

LECTURE 7

7.0. ACCESS CONTROL IN PORTS

Facilitating access to port facilities while maintaining smooth passenger operations, international trade, and recreational activities presents significant challenges. Ports, integral to national and local economies, are attractive targets for criminal activity and terrorism due to their critical infrastructure and economic importance. Damage to port facilities can result in loss of life, environmental harm, and severe disruptions to commerce. This highlights the necessity of implementing robust access control systems and protocols to safeguard these vital areas.

Effective security begins with controlling who and what is allowed entry. Port facilities must strike a balance between operational efficiency and maintaining a clear understanding of individuals and vehicles entering their premises. Just as homeowners screen visitors for safety, ports must develop systems to verify and monitor access to mitigate risks. Although eliminating all threats may not be possible, proactive measures like background checks and monitoring can significantly reduce vulnerabilities. Similarly, a comprehensive approach to identifying, screening, and managing entry points helps address the inherent risks of open systems like seaports.

This discussion focuses on two key elements of port access control: identification and credentialing and restricted area access controls. Identification and credentialing involve systematic processes to verify who is authorized to enter the port. Restricted area access controls include physical infrastructure, procedures, and systems designed to screen and monitor access effectively. Together, these measures create a multilayered defense against potential security threats.

To minimize risks, security measures include thorough background checks, employer authorization verification, and strict enforcement of identification protocols. Additionally, screening vehicles and pedestrians, maintaining an alert security team, and scrutinizing credentials further strengthen port defenses.

VULNERABILITIES IN PORT ACCESS CONTROL

» Frequency of Access

Maintaining awareness of who and what enters port facilities is critical. Frequent access by individuals can expose vulnerabilities, as regular visitors may develop detailed knowledge of port operations, security systems, and personnel. Such familiarity could be exploited by criminals or terrorists. Ports must prioritize understanding the purpose and frequency of access to safeguard against these risks.

Frequent access also increases the chances of criminal conspiracies, as individuals with insider knowledge may identify and exploit weaknesses in security measures. Terrorists and smugglers often mimic traditional smuggling operations to test and bypass port security systems, using these gaps to transport contraband or weapons.

To counteract these threats, ports can implement measures such as:

- Conducting criminal history checks on employees and port users.
- Requiring employer authorization letters to validate employee relationships.
- Enforcing strict credentialing protocols.
- Screening vehicles and individuals thoroughly.
- Training security personnel to respond to potential threats.

» Advance Notice Requirements

Advance notice of arrivals—whether for vessels, cargo, or personnel—provides a crucial layer of security. By knowing who and what is coming to the port, security teams can assess and address potential risks based on factors like cargo type, passenger numbers, and countries of origin or registration.

Regulations in the U.S. require advanced electronic transmission of manifests for passengers and crew. For example:

- Ships departing foreign ports for the U.S. must submit manifests 24–96 hours before arrival.
- U.S.-bound cargo manifests must comply with the Maritime Transportation Security Act (MTSA) of 2002 and the Trade Act of 2002, ensuring electronic submissions well in advance.
- Vessels arriving from foreign or domestic locations must file Notices of Arrival through the U.S. Coast Guard's National Vessel Movement Center.

These systems enable ports to anticipate and mitigate potential threats before individuals, cargo, or vessels arrive, reducing vulnerabilities at the transportation interface.

» Collaborative Security Resources

The U.S. Department of Homeland Security has developed numerous tools and partnerships to enhance port security. By collaborating with agencies like Customs and Border Protection and the Coast Guard, port management can leverage advanced screening systems and regulatory frameworks to minimize risks associated with incoming materials and individuals.

IDENTIFICATION AND ACCESS CONTROL AT PORTS

Ensuring robust access controls is a critical aspect of port security. Identification and credentialing processes are integral to the facility security plan (FSP) to address vulnerabilities. Employees, contractors, and regular visitors, including vendors and service personnel, must be identified to manage and limit access to restricted areas. Port identification cards serve as a foundational tool for tracking individuals and activities at the facility. Port authorities must maintain comprehensive records of personnel and organizations associated with the port while implementing screening measures to ensure that individuals granted credentials are authorized by their employers.

PHOTO IDENTIFICATION AND CREDENTIALS

Providing photo identification badges to authorized individuals is essential for controlling access. These credentials, such as badges or cards, must be displayed visibly at all times when accessing or working in restricted areas. Identification systems should include:

- **Permanent Credentials:** For employees with ongoing, frequent access, issued for a defined validity period.
- **Temporary Credentials:** For short-term workers or contractors, issued with an expiration date aligned with the project timeline.
- **Visitor Passes:** For one-time access, specifying whether the visitor is escorted or unescorted.

