Commander
U.S. Coast Guard Sector Northern New England
259 High Street
South Portland, Maine 04106
(207) 767-0303 / fax (207) 767-0308

# MARINE SAFETY INFORMATION BULLETIN
## [MSIB # 09–13]

**December 24, 2013**

## CYBERSECURITY AND THE MARINE TRANSPORTATION SYSTEM

Cyber systems are an integral part of our nation's maritime transportation system, and are vital to our nation's economy and security. However, cyber systems have unique vulnerabilities, many of which are not apparent to the casual user. Cyber attacks are a growing threat to our nation's maritime infrastructure, which can have costly, long term impacts. You are encouraged to use the information within this Marine Safety Information Bulletin (MSIB), and other source documents, to incorporate cybersecurity methods to prevent damage to, the unauthorized use of, or the exploitation of, electronic information systems, communications networks, and control systems, as well as the data contained therein. These voluntary actions may include:

1. Incorporating cybersecurity elements in relevant security assessments, plans, drills, and exercises.
2. Use of the following sources to educate yourself on cybersecurity:

   - The Department of Homeland Security (DHS) training website is a free source of basic cybersecurity training: http://www.dhs.gov/cybersecurity-training-exercises. The DHS Industrial Control Systems Cyber Emergency Response Team Website also provides information regarding best practices and cyber assessment tools: https://ics-cert.us-cert.gov.
   - A list of other DHS and FEMA funded training can be found at: http://teexweb.tamu.edu/nerrtc/
   - The Coast Guard has a Homeport Community that contains information on various cyber topics. Those interested in joining this community can go to the Homeport Website at https://homeport.uscg.mil and follow the instructions under Missions-Maritime Security-Cybersecurity.
   - Presidential Policy Directive 21 "Critical Infrastructure Security and Resilience", Executive Order 13636 "Improving Critical Infrastructure Cybersecurity," and the National Institute of Standards and Technology cybersecurity framework all provide a national framework for cybersecurity. These documents can be found within the Homeport Cybersecurity Community and also at the following link: http://www.nist.gov/itl/cyberframework.cfm.

3. Reporting all breaches of cybersecurity to the National Response Center (NRC) via their online reporting tool at http://www.nrc.uscg/mil or by phone at (800) 424-8802. Please note that cybersecurity breaches which meet the definition of 33 CFR 101.105 **must** be reported to the National Response Center. A cybersecurity breach that may require reporting occurs when an individual, entity, or application illegitimately enters a private or confidential Information Technology perimeter of a MTSA regulated Facility or Vessel, Maritime Critical Infrastructure/Key Resource, or Supervisory Control and Data Acquisition (SCADA) system, including but not limited to terminal operating systems, global positioning systems, or cargo management systems.

To report cybersecurity best practices, or to ask questions regarding this MSIB, please contact the Sector Northern New England Facilities Branch at 207-767-0333.

B. S. GILDA
Captain, U. S. Coast Guard
Captain of the Port
Sector Northern New England