AMERICAN PETROLEUM INSTITUTE

Aaron P. Padilla
Senior Advisor, International Policy

1220 L Street, NW
Washington, DC 20005-4070
Telephone (202) 682-8468
Fax (202) 682-8408
Email padillaa@api.org
www.api.org

Submitted via cyberframework@nist.gov

Andrea Arbelaez
National Institute of Standards and Technology
100 Bureau Drive
Mail Stop 2000
Gaithersburg, MD 20899

19 January 2018

Subject: **API Comments on Version 1.1 Draft 2 of Framework for Improving Critical Infrastructure Cybersecurity**

Dear Ms. Arbelaez:

The American Petroleum Institute (API) welcomes the opportunity to comment on Version 1.1 Draft 2 of the Framework for Improving Critical Infrastructure Cybersecurity (hereafter referred to as the "Cybersecurity Framework" or "CSF.") API is the only national trade association that represents all aspects of America's oil and natural gas industry. Our more than 625 corporate members, from the largest major oil company to the smallest of independents, come from all segments of the industry. They are producers, refiners, suppliers, marketers, pipeline operators and marine transporters, as well as service and supply companies that support all segments of the industry.

As operators and service providers of energy critical infrastructure in the United States and globally, protecting assets from cyber-attacks is a priority of API's member companies. Cybersecurity is a priority for the oil and natural gas industry in order to protect intellectual property and to protect industrial control systems (ICS) – also referred to as operational technology (OT).

Please see below for overarching comments, followed by more granular comments on specific text in Version 1.1 Draft 2.

- **API member companies continue to support the Cybersecurity Framework (CSF), including V1.1, as the pre-eminent standard for companies' cybersecurity programs and for policy making globally.** We support the CSF because it is (a) comprehensive, (b) a risk management approach, (c) scalable to different types and sizes of companies, and (d) widely used across industry.

- **API understands that Supply Chain Risk Management has been included as a new Category in V1.1 in order to limit revisions to the CSF Core; however, we still prefer for NIST to change this and integrate Supply Chain Risk Management into sub-categories in the next major update of the CSF V2.0.** API supports NIST's updates on supply chain in the "external participation" in the CSF Tiers.

- **API welcomes the revisions reflected in Section 4.0 and the inclusion of further work on metrics and measurement in the Roadmap.** We also recommend that NIST revise the title of Section 4.0 to "Assessing Cybersecurity Risk with the Framework" since the assessment contemplated in Section 4.0 could be done internally (a self-assessment) or by a third party.

- **API encourages NIST to continue global outreach programs to help align cybersecurity regulations or requirements across the world to the CSF.** We recommend that NIST amend Line 119 of V1.1 Draft 2 to include coordination with entities internationally.

- **API supports the concept that privacy and cybersecurity are compatible.** We recommend that NIST clarify by deleting the explanation of a "strong connection" between privacy and cybersecurity in Line 695 and replacing it with text that states the relation between privacy and cybersecurity, such as that effective cybersecurity is essential for safeguarding privacy and such as that effective cybersecurity does not have to compromise an organization's ability to safeguard privacy.

- **API encourages NIST to recognize that use of the CSF extends well beyond critical infrastructure and that the title of the CSF could be changed to "Framework for Improving Cybersecurity.**"

Overall, API continues to support the use of CSF and believes that NIST is a prime example of how government can work cooperatively with industry to manage risks, with the goal of providing reliable and affordable energy to the nation. Specifically, API supports the use of voluntary guidance over regulation in managing cybersecurity as it allows industry critical flexibility in managing threats in a dynamic and ever changing environment.

Sincerely,

Aaron Padilla
Senior Advisor, International Policy

Detailed API Response to NIST CSF Draft 2 Version 1.1

Line #	API Comment
119	Recommendation to clarify text: We recommend that NIST amend Line 119 of V1.1 Draft 2 to include coordination with entities internationally.
171	Recommendation to correct grammatical error and style: We recommend that an "s" be added after the word "support" in the following sentence "The Framework remains effective and supports technical innovation, because it is technology neutral, while referencing a variety of existing standards, guidelines, and practices that evolve with technology"
194-197	Recommendation to streamline text: We recommend that these lines be re-written as follows: "While the Framework was developed to improve cybersecurity risk management of critical infrastructure, it can be used by companies, government agencies, and not-for-profit organizations in any sector of the economy or society regardless of their focus or size."
444	Recommendation to correct grammar: We recommend that the "s" be deleted after the word "landscape" in the following sentence: "Through a process of continuous improvement incorporating advanced cybersecurity technologies and practices, the organization actively adapts to a changing threat and technology landscapes and responds in a timely and effective manner to evolving, sophisticated threats"
668	Recommendation to correct inconsistency: The current text is "This transaction varies from cyber SCRM (Section 3.3) in that it may not be possible to impose a set of cybersecurity requirements on the supplier." The overall concept of not being able to impose cybersecurity requirements is true, but based on the definitions in Section 3.3, buyers are part of SCRM, so the concept that this varies from cyber SCRM does not make sense.
695	Recommendation to clarify text: The paragraph begins by saying that privacy and cybersecurity have a "strong connection" and then lists ways in which cybersecurity activities can impact privacy, but we believe that the concept of a "strong connection" is nebulous. We recommend that NIST clarify by deleting the explanation of a "strong connection" between privacy and cybersecurity in Line 695 and replacing it with text that states the relation between privacy and cybersecurity, such as that effective cybersecurity is essential for safeguarding privacy and such as that effective cybersecurity does not have to compromise an organization's ability to safeguard privacy.
702	Recommendation to clarify text: We are not sure why only the "government and its agents" are singled out to protect civil liberties. Governments may have responsibility for "civil liberties" but rather than listing legislation or other governmental activities, the rest of the paragraph talks about implementing a privacy program, which governments and companies both must do.

Line #	API Comment
745, 752	Recommendation to clarify text: We recommend striking "self" from self-assessment. The section is talking about assessment which as the section says may be done "internally or by seeking a third-party assessment" "Internally" would qualify as "self-assessment" but few would consider a third-party assessment in that vein. Dropping the "self" solves this problem and would not detract from any other text.
782-785	Recommendation to clarify text: We find Lines 782-785 confusing. The text states " While it is sometimes important to determine whether or not an organizational objective was achieved through lagging measurement, leading measurements of whether a cybersecurity risk may occur, and the impact it might have, are typically more important to determining likelihood of accomplishing an organizational objective." We believe that NIST is trying to establish that measuring risk is a key activity, but including the terms "lagging" and "leading" measurement clouds the meaning, particularly since these terms are not defined in this version of the draft nor used elsewhere. This sentence may be a left over from the longer measurement section of the previous Draft 1 V1.1, which covered more theoretical elements of metrics. We recommend rewriting the sentence to focus on measuring the likelihood and impact of risk and leave off whether the measures are "lagging" or "leading." Alternatively, if the risk measurement is only an example, we would recommend that the text focus on measuring future or proactive items like risk rather than looking backward at block executables and the like.