Key features of identification badges include a current photograph, the individual's name, date of birth, physical description, employer's name, and a unique ID number. Security procedures must address the issuance, renewal, and retrieval of badges to ensure proper control.

BACKGROUND SCREENING AND CRIMINAL HISTORY CHECKS

Credentialing systems may incorporate criminal history background checks for all applicants. Where permitted by law, these checks can exclude individuals with criminal records that indicate a potential security risk. Many jurisdictions mandate such checks for employees working in sensitive areas. For example, U.S. and U.K. regulations require criminal record screenings for employees accessing restricted areas of transportation hubs, emphasizing compliance with national and local legislation.

BIOMETRIC TECHNOLOGY AND ADVANCED CREDENTIALING

The Transportation Worker Identification Credential (TWIC) is a notable example of a uniform system incorporating biometric identifiers such as fingerprints. Administered by the Transportation Security Administration (TSA) and U.S. Coast Guard, TWIC cards facilitate secure, tamper-resistant identification for individuals requiring unescorted access to secure areas of ports and transportation facilities.

While TWIC ensures a standardized background screening process, port authorities maintain the discretion to grant access to specific facilities. TWIC readers, which validate biometric data, are being pilot-tested at various locations, with full implementation dependent on infrastructure and operational needs.

CREDENTIALING SYSTEMS AND PROCEDURES

Credentialing systems at ports should classify individuals based on their access requirements:

1. **Permanent Employees:** Granted wide-ranging access, with restrictions during off-hours or non-operational times.

- 2. Temporary Workers:** Issued credentials for specific durations, with logs maintained for lost or stolen badges.
- 3. Port-Related Businesses:** Employees of companies operating at the port but not requiring access to restricted areas.
- 4. Ship Crews:** Issued limited credentials to transit between vessels and public areas.
- 5. Passengers and Visitors:** Categorized and provided appropriate credentials for restricted or public areas, with specific protocols for large groups.

CREDENTIAL CLASSIFICATION AND CODING

To enhance efficiency, credentials should be coded visually, such as through color schemes, to indicate access levels and areas. Security personnel should be equipped with tools and references to verify access permissions quickly.

INFRASTRUCTURE AND SYSTEM REQUIREMENTS

Port access systems must accommodate a variety of scenarios, from pedestrian gates to vehicle access points. Biometric readers should be strategically deployed to support seamless verification processes. Additionally, facilities should invest in adequate infrastructure, such as kiosks and enclosures, to house biometric and credential verification equipment effectively.

VISITOR MANAGEMENT

Visitor credentials must clearly indicate escort requirements and display instructions for proper usage. Procedures for reporting lost or stolen badges and guidelines for returning temporary credentials are crucial to maintaining security standards.

By integrating robust identification, credentialing, and biometric systems, ports can better safeguard their restricted areas, ensuring compliance with evolving regulations while minimizing security risks.

PRODUCTION PROCESSES

Identification cards should be created using methods that ensure durability and resistance to tampering. If credentials are not durable, they may fade, warp, or become unreadable over time. To mitigate these issues, production systems should generate laminated credentials that resist deterioration. Using tamper-evident materials can make unauthorized alterations apparent. Staff responsible for verifying credentials should receive training to identify altered or damaged cards. Procedures must also require individuals with damaged credentials to return them for replacement.

CREDENTIAL SEQUENCING

Port identification cards should be issued in sequential order to enhance control and accountability.

Sequential issuance enables administrators to track lost or stolen credentials and maintain better inventory management. Maintaining strict accountability for issued credentials reduces risks associated with stolen cards being used for illegal activities. Personnel responsible for ordering card stock should ensure proper sequencing to avoid unnecessary expenses, especially in systems involving electronic data embedded in credentials.

LOST OR STOLEN CREDENTIALS

Policies should mandate the reporting of lost or stolen port identification cards. Cardholders must be instructed to report such incidents formally. Ports may require a police report to accompany reissuance requests. This documentation provides law enforcement with a way to track lost credentials and adds legitimacy to the reissuance process.

ROLE OF PORT USERS IN CREDENTIALING PROGRAMS

Port employees and users play a vital role in mitigating risks and ensuring secure access to restricted areas. The following responsibilities apply to cardholders:

- **Keep credentials up to date:** Expired credentials should be renewed promptly to avoid access issues and security vulnerabilities.
- **Display credentials visibly:** Employees must always carry and visibly display their credentials. Security personnel may question individuals who fail to do so.
- **Managerial oversight:** Supervisors must ensure all team members adhere to credential rules. Visible enforcement of these policies is essential to maintaining a secure environment.
- **Zero tolerance for violations:** Non-compliance with credential rules should result in restricted access to port facilities.

