U.S. Coast Guard Sector New York

LCDR Sarah Brennan

LT Emily Miletello

Basic Coast Guard Authorities

- ***What we are:***

✓ **Military**
✓ **Multi-mission**
✓ **Maritime**

An Armed Service

- Title 10 (Armed Services)
- Title 50 (War & National Defense)

Member of the IC

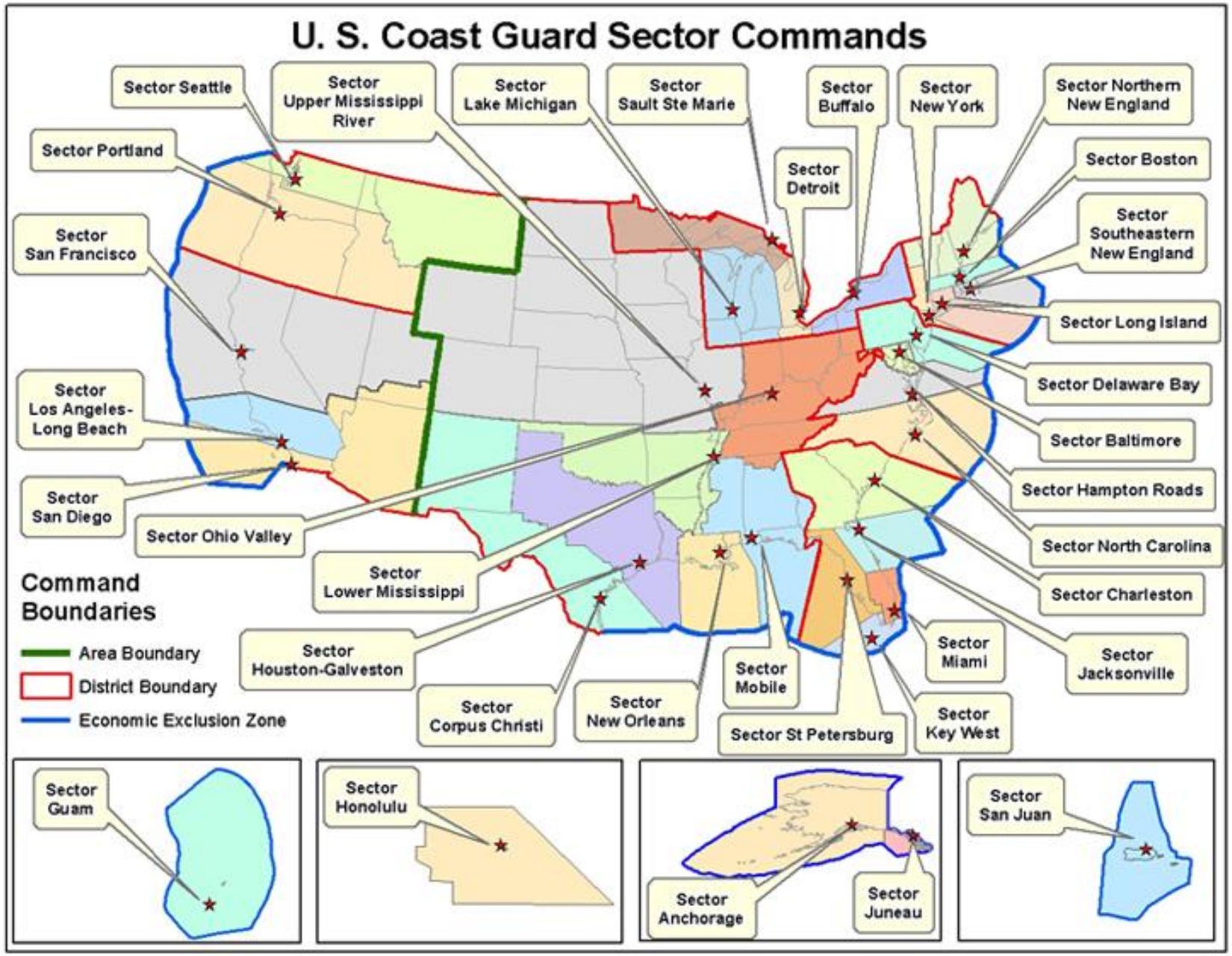
- Title 50 App (Member of Intel Community)

A Law Enforcement agency

- Title 6 (Homeland Security)
- Title 14 (Coast Guard)
- Title 19 (Customs)

A Regulatory Agency

- Title 33 (Navigable Waters, Environment)
- Title 46 (Shipping)
- Title 49 (Transportation)


U. S. Coast Guard Sector Commands
Sector Seattle
Sector Upper Mississippi River
Sector Lake Michigan
Sector Sault Ste Marie
Sector Buffalo
Sector New York
Sector Northern New England
Sector Portland
Sector Detroit
Sector Boston
Sector San Francisco
Sector Southeastern New England
Sector Long Island
Sector Los Angeles-Long Beach
Sector Delaware Bay
Sector Baltimore
Sector San Diego
Sector Hampton Roads
Sector Ohio Valley
Sector North Carolina
Sector Lower Mississippi
Sector Charleston
Command Boundaries
Area Boundary
District Boundary
Economic Exclusion Zone
Sector Houston-Galveston
Sector Miami
Sector Jacksonville
Sector Corpus Christi
Sector New Orleans
Sector Mobile
Sector St Petersburg
Sector Key West
Sector Guam
Sector Honolulu
Sector Anchorage
Sector Juneau
Sector San Juan

