The American Waterways Operators
www.americanwaterways.com

801 North Quincy Street
Suite 200
Arlington, VA 22203

PHONE: (703) 841-9300
FAX: (703) 841-0389
EMAIL: jcarpenter@vesselalliance.com

Jennifer A. Carpenter
Executive Vice President

April 15, 2015

Docket Management Facility (M-30)
U.S. Department of Transportation
West Building Ground Floor, Room W12-140
1200 New Jersey Avenue, SE
Washington, DC 20590-0001

RE: Guidance on Maritime Cybersecurity Standards (Docket No. USCG-2014-1020)

Dear Sir or Madam:

The American Waterways Operators is the national trade association for the tugboat, towboat and barge industry. AWO's members account for approximately 80 percent of the barge tonnage and two-thirds of the towing vessel horsepower in this critical industry segment, moving cargoes essential to the American economy on the inland rivers, the Atlantic, Pacific and Gulf coasts, and the Great Lakes. Tugboats also provide essential services, including shipdocking, tanker escort and bunkering, in ports and harbors around the country. On behalf of AWO's members, thank you for the opportunity to comment on the U.S. Coast Guard's development of guidance on maritime cybersecurity standards.

AWO is committed to working in partnership with the Coast Guard to ensure high standards of maritime domain awareness and security. Immediately after September 11, 2001, AWO began working with the Coast Guard and the U.S. Army Corps of Engineers to develop a Model Vessel Security Plan for towing vessels, more than a year before such plans were required by law. When the Maritime Transportation Security Act was enacted in November 2002, AWO worked with the Coast Guard to transform the Model Vessel Security Plan into one of the first Coast Guard-approved Alternative Security Programs, currently the most widely used ASP in the maritime industry. In addition to compliance with the AWO ASP, many members have also developed facility security plans in accordance with 33 CFR Part 105, and AWO has worked with the Coast Guard to develop training requirements for facility personnel. In the spirit of this strong partnership, we offer the following comments to assist the Coast Guard in developing guidance to assist vessel and facility owners and operators in identifying and addressing cybersecurity vulnerabilities.

In order to be successful, a cybersecurity strategy for the maritime industry must be able to be applied across all industry sectors and must be designed to accommodate the realities of diverse industry operations. Thus, it is especially important that the Coast Guard's cybersecurity guidance be both scalable and risk-based.

AWO's member companies are incredibly diverse in size and complexity. The largest companies have thousands of employees, more than a hundred towing vessels and thousands of barges, all managed with complex information systems. The smallest employ a small number of mariners, operate one or two vessels, and still keep paper records. Many of AWO's largest members manage their operations using systems that have multiple layers of firewalls and other protections against cyber incursions. Some of these companies have also developed social engineering and security awareness programs to help combat cybersecurity threats. However, these companies are not representative of the tugboat, towboat and barge industry as a whole, and we urge the Coast Guard not to consider them as models as the agency develops its cybersecurity guidance. The safeguards necessary to defend these companies' systems against cyber attack or disruption are not necessary or practicable for all tugboat, towboat and barge companies to implement.

Different companies of different sizes utilizing different systems will naturally have different risk profiles. We therefore urge the Coast Guard to ensure that any cybersecurity assessment methods it develops allow vessel and facility operators to identify their own critical cyber systems and cybersecurity risks and develop fleet- or facility-specific procedures to address them, as opposed to a "one size fits all" approach. This process could be supported by sector-specific guidance offered by the Coast Guard or general guidance such as the Cybersecurity Framework published by the National Institute of Standards and Technology.

Cyber Questions

To answer the questions that the Coast Guard posed to industry stakeholders in its December 12 *Federal Register* notice and at its January 15 public meeting, AWO canvassed its Security Working Group. The membership of this working group, comprising operational experts from AWO member companies, reflects the diverse profile of the tugboat, towboat and barge industry, with representation from large companies with expansive operations as well as small companies operating one or two vessels. While we have summarized the responses of working group members below, these should not be considered characteristic of industry-wide cybersecurity practices.

What cyber-dependent systems commonly used in the maritime industry could lead or contribute to a TSI if they failed or were exploited by an adversary?

On-board cyber-based systems that are commonly utilized by tugboats and towboats include Automatic Identification Systems (AIS), Global Positioning Systems (GPS) and satellite communication systems for voice and data services. The security of these systems is largely dependent upon the service provider rather than the user. Moreover, in the event that these

systems are compromised, vessels can operate safely without their assistance by utilizing secondary systems such as paper charts and radios. Personal computers are also utilized on board vessels for communication, storing charts and mapping waypoints. Appropriate firewalls and anti-virus software are installed on these PCs.

What procedures or standards do vessel and facility operators employ to identify potential cybersecurity vulnerabilities to their operations?

AWO members' cybersecurity risk assessment procedures range from widely-used commercial cybersecurity software to dedicated Information Technology departments and security consultants. Some larger member companies noted that cybersecurity is not usually an area of responsibility for a Vessel Security Officer or the Facility Security Officer. Since vessels are not dependent on cyber-based systems, cybersecurity is more often addressed by company IT departments, which function separately from vessel operations departments.

Are there existing cybersecurity assurance programs in use by industry that the Coast Guard could recognize?

To the best of our knowledge, any existing cybersecurity assurance programs in use in the tugboat, towboat and barge industry are unique to individual companies and have been developed in-house. However, some AWO members are in the process of aligning their cybersecurity policies with the NIST framework for critical infrastructure security as well as the International Organization for Standardization's ISO 27001.

What, if any, existing cybersecurity training programs does your company use?

As with cybersecurity assurance programs, there are no standard training programs in the tugboat, towboat and barge industry and any existing programs have been developed by individual vessel and facility operators. Those companies that have developed cybersecurity training programs report that annual cybersecurity awareness training, parameters for technology use while on board vessels and social engineering awareness are common training routines and topics for employees.

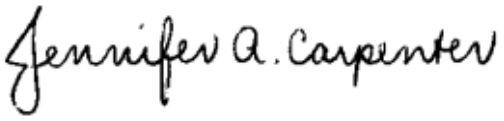
Are there existing best practices – from classification societies, protection and indemnity clubs or insurers – that your company has used or is currently using to inform your own cybersecurity policies and programs?

AWO members report that classification societies, P&I clubs and insurers have not provided them with cybersecurity best practices. Some larger vessel operators have cybersecurity parameters written into their insurance policies, but these are largely non-specific and provide requirements for systems that are not central to marine operations.

Conclusion

Thank you again for the opportunity to comment on the development of guidance on maritime cybersecurity standards. AWO appreciates the consideration that the Coast Guard has given to this issue and we look forward to working with the agency to develop cybersecurity guidance for the maritime industry that is scalable and risk-based. We would be pleased to discuss these comments further or to provide additional information and assistance as the Coast Guard sees fit.

Sincerely,



Jennifer A. Carpenter