VISUALIZING AND INSPECTING ACCESS CREDENTIALS

Security personnel must be trained to inspect credentials thoroughly and confirm their validity. Key areas of focus include:

- **Verifying credential details:** Inspectors should confirm the information on the card, such as the name, date of birth, employer, physical description, and expiration date.
- **Comparing photographs and descriptions:** Inspectors should ensure the photo and physical description match the cardholder. Practical exercises, such as drills or red teaming, can enhance screening skills.
- **Identifying counterfeit or altered cards:** Personnel should be familiar with the design and features of authorized credentials. Training should include examples of how unauthorized modifications might appear.

VISITOR CONTROLS

Clear procedures must govern visitor access to secured port areas. Key considerations include:

- Visitors should be authorized and limited to specific areas relevant to their business.
- Valid government-issued photo identification, such as a driver's license or passport, should be required for issuing visitor credentials.
- Visitor credentials must be temporary, with clear expiration times and visible placement on outer garments.
- Visitor vehicles should have temporary identification documents and comply with parking regulations.
- Visitors accessing restricted areas must display valid credentials and remain escorted by authorized personnel.
- All visitors are subject to local, state, and federal regulations while on port property.

VISITOR BROCHURE

Visitors should receive an informational brochure outlining security and safety policies, including:

- **Security policies:** Overview of access control measures and restricted area protocols.
- **Credential requirements:** Examples of acceptable identification and information on security screening processes.
- **Port information:** Maps, transportation details, and guidelines for reporting suspicious activity.
- **Regulations and restrictions:** Information on prohibited items, smoking, and the use of cameras or electronic devices.
- **Emergency procedures:** Contact details for reporting emergencies or requesting assistance.

By adhering to these practices, ports can maintain a secure and efficient environment for employees, visitors, and operations.

ACCESS CONTROL IN RESTRICTED PORT AREAS

Effective access control is a critical aspect of maintaining security at port facilities. This involves establishing protocols to determine who, what vehicles, and what materials are allowed entry. Such measures may include issuing ID cards for employees and visitors, requiring advance delivery notifications, and conducting thorough screenings of vehicles, pedestrians, and cargo.

BALANCING SECURITY AND OPERATIONAL EFFICIENCY

Achieving security without disrupting port operations is a complex challenge. Port administrators must establish access control measures that strike an optimal balance between safeguarding the facility and ensuring smooth commercial activities. Overly strict access controls could drive users to alternative ports.

Involving port stakeholders in developing realistic security measures fosters collaboration and ensures the design of practical access control systems.

DEFINING RESTRICTED AREAS

Port administrators must identify and designate restricted access zones within the facility. These areas should be clearly marked and only accessible to authorized personnel. Key restricted zones include:

- 1. Cargo Storage Areas:** Locations such as container yards, warehouses, and staging areas must be secured to prevent tampering, theft, or illegal activities related to cargo.
- 2. Dock and Wharf Areas:** Access to these zones should be limited to essential personnel to prevent unauthorized access to cargo, vessels, and luggage. Screening and security measures should ensure these areas remain secure.
- 3. Fuel Storage Facilities:** Ports housing fuel storage and transfer stations must restrict access to authorized personnel only, to prevent misuse or sabotage.
- 4. Passenger Terminals:** Cruise and ferry terminals must be safeguarded to protect both passengers and vessels. Only passengers and designated staff should have access.

All restricted areas must feature prominent signage and barriers to inform and deter unauthorized access. These warnings should outline applicable laws and potential penalties.

GATES AND ENTRY POINTS

Gates play a central role in controlling access between restricted and general areas. Entry points should be designed to support security without impeding port operations. Measures may include physical barriers, ID checks, surveillance cameras, security personnel, alarms, and adequate lighting.

PREVENTING UNAUTHORIZED ACCESS

Ports must proactively address vulnerabilities that could lead to unauthorized entry. This includes ensuring security personnel are well-trained and vigilant. Supervisors must regularly monitor compliance with access control protocols. Repeated security breaches should prompt immediate staff retraining to reinforce the importance of their roles and responsibilities.

CONTROLLING VEHICLE ACCESS

The movement of vehicles within restricted areas, such as cargo docks and wharves, must be strictly controlled. Unauthorized vehicles, including personal vehicles, are generally prohibited unless explicitly permitted for specific tasks, such as construction or maintenance. Temporary access credentials can be issued when needed, ensuring proper identification and adherence to regulations.

