FACT SHEET: Cybersecurity

The American Fuel & Petrochemical Manufacturers (AFPM) is a national trade association representing more than 400 companies, including a majority of all U.S. refiners and petrochemical manufacturers. AFPM members operate 120 U.S. refineries comprising more than 95 percent of U.S. refining capacity. Additionally, AFPM represents the majority of petrochemical manufacturers who make the chemical building blocks that go into products ranging from medicines and medical devices, automobile parts, cosmetics, appliances and computers, furniture, solar panels and wind turbines. AFPM members make modern life possible while keeping America moving and growing as we meet the needs of our nation and local communities, strengthen economic and national security, and support 2 million American jobs.

Background

Cybersecurity is a critical component to protecting refineries and petrochemical facilities, and as such, the industry has developed several of its own standards, technologies, controls, strategies, and/or processes to manage cybersecurity threats. Many AFPM members also work with external sources such as the National Institute of Standards and Technology (NIST) to assist with industry-developed cybersecurity mitigation and response measures. Additionally, the industry has established public-private partnerships with the Federal government to advance cybersecurity mitigation and response measures. Examples include LOGIIC (Linking the Oil and Gas Industry to Improve Cybersecurity), CISP (Cyber Information Sharing and Collaboration Program), ICSJWG (Industrial Control Systems Joint Working Group), and CIS (Center for Information Security). Even though the risk of cyber breaches is ever-present, tremendous steps have been taken to ensure refineries and petrochemical facilities are safe against the increasing amounts of cyber threats facing our facilities.

AFPM Position

AFPM supports legislation that will help its members' IT and Industrial Control Systems (ICS) maintain their security. However, it should be noted that expertise in IT and ICS is with the owners and operators who work with these systems. AFPM also supports legislation that will allow member companies to freely share information with the government and other private companies—in a timely manner and secure environment—while also being provided with adequate liability and antitrust protections. Importantly, cybersecurity legislation should not impose mandatory standards on the private sector nor duplicate existing requirements already being implemented.

AFPM believes the following concepts should be taken into consideration if AFPM members' facilities are to be properly maintained and protected:

<u>NIST Cybersecurity Framework must remain a voluntary, evergreen document.</u>

The Cybersecurity Framework is designed to provide guidance to facilities deemed to be part of the Critical Infrastructure as defined by Executive Order 13636, "Improving Critical Infrastructure Cybersecurity." The Framework relies on existing standards and best practices to achieve outcomes that can assist organizations in managing their cybersecurity risk. The Framework is an evergreen document, evolving with technological and business advances.

AFPM believes that in order for the Framework to be the most effective in critical infrastructure, it must remain voluntary. A Framework that is mandated through regulation or legislation will not benefit private industry. AFPM members will use the Framework along with other tools to ensure secure systems. If the Framework were to become a mandated regulation, AFPM members would not be able to utilize the Framework as the useful tool that it is intended to be, as they might have to implement portions of the Framework which may conflict with existing industry practices.

AFPM believes that the Framework would be incomplete without the enactment of information-sharing legislation that is supported by the industry, and we welcome working Congress and the administration toward this goal.

Information sharing of cyber threats is key to mitigation, protection and response capabilities.

AFPM members strongly believe and support the sharing of cyber threat information among the refining and petrochemical industries, and government entities. The creation of a timely information sharing system that recognizes threats and potential attacks, while also providing adequate liability and antitrust protections, will better facilitate and ensure success against increasing cyber threats. Moreover, the refining and petrochemical industries need certainty that cyber threat information can be shared on a voluntary basis and prohibited from use by officials in regulatory matters; and that privacy and civil liberties are safeguarded. Increasing the collaboration between government and industry, and improving upon sector-based cybersecurity information sharing processes already established will be the greatest asset and most effective tool in advancing our nation's cybersecurity systems.

Liability and antitrust protections must be in place.

The refining and petrochemical industries need practical safeguards to increase their information-sharing capabilities. Liability, disclosure and antitrust protections must be in place, as they would influence an industry company's decision to share cyber threat data and countermeasures in a timely manner. Without these protections, AFPM members would be unable to share cyber threat information with each other—ultimately putting the industry as risk to perhaps more frequent and more innovative attacks which can not only cripple a company, but have negative repercussions on the industry as a whole.