Sector Commander Roles & Authorities

Captain of the Port (COTP)	**Search and Rescue Mission Coordinator (SMC)**	**Federal On-Scene Coordinator (FOSC)**	**Federal Maritime Security Coordinator (FMSC)**	**Officer in Charge, Marine Inspections (OCMI)**
Ensures the Safety and Security of the COTP Zone.	Coordinates all maritime Search and Rescue.	Coordinates and directs oil spill and hazmat response out to 200nm.	Oversees the Area Maritime Security Committee and Plan.	Vessel & Port Facility Inspections, Investigations, Licenses & Documentation

Sector New York
Area of Responsibility

Stations

- STA New York: 9 boats
- STA Sandy Hook: 4 boats
- STA Kings Point: 3 boats

Aids to Navigation Teams

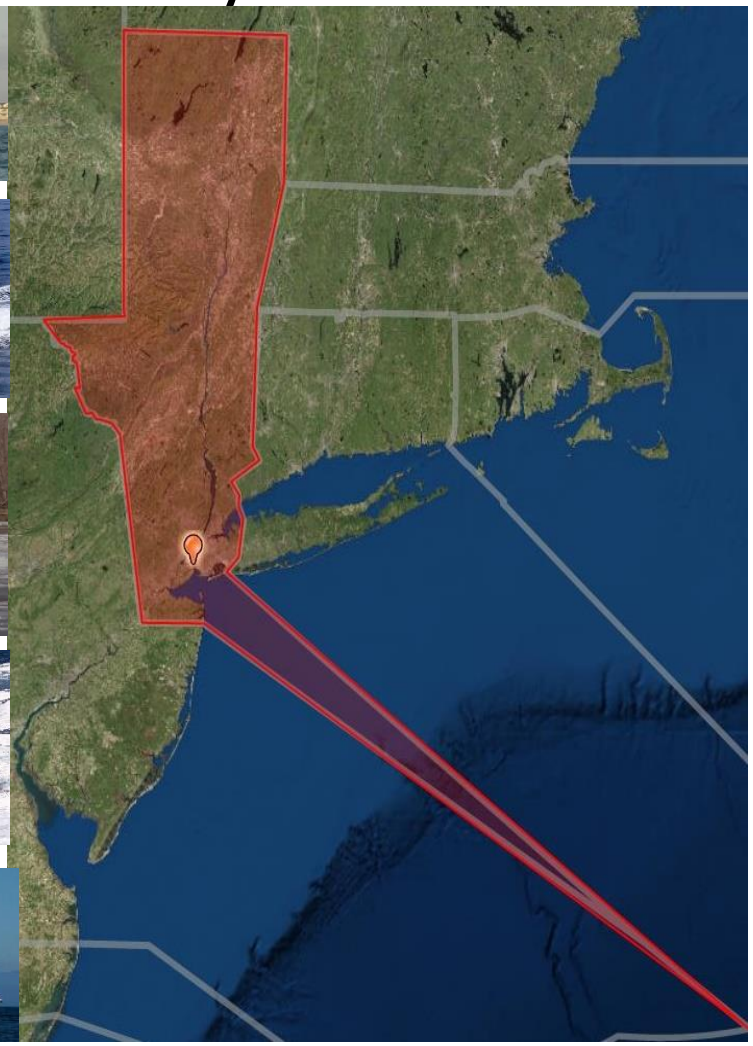
- ANT New York: 4 boats
- ANT Saugerties: 2 boats

Cutters

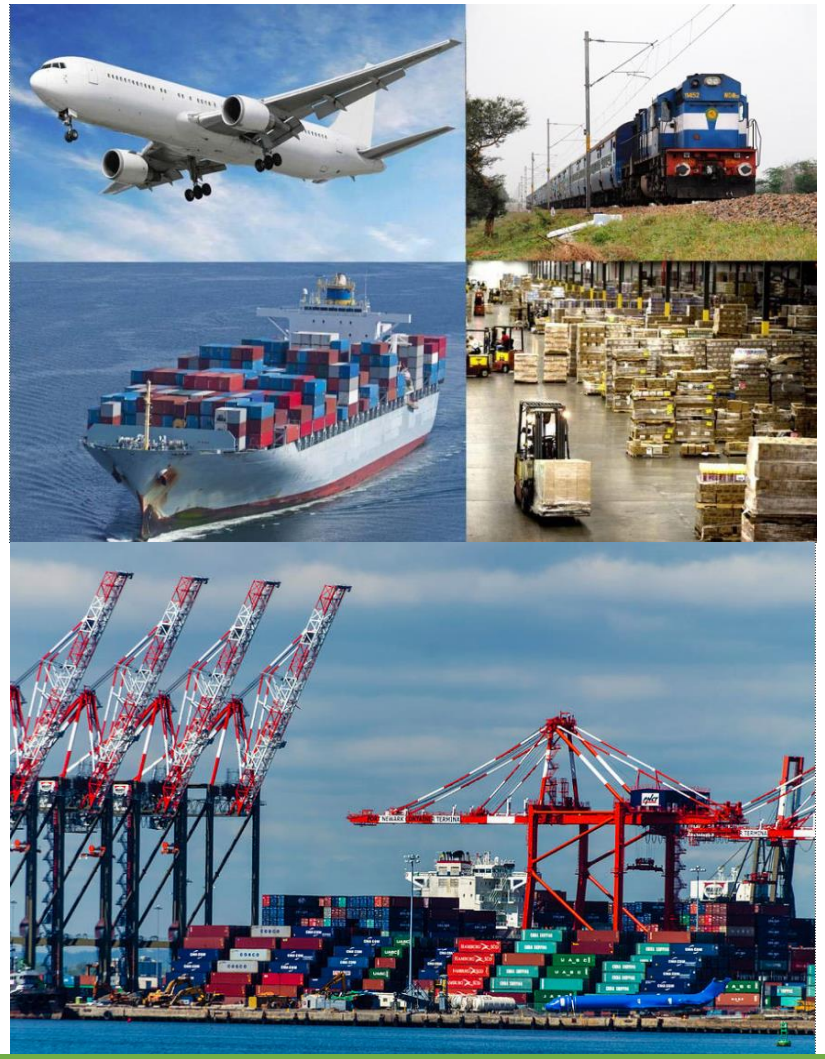
- (1) 175-ft Buoy Tender
- (2) 140-ft Ice-breaking Tugs
- (1) 110-ft Patrol Boat
- (1) 87-ft Coastal Patrol Boat
- (3) 65-ft Harbor Tugs

