National Grain and Feed Association

North American Export Grain Association

1250 Eye Street, N.W., Suite 1003, Washington, D.C., 20005-3922
NGFA: (202) 289-0873 NAEGA: (202) 682-4030

April 15, 2015

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

RE: Comments on US Coast Guard's Proposal to Develop Policy on Maritime Cyber-Related Vulnerabilities

To Whom It May Concern:

The National Grain and Feed Association (NGFA) and the North American Export Grain Association (NAEGA) are pleased to submit these joint comments on the U.S. Department of Homeland Security's notice of proposed rulemaking, published in the December 18, 2014 edition of the ***Federal Register***, to develop a policy to assist vessel and facility operators identify and address cyber-related vulnerabilities.

The NGFA, established in 1896, consists of more than 1,050 grain, feed, processing, exporting and other grain-related companies that operate more than 7,000 facilities and handle more than 70 percent of all U.S. grains and oilseeds. Its membership includes grain elevators; feed and feed ingredient manufacturers; biofuels companies; grain and oilseed processors and millers; exporters; livestock and poultry integrators; and associated firms that provide goods and services to the nation's grain, feed and processing industry. The NGFA also consists of 26 affiliated State and Regional Grain and Feed Associations.

NAEGA, a not-for-profit trade association established in 1912, consists of private and publicly owned companies and farmer-owned cooperatives that are involved in and provide services to the bulk grain and oilseed exporting industry. NAEGA's membership largely is domiciled in both the United States and Canada. NAEGA's mission is to promote and sustain the development of commercial export of grain and oilseeds and their primary products. Through a reliance on member action and support, NAEGA acts to accomplish its mission from its office in Washington D.C., and in markets throughout the world.

The NGFA, NAEGA and their member companies take homeland security issues very seriously, and we have repeatedly demonstrated our high level of cooperation with the government in countless activities in the aftermath of the Sept. 11, 2001 tragedies.

Specifically, the NGFA was among the first agricultural organizations to prepare and distribute generic industry guidance on facility security in the aftermath of 9/11. That guidance has been updated periodically – including as recently as this fall – based upon new information and findings. In addition, the NGFA and NAEGA participated actively in the Food and Drug Administration's (FDA) rulemakings under the Bioterrorism Act of 2002, and developed industry guidance and education programs for the facility registration, recordkeeping and prior notification provisions of those regulations.

Shortly thereafter, NGFA and NAEGA formed a joint Agroterrorism and Facility Security Committee to bring together top security and food- and feed-defense experts from our respective industry memberships to collaborate on industry initiatives and interact with government on these important issues.

One of those subsequent efforts involved NAEGA's collaboration with the U.S. Coast Guard to establish an Alternative Security Program (ASP) for vessel and barge-loading facilities required to comply with the security requirements of federal maritime safety laws. All NAEGA- and NGFA-member companies are eligible to participate in the program.

In addition, the NGFA has been an active participant in the Food and Agriculture Sector Coordinating Council, the presidentially sanctioned partnership consisting of federal, state, tribal, territorial and private sector organizations and entities that are focused on continually assessing and addressing risks of intentional adulteration of the food and feed supply. NGFA's president currently serves as the Sector Coordinating Council co-chair.

Recently, the NGFA and NAEGA partnered with FDA to offer a **Food Defense Awareness Workshop** that was conducted on **July 29, 2014 in Kansas City, MO**. The full-day workshop provided members of the grain, grain and oilseed processing, feed manufacturing, flour milling, export and other industry sectors with information on food defense, the tools and resources available from FDA (i.e., FDA's Food Defense Plan Builder Tool and industry), and to walk participants through a series of exercises on how to create a food defense plan for their facilities.

Significantly, the NGFA also worked previously with FDA to assess and identify mitigation strategies at grain handling facilities and animal feed mills through the Strategic Partnership Program Agroterrorism (SPPA) – a public-private cooperative effort between the U.S. Department of Agriculture (USDA), the Federal Bureau of Investigation and Department of Homeland Security, in partnership with state and industry partners. The SPPA vulnerability assessments sponsored by NGFA included: 1) tours of a country grain elevator, export grain elevator and an animal feed mill; 2) an analysis of the processes at typical facilities; and 3) identification of potential risks and risk-mitigation strategies.

