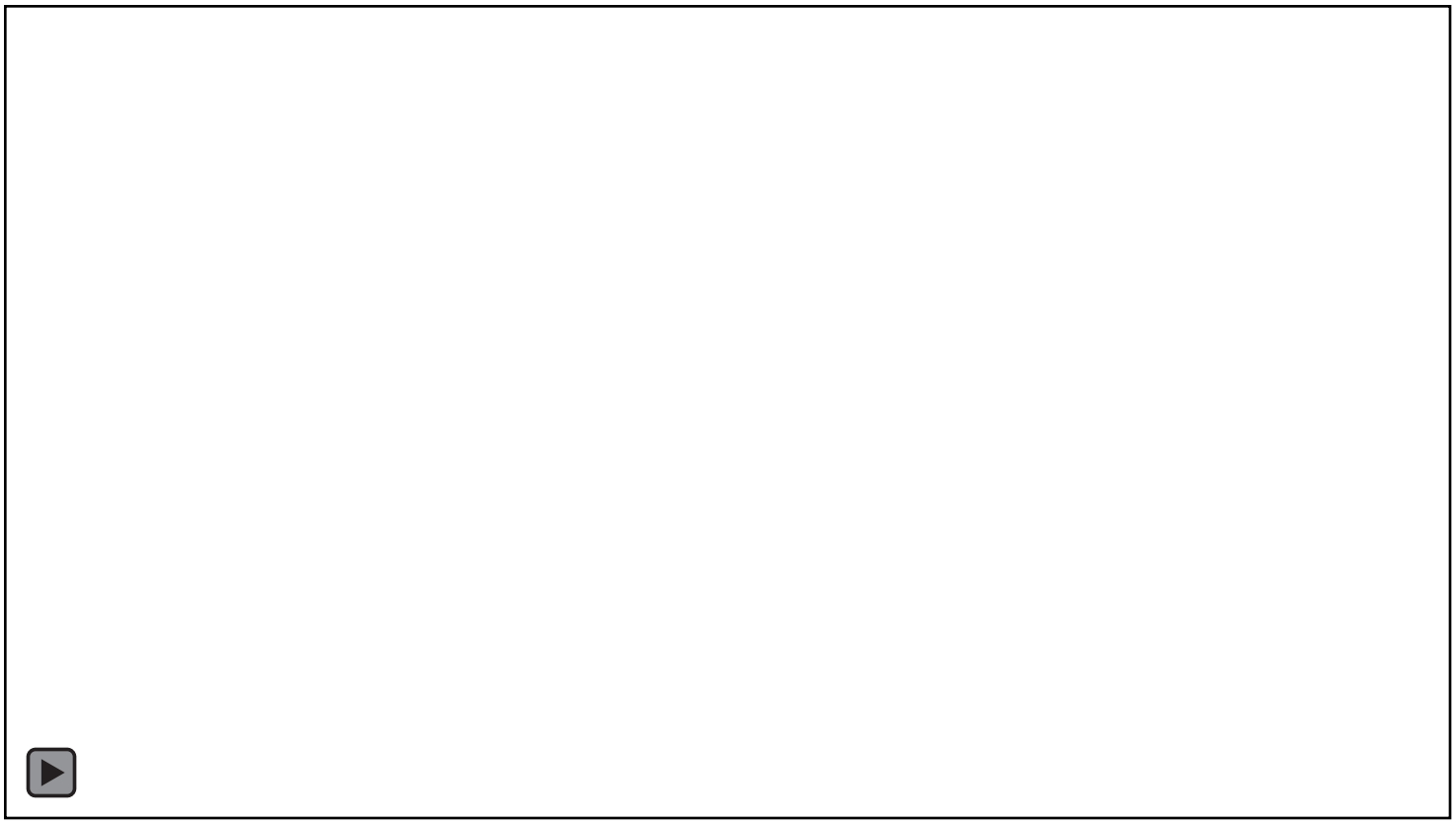
- Recognition Skills
- Security Threats and Suspicious Behavior
- Dangerous Goods and Substances
- Small Arms, Infantry Weapons, and Explosives
- Identification Skills
- Methods Used to Circumvent Security





