Interfacing Cruise Terminal Security & Technology

Captain Barry Compagnoni
Senior Director
Public Safety & Security
What Do We Protect?

• People:
  – employees, crews, passengers, vendors, public

• Ships:
  – tankers, cruise, container, bulk, commercial fishing, recreational

• Maritime facilities:
  – piers, wharves, quays, cruise terminals, bulk facilities, oil and gas infrastructure
  – baggage/waiting areas, approaches to terminals

• Critical infrastructure:
  – pipelines, bridges, railroads, highways, IT networks

• Key assets:
  – military facilities, historically significant icons
From What?

• Maritime Domain Awareness
  • Defined as:
    – “effective understanding of anything associated with the maritime domain that could impact the security, safety, economy, or environment.”
  • What this means
    – Threats: physical and cyber attacks or criminal activity
    – Vulnerabilities: susceptibility of facilities, infrastructure, and systems
    – Consequences: primary and cascading impact
    – Risk: method to analyze and rank risk across maritime domain
      • $R = T \times V \times C$
  • Common Information Sharing Environment
    – Common Operating Pictures
Layers of Maritime Security

Terrorist Paths

- Intelligence/MDA
- US Coast Guard
- Joint Terrorism Task Force
- Customs and Border Protection
- State and local law enforcement
- VIPR
- Facility Security Officers
- MTSA
- Canines
- TWIC
- Baggage Screening
- Crew Vetting
- Passenger Screening
- Passengers

Facility Security Personnel

Layers include:

- Terrorist Paths
- Intelligence/MDA
- US Coast Guard
- Joint Terrorism Task Force
- Customs and Border Protection
- State and local law enforcement
- VIPR
- Facility Security Officers
- MTSA
- Canines
- TWIC
- Baggage Screening
- Crew Vetting
- Passenger Screening
- Passengers
Maritime Security Regulations

• Maritime Transportation Security Act of 2002
  – Vessels, Facilities, OCS activities
  – Access control and identity verification
  – Continuous monitoring of facility and access control points
  – Communication, tactical and routine
  – Response and notifications, vertical and horizontal

• MTSA also required USCG to develop
  – Area Maritime Security Committees
  – Area Maritime Security Plans
Web of Security & Technology

• Wide area
  – Radar: surface search radars
  – Communications: VHF, satellite, etc.
  – Automated Identification System: 300+ ton ships

• Cruise Terminals
  – Identity verification: TWIC, port cards, biometrics, facial recognition
  – Access control systems: secure and restricted facilities
  – CCTV: continuous monitoring coordinated with other sensors
  – License plate readers: approaches to facilities
  – Fire sensors
  – Environmental systems, air monitoring, etc.
Identity Verification Technologies

• Primary focus is verification and access control
• Identity Verification and Access Management
  – Networked systems include sensors and communications network
  – Transportation Worker Identification Credential
  – Local permissions through port identification badge
• What is ICAM?
  – ICAM - Identity, Credential, and Access Management - is the set of security disciplines that allows an organization to:
    – enable the right individual to access the right resource at the right time for the right reason
Identity Management
...allows an organization to construct a trusted digital identity based on an individual’s defining attributes.

Credential Management
...allows an organization to associate a digital identity with authoritative proof of that claimed identity.

Access Management
...allows an organization to leverage trusted identities and authoritative credentials to ensure only permitted individuals are granted access to protected resources.

Governance
Enterprise Governance
Auditing & Reporting
Redress
Recovery

Federation
Attribute Exchange
Credential Translation
Credential Holding
Policy Alignment

Identity Proofing • Creation • Maintenance
Identity Resolution • Deactivation

Sponsorship • Registration • Issuance
Maintenance • Revocation

The functions that enable organizations to make programmatic decisions, manage enterprise policies, and promote program efficiency.

The functions that allow an organization to access IAM information and decisions across organizational boundaries based on established trust.
Surveillance Technologies

- AIS, Radar, CCTV, LPR systems
- Port Canaveral has over 770 networked cameras
  - Various types: Fixed, PTZ, Optical, and low light
  - Focused on access control points, security monitoring areas, critical infrastructure
- Trac-tic system for patrol monitoring
Bringing It Together

• Command Bridge Common Operating Picture
  – Vessel information
  – Facility information
  – Cameras
  – AIS
  – Radar
  – Patrol assets