energy API
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 NISTIR-8200@nist.gov

Michael Hogan and Ben Piccarreta
Editors of NISTIR 8200
National Institute of Standards and Technology (NIST)
100 Bureau Drive
Gaithersburg, MD 20899

18 April 2018

Subject: **API Comments on *NIST Interagency Report (NISTIR) 8200, Status of International Cybersecurity Standardization for Internet of Things (IoT)***

Dear Mr. Hogan and Mr. Piccarreta:

The American Petroleum Institute (API) welcomes the opportunity to comment on the *NIST Interagency Report (NISTIR) 8200, Status of International Cybersecurity Standardization for Internet of Things (IoT)* (hereafter referred to as "NISTIR 8200.") 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 some additional details in the comment template.

- **API member companies recommend that the NISTIR 8200 be condensed by deleting Sections 5 and 7 and by combining Sections 6 and 8.**
    - **Rationale for deleting Sections 5 and 7:**
      (1) The use cases are mostly superfluous with regards to the document's focus on standards. Apart from Section 9, all of the other standards are referenced within cybersecurity areas, not use cases. The use cases may inform the selection of standards included in the document, but relevant standards can be selected without the detail of the use cases.
      (2) The use cases define potential cybersecurity risks and threats but do not provide insight into potential solutions, which extend beyond the standards listed. Many of IoT security risks/threats are nuanced and are managed by multiple controls at different levels, so a listing of standards does not nearly cover these solutions. Virtually all of the text in Section 7 covers "threats" but not overall risks that would also take into account mitigations to address threats. This is an incomplete picture and makes the use cases, as currently written, susceptible to being excerpted

from the NISTIR and presented as evidence of the inadequacy writ large of cybersecurity for IoT in our society, which would be an incomplete depiction, for example, of cybersecurity measures that many companies in the oil and natural gas industry have in place for the deployment of Industrial IoT (IIoT).
(3) The use case content that is currently in the document appears to have been spliced from different other sources. This disrupts the flow of the document as different subsections within Sections 5 and 7 read very differently: the health and smart buildings use cases are documented via examples while the others are objectively described; other content is inappropriate for the section as Section 5 is supposed to define the use case and Section 7 cover the risk/threats, but Section 5 for smart manufacturing includes a discussion of security.

If NIST believes it is necessary to retain the use cases, API member companies recommend that NIST pull out the use cases into a separate document and then dedicate more thought and work to developing an IoT security profile-like depiction of standards as they apply to particular use cases.

  - **Rationale for combining Sections 6 and 8:** Both sections are organized according to the same headings, so it would be natural to combine the definitions and then standards into the same section under their common headings.

- **API member companies recommend that NIST distinguish IoT (especially as the term is commonly understood: as consumer IoT devices) from the Industrial Internet of Things (IIoT).** Making this delineation would help readers and policy makers to understand that IIoT is not interchangeable with IoT and that their risks and threats are different.

- **API member companies urge NIST to ensure that this document includes relevant standards that address specifically the compatibility between privacy and IoT security.** As oil and natural gas companies operate around the world, achieving privacy and cybersecurity together is increasingly important.

Sincerely,

Aaron Padilla

Aaron Padilla
Senior Advisor, International Policy

April 18, 2018

API Comments - Using Template – for Draft NIST Interagency Report (NISTIR) 8200

COMMENT #	SOURCE	TYPE i.e., Editorial Minor Major	LINE # PAGE etc.	RATIONALE for CHANGE	PROPOSED CHANGE (specific replacement text, figure, etc. is required)
1	API	Major	PP. 9-21; 33-45	Delete Sections 5 and 7: The use cases are not necessary for the documents purpose to compile standards, only address threats but not solutions, do not follow a consistent format	Delete Sections 5 and 7 If necessary to retain the use cases, consider pulling them out into a separate document and then dedicate more thought and work to developing an IoT security profile-like depiction of standards as they apply to particular use cases.
2	API	Major	PP. 22-32; 46-52	Combine Sections 6 and 8: Both sections are organized according to the same headings, so it would be natural to combine the definitions and then standards into the same section under their common headings	Combine Sections 6 and 8.
3	API	Major	P. 2 and Throughout	As companies operate around the world, achieving privacy and cybersecurity together is increasingly important.	Include standards that address specifically the compatibility of privacy and IoT security.
4	API	Minor	P. 6	Diagram after definitions is not clear – especially the components IoT domains in the blue boxes.	Make tighter the diagram after the definitions: distinguish between IoT “Environment,” “System,” and “Component” – it is not currently clear.
5	API	Minor	PP. 4-8 and P. 45 / Line 1648	The Industrial Internet of Things (IIoT) is distinct from IoT IoT for a consumer/retail market. The NISTIR should make this delineation by defining IIoT and stating that IIoT is not interchangeable with IoT. For example, IIoT may have more controls available [e.g., secure deployment of IIoT often means that it is not connected to the Internet]. Distinguishing IIoT from IoT would help to underscore that the risks and threats are different.	Define IIoT in Section 4 or eliminate the lone reference to it on page 45 / line 1648. [Note: if Comment #1 is accepted, this reference would be deleted.]
6	API	Minor	PP. 22-32	The “Cybersecurity Areas” in Section 6 introduce a new set of headings that could have been appropriated from the NIST Cybersecurity Framework, which is widely used.	NIST should use categories/subcategories from the NIST Cybersecurity Framework rather than creating a new list of “Cybersecurity Areas.”
7	API	Minor	Throughout	The document’s current more expansive discussion of IoT threats presents an unbalanced view since these threats are not matched to standards to mitigate them.	Eliminate any extended discussion of potential threats to IoT in order to retain a narrow focus on standards.