Personnel

- ~ 1,000 Active Duty, Civilians & Reservists
- ~ 2,000 Auxiliarists



Global Logistics Network



Port Newark

Port of New York and New Jersey

- Largest quantity of refined petroleum products in U.S.
- 2nd largest U.S. container port, 7.2 million TEU's in 2018
- 550,000 vehicles imported annually
- 1/3 of Nation's GDP generated within 250 miles

Port of New York and New Jersey

- Largest passenger ferry port in U.S., 2nd worldwide
  - Approximately 1,700 daily ferry movements
  - Staten Island Ferry busiest ferry route in U.S.
  - NYC EDC ferry fleet is the Nation's fastest growing
- High-volume cruise ship port

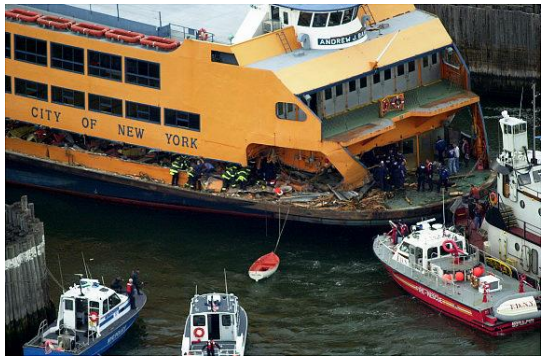
Port of New York and New Jersey

Dense multi-use port with heavy traffic congestion:

- Cruise ships
- Ferries
- Tugs & barges
- Ultra-large container vessels
- Tankers
- Recreational vessels
- Human-powered watercraft

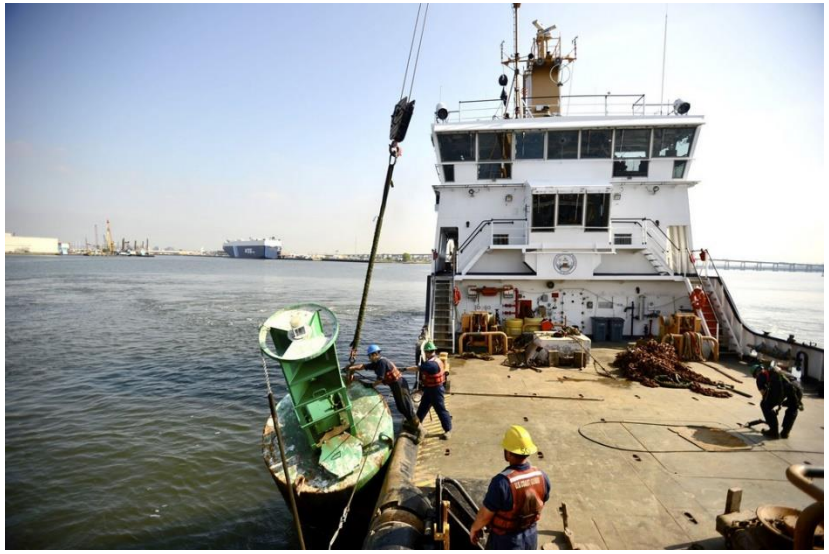
Inspections & Investigations

- Inspections
  - Safety, security, and environmental compliance – oversee all aspects of ship & facility operations
  - US Flagged vessels
  - Foreign Flagged ships
- Investigations
  - Casualty, injury, death investigations
  - Merchant Mariner credentialing