Security Threats and Suspicious Behavior

Security Threats and Suspicious Behavior



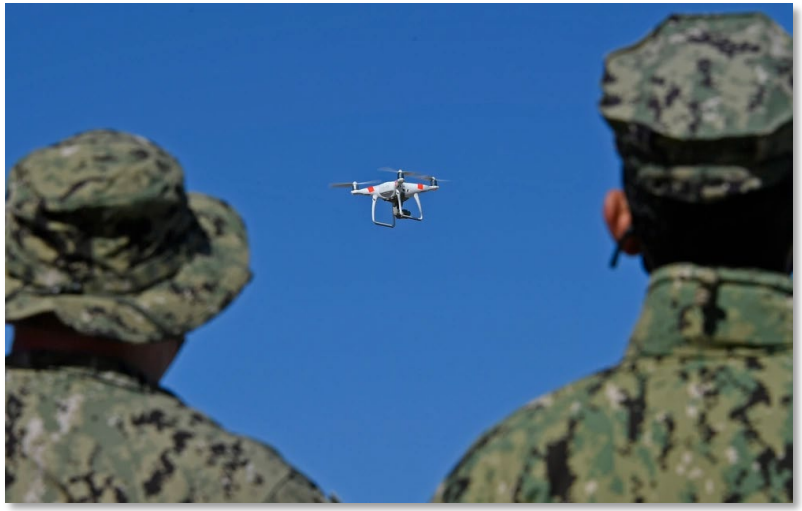
Video: Midnight Express

The Nature of Threats in Port Security

What is a threat?

- the likelihood that an unlawful act will be committed against a specific target, based on a perpetrator's intent and capability.

- Threats to port facilities can be:
  - land-based
  - sea-based
  - internal





Identifying Suspicious Activity and Behavior

Suspicious activity and behavior refers to the actions of an individual or group that fall outside what is considered normal for people in that particular area.



Asking Unusual or Unnecessary Questions



Not Wearing an ID Badge in Required Areas



Avoiding Security Personnel or Systems

Examples of Suspicious Behavior

Threat Categories and Identification Tools

Two Threat Categories

- Internal
- External

Knowledge is your primary tool for identifying suspicious activity and behavior.

- Know the people that work in and around the port facility
- Be aware of work routines (places, schedules, deliveries, etc.)
- Know your port facilities' vulnerabilities or valuables
- Recognize how others might circumvent security measures

Security Threats and Suspicious Behavior

Recognize the Signs (1)

- Expressed / Implied Threat
- Aviation Activity
- Photography
- Breach / Attempted Intrusion
- Theft / Loss / Diversion
- Gaining Skills
- Testing Security
- Eliciting Information

Security Threats and Suspicious Behavior

Recognize the Signs (2)

- Misrepresentation
- Cyberattack
- Recruiting / Financing
- Sabotage / Tampering / Vandalism
- Materials Acquisition / Storage
- Weapons Collection / Storage
- Section-Specific Incident

Responding to Situations

Not all suspicious activity is malicious but must be investigated according to Port Facility Security Plan (PFSP) procedures.

- Bags / Packages
  - Is the item clearly visible, or are there attempts to hide it?
  - Are suspicious items, like wires, showing?
- Identification
  - Does the person have a badge? If not, request to see it.
- Location
  - Who is the jurisdiction of authority?
- Support
  - If a person appears dangerous, call for support.

Dangerous Goods and Substances

Lessons Learned Through Tragedy

Anthrax Attacks, (September 18, 2001)

- Letters containing anthrax mailed to senators and news media offices
- Harm Caused:
  - 5 deaths
  - 17 people infected

Oklahoma City Bombing, (April 19, 1995)

- VBIED containing ammonium nitrate fuel oil and fertilizer used to target a federal government building
- Harm Caused:
  - 198 deaths
  - 720 + injured

IMDG Code

The International Maritime Dangerous Goods (IMDG) Code governs the majority of maritime hazardous materials shipments.

The IMDG Code is updated every two years. It provides ports with guidance including:

- Procedures port personnel must follow when handling dangerous goods and substances.
- A mandatory framework for handling dangerous goods and marine pollutants in sea transport.
- Requirements to maintain compliance applicable to individual substances and materials.

