American
Fuel & Petrochemical
Manufacturers

1667 K Street, NW
Suite 700
Washington, DC
20006

202.457.0480 office
202.457.0486 fax
afpm.org

January 19, 2018

Department of Commerce
National Institute of Standards and Technology
100 Bureau Drive
Stop 8930
Gaithersburg, MD 20899
cyberframework@nist.gov

Re: AFPM Comments on the National Institute of Standards and Technology's "Framework for Improving Critical Infrastructure Cybersecurity," Version 1.1 Draft 2

To Whom It May Concern:

The American Fuel & Petrochemical Manufacturers ("AFPM") appreciates this opportunity to provide comments on Version 1.1 Draft 2 ("Draft 2") of the National Institute of Standards and Technology's ("NIST") "Framework for Improving Infrastructure Cybersecurity" (the "Framework").[1] AFPM is a national trade association whose members comprise virtually all U.S. refining and petrochemical manufacturing capacity. AFPM's member companies produce the gasoline, diesel, and jet fuel that drive the modern economy, as well as the chemical building blocks that are used to make millions of products that make modern life possible.

AFPM members have been at the forefront of cybersecurity efforts, participating in a wide range of industry and government initiatives to enhance cybersecurity for critical infrastructure within the oil and natural gas, and chemical sectors. AFPM members utilize the Framework as a tool in their own facility cybersecurity risk assessments, using it as guidance to better measure their facilities' cybersecurity risk management programs. Further, AFPM assisted in developing the first version of the Framework (the "Original Framework"), released in 2014, and has continued working with NIST on subsequent updates.

Given AFPM's collaborative relationship with NIST and our members' clear commitment to critical infrastructure cybersecurity, we welcome this opportunity to provide comments on NIST's proposed amendments to the Framework.

I. BACKGROUND

On February 12, 2013, President Barack Obama issued Executive Order ("EO") 13636,[2] "Improving Critical Infrastructure Cybersecurity," which directed NIST to lead the development of a voluntary framework for critical infrastructure to use in reducing cyber-related risks. In

[1] *See* National Institute of Standards and Technology, "Framework for Improving Critical Infrastructure Cybersecurity," Version 1.1 Draft 2, Revised December 5, 2017, https://www.nist.gov/file/412461.
[2] *See* "Executive Order – Improving Critical Infrastructure Cybersecurity," February 12, 2013, https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity.

accordance with this directive, on February 12, 2014, NIST issued the Original Framework[3] following a year-long collaborative process involving industry, academia, and government stakeholders.

In December 2014, Congress mandated that NIST continue facilitating further developments to the Framework through the *Cybersecurity Enhancement Act of 2014*.[4] Over the past three years, NIST has fulfilled this responsibility by performing significant stakeholder engagement, including holding several workshops, publishing multiple requests for information in the *Federal Register*, and conducting other stakeholder outreach with relevant parties.[5]

Based on feedback received through these varying forms of stakeholder engagement, NIST published its first draft of proposed changes to the Framework, Draft Version 1.1 ("Draft 1"),[6] on January 10, 2017, and a second draft of proposed changes, Draft 2, on December 5. The proposed changes in Drafts 1 and 2 of the revised Framework aim to clarify, refine, and enhance the Framework while minimizing changes to current users.

II. COMMENTS

Below are AFPM's general comments on the Framework. More specific comments on NIST's proposed amendments from both Drafts 1 and 2 of the Framework can be found in the Appendix to this document.

A. General Comments

In comments submitted on Draft 1 of the Framework,[7] AFPM supported several proposed amendments, including: 1) the addition of Section 4.0; 2) the addition of subcategory PR.AC-6; and 3) the more detailed explanation of the relationship between Implementation Tiers and Profiles. We are pleased that NIST retained these proposed changes in Draft 2 of the revised Framework.

AFPM also supports proposals to further update the Framework, including the proposal to include cyber supply chain risk management ("C-SCRM") as a critical organizational function and the differentiation between a cybersecurity event and a cybersecurity incident. More specific comments on NIST's proposed amendments from both Drafts 1 and 2 of the Framework can be found in the Appendix to this document.

---

[3] *See* National Institute of Standards and Technology, "Framework for Improving Critical Infrastructure Cybersecurity," Version 1.0, February 12, 2014, https://www.nist.gov/sites/default/files/documents/cyberframework/cybersecurity-framework-021214.pdf.

