American Association of Port Authorities

Navigating the Cyber Domain

Captain James Cash
Deputy Director
U.S. Coast Guard Cyber Command
Vision & Mission

VISION

“A safe, secure and resilient cyber operating environment that allows for the execution of Coast Guard missions and maritime transportation interests of the United States.“

MISSION

The CGCYBERCOM mission is to identify, protect against, enhance resiliency in the face of, and counter electromagnetic threats to the Coast Guard and maritime interests of the United States, provide cyber capabilities that foster excellence in the execution of Coast Guard operations, support DHS cyber missions, and serve as the Service Component Command to U.S. Cyber Command.

Computer Network Defense…Protecting MCIKR…Creating a Decision Advantage for the Service
Mission Areas

DHS Mission 1: Critical Infrastructure
DHS Mission 2: Secure Borders
DHS Mission 3: Enforcing Immigration Laws
DHS Mission 4: Cybersecurity
DHS Mission 5: Resiliency

Provide a Secure Platform
Secure Ports and Waterways
Provide Decision Advantage

Ports, Waterways, and Coastal Security
Living Marine Resources
Law Enforcement, Marine Safety
Counter Drug
Migrant Interdiction
The CGCYBERCOM mission strategy for MCIKR Protection is being developed within the context of an existing strategy and policy framework that starts with the National Security Strategy.
Sector-Specific Plans (SSPs)

- Each SSA is responsible for writing a Sector-Specific Plan.

- Latest Transportation Systems Sector-Specific Plan issued in 2010, with modal Annexes. Maritime Annex is not subordinate to the TS SSP, but is a component of.

- The Transportation Systems Sector has four primary goals: (TSSSP, 2010, p. 25-26)
  - Goal 1: Prevent and deter acts of terrorism using, or against the transportation system;
  - Goal 2: Enhance the all-hazard preparedness and resilience of the global transportation system to safeguard U.S. national interests;
  - Goal 3: Improve the effective use of resources for transportation security;
  - Goal 4: Improve sector situational awareness, understanding and collaboration.
Maritime Critical Infrastructure Protection

- CG is the Sector-Specific Agency (SSA) for Maritime Transportation
  - Roles and responsibilities directly linked to national policy
  - Transportation Systems Sector – Specific Plan - coordinate protection of cyber systems within Marine Transportation System & Critical Infrastructure/Key Resources
- CG Chairs each Port’s Area Maritime Security Committee
  - Port partnerships/maritime stakeholders…proven trust and credibility; well established Maritime Security Comms Plan.
- Service level lead cyber involvement in key DHS initiatives
- Direct Support to front line operational commands (I&W, exercise support, awareness briefings, etc.)
CGCYBER NIPP/CIKR Priorities

- Raise awareness and understanding of maritime cyber issues with port partners
- Develop proactive public-private partnerships utilizing existing Captain of the Port structures
- Form a comprehensive cyber risk picture
  - Cybersecurity Assessment and Risk Management Approach (CARMA)
  - Maritime Security Risk Analysis Model (MSRAM)
- Effectively share information
  - Cross-Sector Cyber Security Working Group (CSCSWG)
  - Industrial Control Systems Joint Working Group (ICSJWG)
  - Transportation Systems Sector Cyber Working Group (TSS CWG)
  - Cyber Unified Coordination Group (CYBER UCG)
MTSA 2002

- Public law enacted in response to the attacks of 9-11
- Tasked to identify weaknesses in physical security, passenger and cargo security, structural integrity, protection systems, procedural policies, communications systems, transportation infrastructure, utilities, contingency response and other areas
- Primarily focused on the physical security of ports, waterways, vessels, and facilities (although there is mention of computers and other electromagnetic systems)
The New Reality

- Cyber is a domain... like land, air, water, and space
- Touch-points within all 18 Sectors
- Critical infrastructure and key resources (CIKR) as well as global supply chain highly dependent on cyber technologies
- A threat vector that can have physical/kinetic effects inside our ports and waterways

“You can’t have good physical security without good cybersecurity.”
- Mark Weatherford, Deputy Undersecretary DHS NPPD
Success of the MTS...Cyber Dependence

Devices communicating over a network world wide

Source: John Gantz, The Embedded Internet: Methodology and Findings, IDC, January 2009
Economic Impact of the Maritime Domain

- 95% of all U.S. foreign trade through 361 ports
- $800 billion/year in freight
- $2 billion/day trade with Canada
- 7,000 oceangoing vessels made 55,560 port calls annually

(Source MARAD & RITA)
Cruise Lines

Figure 1. North American Cruises, Traffic and Capacity
(Million Passenger Nights)

Source: Maritime Administration.
Intermodal Touch-points
The Threat

NATURAL DISASTERS

CRIMINALS

INSIDERS

HACKTIVISTS

NATION STATES
The Vulnerabilities

INDUSTRIAL CONTROL SYSTEMS

WIRELESS NETWORKS & SMARTPHONES
The Impacts

 Scenario: Los Angeles/Long Beach Port
 Cyber incident could lead to disruption or uncertainty in Port of Los Angeles/Long Beach where $520 million of cargo is handled daily.

 Vulnerabilities: Port Industrial Control Systems
 Compromised systems such as supervisory control and data acquisition (SCADA) would cause major disruption in maritime environment.

 2011 Example Cyber Incident: Houston
 A cyber intrusion was conducted against a Houston water utility facility. Individual gained access to system diagrams and potential control of SCADA system.
Cyber Security...a “Team Sport”

**USCG/TSA/DOT**
- Strength through partnership
- Unit of effort to protect the transportation sector

**National Cybersecurity and Communications Integration Center**
- DHS 24X7 cyber operations center
- National response center for coordination federal response to a cyber incident

**US-CERT**
- Coordinate cyber information sharing
- Vulnerability and risk assessments

**ICS-CERT**
- Basic, intermediate and advanced cybersecurity and industrial control systems training
- On-site emergency response
National Cyber Security Awareness Month

October 2012 marks the ninth annual *National Cyber Security Awareness Month* sponsored by the Department of Homeland Security

- Being safer online is a shared responsibility
- Defeating cyber threats requires engagement from all of us – from government and law enforcement to the private sector and most importantly, members of the public to create a safer cyber environment

Where you can go for information:

www.dhs.gov/stophinkconnect
ACT
Achieving Cybersecurity Together

“It’s our Shared Responsibility”.