Hazardous Materials (HAZMAT) (1)

Class 1: Explosives



Class 2: Gases



Class 3: Flammable Liquid and Combustible Liquid



Class 4: Flammable Solid, Spontaneously Combustible, and Dangerous When Wet



Class 5: Oxidizer and Organic Peroxide



HAZMAT (2)

Class 6: Poison (Toxic) and Poison Inhalation Hazard



Class 7: Radioactive



Class 8: Corrosive



Class 9: Miscellaneous



Security Provisions and Storage Best Practices

Dangerous goods should be stored separately in secure locations and away from areas that may present security or safety concerns.

Storage areas should have security monitoring measures in place to prevent unauthorized entry.

- Surveillance system
- Adequate lighting
- Additional patrols
  - Dedicated guard
- Restricted access mechanism
  - Electronic card entry
  - Intrusion detection system.



Methods Used to Circumvent Security

Is Your Port Facility Secure?

All Security Systems Have Vulnerabilities

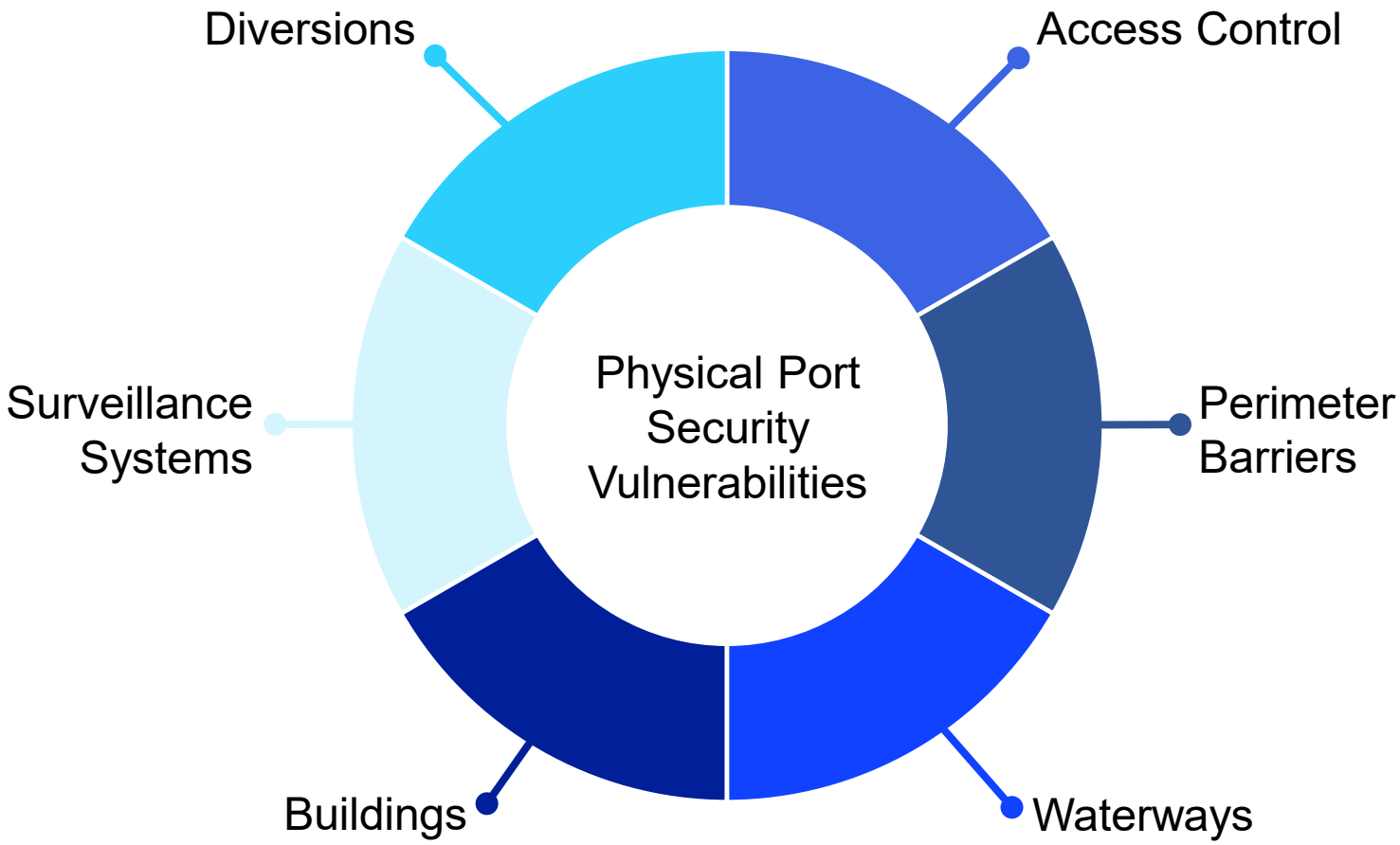
- Knowing your security system and how others might circumvent it is important to overcome vulnerabilities
- Individuals who seek unauthorized access to a port facility are often aware of its security vulnerabilities beforehand and plan accordingly