[4] *See Cybersecurity Enhancement Act of 2014*. Pub. L. 113-274. 124 Stat. 3989. December 18, 2014. https://www.gpo.gov/fdsys/pkg/PLAW-113publ274/content-detail.html.

[5] *See* "Update to Cybersecurity Framework," December 5, 2017, https://www.nist.gov/news-events/news/2017/12/update-cybersecurity-framework.

[6] *See* National Institute of Standards and Technology, "Framework for Improving Critical Infrastructure Cybersecurity," Draft Version 1.1, January 10, 2017, https://www.nist.gov/sites/default/files/documents////draft-cybersecurity-framework-v1.11.pdf.

[7] *See* AFPM Comments on "Proposed Update to the Framework for Improving Critical Infrastructure Cybersecurity," April 10, 2017, https://www.afpm.org/uploadedFiles/Content/Policy_Positions/Agency_Comments/AFPM%20comments%20NIST%20Framework%20Proposed%20Update%20041017.pdf.

B. The Framework Should Remain Voluntary and Flexible

NIST consistently acknowledges the Framework "is not a one-size-fits-all approach to managing cybersecurity risk for critical infrastructure…and will continue to be updated and improved as industry provides feedback on implementation."[8] AFPM applauds this approach to the Framework; however, we also encourage other regulatory agencies to uphold the Framework's voluntary nature when referencing it in regulations or guidance documents.

Critical infrastructure facilities are unique in purpose, equipment, materials stored on site, personnel, site configuration, and security risks. Moreover, cybersecurity threats are dynamic. Cyberthreats have evolved tremendously in the past decade and will continue to evolve in complexity. Consequently, there is virtually no way to accurately predict the cyberthreats of the future or the best way to address these vulnerabilities. Thus, retaining the voluntary nature of the Framework, as opposed to mandating its use, would be the most beneficial approach for critical infrastructure facilities as it would allow these sites to adopt more flexible cyber standards that can be tailored to each individual site and adapted to address emerging threats.

In comments submitted by AFPM to NIST on the Original Framework and on subsequent revisions, we advocated for this continued approach. That recommendation remains valid; the Framework and any cyber-related regulations should not become prescriptive, but rather remain voluntary guidance. This will allow greater flexibility in how industry responds to the dynamic nature of threats within the cyber arena.

III. CONCLUSION

AFPM thanks NIST for the opportunity to provide input on the proposed revisions to the Framework. AFPM recognizes that cybersecurity is a dynamic threat that could have direct consequences for critical infrastructure sites. As such, we broadly support the proposed amendments to the Framework and urge NIST to retain the voluntary nature of its Framework to enable more successful and efficient critical infrastructure cybersecurity programs.

We look forward to continuing to work with NIST and other stakeholders on developing guidance for improving cybersecurity efforts at critical infrastructure facilities. If you have any questions or if AFPM can be of any assistance in this process, please contact the undersigned at (202) 552-8475 or dstrachan@afpm.org.

Sincerely,

Daniel J. Strachan
Director, Industrial Relations and Programs

[8] *See, e.g.,* NIST Framework Version 1.0 at 2.

APPENDIX

The table below outlines AFPM's comments on NIST's proposed amendments to the Framework, in order of appearance in Draft 2 of the Framework. We broadly support these changes because they meet one or more of the following outcomes: 1) reflection of current cyberthreats; 2) better clarification to items identified through the Framework; 3) increased usability for new users; and/or 4) expansion of usability and applicability across industry sectors. In addition, we believe these changes would minimally impact current users of the Framework. For these reasons, we encourage NIST to finalize these proposed changes in Version 1.1 of the Framework.

Table 1: AFPM Comments on Proposed Updates to the Framework

Proposed Update	AFPM Comments
Section 1.0 "Framework Introduction" Updated to reflect security implications of a broadening use of technology (*e.g.*, Information Control Systems) and to more clearly define Framework uses	AFPM supports this proposed update because it more clearly reflects current and evolving cyberthreats and increases the likelihood of Framework use by clarifying Framework usability/applicability.
Section 2.1 "Framework Core" Differentiates between a cybersecurity "event" (*i.e.*, an action that may not have a response or recovery associated with it) and a cybersecurity "incident" (*i.e.*, an action that may require a response and recovery)	NIST is proposing to categorize the term "cybersecurity event" into two separate concepts: a cybersecurity event and a cybersecurity incident. AFPM supports this differentiation because it provides clarity surrounding the applicability and severity of such actions and any relevant company response.
Section 2.2 "Framework Implementation Tiers" Provides more detailed explanation of the relationship between Implementation Tiers and Profile[9]	This proposed change would further clarify the use and purposes of various Tiers in the Framework. Such clarification would better enable businesses to adopt the Framework and would increase its use across industry sectors.

