TO: National Security Advisor
FROM: Georgetown University - STIA Cyber Team
SUBJECT: SEAFARER Cargo Management Software Cyber-Attack

Judgements: The cyberattack on Long Beach Port threatens U.S. economic stability and impacts Trans-Pacific trade and failing to deter future attacks will harm U.S. interests. While it is *not* possible to attribute this attack currently, the dissemination of the malware kit online *poses an immediate potential threat to ports in over 30 countries which endangers the global economic system*. A rapidly deployed patch and successful multi-layered approach addressing our immediate, short, and long-term approach will mitigate the impact of future attack attempts and build strategic deterrence.

Background: On October 23 a cyber-attack against a widespread vulnerability the SEAFARER cargo management software corrupted manifests on three sea vessels that departed from Long Beach Port in California. The vulnerability could damage U.S. shipping processes at large, especially during the holiday season. Attackers exploited a Windows XP vulnerability affecting SEAFARER management software. After departing Long Beach Port in November, two vessels identified problems with their manifests while en route to Shanghai. One vessel's manifest did not correspond with containers taken in at Long Beach. Early indications are that *this attack is not limited to just American vessels and there is potential that it may impact dozens of other vessels internationally.*

On November 5, an unknown actor released a cache of sophisticated cyber weapons that threatens shipping entities utilizing SEAFARER systems. SEAFARER software is owned by Little Ocean Big Heart (LOBH), a major player in the shipping industry. LOBH maintains identification, tracing, and manifest systems for more 70% of the containerized and break-bulk cargo. The company handles more than 90% of gross tonnage for the Trans-Pacific market. If SEAFARER system malware is deployed, it could severely impact maritime trade between the U.S. and the Pacific region. 50% of global shipping passes through Asia by sea, and China's economy directs 33% of all world trade through the South China Sea.

Substantiation: We recommend a comprehensive multi-faceted approach to mitigate the immediate impact of this attack against U.S. values and interests. Our approach is designed to limit the potential of further attacks disrupting U.S. commerce, global supply chains, and the international economy. We recommend that the Department of Homeland Security (DHS) Cybersecurity Division spearhead the U.S. government response. DHS will work in tandem with USCYBERCOM's National Mission Teams (NMTs), the National Security Agency's (NSA) Cybersecurity Directorate, and the Federal Bureau of Investigation (FBI) Cyber Crime Division.

We propose a public-private approach, bringing together the DHS led-government response with private stakeholders including Microsoft, who runs the operating system; Symantec, for security expertise; and Cisco Talos, for forensic investigation. We attempt to move away from a *zero-defect approach* to focus on *strategic thinking, agility and innovation*. Private partners will be tasked with developing an immediate solution and patch to the Windows vulnerability. These

companies will also contribute to a mitigation process formulation led by DHS to train SEAFARER users in effective cyber hygiene procedures.

In the immediate term, we recommend that shipping companies cross reference software manifests with paper manifest copies. Container verification will diminish the impact of current attacks until a patch is in place. The U.S. federal government should facilitate inter-state, inter-agency, and public-private communication. The Department of State will act as the executive agent to liaise with other potentially impacted nations, and NSA and FBI will conduct cyber forensics and attempt to attribute the attack.[1]

In the short-term, we recommend that the Department of State engage with international partners to facilitate an international response that corresponds with the U.S. DHS-led effort to unite our partners under a clear set of common objectives. We also recommend that the DHS, NSA, FBI cyber teams, alongside CYBERCOM, engage with private sector and international partners to coordinate technical responses, build resilience, and deter future attacks.[2] Meanwhile, the NSA, CYBERCOM, and FBI should work towards attribution.[3]

In the long-term, the FBI criminal investigation and the Department of Justice should prosecute or indict the parties found responsible. An FBI criminal investigation will enable the Justice department to build an internationally accepted perception of legal normative costs for any actions that fall outside the boundaries of legal behavior in cyberspace and foster long-term deterrence.[4] This step also legitimizes potential retaliation, whether by conventional kinetic means or cyber operations. The criminal investigation sets the stage to provide definitions that allow the formation of legal codes that result in criminal convictions.[5] Furthermore, the results of the criminal investigation *underpin the emergence, acceptance, and internalization of institutional mechanisms that foster legal norms for the scope of actions that constitute legal behavior in cyberspace.*[6] The proposal also establishes a lower threshold in which the U.S. can legitimately respond with the full force of the U.S. criminal justice system to punish and deter other types of attacks.

These steps lay out a tactical and strategic path to protect and advance U.S. security and interests. They clarify government priorities and call for a multi-organizational technical response to mitigate impact of potential future attacks. The response addresses priorities and immediate steps to build up resilience to maintain normal global economic trade. It also calls for

[1] Under FISA, the government can gain evidence to attribute the attack and prosecute the attacker.
[2] Under the Third-Party Doctrine, individuals who give information to private companies have "no reasonable expectation of privacy" and the government can coordinate with private companies under this.
[3] Using methods such as PRISM and UPSTREAM, and under the Cybersecurity Act (2015).
[4] Under 18 USC 1030, the Computer Fraud and Abuse Act, various illegal behaviors related to computer use are outlined.
[5] Under USC 18 USC 2702, the Foreign Computer Crime Law, prosecution of a foreign actor is discussed.
[6] According to PPD-21, DHS "shall provide strategic guidance, promote a national unity of effort, and coordinate the overall Federal effort to promote the security and resilience of the Nation's critical infrastructure."

a U.S.-led coalition response alongside our allies and partners, which conveys a joint effort that fosters international cooperation and advances U.S. political legitimacy and norms in cyberspace.