Methods Used to Circumvent Security

The Vulnerability Kaleidoscope Model



Methods Used to Circumvent Security

Access Control

- Fake or stolen identification
- Fraudulent authorization
- Stolen uniforms
- Skirting under or around personnel barriers and turnstiles



What can you do to limit individuals from taking advantage of port security access control vulnerabilities?

Methods Used to Circumvent Security

Perimeter Barriers

- Wall and fence meeting points
- Riprap, shoreline, ditch or culvert meeting points
- Areas with vegetation or soft soil
- Areas that are unlit, remote, or with no camera coverage



What can you do to limit individuals from taking advantage of port security perimeter barrier vulnerabilities?

Methods Used to Circumvent Security

Waterways

- Low profile or stealthy boats
- Swim, snorkel, scuba
- Appearing benign or routine (fishing, etc.)
- Dropping from a passing vessel



What can you do to prevent individuals from accessing the port facility by water?

Methods Used to Circumvent Security

Buildings

- Leaving windows open, breaking or cutting glass
- Leaving doors open, wedging doors, disabling latches
- Slipping behind others (“piggybacking”)
- Less secure back doors, loading docks, fire escapes, trash or storage rooms, etc.



What actions can you take to limit individuals from taking advantage of vulnerabilities in and around the port security buildings?

Methods Used to Circumvent Security

Surveillance Systems

- Cyber attack
- Cutting power feeds, data feeds, or disrupting wireless signals
- Disabling or masking cameras
- Disabling motion sensors



What actions can you take to limit individuals from accessing port security surveillance systems and/or disabling the system's cameras or motion sensors?

