Identify – Protect – Detect – Respond - Recover

Maritime & Port Security
Information Sharing & Analysis Organization

TLP-GREEN

Federal Cybersecurity Policy

Presidential Executive Order 13691 – Feb. 2015

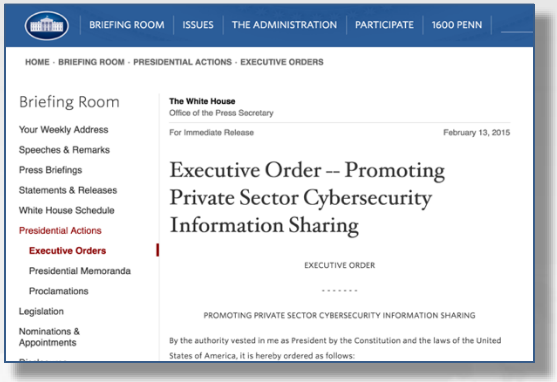
Promoting Private Sector Cybersecurity Information Sharing

Protecting Public Health & Safety, National and Economic Security

Critical Infrastructure | Sector & Sub-Sector

Business, Industry & Academia | Geographic

Public/Private Collaboration



BRIEFING ROOM | ISSUES | THE ADMINISTRATION | PARTICIPATE | 1600 PENN

HOME · BRIEFING ROOM · PRESIDENTIAL ACTIONS · EXECUTIVE ORDERS

Briefing Room

- Your Weekly Address
- Speeches & Remarks
- Press Briefings
- Statements & Releases
- White House Schedule
- Presidential Actions
  - Executive Orders
  - Presidential Memoranda
  - Proclamations
- Legislation
- Nominations & Appointments

The White House
Office of the Press Secretary

For Immediate Release February 13, 2015

Executive Order -- Promoting Private Sector Cybersecurity Information Sharing

EXECUTIVE ORDER

- - - - - - -

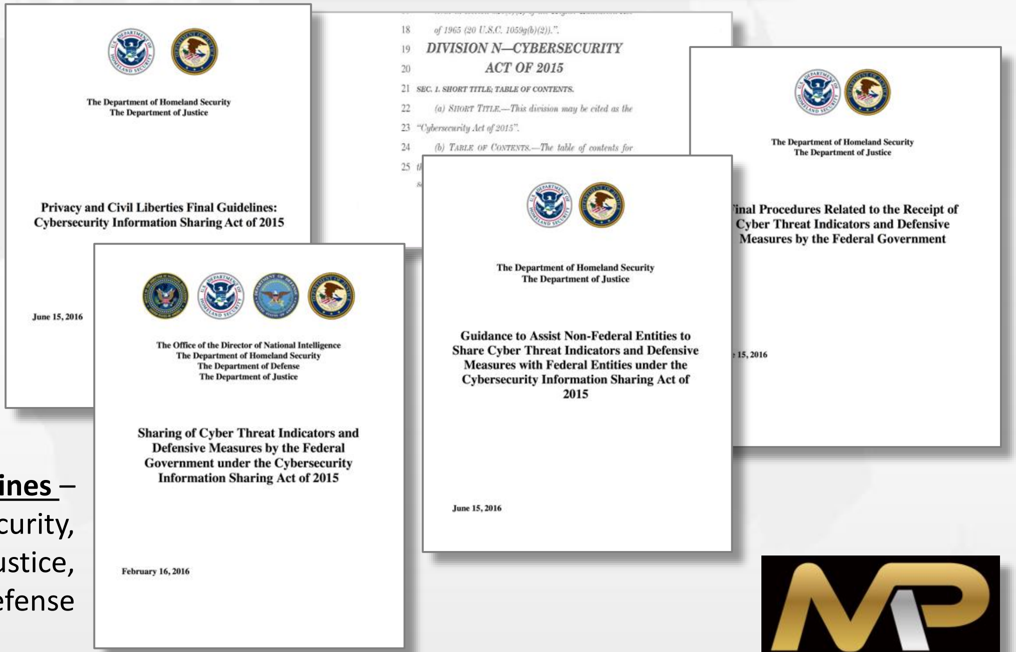
PROMOTING PRIVATE SECTOR CYBERSECURITY INFORMATION SHARING

By the authority vested in me as President by the Constitution and the laws of the United States of America, it is hereby ordered as follows:

Cybersecurity Information Sharing Act of 2015….

Signed into law – December 2015

- Definitions
- Federal Sharing
- Protection - Personal Information
- Private Sector Sharing and Liability Protection



The Department of Homeland Security
The Department of Justice

Privacy and Civil Liberties Final Guidelines: Cybersecurity Information Sharing Act of 2015

June 15, 2016

of 1965 (20 U.S.C. 1059g(b)(2)).".

DIVISION N—CYBERSECURITY ACT OF 2015

SEC. 1. SHORT TITLE; TABLE OF CONTENTS.

(a) SHORT TITLE.—This division may be cited as the "Cybersecurity Act of 2015".

(b) TABLE OF CONTENTS.—The table of contents for

The Department of Homeland Security
The Department of Justice

inal Procedures Related to the Receipt of Cyber Threat Indicators and Defensive Measures by the Federal Government

15, 2016

The Department of Homeland Security
The Department of Justice

Guidance to Assist Non-Federal Entities to Share Cyber Threat Indicators and Defensive Measures with Federal Entities under the Cybersecurity Information Sharing Act of 2015

June 15, 2016

The Office of the Director of National Intelligence
The Department of Homeland Security
The Department of Defense
The Department of Justice

Sharing of Cyber Threat Indicators and Defensive Measures by the Federal Government under the Cybersecurity Information Sharing Act of 2015

February 16, 2016

<u>Federal Government Published Guidelines</u> –
US Dept. Homeland Security,
US Dept. of Justice,
US Dept. of Defense

