TO: National Security Council
FROM: NSC Cybersecurity Task Force 'Couldn't Hack It 2.0'
Subject: *Policy to Prevent Economic Disruption and Preserve Safety of Navigation and U.S. Personnel*

Summary:

We believe that the primary objectives for the USG are to **prevent economic disruption** and **preserve safety of navigation and U.S. personnel**. To accomplish this, we recommend DHS coordinate national response and increase information sharing regarding vulnerabilities between stakeholders. State Department should work with foreign partners to inform and coordinate international response. Department of Transportation should bolster manning on U.S. flagged shipping while USCG works to secure U.S. ports and preserve safety of navigation and personnel in U.S. territorial waters.

Policy Options:

A) Minimum Response:

- Direct DHS to coordinate activities in the United States
- Share information on CMS vulnerability at POLB with Maritime and Port Authority of Singapore
- Clarify end destination for all three infected vessels
- State Department to advise strategic partners in the region to coordinate response. Warn authorities in Manila, Yokohama, Qingdao, Hong Kong of malware threat
- U.S. Embassy (FBI, CBP, and TSA) should also coordinate with East Asian and Pacific Affairs (EAP) to inform host governments of potential threats and engage them as necessary. U.S. Embassy in Beijing should inquire about raised security level for shipping vessels
- DHS CISA to coordinate with Big Oceans Little Hearts LLC to conduct an investigation of the SEAFARER vulnerability

We assess that Policy A is necessary but insufficient. Due to the unintrusive nature of these recommendations, they do not adequately address safety concerns and will not sufficiently prevent the spread of the malware. Policy A should be carried out in concert with Policy B.

B) Moderate Response **(RECOMMENDED):**

- DHS CISA to work with BOLH and local Port Authorities to ensure ships with possible infections do not transfer data with other ports
- DHS USCG to prevent incoming vessels from interfacing directly between infected POLB systems and provide assistance to the Singaporian Government, if necessary
- U.S. Embassy in Singapore encourages Singaporian Government to deploy its Coast Guard to aid vessels in trouble and to provide USG assistance as necessary with US Embassy personnel
- U.S. Department of Transportation to increase manning on all US-flagged commercial shipping.
- USINDOPACOM to inquire if MSC ships use SEAFARER. NCIS to screen U.S. Navy ports in region

The following responses were considered extreme at the moment as they would place undue pressure on shipping routes and companies. They are worth revisiting should the threat escalate.

C) Severe Response:

- State Department to recommend Singapore divert shipping vessels for non essential trade to Sunda and Lombok Straits and provide Foreign Assistance to help bear the cost of associated diversions
- Department of Homeland Security to enact regulations on incoming commercial vessels to US territorial waters for safety of navigation and prevent smuggling

Recommendation Justification:

NSC should focus on preventing economic disruption and safety of U.S. personnel while minimizing disruption to shipping activities. Our recommended policy (B) enables responding organizations to contain the spread of the malware and implement measures to protect U.S. shipping operations and personnel, without disrupting shipping routes and imposing restrictions on foreign shipping vessels entering U.S. waters.