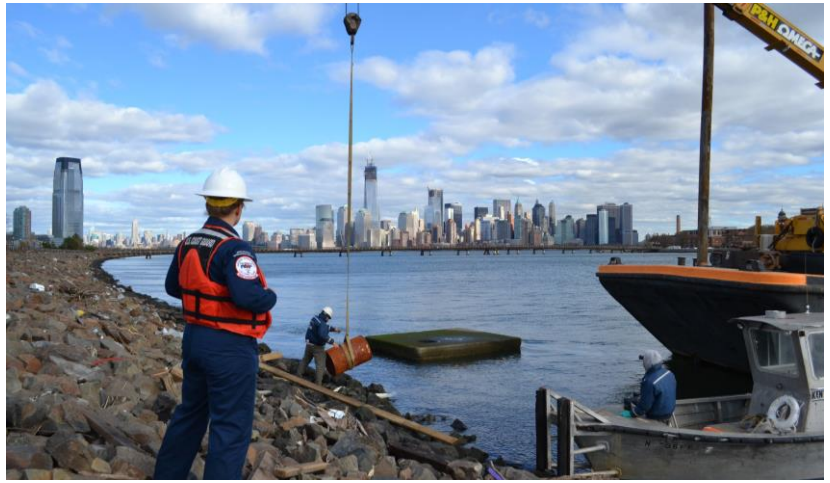


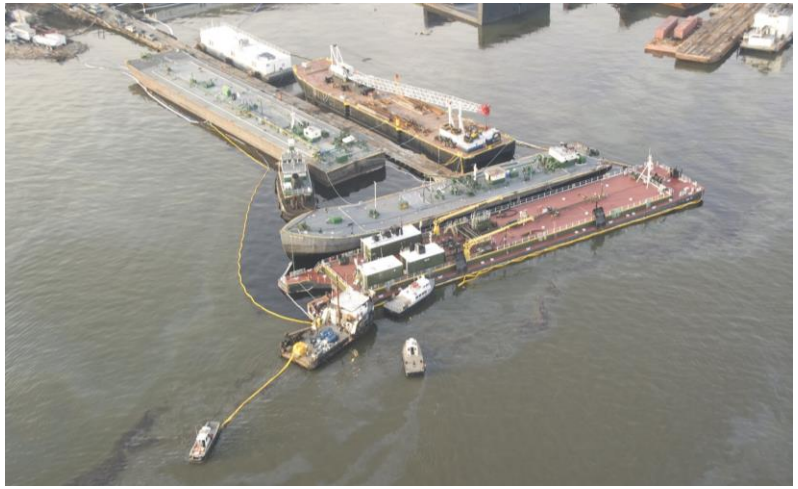
Waterways Management

- Aids to navigation maintenance
- Marine event permits
- Vessel Traffic Service
- Ice Breaking
  - 90% of US heating oil is used in the Northeast
  - 80% of that heating oil comes by barge