MARITIME & PORT SECURITY ISAO

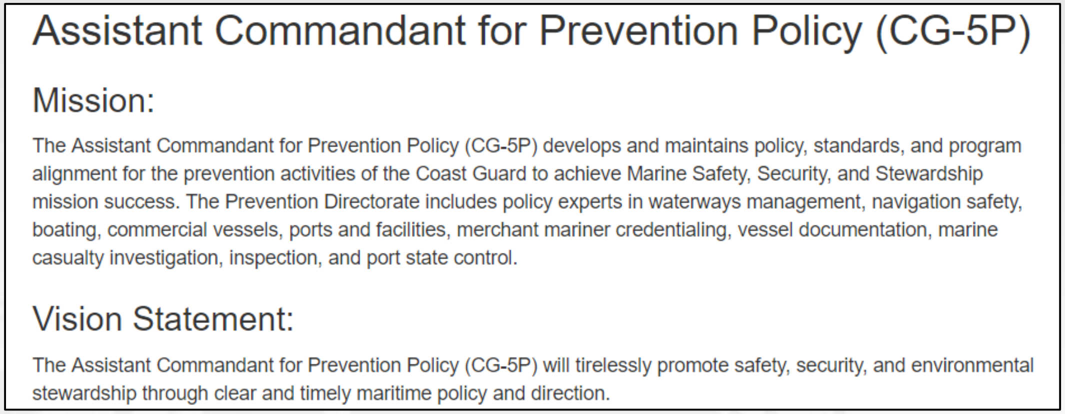
U.S. Coast Guard Guidance

Policy Letter CG-5P

January 2017

Provides instructions to report suspicious and malicious cybersecurity activity

- To whom
- What kind



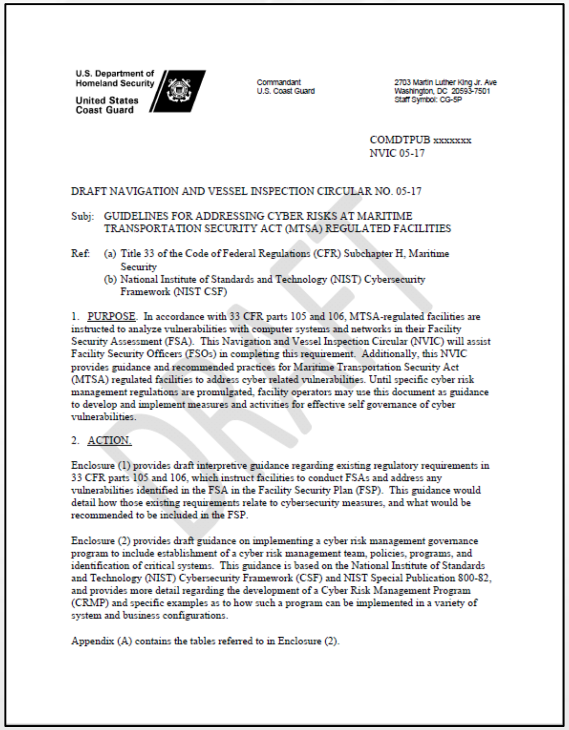
Assistant Commandant for Prevention Policy (CG-5P)

Mission:

The Assistant Commandant for Prevention Policy (CG-5P) develops and maintains policy, standards, and program alignment for the prevention activities of the Coast Guard to achieve Marine Safety, Security, and Stewardship mission success. The Prevention Directorate includes policy experts in waterways management, navigation safety, boating, commercial vessels, ports and facilities, merchant mariner credentialing, vessel documentation, marine casualty investigation, inspection, and port state control.

Vision Statement:

The Assistant Commandant for Prevention Policy (CG-5P) will tirelessly promote safety, security, and environmental stewardship through clear and timely maritime policy and direction.



U.S. Department of
Homeland Security

United States
Coast Guard

Commandant
U.S. Coast Guard

2703 Martin Luther King Jr. Ave
Washington, DC 20593-7501
Staff Symbol: CG-5P

COMDTPUB xxxxxxx
NVIC 05-17

DRAFT NAVIGATION AND VESSEL INSPECTION CIRCULAR NO. 05-17

Subj: GUIDELINES FOR ADDRESSING CYBER RISKS AT MARITIME TRANSPORTATION SECURITY ACT (MTSA) REGULATED FACILITIES

Ref: (a) Title 33 of the Code of Federal Regulations (CFR) Subchapter H, Maritime Security
(b) National Institute of Standards and Technology (NIST) Cybersecurity Framework (NIST CSF)

1. PURPOSE. In accordance with 33 CFR parts 105 and 106, MTSA-regulated facilities are instructed to analyze vulnerabilities with computer systems and networks in their Facility Security Assessment (FSA). This Navigation and Vessel Inspection Circular (NVIC) will assist Facility Security Officers (FSOs) in completing this requirement. Additionally, this NVIC provides guidance and recommended practices for Maritime Transportation Security Act (MTSA) regulated facilities to address cyber related vulnerabilities. Until specific cyber risk management regulations are promulgated, facility operators may use this document as guidance to develop and implement measures and activities for effective self governance of cyber vulnerabilities.

2. ACTION.

Enclosure (1) provides draft interpretive guidance regarding existing regulatory requirements in 33 CFR parts 105 and 106, which instruct facilities to conduct FSAs and address any vulnerabilities identified in the FSA in the Facility Security Plan (FSP). This guidance would detail how those existing requirements relate to cybersecurity measures, and what would be recommended to be included in the FSP.

Enclosure (2) provides draft guidance on implementing a cyber risk management governance program to include establishment of a cyber risk management team, policies, programs, and identification of critical systems. This guidance is based on the National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF) and NIST Special Publication 800-82, and provides more detail regarding the development of a Cyber Risk Management Program (CRMP) and specific examples as to how such a program can be implemented in a variety of system and business configurations.

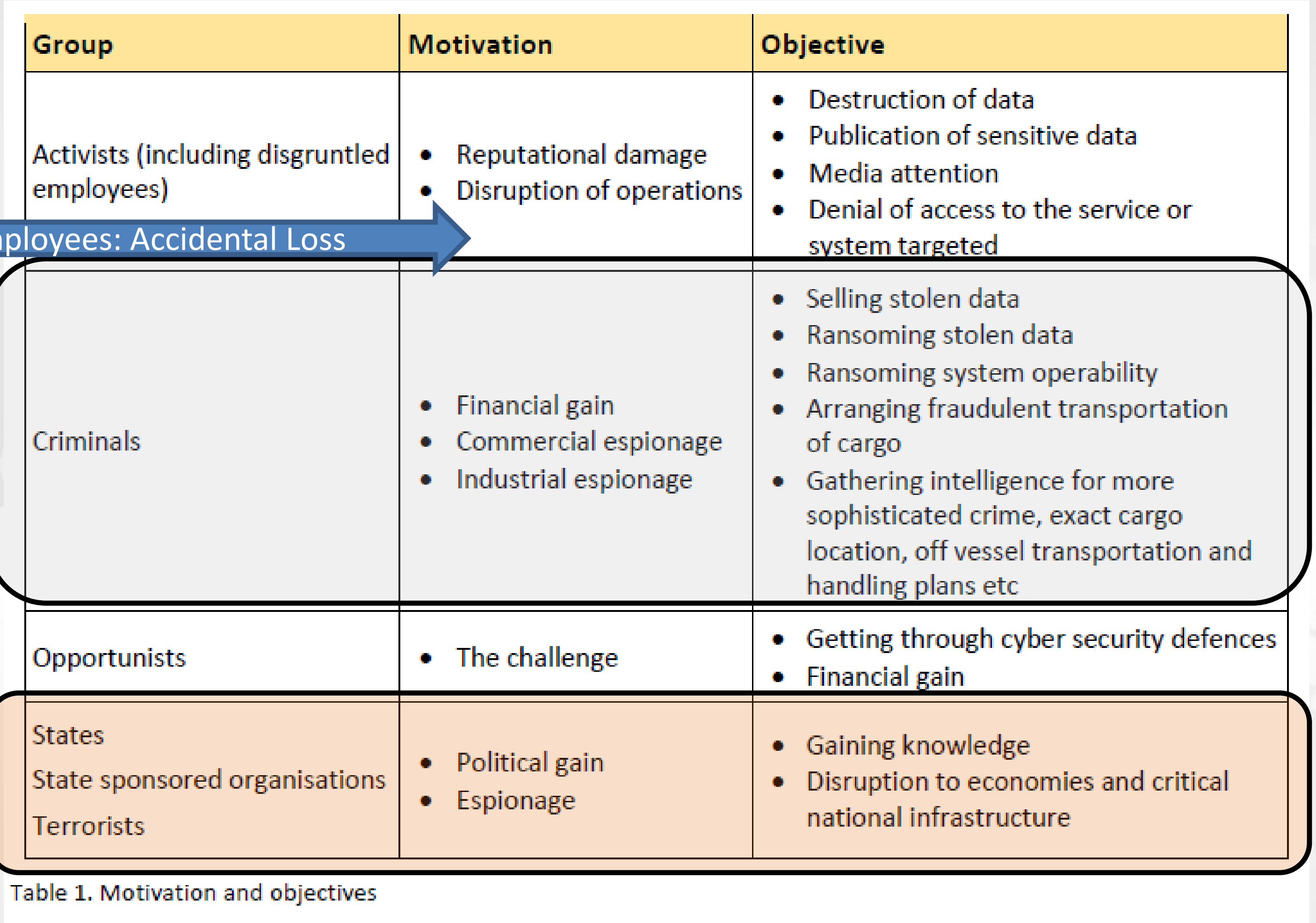
Appendix (A) contains the tables referred to in Enclosure (2).