[9] This item was addressed in AFPM's comments on Draft Version 1.1 of the Framework.

Proposed Update	AFPM Comments
Section 2.2 "Framework Implementation Tiers" – Tier 4 "Adaptive" Modified to clarify senior executives' role(s) in cybersecurity efforts	AFPM applauds the proposed statement surrounding senior executives' emphasis on cybersecurity risk because it would help ensure such executives are actively involved in a company's cybersecurity efforts and highlights the critical relationship between cybersecurity and a business's financial and organizational objectives.
Section 2.2 Tier 4 "External Participation" Updated language on a company's external participation in relation to cybersecurity efforts	AFPM commends NIST's proposed language on "External Participation," including the emphasis on an organization's role in the larger ecosystem, the importance of safeguarding sensitive information while sharing risk information both internally and externally with other stakeholders, and the stress on receiving risk information in real time or near real time and communicating such risks proactively. Adding this language to the Framework would help foster a collaborative environment in the critical infrastructure arena, thereby further reducing potential cyber risks across the board.
Section 3.0 "How to Use the Framework" Update to include language on when to incorporate desired cybersecurity outcomes prioritized in a Target Profile (*i.e.*, when developing the system during the build phase and purchasing or outsourcing the system during the buy phase)	AFPM agrees with this proposed change, as it would ensure critical infrastructure cybersecurity specifications meet the needs and risks associated with a particular organization. For these same reasons, we further support the proposed language that desired cybersecurity outcomes "should serve as a basis for ongoing operation of the system…to verify that cybersecurity requirements are still fulfilled."
Section 3.2 "Establishing or Improving a Cybersecurity Program" – Step 6: "Determine, Analyze, and Prioritize Gaps" Language modified to propose that businesses' action plans also address any gaps surrounding costs, benefits, and risks in order to achieve the outcomes identified in the Target Profile and that businesses then determine resources such as funding and workforce to more fully address such gaps	AFPM commends these proposed changes, as they would better enable businesses to make informed decisions and improvements surrounding cybersecurity and risk management.

Proposed Update	AFPM Comments
Section 3.3 "Communicating Cybersecurity Requirements with Stakeholders" Modified to include cyber supply chain risk management ("C-SCRM")	As with many other critical infrastructures, fuel and petrochemical manufacturers are dependent on the supply chain to continue the production and distribution of their products. Addressing C-SCRM as a critical organizational function in the Framework would help businesses make better-informed decisions in the face of cyber risks posed by the supply chain and vendor partners.
Section 3.4 "Buying Decisions" This section was added to demonstrate another example of using the Framework	AFPM agrees that Target Profiles may be used by an organization in order to make better informed decisions on the purchases of products and services. We also agree that this type of transaction should be separated from C-SCRM because it may not be feasible to impose cybersecurity requirements on suppliers or vendors. As such, it may be in a company's best interest to develop a separate set of requirements they may then use to compare multiple suppliers and make the best possible buying decision.
Section 4.0 "Self-Assessing Cybersecurity Risk with the Framework"[10] This section was added to clarify the relationship between measurements and the Framework	AFPM supports the addition of this section, as it makes the Framework more applicable to business objectives through various matrices and measurements. Many users of the Framework have already developed measurement systems to incorporate the Framework at their facilities. The addition of Section 4.0 would allow users to easily apply the Framework to their current risk management strategies.
Table 2: "Framework Core" Addition of subcategories PR.AC-6[11] and PR.AC-7	The addition of PR.AC-6 and PR.AC-7 would enable businesses to better account for authentication, authorization, and identity proofing. AFPM agrees this area of the Framework needed clarification, and thus supports the addition of these subcategories.

[10] This item was addressed in AFPM's comments on Draft Version 1.1 of the Framework.
[11] This item was addressed in AFPM's comments on Draft Version 1.1 of the Framework.