Methods Used to Circumvent Security

Diversions

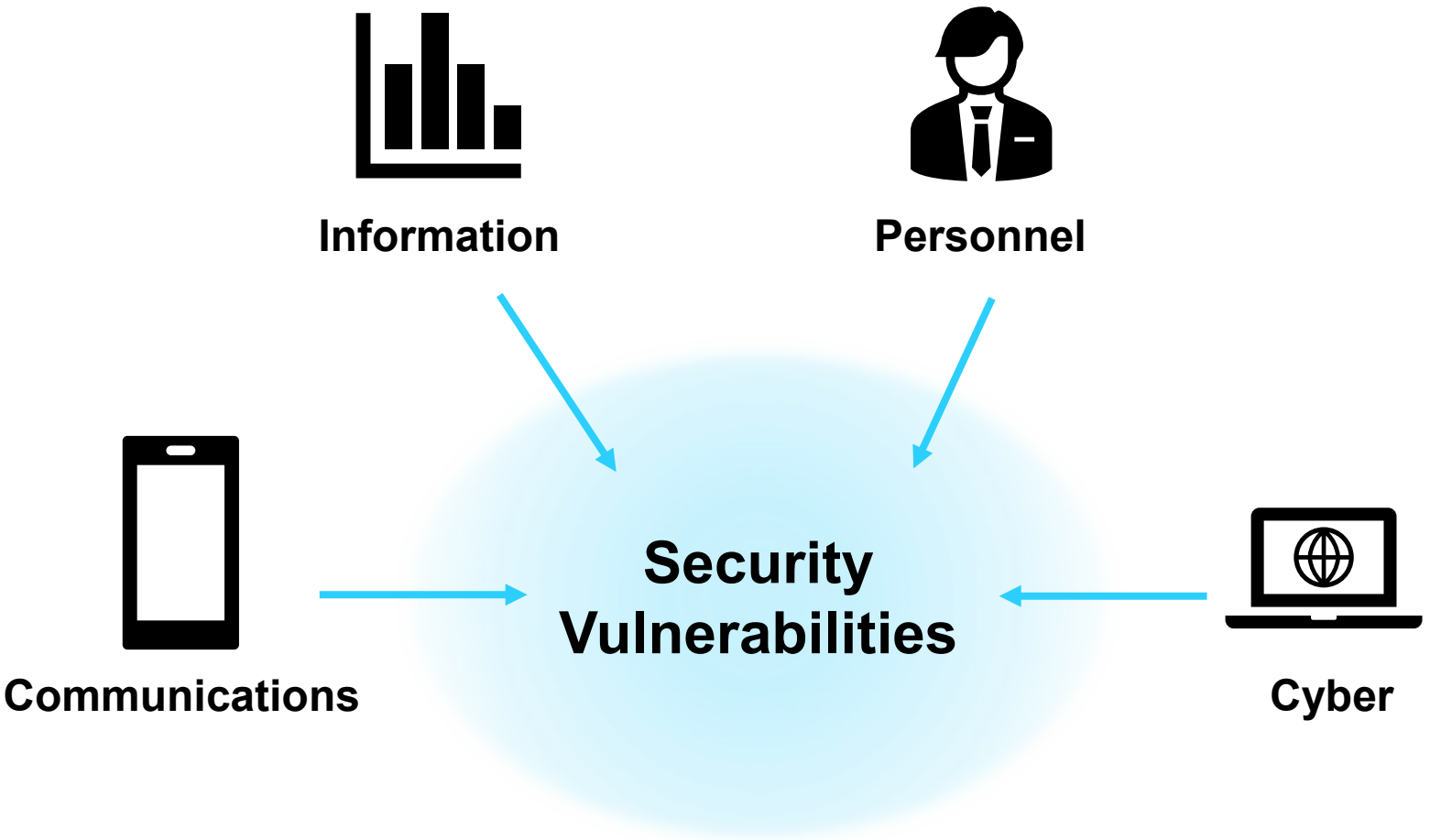
- Faking a medical emergency
- Faking an accident
- Penetrating multiple points at the same time
- Causing a disturbance (fight, fire, blown tire, bomb threat, etc.)

?

What actions can you take to limit an individuals' ability to create diversions or attempt unauthorized access to the port facility or other restricted areas?