DRAFT NVIC

May 2017

“MTSA-regulated facilities are instructed to analyze vulnerabilities with computer systems and networks in their Facility Security Assessment (FSA).”

Adversaries 101



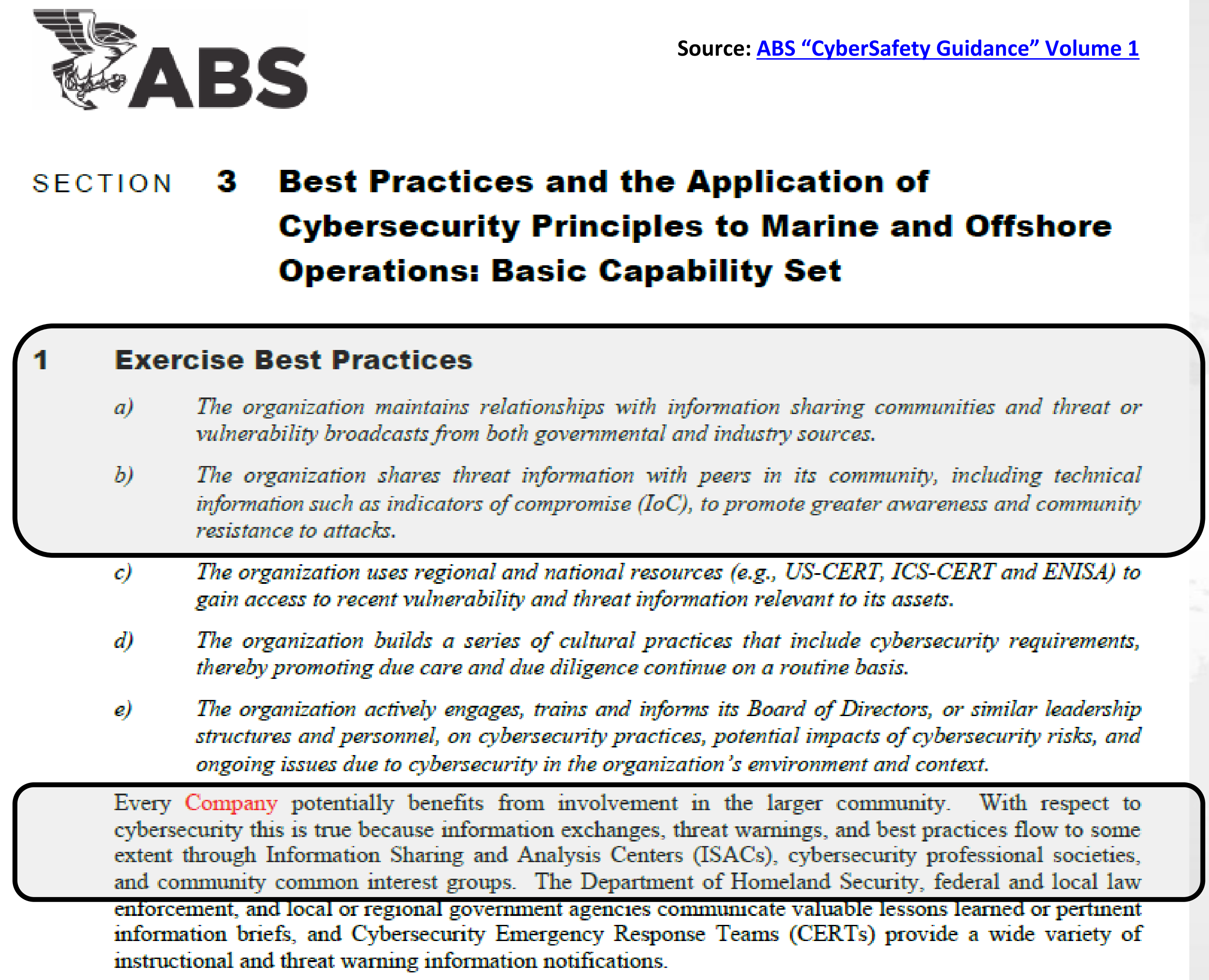
Group	Motivation	Objective
Activists (including disgruntled employees)	• Reputational damage • Disruption of operations	• Destruction of data • Publication of sensitive data • Media attention • Denial of access to the service or system targeted
Criminals	• Financial gain • Commercial espionage • Industrial espionage	• Selling stolen data • Ransoming stolen data • Ransoming system operability • Arranging fraudulent transportation of cargo • Gathering intelligence for more sophisticated crime, exact cargo location, off vessel transportation and handling plans etc
Opportunists	• The challenge	• Getting through cyber security defences • Financial gain
States State sponsored organisations Terrorists	• Political gain • Espionage	• Gaining knowledge • Disruption to economies and critical national infrastructure

Table 1. Motivation and objectives

Employees: Accidental Loss

Source: BIMCO "The Guidelines on Cyber Security Onboard Ships"

