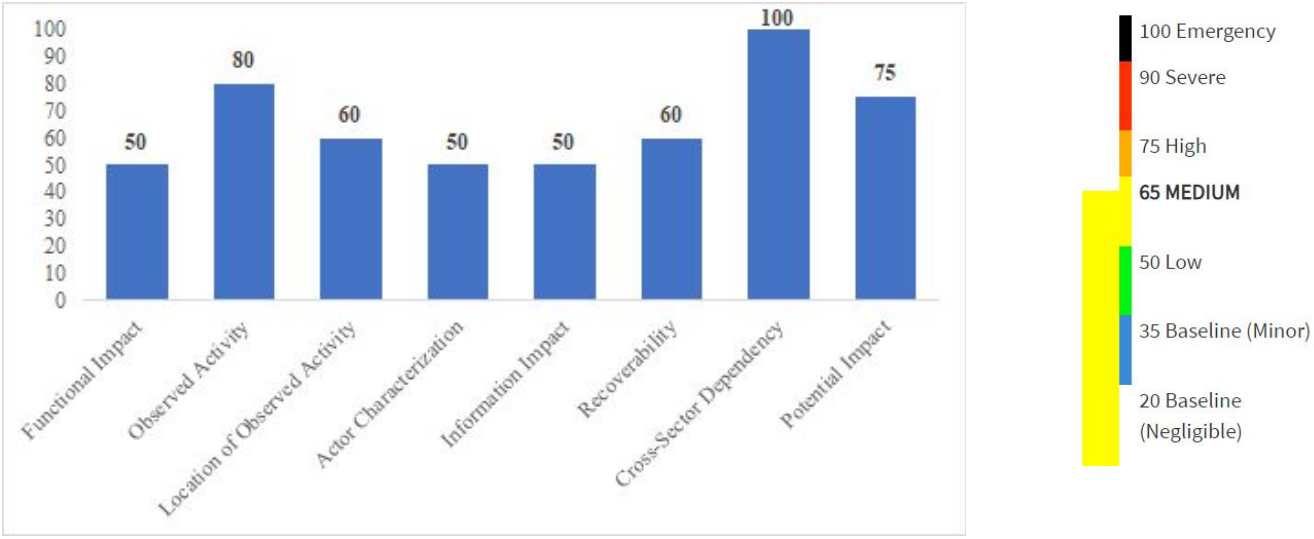
DECISION DOCUMENT

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.