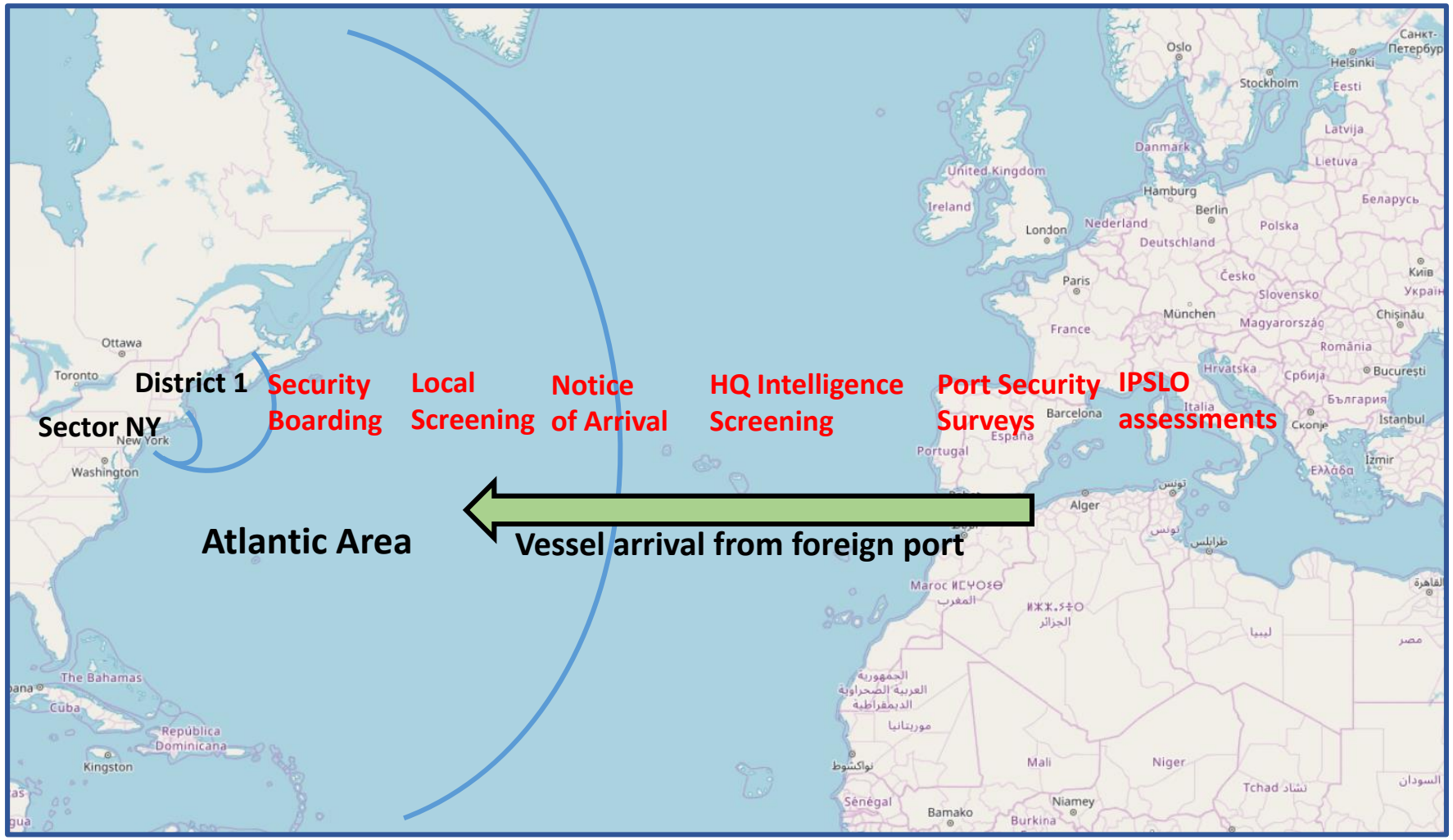


Search and Rescue
Marine Environmental Protection



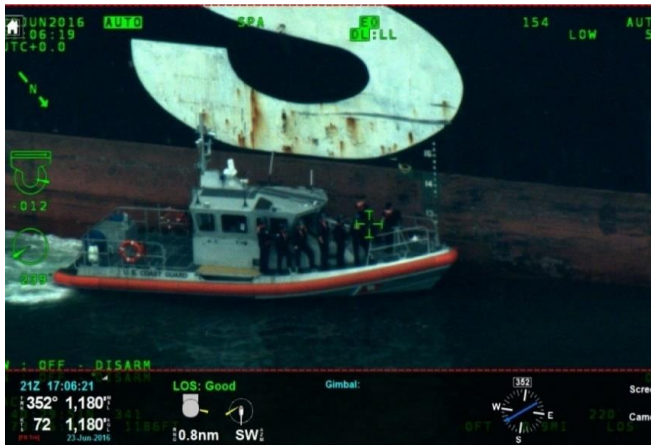


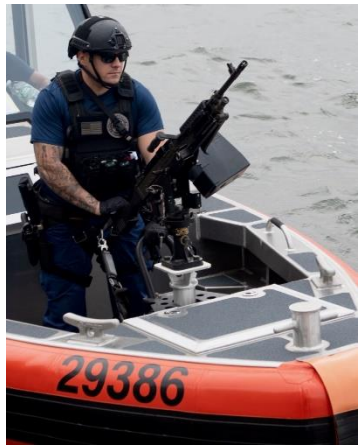
Layered Security Strategy



Port Security

- Offshore High-Interest Vessel boardings
- Security zone enforcement
- Maritime critical infrastructure protection
- High-capacity passenger vessel escorts
- Active shooter and active threat response



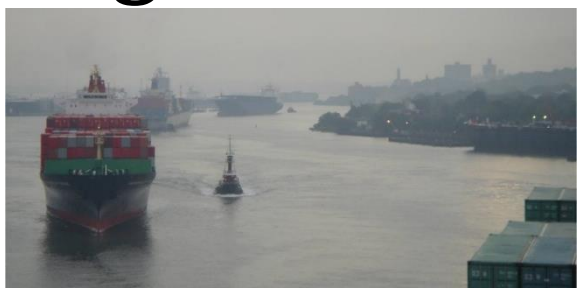


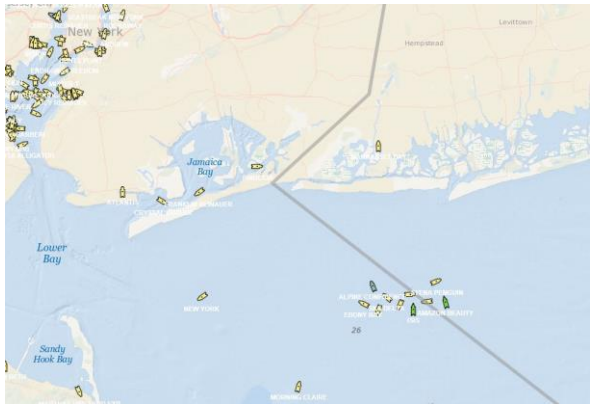
Interagency Relationships

- Extraordinary partnerships with federal, state, and local officials.
- Nation’s largest annual Port Security Grant allocation.

Congestion Challenges

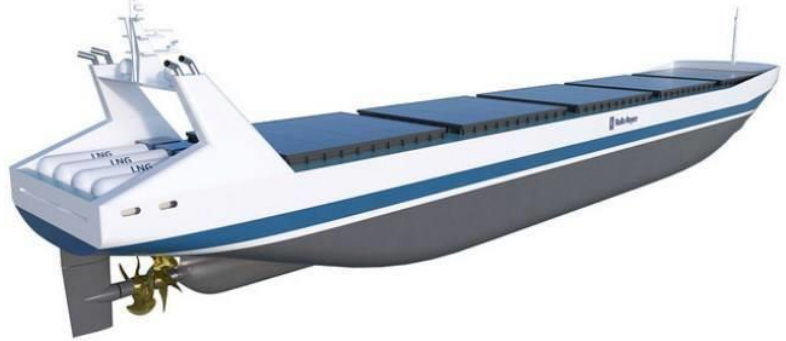
- Continued increase in vessel traffic
- Larger ships continue to push limits of existing port infrastructure
  - Channels
  - Bridges
  - Port Facilities/Cranes
  - Anchorages, etc