ABS' CyberSafety™ Says, "Share"



Source: ABS "CyberSafety Guidance" Volume 1

SECTION 3 Best Practices and the Application of Cybersecurity Principles to Marine and Offshore Operations: Basic Capability Set

1 Exercise Best Practices

a) *The organization maintains relationships with information sharing communities and threat or vulnerability broadcasts from both governmental and industry sources.*

b) *The organization shares threat information with peers in its community, including technical information such as indicators of compromise (IoC), to promote greater awareness and community resistance to attacks.*

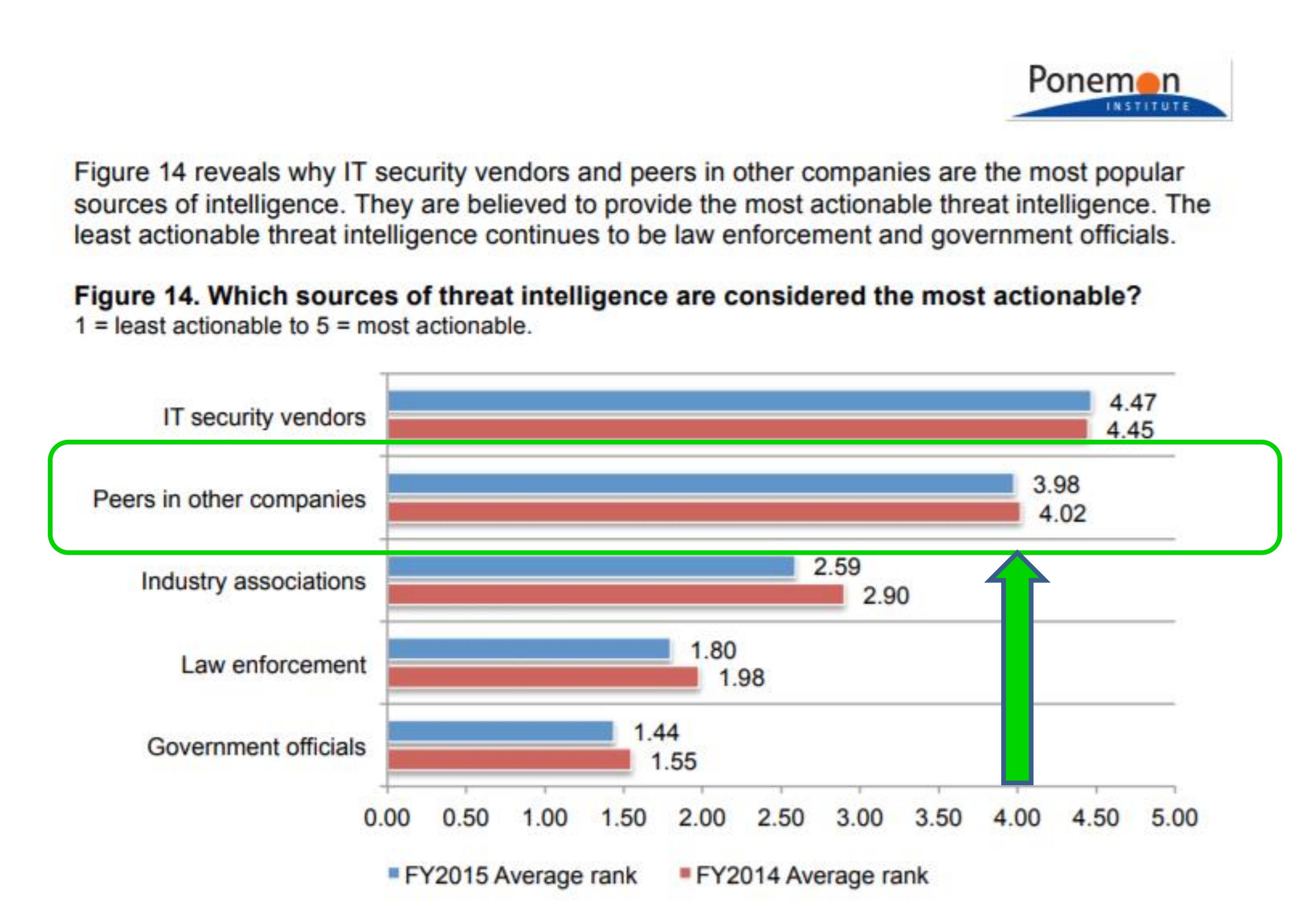
c) *The organization uses regional and national resources (e.g., US-CERT, ICS-CERT and ENISA) to gain access to recent vulnerability and threat information relevant to its assets.*

d) *The organization builds a series of cultural practices that include cybersecurity requirements, thereby promoting due care and due diligence continue on a routine basis.*

e) *The organization actively engages, trains and informs its Board of Directors, or similar leadership structures and personnel, on cybersecurity practices, potential impacts of cybersecurity risks, and ongoing issues due to cybersecurity in the organization's environment and context.*

Every Company potentially benefits from involvement in the larger community. With respect to cybersecurity this is true because information exchanges, threat warnings, and best practices flow to some extent through Information Sharing and Analysis Centers (ISACs), cybersecurity professional societies, and community common interest groups. The Department of Homeland Security, federal and local law enforcement, and local or regional government agencies communicate valuable lessons learned or pertinent information briefs, and Cybersecurity Emergency Response Teams (CERTs) provide a wide variety of instructional and threat warning information notifications.