SCREENING VEHICLES AND PEDESTRIANS

All individuals and vehicles entering restricted areas must undergo rigorous screening to detect weapons, contraband, or hazardous materials. Security personnel must be trained to identify potential threats, including improvised devices or materials that could be weaponized. Screening protocols should utilize tools such as metal detectors, x-ray machines, and handheld scanners to enhance effectiveness.

SUSPICIOUS INDICATORS

Effective screening also requires awareness of behavioral patterns that may indicate malicious intent. Security teams should remain alert to individuals seeking unauthorized access or gathering information on facility layouts, entry points, or security measures. Suspicious activity should be promptly reported to authorities.

ENHANCING SCREENING WITH TECHNOLOGY

Specialized equipment like metal detectors, x-ray scanners, and vehicle imaging systems can bolster security efforts. These technologies streamline the process of inspecting people, cargo, and vehicles, reducing the likelihood of threats bypassing security checkpoints.

MANAGING DELIVERY OF VESSEL PROVISIONS

Delivery vehicles supplying provisions to vessels must comply with strict screening procedures. Advance notification, driver identification, and thorough inspections of both vehicles and provisions are essential. Digital solutions, such as password-protected platforms, can facilitate coordination between vendors and port authorities, enhancing efficiency while meeting regulatory requirements.

COMPREHENSIVE ACCESS CONTROL MEASURES FOR PORT FACILITIES

Effective access control is critical for ensuring the security of port facilities. Guidance for such measures has evolved significantly, especially with the introduction of the Maritime Transportation Security Act (MTSA) and related advisories. These measures aim to safeguard restricted and operational areas while supporting compliance with regulatory standards.

KEY MEASURES FOR CONTROLLING ACCESS

To ensure effective access control, facilities should incorporate the following strategies:

1. Reduce Access Points

Limit the number of entry points by closing unused gates and funneling all traffic through critical access areas. This helps concentrate monitoring efforts and reduces security vulnerabilities.

2. Monitor and Secure Entrances

Use a combination of physical barriers, electronic surveillance, and personnel to oversee all entry points, ensuring they are continuously monitored and controlled.

3. Screen and Inspect Thoroughly

Implement procedures to inspect vehicles, cargo, packages, and personnel entering the facility. Credentialing systems should be in place to verify identities and track access.

4. Deny Access for Noncompliance

Refuse entry to individuals or vehicles that fail to comply with security requirements, referring such cases to law enforcement as necessary.

5. Restrict Access to Authorized Personnel

Employ credentialing systems to grant access only to verified employees and authorized visitors with valid identification.

6. Control Parking Areas

Designate specific zones for parking and enforce restrictions through permits or similar systems to regulate vehicle access.

7. Restrict Vessel Access

Allow only authorized individuals, including crew members, passengers, and approved service providers, to access vessels.

8. Coordinate Arrivals and Activities

Schedule vessel arrivals and operations in advance to ensure heightened awareness and reduce the risk of unauthorized activities.

9. Establish Physical Boundaries

Use fences, barriers, and clear signage to define restricted areas and create physical and visual separation from public zones.

10. Implement Visitor Escort Procedures

Require escorts for contractors, vendors, and other non-facility personnel to maintain oversight of their movements within the port.

ENHANCING SECURITY THROUGH TECHNOLOGY AND COMPLIANCE

Port facilities must strike a balance between robust security and operational efficiency. Given the critical role ports play in economic and logistical networks, they are potential targets for unauthorized access or malicious activities.

To mitigate risks, facilities should consider:

- **Identification and Credentialing Systems:** Implementing durable, tamper-resistant credentials with access-level classifications ensures that only authorized individuals gain entry to restricted areas.
- **Advanced Scheduling and Monitoring:** Pre-arranged schedules for personnel and activities help minimize vulnerabilities.
- **Screening and Inspection Tools:** Technologies like metal detectors, X-ray systems, and handheld wands enhance the detection of unauthorized materials or individuals.

- **Regulatory Compliance:** Adhering to MTSA-mandated requirements, such as the screening of vehicles delivering goods to vessels, ensures consistent and lawful security practices.

// CONCLUSION //

A robust access control system integrates physical security measures, advanced technology, and well-defined procedures, supported by regular training and rigorous enforcement. By implementing these measures, port facilities can maintain operational efficiency while addressing potential security threats and ensuring compliance with regulatory standards.