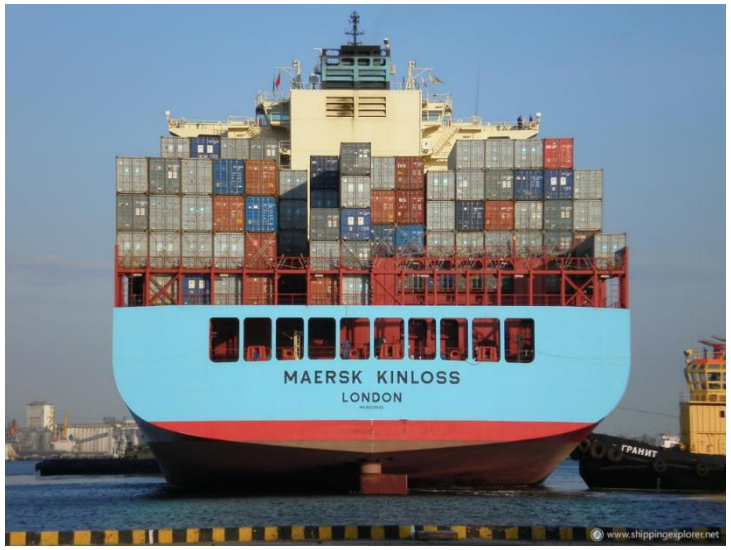




Emerging Technologies

- Cyber Security
  - MTSA facilities
  - Vulnerable ship systems
- LNG powered vessels expect to arrive within 5 years
- Unmanned systems
  - USCG force multiplier
  - New regulatory challenge for commercial vessels
  - Security vulnerability





"Cyber threats collectively now exceed the danger of physical attacks against us. This is a major sea change now exceed for my department and for our country's security."

- Secretary Kirstjen Nielson; DHS Cyber Security Summit
Manhattan, NY, 31 July 2018

Sector NY's Cyber initiatives

- Industry Training
  - Marine Inspector training with cyber leaders in the financial sector.
- Cross-sector collaboration through the Area Maritime Security Committee
  - Cybersecurity subcommittee includes members across industry, law enforcement, academia, etc.
- Exercises
  - TTX, workshops, cyber game (red team/blue team)
- Port Security Grants
  - Leveraging grant funds to improve cyber resilience in the Port.
  - Sustainable Terminal Services conducting first-of-its-kind joint cyber assessment.
- Spread awareness through public engagement

REAL WORLD THREATS

- **2013** – Port of Antwerp drug trafficking via cyber attack
- **2013** – Malware impacted a Mobile Offshore Drilling Unit's (MODU) computer system, disabling signals to the positioning thrusters, causing the rig to "walk off" & shutting down operations.
- **January 2015** – ECDIS vulnerabilities
- **June 2017** – "NotPetya" – debilitated world's largest shipping line.
- **September 2018** – Port of San Diego Cyber Attack
- **March 2019** – Cyber Incident aboard underway deep draft cargo ship bound for Port of NY/NJ – debilitated shipboard IT network.

1000’ U.S. Flagged Container Ship
Cyber Incident
Reported to the NRC 04 March 2019
Berthed in Port of NY/NJ 06 March 2019

“The ship is essentially operating with zero cyber security.”

- Cyber Protection Team Lead

Cyber Incident

March 2019

U.S. Flagged Container Ship bound for Port of NY/NJ

Initial Report/Actions

- Vessel reports that virus on ship's networked computers had spread to the system's server and was resistant to generic antivirus software.

- Not immediately clear whether industrial control systems or other critical systems were impacted by the malware.

- To determine whether vessel presented risk to the Port, Sector NY requested assistance from CGCYBER CPT and FBI Cyber Security Taskforce to inform risk management decisions: **RISKS / OPTIONS / MITIGATIONS?**

Response

- Sector NY MIs, CGCYBER/ CPT, FBI completed boarding/ship ride and dockside inspection.
- FBI conducted forensic analysis of recovered hard drive and USB flash drives.

CPT/FBI Findings

Essential vessel control systems are “air-gapped” from impacted network, **but…**

- Impacted network used for cargo data management, voyage planning, updating electronic charts, ANOA submission, etc.
- Malware identified as **EMOTET** (modular banking Trojan)
- Malware **slowed systems**; automated emails forwarded from legitimate company email accounts to 3rd parties.
- **Unknown source-** virus could have been transferred by USB or downloaded by any internet user on board.
- **Liberal use of thumb-drive data transfer** at all ports of call. No active scanning of networks/external drives.
- **Generic login/password** used by all personnel with access to the vessel; no network monitoring or consistent use of anti-virus software.

Note: Persistent network access is critical to life underway.

Cyber Safety Alert

UNITED STATES COAST GUARD
U.S. Department of Homeland Security

MARINE SAFETY ALERT

Inspections and Compliance Directorate

July 8, 2019
Washington, D.C.