Methods Used to Circumvent Security

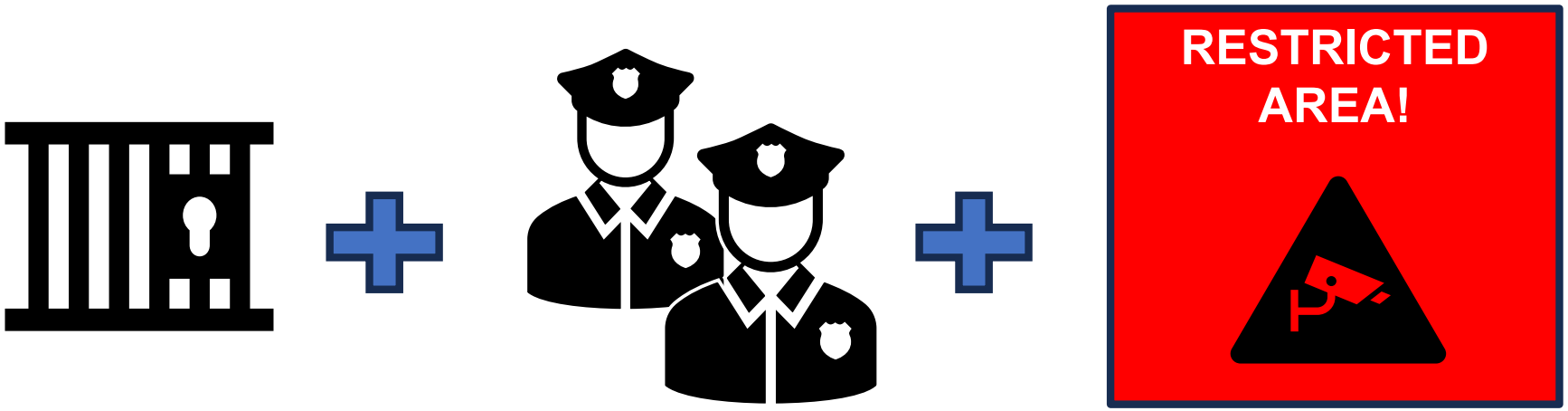
Additional Types of Vulnerability



Methods Used to Circumvent Security

Multiple Factor Authentication Systems

Any single, physical security measure can likely be beaten, but it is much more difficult to circumvent a system of multiple security measures.





Four Categories of Security Communications

Security Communications

Interagency communication is essential to establish robust communication procedures ensuring updates in security levels is provided without delay.

Communicate to

- Port facilities
- Ships
- Foreign-flagged ships
  - In port facilities
  - Intending to enter port facilities
  - Intending to transit their territorial sea

Four Categories



Set Security Levels



Communicate Threat Information



Communicate Security Incidents



Improve Security Awareness

Set Security Levels

- PFSO is the point of contact to receive security information from the national authority.
- Distribute immediately to:
  - Port facility security personnel
  - Port facility operations personnel
  - Port facility management officials
  - Security personnel on all vessels moored at the port facility
- Implement the security level in accordance with the PFSP.



Communicate Threat Information

- Establish a system and mechanisms to rapidly transmit threat information to:
  - Port facility security personnel
  - Port facility operations personnel
  - Port facility management officials
  - Security personnel on all vessels moored at the port facility



Communicate Security Incidents

- Document procedures to report security incidents
- Reporting may include:
  - Facility-level: All incidents
  - Authorities: Serious security incidents
- PFSO conducts an investigation of the incident.



Discussion

How serious is an incident?

- Does the incident impact only my facility?
- Does the incident impact global security?



How Serious is …

Less Serious

Suspicious packages in / near facility

More Serious

Report to PFSO

Report to Authorities

Security Communications

Discussion

How serious is an incident?

- Does the incident impact only my facility?
- Does the incident impact global security?



How Serious is …

Less Serious

Unauthorized disclosure of the PFSP

More Serious

Report to PFSO

Report to Authorities

Examples of Security Incidents

Less Serious Security Incidents

- Breaches of screening points
- Inappropriate uses of passes
- Damage to security equipment through sabotage or vandalism
- Suspicious behavior in/near the facility
- Suspicious packages in or near the facility
- Unsecured access points

Serious Security Incidents

- Unauthorized access to restricted areas
- Unauthorized carriage or discovery of weapons or prohibited items
- Incidents with media awareness
- Bomb warnings
- Unauthorized disclosure of the PFSP

Improve Security Awareness

- Establish / lead Security Awareness Program.
- Establish a system of communication, with focuses on:
  - PFSP requirements.
  - Port facility security policies and procedures.
  - Contingency plan provisions.
  - Recognition of security threats.



Threat Awareness Communications

The PFSO should provide frequent communication to Security Personnel on how to recognize a security threat.

Communications focus on

- Techniques to circumvent security measures
- Weapons, dangerous goods, and devices
  - Recognition
  - Awareness of impact
  - Security-related provisions
- Crowd management and control techniques
- Behavioral characteristics
  - Recognition of behavioral patterns / characteristics of people

Reporting Standards

Every port must have a standardized report format for filing an incident report.

File a report when:

- Security measures have been circumvented, eluded, or violated.
  - Includes Cyber
- Security incidents require activation of procedures from the security plan.
  - Loss of life, environmental damage, transportation system disruption, economic disruption

Develop retention policies for reports previously filed.

Report Components

- Date
- Time
- Personnel Involved
- Detailed description of the breach
- Indicate whether the breach caused an incident
- Security measures implemented to address the incident
- Did existing security measures prevent or mitigate negative impact of the incident?