TLP: RED

WRITTEN BRIEF

November 11, 2022

TO: National Security Council
FROM: Still Cool With Whatever [Kaitlyn Colin, Jared Stancombe, Oyedotun Oyesanmi, Ryan Walsh]
RE: Situation, Assessment, and USG Responses to Reported Cyber Incidents Involving US MTS

Situation Summary: As we enter peak shipping season, a series of reported cyber incidents are threatening to impact the Maritime Transportation System (MTS) and shipping operations. These threats include an ongoing cyber incident where shipping manifests appear compromised on three vessels recently moored at the Port of Long Beach (POLB), as well as a credible ransomware threat against major shipping companies. These incidents have potential to threaten US port security as well as the overall economy, and they require a coordinated federal response with state and private sector partners led by the US Coast Guard (USCG) under PPD-21.

Recommended Plans of Action:

- **Recommendation 1:** USCG will direct the investigation of threats to physical and cyber security at the POLB and the MTS in coordination with USG, SLTT, and private sector stakeholders.
- **Recommendation 2:** CISA will coordinate asset response with USG and SLTT partners to support maritime stakeholders' response to the cargo management software vulnerability and ransomware threats.
- **Recommendation 3:** US Intelligence Community partners will provide intelligence and support to relevant USG and SLTT agencies for law enforcement investigations, critical infrastructure protection, and global threat intelligence.

Situation Severity: This series of incidents is categorized as a "cyber incident" under PPD-41. There may be impacts related to national and economic security interests, but at this time given factors such as functional impact, observed activities, and information impacts, it is unlikely that there could be a demonstrable impact.

There are risks of escalation to a "significant cyber incident" due to factors such as recoverability, threat actor characteristics, and cross-sector dependencies between the MTS and other critical infrastructure sectors such as critical manufacturing, food and agriculture, and energy services. This triggers mechanisms outlined in PPD-41, including a Cyber Unified Coordination Group (UCG).

Response Implementation:

Recommendation 1: USCG will direct the investigation of threats to physical and cyber security at the POLB and the MTS in coordination with USG, SLTT, and private sector stakeholders.

- The USCG Investigative Service (CGIS) will coordinate with FBI Los Angeles Field Office with intelligence support from the DHS Intelligence & Analysis (DHS I&A) Deployed Intelligence Officer (IO) to review personnel records to identify any affiliations with foreign terrorist

organizations (FTOs) or homegrown violent extremist (HVE) organizations and identify potential precursors to terrorist activities.
- Deploy CISA Protective Security Advisors (PSAs) to support USG, SLTT, and private sector stakeholders to identify weaknesses in physical security at the POLB.
- Maritime & Port Security Information Sharing and Analysis Organization (MPS-ISAO) will coordinate with relevant partners to provide threat intelligence regarding cybersecurity and physical security information to MTS partners.

Recommendation 2: CISA will coordinate asset response with USG and SLTT partners to support maritime stakeholders' response to the cargo management software vulnerability and ransomware threats.

- US-CERT will coordinate with software vendor on mitigating the software vulnerability.
- ICS-CERT and National Cybersecurity and Communications Integration Center Hunt and Incident Response Team (NCCIC HIRT) will coordinate with affected companies whose vessel and cargo management systems have been compromised to identify if ICS systems have also been compromised.
- Deploy CISA Cybersecurity Advisors (CSAs) to work with maritime companies to strengthen systems and networks against physical and cyber threats and coordinate responses to immediate ransomware threats.
- The USCG will (1) provide support to US-CERT, ICS-CERT, HIRT, and other stakeholders if requested (2) issue a Marine Safety Information Bulletin (MSIB) regarding the ransomware threat; and (3) inform members of the Maritime Sector Coordinating Council (SCC) on the ransomware threat and software vulnerability.
- MPS-ISAO will issue a threat intelligence advisory regarding the nature of the software vulnerability and steps to report potential issues.

Recommendation 3: Intelligence Community partners will provide intelligence and support to relevant USG and SLTT agencies for law enforcement investigations, critical infrastructure protection, and global threat intelligence.

- NSA will continue monitoring TPM activities for risk indicators.
- DHS I&A will coordinate with Coast Guard Intelligence (CGI) and CISA to monitor threats to US ports and maritime security.
- FBI Cyber Division Cyber Assistant Legal Attachés (ALATs) will work with foreign law enforcement on identifying, disrupting, and dismantling cyber threat actors and organizations attacking foreign ports and maritime critical to the US.
- The Office of Naval Intelligence (ONI) and the CIA will monitor cyber threats in international waters, focusing on nation-state and terrorist threats in the Strait of Malacca and South China Sea.
- ODNI will monitor whether a combination of this intelligence indicates a threat at level 3 or higher.

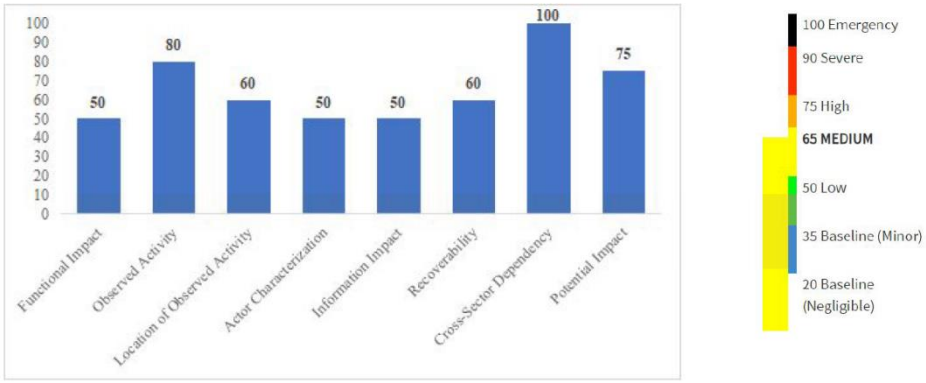
This team will monitor these ongoing incidents and keep the NSC informed of further updates or escalation recommendations as the situation evolves.