In short, the NGFA and NAEGA take the importance of agricultural facility security and food/feed defense very seriously, and have endeavored to cooperate with and assist DHS in accomplishing its mission – to protect the homeland.

It is from this perspective that the NGFA and NAEGA begin this statement by indicating that each company and each facility within that company is unique in how it operates and specifically addresses security vulnerabilities, including cybersecurity. As substantiated by the SPPA reports and underpinned by existing USDA facility security requirements, provide ample justification for no further requirements to be added.

Specifically, the notice asks how the U.S. Coast Guard could leverage the ASP to help vessel and facility operators address cybersecurity related issues. As previously mentioned, NAEGA worked with the U.S. Coast Guard to develop an ASP in order to address industry-specific maritime-related issues. Further, many of the individual companies that participate in the ASP have their own unique security needs and their own cybersecurity policies to address potential threats.

Concerning cybersecurity, NGFA and NAEGA believe a much more effective and useful mechanism for coordination on cybersecurity is the partnership model developed by DHS's National Cybersecurity and Communications Integration Center (NCIC), whose Cybersecurity Director specifically is charged by the President to work closely with all key players in U.S. cybersecurity, including state and local governments and the private sector to ensure an organized and unified response to future cyber incidents. In close collaboration with the U.S. Department of Defense and U.S. Justice Department and FBI, the NCIC disseminates domestic cyber threat information, protects critical infrastructure, and ensures telecommunications and emergency preparedness – all with the goal of reducing the likelihood and severity of cyber and communications incidents that may significantly compromise the security and resilience of the nation's critical infrastructure and government systems. Among other things, NCIC has developed a web-based cybersecurity evaluation self-assessment tool for use by industry facilities, and issues daily and weekly alerts and advisories.

Moreover, the current cybersecurity threat to the maritime sector is primarily to port and vessel network systems, where "hackers" shut down large-scale operations, such as the use of commercial vessels and terminals through a kinetic attack. Grain handling facilities are not part of these network systems.

Therefore, a one-size fits all policy related to cybersecurity would be difficult to apply to each individual facility based on the limited risks at each facility. In addition, this type of policy may conflict with each company's specific cybersecurity protocol.

For these reasons, NGFA and NAEGA recommend that the DHS allow facilities under the ASP to include a cybersecurity system as an annex to the facility-specific part of the ASP, if the facility so chooses. Cybersecurity could be handled more efficiently as an annex/supplement since access control is covered generally in the ASP.

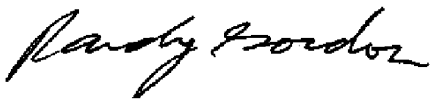
Under the approach suggested by NGFA and NAEGA, each facility would make a determination as to whether to develop a cybersecurity program to fit its own unique needs.

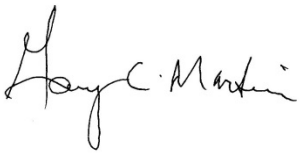
Since the ASP is coordinated through the Washington, D.C., office of the U.S. Coast Guard, the NGFA and NAEGA recommend that each individual facility's cybersecurity program be added as an appendix to the existing ASP. As a result, each individual facility, that so chooses to participate, then would submit the program to the appropriate Captain of the Port (COTP) for review and approval.

In closing, the NGFA and NAEGA suggest that DHS allow individual facilities to add a cybersecurity system to their current ASP, if the facility so chooses. The appropriate COTP then would review and approve the document. While the NGFA and NAEGA support homeland defense, we are concerned that the requirements for a cybersecurity program will be duplicative of existing requirements or practices which will be an additional and potentially costly burden on facilities, both in terms of administrative and capital costs.

Thank you in advance for your consideration of our views on this extremely important matter. We would be pleased to respond to any questions you or your colleagues may have.

Sincerely,





Randall C. Gordon
President
National Grain and Feed Association

Gary C. Martin
President and Chief Executive Officer
North American Export Grain Association