American
Petroleum
Institute

Suzanne Lemieux
Manager, Operational Security & Emergency Response
Corporate Policy
200 Massachusetts Ave., NW
Washington, DC 20001
Telephone (202) 682-8453
Fax (202) 682-8408
Email lemieuxs@api.org
www.api.org

November 23, 2020

NISTIR 8323 (Draft)

SUBJECT: Cybersecurity Profile for the Responsible Use of Positioning, Navigation, and Timing (PNT) Services

The American Petroleum Institute (API) offers the following comments on the National Institute for Standards and Technology's Cybersecurity Draft Profile for the Responsible Use of Positioning, Navigation, and Timing. API is a national trade association that represents over 600 members involved in all aspects of the oil and natural gas industry, including producers, refiners, suppliers, pipeline operators and marine transporters, as well as service and supply companies that support all segments of the industry. API members are deeply committed to safe, secure, and environmentally responsible operations which eliminate or reduce potential risks to the public, as well as employees, contractors, and operations. Safety and security are key elements in all operations and we continue to work with regulators and stakeholders across government to ensure we are operating in a manner that protects our workers and communities, promotes safe practices, meets regulatory requirements, and improves our country's access to reliable energy, while delivering oil and natural gas products over water efficiently and safely worldwide.

First, API applauds the explanatory text explaining how a particular sub-category in scope for the profile applies to PNT. While it is clear how the sub-category applies to PNT, what is not present is a prioritization of the sub-categories as appears in the Manufacturing and U.S. Coast Guard profiles. The profile tends to treat PNT as a whole but different use cases have different priorities. For example, position/navigation used to position Drill Ships or navigate drones should focus on detect and respond/recover controls because disruption or spoofing of PNT can result in health, safety, and/or environmental damage. For these one needs to know whether the PNT signal is trustworthy (detect a spoofing attack) and once detected, what to do about it (address the attack and/or fall back to positioning or navigational solutions which do not rely on PNT). On the other hand, if positioning is being used to track/locate a worker in a remote West Texas field, then data protection of PNT information likely becomes paramount as the location information is personal data. Protection of PNT data may be less of an issue with drill ships or drones. Inventory is probably of less interest in the personal case (a person has a phone with PNT or not) but may be of utmost importance in a plant (where multiple sensors deployed may rely on PNT for timing). Different use cases have different impacts and therefore we suggest NIST identify different priorities for the sub-categories. For instance, the Coast Guard displayed its profiles in terms of mission (business) objectives; perhaps NIST could vary this approach by including use cases in the core and prioritizing the sub-categories within.

Privacy Suggestion

API notes there is only a single mention in the core about protecting personal information and that was one of the use cases that we provided in the RFI response. API suggests NIST consider supplementing the PNT Cybersecurity Framework Profile with a PNT Privacy Framework Profile. Since the Privacy Framework was just published this year, none of the existing profiles (Manufacturing, Coast Guard) could have developed a Privacy Framework Profile (and in some cases, like the hazardous liquids transport profile, there probably is not much data that would be subject to privacy regulation). In the PNT case, though, there are use cases around personal information so it may be worth creating a profile based on the Privacy Framework and either publishing it separately or include as a section or appendix to the Cybersecurity Profile. API believes this would be beneficial to readers who would have both the cybersecurity and privacy view of PNT risk and beneficial to NIST as well as it would illuminate the Privacy Framework and illustrate how the Cybersecurity and Privacy Frameworks could be used together.

As we noted in our previous comments, the Oil and Natural Gas industry makes significant use of PNT services and API is pleased that NIST continues to work on this effort to establish a cyber security profile for these services. API is pleased at the continued engagement with NIST on this topic and looks forward to publishing of the final profile. API and our members encourage NIST to continue engaging stakeholders and users, as they continue to explore PNT uses, criticality, and resilience.

Regards,

Suzanne Lemieux
Manager, Operations Security & Emergency Response Policy
Corporate Policy
American Petroleum Institute