DECISION DOCUMENT – DAY ONE

Still Cool With Whatever - Kaitlyn Colin, Jared Stancombe, Oyedotun Oyesanmi, Ryan Walsh, Rachel Dockery

Methodology: PPD-41 (US Cyber Incident Coordination), PPD-21 (Critical Infrastructure Security and Resilience), and the National Incident Preparedness Plan (NIPP) are instructive when identifying the lines of effort, response activities, and sector specific agencies (SSA) for the maritime sector. The Cyber National Incident Response Plan (NCIRP) and the NCCIC Cyber Incident Scoring System (NCISS) are used to assess the severity of the incidents and develop recommended actions. Each response has three lines of effort--threat response, asset response, and intelligence support coordination involving USG, SLTT, and private sector partners.

Severity Analysis: This situation is currently a **Level 2 (medium)** according to PPD-41 and NCCIC NCISS with a score of **62.**



Response Priority:

	High Priority (24 hrs)	**Medium Priority (48-72 hrs)**	**Low Priority (1 week)**
Recommendation 1	CGIS/FBI investigation CISA IO deployment to POLB	Deploy PSAs to POLB	MPS-ISAO threat intelligence to MTS partners
Recommendation 2	NCCIC coordination	Deploy CSAs to POLB MSIB dissemination to MTS partners	USCG and SCC coordination MPS-ISAO threat intelligence
Recommendation 3	DHS I&A coordination FBI ALATs coordination	NSA monitoring TPM ONI & CIA coordination	ODNI monitoring

Additional Policy Considerations:

- The US Coast Guard is the (SSA) as defined in the National Incident Preparedness Plan (NIPP) for maritime/ports. We assess that DOT involvement is not required at this time, but could be if this grows to involve more MTS stakeholders.
- Further DOD involvement with ODNI leading intelligence coordination could be necessary if the situation severity level increases, but the current assessment does not warrant direct involvement given the information at this time.

- If additional information gathering merits categorizing this as a “significant cyber incident” or above, this would require Cyber UCG formation.

Escalation Risks:

- It is currently unknown if threat actors are acting on behalf of nation-state actors and/or domestic terrorist organizations.
- Many critical infrastructure sectors are dependent upon the MTS, including but not limited to energy, food and agriculture, critical manufacturing, and information technology. Disruptions could significantly impact American economy.
- Current activities could be cyber/physical attack precursors that threaten a larger number of vessels.

DECISION DOCUMENT – DAY TWO

Objectives

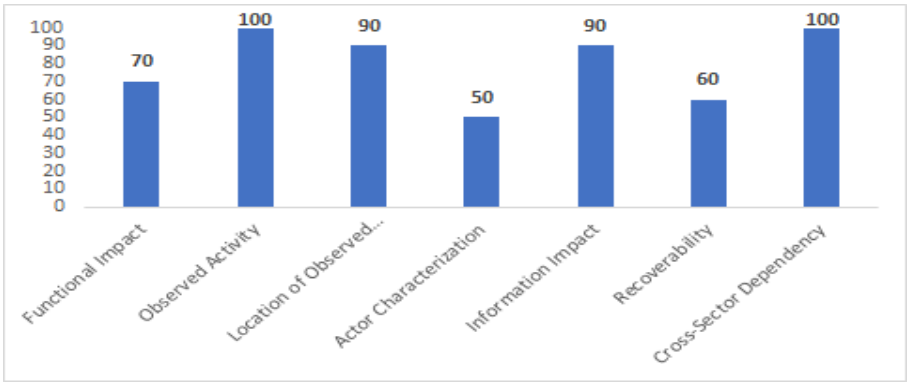
1. To protect and restore global shipping
2. To protect national security and critical infrastructure
3. To respond to and mitigate domestic and global economic effect

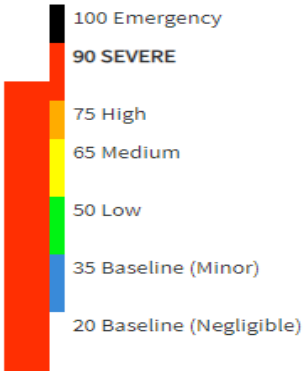
Recommendations

1. A Cyber UCG should be created to coordinate response to the current maritime cyber incidents
2. The FEMA Administrator should activate the FEMA NRCC to Level 2
3. DOS, DOT, DOC continuing to work with their partners to coordinate a global economic response

Severity Analysis:

- This situation requires a **Level 2 activation of FEMA** due to economic and public safety impacts
- This situation is currently a **Level 4 (SEVERE)** according to PPD-41 and NCCIC NCISS with a score of **80.**





Response Priority:

	Severe Priority (12-24 hrs)	**High Priority (24-36 hrs)**	**Medium Priority (36-48+ hrs)**
Objective 1	Cyber UCG asset response through NCCIC	USINDOPACOM will protect U.S. maritime interests	USCG coordinates racom implementation
Objective 2	Activate FEMA NRCC to Level 2 Create Cyber UCG	ODNI will monitor Pacific region	
Objective 3	DOS will coordinate with Indonesia, Malaysia, & Singapore on economic response	DOT will coordinate with IMO	USTR will coordinate with ASEAN on economic response

Escalation Risks

- It is currently unknown if threat actors are acting on behalf of nation-state actors and/or domestic terrorist organizations.
- The potential further impact on the global economy leading to supply chain shocks or civil unrest.
- Current activities could be cyber and/or physical attack precursors that threaten a larger number of vessels.