To: National Security Council
From: NSC Cybersecurity Task Force ‘Couldn’t Hack It 2.0’
Subject: Policy Recommendations to Restore Global Ports, Shipping Routes, and Supply Chains

Summary:
The malware affecting SEAFARER cargo management system has spread to ships and ports globally, causing massive port delays and safety of navigation concerns and severely impacting maritime trade. The primary objective for the USG is to **protect our homeland security** and the **global economy** by restoring ports, clearing shipping routes, and protecting supply chains. The situation is no longer purely domestic and will require NSC action to initiate robust international engagement to prevent further spread of the malware and ensure safety of navigation, while launching domestic efforts to alleviate port congestion and identify and deter the threat actor.

Recommendations:
It is necessary for the NSC to coordinate an interagency approach with the following policy responses:

- **Launch an FBI investigation** into potential U.S. based threat actors and gather additional intelligence on North Korean activity from the NSA to anticipate future threats and prevent additional attacks.
- **Engage trade associations through DOC** and **engage ICT Supply Chain Risk Management Task Force** through CISA to work to protect supply chains and manage shipping crises.
- **Work with the International Maritime Organization (IMO) to issue regulations r**egarding Automatic Identification Systems (AIS) through the USCG to ensure safety of navigation.
- **Sanitize all merchant vessels in U.S. waters;** issuing DOT to follow IMO Guidance on Cyber Risk Managemen**t** to prevent the spread of malware.
- **Engage with the Chinese Government** using the DHS CISA’s Cybersecurity Hotline to coordinate a USG-Chinese response to alleviate port congestion.
- **DOS begin dialogue with S. Korea, Japan, India, and Australia** through our security cooperation agreements; encouraging China to engage in USG international response plan
- **Mirror Port of Osaka response** with development of new systems that prioritize critical functions for Port Authority in Long Beach and make it an open-source system through a Public Private Partnership
- **Unlock FEMA emergency grants** to provide assistance to U.S. shipping companies and Local Port Authorities to bolster cybersecurity incident response to restore ports.

Decision Process (Assessment and Risks of Recommendations):
It is important that the USG take swift action to resolve the disruption of maritime trade and supply chains by implementing the policy recommendations above. These options seek to mitigate the global crisis by working to gather intelligence to prevent further attacks and initiate law enforcement efforts to deter potential domestic threat actors, engage China through law enforcement channels, take global lead in response through International Organizations and partnerships, and provide assistance to U.S. companies and Local Government.

However, there are key risks associated with these recommendations that should be weighed carefully before implementation. First, there is the risk that the USG is unable to fully mitigate and contain the cybersecurity threat. Second, there is the risk that the International Community is less responsive to USG actions due to our inability to contain the malware spread originally. Additionally, if the USG takes charge of the situation internationally, our lead could result in an increase in Chinese defensive posture.

Additional Response Options Considered to Alleviate Port Congestion and Further Engage with China

- (Severe) DoD to increase military posture in the South China Sea to aid ship navigation
- (Severe) Declaring National Emergency to unlock funding to provide federal money to ports in need until the other efforts are exhausted