Ponenom Institute



Ponemon INSTITUTE

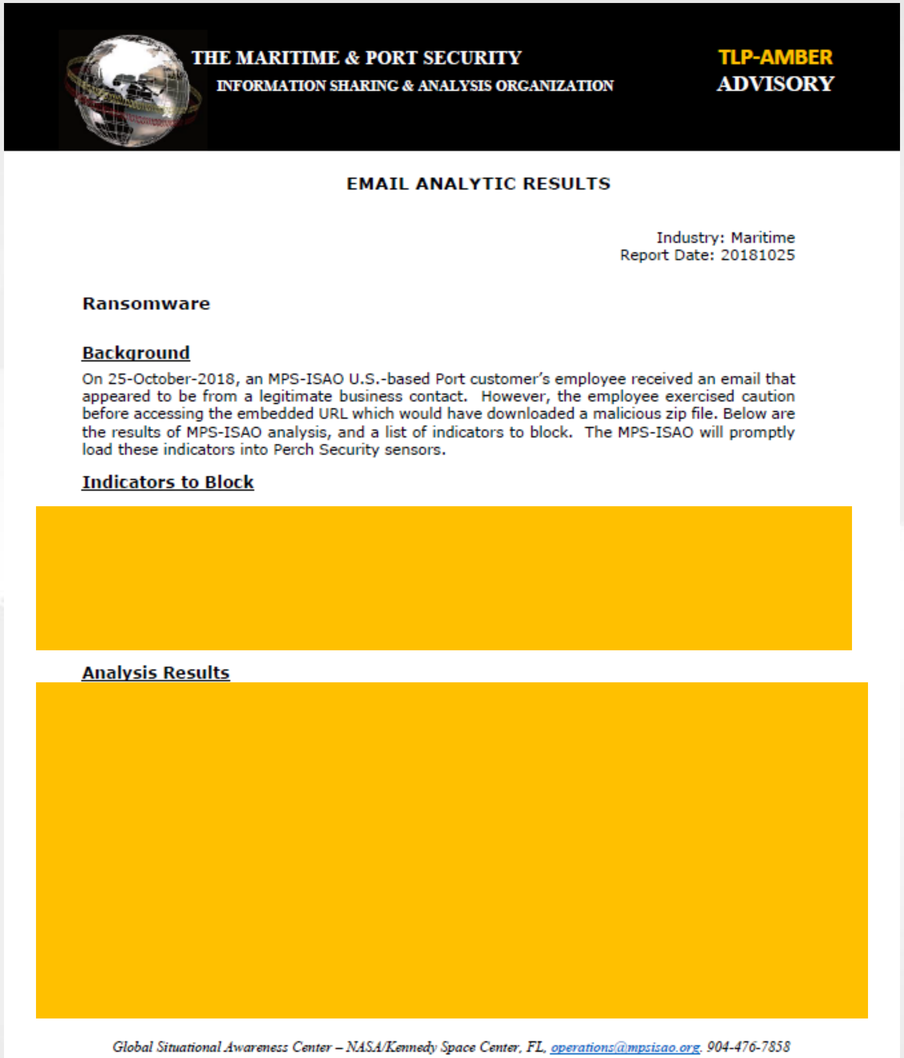
Figure 14 reveals why IT security vendors and peers in other companies are the most popular sources of intelligence. They are believed to provide the most actionable threat intelligence. The least actionable threat intelligence continues to be law enforcement and government officials.

Figure 14. Which sources of threat intelligence are considered the most actionable?
1 = least actionable to 5 = most actionable.

Ponemon Institute: Second Annual Study on Exchanging Cyber Threat Intelligence There Has to Be a Better Way

When things go “south”…

Ransomware



THE MARITIME & PORT SECURITY
INFORMATION SHARING & ANALYSIS ORGANIZATION

TLP-AMBER
ADVISORY

EMAIL ANALYTIC RESULTS

Industry: Maritime
Report Date: 20181025

Ransomware

Background

On 25-October-2018, an MPS-ISAO U.S.-based Port customer's employee received an email that appeared to be from a legitimate business contact. However, the employee exercised caution before accessing the embedded URL which would have downloaded a malicious zip file. Below are the results of MPS-ISAO analysis, and a list of indicators to block. The MPS-ISAO will promptly load these indicators into Perch Security sensors.

Indicators to Block

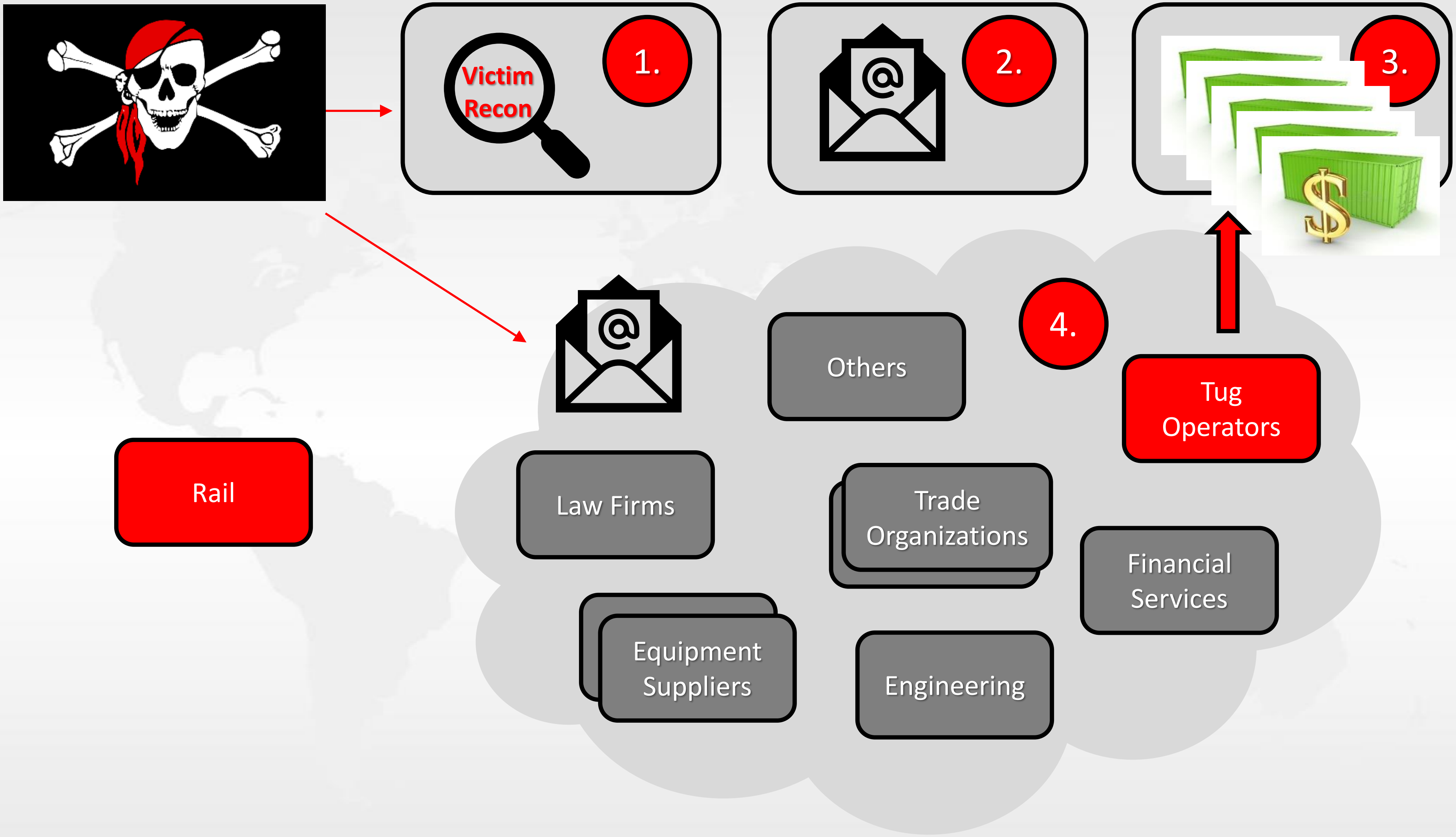
[redacted]

Analysis Results

[redacted]

Global Situational Awareness Center – NASA/Kennedy Space Center, FL, operations@mpsisao.org, 904-476-7858

Partners / Supply Chain



1.