Safety Alert 06-19

Cyber Incident Exposes Potential Vulnerabilities Onboard Commercial Vessels

Recommendations:

- Segment Networks:
- Per-user Profiles & Passwords
- Be wary of external media
- Install basic antivirus software
- Don’t forget to patch

Media Coverage

U.S. Coast Guard Issues Alert After Ship Heading Into Port Of New York Hit By Cyberattack

- Forbes

U.S. Coast Guard Warns Shipping Industry on Cybersecurity

Hackers attempted to digitally seize control of a vessel in February, an incident that shows risks the sector faces

- Wall Street Journal

Coast Guard issues safety alert following 'significant cyber incident'

- Washington Times

USCG: Malware Attack Exposes Cyber Vulnerabilities at Sea

- Maritime Executive

Coast Guard calls for ships to update their systems after malware attack

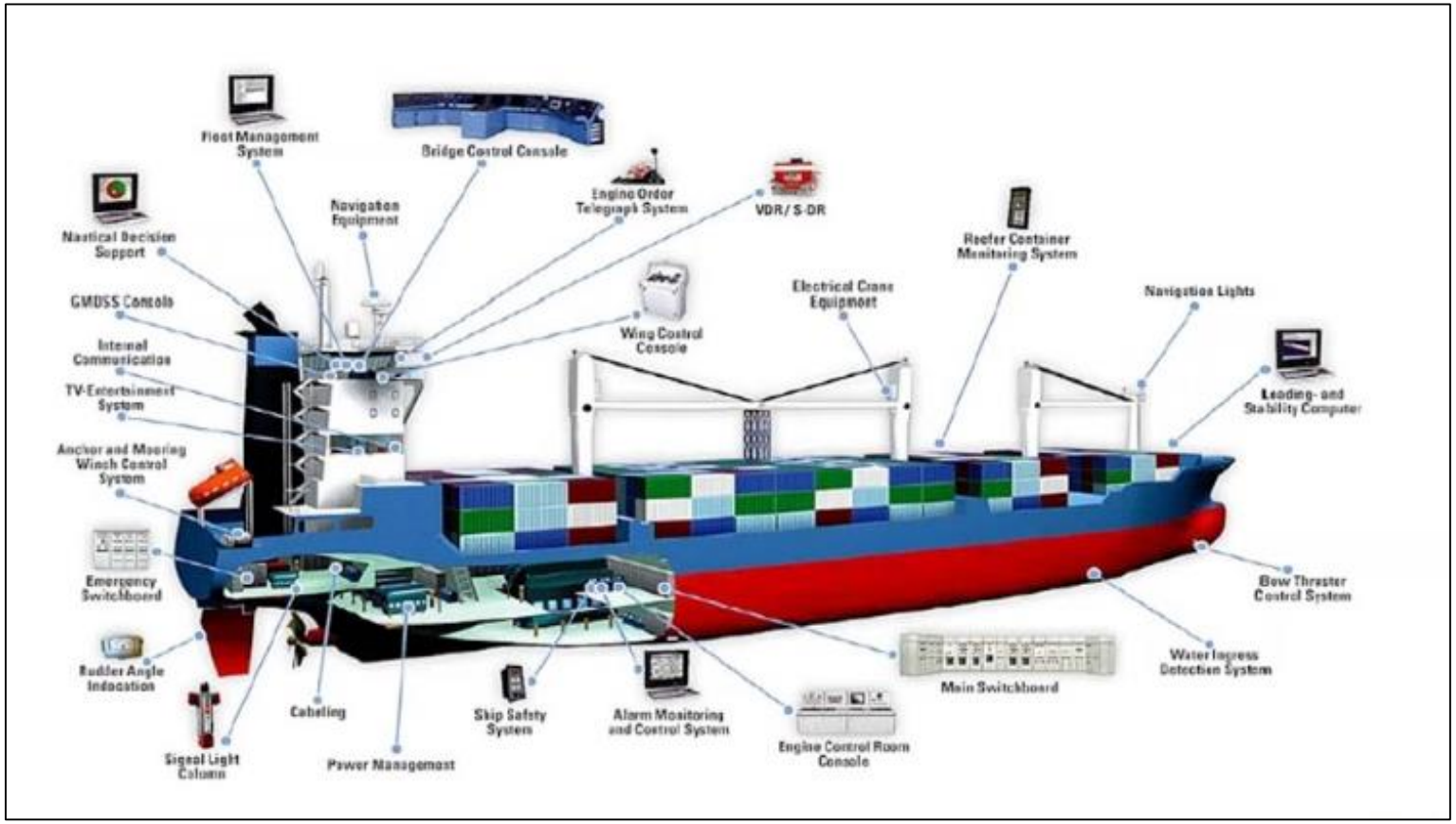
- The Hill

USCG Approach:
Cyber Risk Management

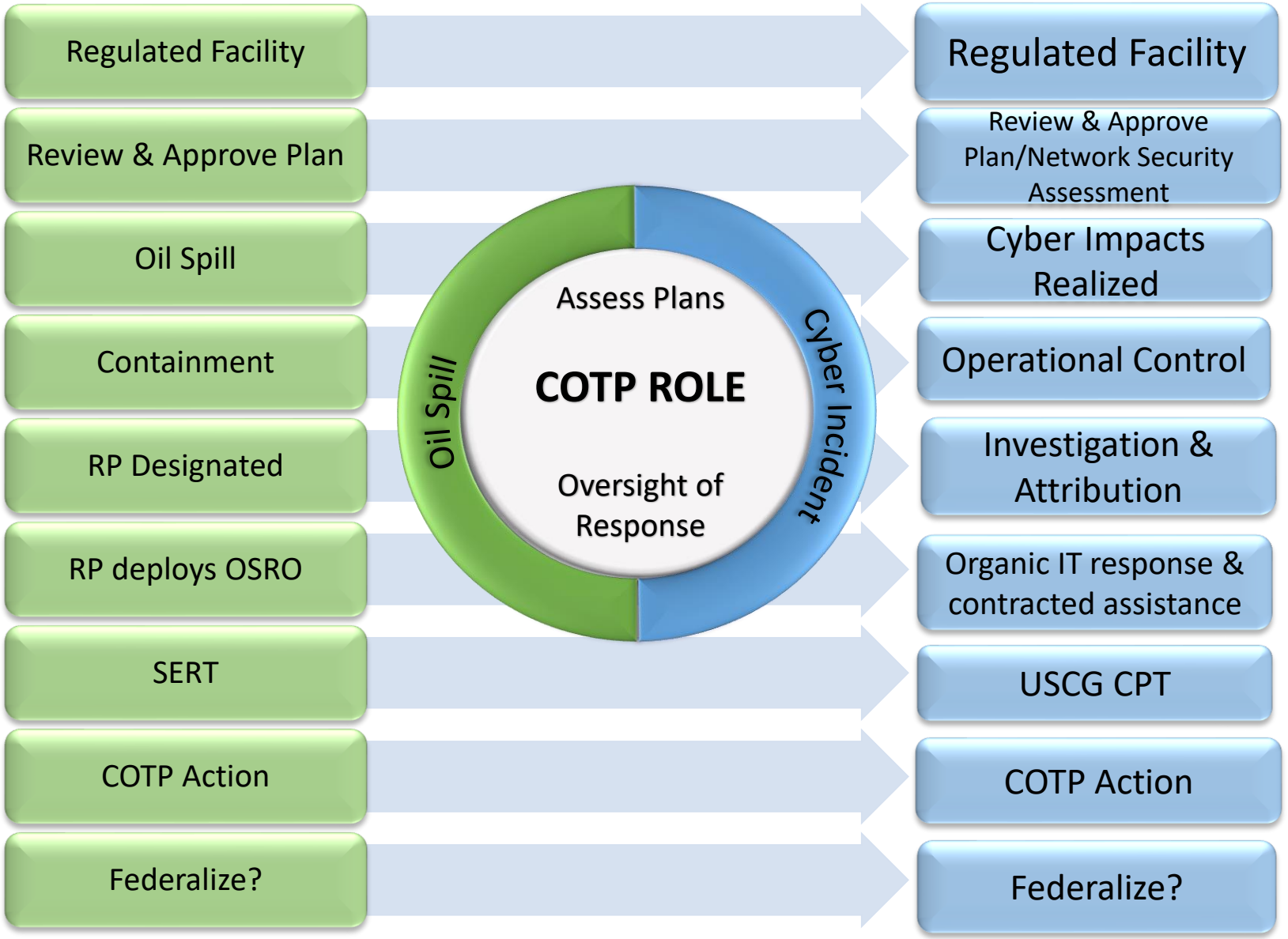
- Enhance Awareness
  - Targeted vs. “target of opportunity” cyber incidents
  - Both security AND safety issue
  - More than just an IT issue
  - New operational risk that needs to be managed
- Improve Cyber Governance (ISM Code)
- Develop Appropriate Standards
  - Incorporate cyber risk at every stage of ship design, construction and operation.

Cyber Risk, Potential Loss & Increasing Vulnerabilities

- Operational impacts due to cyber disruptions are growing in magnitude and frequency.
  - Persistent connectivity vs. continuity of global operations
- Industry standards and expectations are increasing.
  - "cyber seaworthiness"
  - What constitutes a "substandard" vessel?



Cyber Incident Prevention and Response Model



State of Cyber Security in our Ports

- Some Successes:
  - Local efforts to build resiliency across container terminals with shared equities/operating systems.
  - Area Maritime Security Committee is model for public-private partnership.
