Office of Cyber and Infrastructure Analysis

Terminal Automation and Cybersecurity Risks

20 July, 2017

Andrew Pasternak
Overview

- OCIA 101
- Importance of Container Shipping to DHS
- Infrastructure System Overview
  - Automated Container Overview
  - Terminal Operating System
- Cybersecurity Risk Analysis
  - OCIA
  - Regional Resiliency Assessment Program
OCIA Vision

Strengthen the security and resilience of the Nation’s critical infrastructure through innovative cyber and physical analysis.

OCIA Mission

Inform the decisions that protect the Nation’s critical infrastructure.
OCIA Core Functions

Strategic Analysis

Capability Development

Infrastructure Prioritization

Operational Analysis
Importance of Container Shipping to DHS
OCIA is developing an Infrastructure System Overview (ISO) of automated container terminals because:

- Increase in automation at container terminals
  - Environmental
  - Safety
  - Operational
- Limited knowledge of automation outside of industry
- Create baseline understanding for future risk analysis
Automated Container Terminal Overview
Terminal Operating System (TOS)

- Automated Vehicles and Cranes
- Automated Indentification and Data Collection Systems
- Gate Operating System
- Terminal Operations Staff
- Terminal Front Office
- TOS Vendor

- Terminal Clients (truckers, freight forwarders, agents, etc.)
- Vessel, Container Planner, Other Terminals
- Customs and Border Protection
- Shipping Company/Ship’s Agent

- Vessel Visits, Export Bookings, Container VGM, Stowage Plan, Vessel Loading/Discharge Orders
- Terminal Performance, BAPLIE
- Container Movements
- Location of containers, automated vehicles, trucks, personnel
- Booking Data, Container Movement Orders
- Data Input, Vessel Planning, Terminal Planning
- Terminal Operations/ Data/Analytics
- Maintenance

- ACE Disposition Code
- Container Availability/Status, Fee Notification, Vessel Schedule
- Fee Payments, Outbound Transportation, Vehicle Booking Systems
- BAPLIE

- Shoreline
- External
- Administrative
Cybersecurity Risk Analysis - OCIA

- Future Risk Analysis on Automated Container Terminals
  - Vulnerabilities
    - Interconnectivity Among Systems, COTS Technologies, Insider Threat, etc.
  - Threat Actions and Consequences
    - Data Denial (deletion, ransomware), Denial of Service, Physical Damage (ICS), Manipulating Databases, etc.

Previous OCIA Product: Consequences to Seaport Operations from Malicious Cyber Activity
Regional Resiliency Assessment Program (RRAP)

- The RRAP is a *cooperative* assessment to assist critical infrastructure owners and operators and state and local agencies
  - Resolves infrastructure security and resilience knowledge gaps
  - Informs risk management decisions
  - Identifies resilience-building opportunities and strategies
  - Improves critical partnerships among stakeholders
- Sensitive information protected from public disclosure

https://www.dhs.gov/regional-resiliency-assessment-program
PSCDOperations@hq.dhs.gov

Office of Infrastructure Protection
Protective Security Coordination Division
Andrew Pasternak
Risk and Vulnerability Analyst
andrew.pasternak@hq.dhs.gov

Homeland Security

For more information visit:
www.dhs.gov/office-cyber-infrastructure-analysis