Victim Recon

2.

3.

4.

Others

Tug Operators

Rail

Law Firms

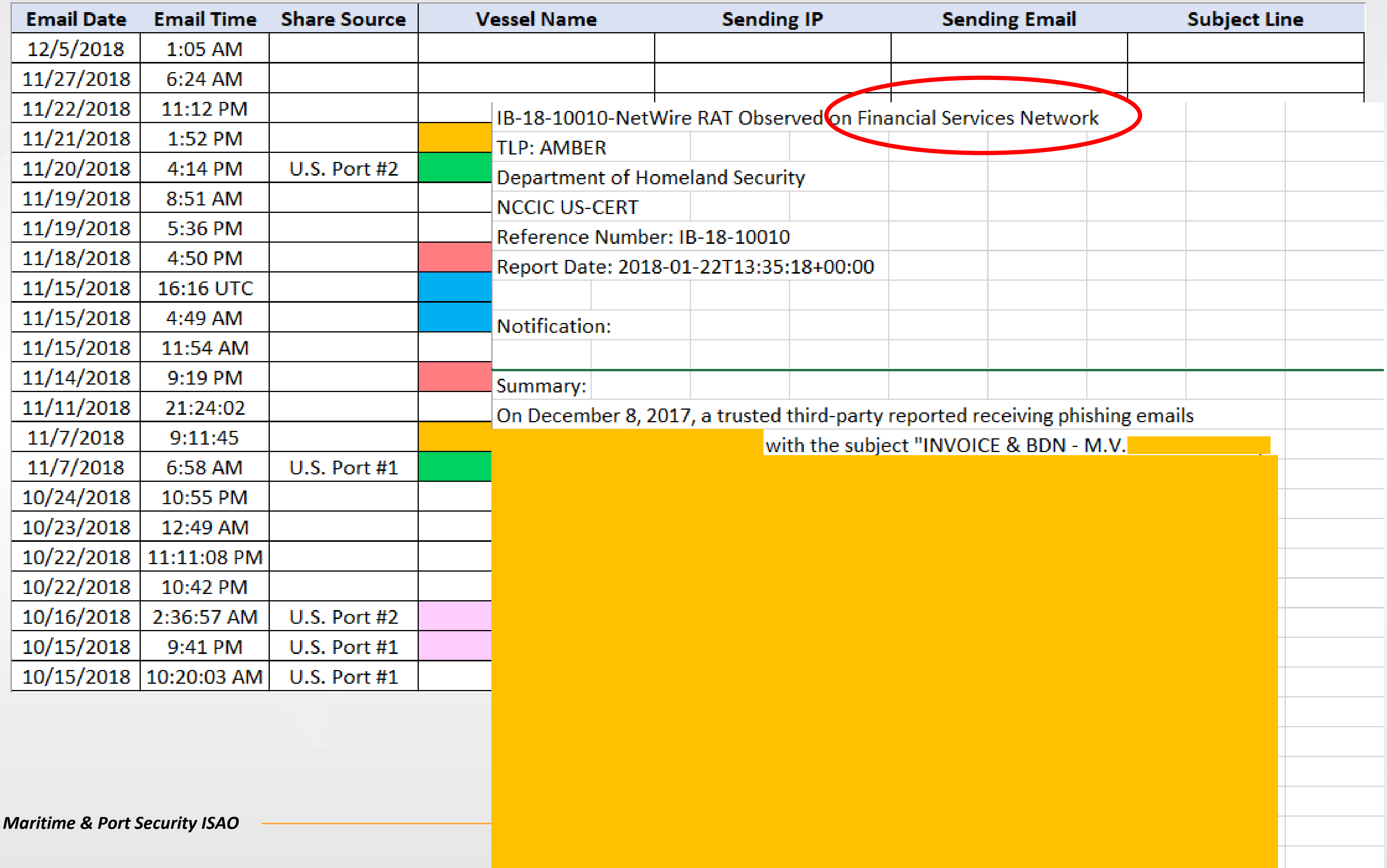
Trade Organizations

Financial Services

Equipment Suppliers

Engineering

Malicious Vessel Impersonation Emails



Email Date	Email Time	Share Source	Vessel Name	Sending IP	Sending Email	Subject Line
12/5/2018	1:05 AM					
11/27/2018	6:24 AM					
11/22/2018	11:12 PM					
11/21/2018	1:52 PM		🟧			
11/20/2018	4:14 PM	U.S. Port #2	🟩			
11/19/2018	8:51 AM					
11/19/2018	5:36 PM					
11/18/2018	4:50 PM		🟥			
11/15/2018	16:16 UTC		🟦			
11/15/2018	4:49 AM		🟦			
11/15/2018	11:54 AM					
11/14/2018	9:19 PM		🟥			
11/11/2018	21:24:02					
11/7/2018	9:11:45		🟧			
11/7/2018	6:58 AM	U.S. Port #1	🟩			
10/24/2018	10:55 PM					
10/23/2018	12:49 AM					
10/22/2018	11:11:08 PM					
10/22/2018	10:42 PM					
10/16/2018	2:36:57 AM	U.S. Port #2	🟪			
10/15/2018	9:41 PM	U.S. Port #1	🟪			
10/15/2018	10:20:03 AM	U.S. Port #1				

IB-18-10010-NetWire RAT Observed on Financial Services Network

TLP: AMBER

Department of Homeland Security

NCCIC US-CERT

Reference Number: IB-18-10010

Report Date: 2018-01-22T13:35:18+00:00

Notification:

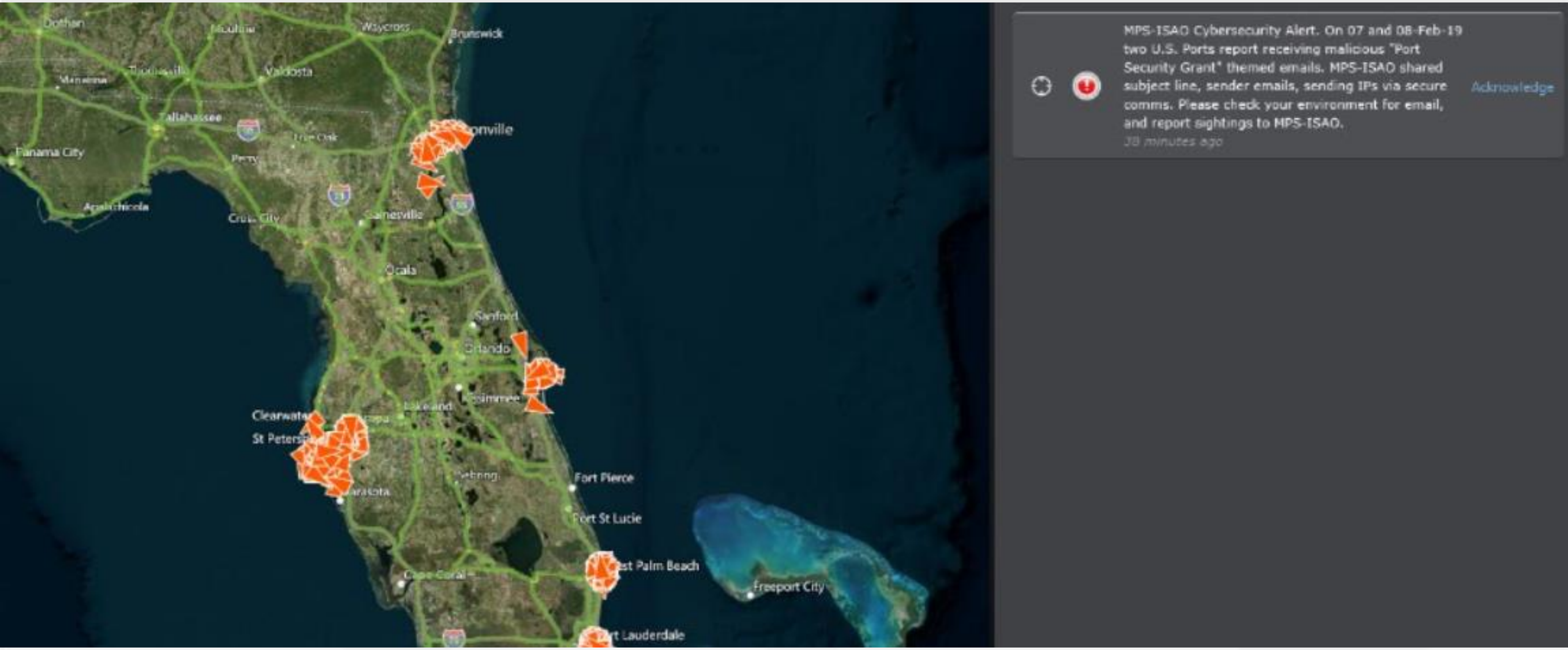
Summary:

On December 8, 2017, a trusted third-party reported receiving phishing emails

[redacted] with the subject "INVOICE & BDN - M.V. [redacted]

[redacted]

Early Situational Awareness

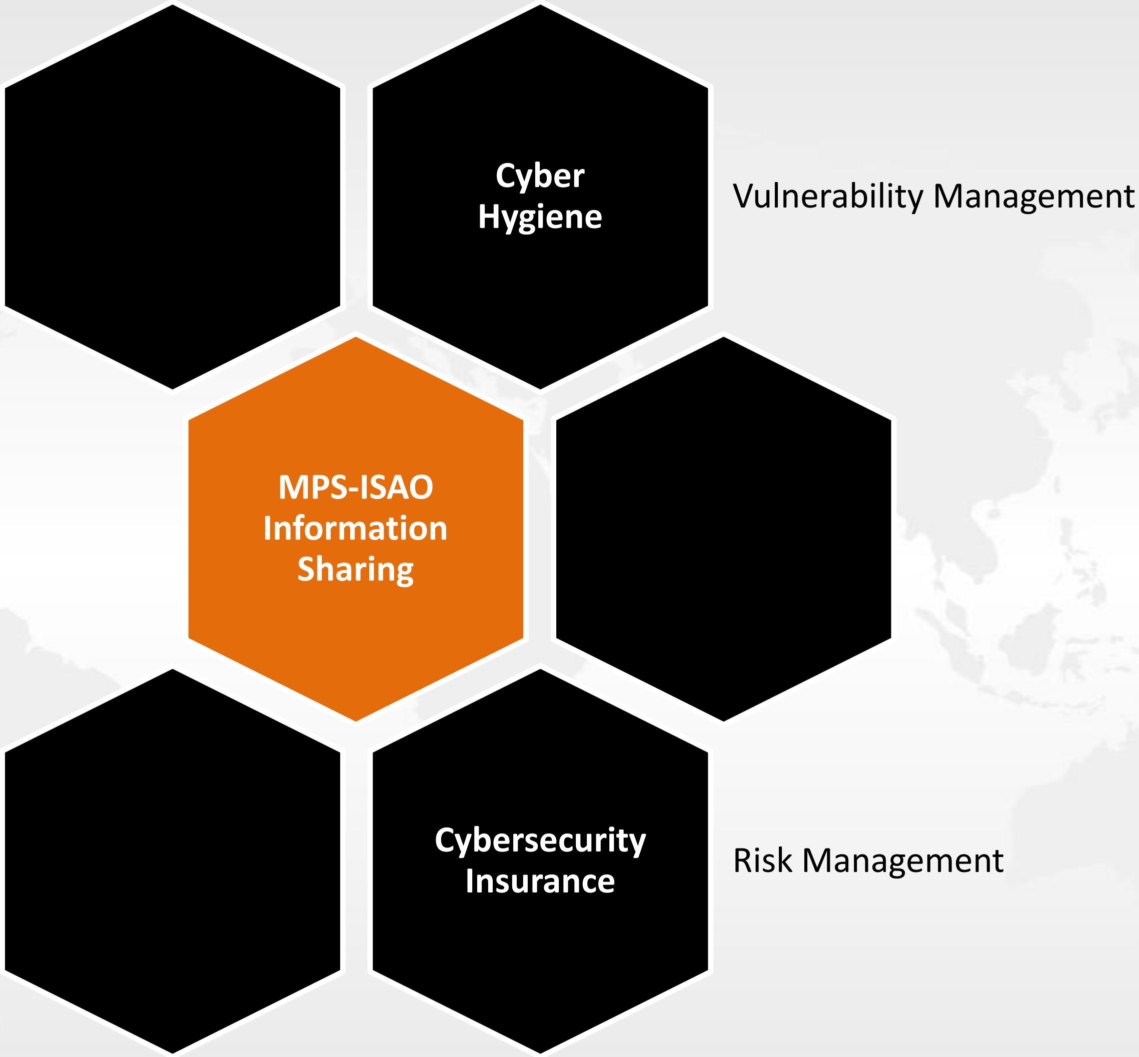


MPS-ISAO Cybersecurity Alert. On 07 and 08-Feb-19 two U.S. Ports report receiving malicious "Port Security Grant" themed emails. MPS-ISAO shared subject line, sender emails, sending IPs via secure comms. Please check your environment for email, and report sightings to MPS-ISAO.

38 minutes ago

MPS-ISAO Alert via CommandBridge Platform

What do you do?