  - Regular drills/exercises.

- Challenges:
  - Cyber security not consistently addressed in vessel & facility security plans.
  - Cyber is modally agnostic – more robust coordination/info-sharing is needed.
  - Aging IT/OT aboard ships and in facilities.
  - **Bottom Line: in spite of growing cyber emphasis, maritime industry lags behind many other sectors.**

Sector Commander Tools

PREVENTION

Maritime Transportation Security Act

- Vessels and Facilities are required to address cyber vulnerabilities in their security plans.
- Marine inspectors review and approve plans.
- Plans that do not assess network vulnerabilities are returned for revision.

RESPONSE

Ports and Waterways Safety Act

- COTP can issue orders to vessel and facilities requiring that they take certain actions to mitigate a cyber incident (i.e., denied entry, cease cargo ops, conduct third-party assessment)

Major Takeaways

- **<u>This is uncharted territory-</u>** This could have been the first cyber incident reported to USCG from underway deep draft vessel.

- **<u>This was ONE vessel-</u>** is it representative of the majority of the fleet?

- **<u>Risk Management -</u>** Development of cyber capability is critical to fulfilling our statutory responsibilities in our ports. **However, at the end of the day, this is about risk management**.

Ongoing Initiatives

CYBER ANNEX

- Information Sharing
- Required Training
- COTP Advisory Committee
- Awards Program

EXERCISES

- Technical, field level exercise
- Multi-Sector roundtable
- Hacking Event

PARTNERSHIPS

- Continue to leverage partnerships with DoD, FBI, industry, financial/energy sectors, etc.

OUTREACH

- Spread awareness
- Case studies, interviews, speaking engagements, industry outreach.

Questions & Discussion

LCDR Sarah Brennan
Sarah.E.Brennan1@uscg.mil
Office: (718) 354-4063

LT Emily Miletello
Emily.C.Miletello@uscg.mil
Office: (718) 354-4353