Cyber Hygiene

Vulnerability Management

MPS-ISAO Information Sharing

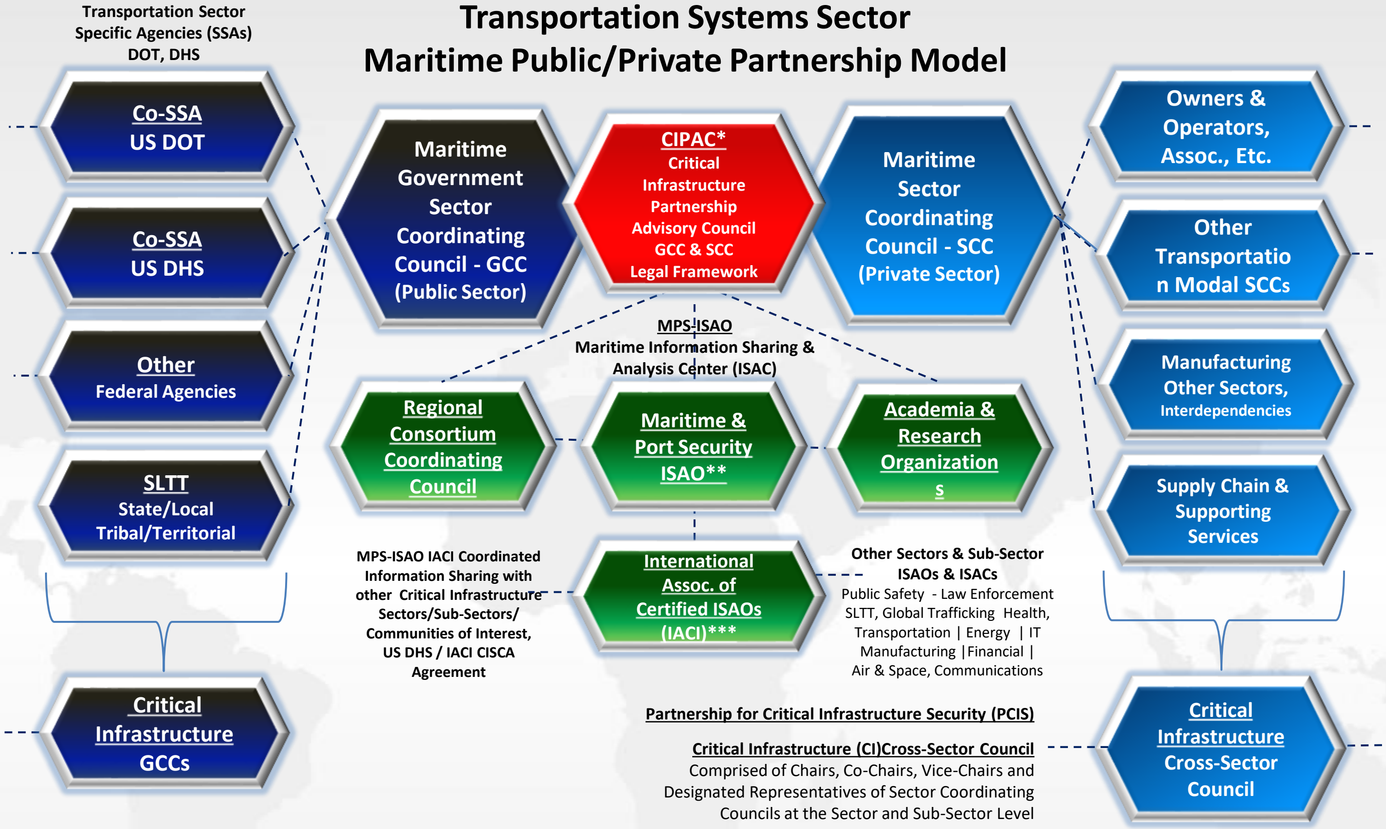
Cybersecurity Insurance

Risk Management

Christy.Coffey@mpsisao.org

Sector Coordinating Council

Transportation Systems Sector
Maritime Public/Private Partnership Model



Transportation Sector Specific Agencies (SSAs) DOT, DHS

Co-SSA US DOT

Co-SSA US DHS

Other Federal Agencies

SLTT State/Local Tribal/Territorial

Critical Infrastructure GCCs

Maritime Government Sector Coordinating Council - GCC (Public Sector)

CIPAC* Critical Infrastructure Partnership Advisory Council GCC & SCC Legal Framework

Maritime Sector Coordinating Council - SCC (Private Sector)

Owners & Operators, Assoc., Etc.

Other Transportatio n Modal SCCs

Manufacturing Other Sectors, Interdependencies

Supply Chain & Supporting Services

Critical Infrastructure Cross-Sector Council

MPS-ISAO Maritime Information Sharing & Analysis Center (ISAC)

Regional Consortium Coordinating Council

Maritime & Port Security ISAO**

Academia & Research Organization s

International Assoc. of Certified ISAOs (IACI)***

MPS-ISAO IACI Coordinated Information Sharing with other Critical Infrastructure Sectors/Sub-Sectors/ Communities of Interest, US DHS / IACI CISCA Agreement

Other Sectors & Sub-Sector ISAOs & ISACs
Public Safety - Law Enforcement
SLTT, Global Trafficking Health,
Transportation | Energy | IT
Manufacturing |Financial |
Air & Space, Communications

Partnership for Critical Infrastructure Security (PCIS)

Critical Infrastructure (CI)Cross-Sector Council
Comprised of Chairs, Co-Chairs, Vice-Chairs and Designated Representatives of Sector Coordinating Councils at the Sector and Sub-Sector Level

Chemical
Commercial
Communications
Critical Manufacturing
Dams
Defense
Emergency Services
Energy
Financial Services
Food & Agriculture
Government Facilities
Healthcare & Public Health
Information Technology
Nuclear Reactors & Waste Management
Water & Wastewater

Chemical
Commercial
Communications
Critical Manufacturing
Dams
Defense
Election
Emergency Services
Energy
Financial Services
Food & Agriculture
Government Facilities
Healthcare & Public Health
Information Technology
Nuclear Reactors & Waste Management
Water & Wastewater

* *CIPAC provides the legal framework (mechanism) for GCC (public) and SCC (private-sector) Members to engage (coordination and collaboration) in joint critical infrastructure protection activities.*

** *The Maritime & Port Security ISAO (MPS-ISAO), a nonprofit Information Sharing Analysis Organization (ISAO) is the Information Sharing Analysis Center (ISAC) for the Maritime Sector – ISAO Authorized by Presidential EO 13691, CISA Act, and US DHS / MPS-ISAO - CISCA Agreement*

*** *International Association of Certified ISAOs (IACI) – "Center of Gravity", Global ISAO Association Supporting and Connecting ISAO/ISAC Information Sharing & Response ISAO Authorized by Presidential EO 13691, CISA Act, and US DHS/IACI – CISCA Agreement*