From: James Crandall <crandallj@api.org>
Sent: Thursday, October 24, 2019 6:26 PM
To: privacyframework <privacyframework@nist.gov>
Subject: Draft NIST Privacy Framework

Dear NIST,

Please find attached the comments of the American Petroleum Institute on the draft NIS Privacy Framework.

Regards,

James Crandall

API

200 Massachusetts Ave. NW

Washington, D.C. 20001
Telephone: 202-682-8357

Cell: 202-360-2134

AMERICAN PETROLEUM INSTITUTE

James Crandall
Policy Analyst, Tax and Accounting Policy

200 Massachusetts Ave.
Washington, DC 20001
Telephone (202) 682-8357
Fax (202) 682-8408
Email crandallj@api.org
www.api.org

Submitted via e-mail to privacyframework@nist.gov

Thursday, October 24, 2019

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

Subject: Comments on Preliminary Draft of the Privacy Framework

Dear NIST,

The American Petroleum Institute (API) welcomes the opportunity to comment upon NIST's preliminary draft of the Privacy Framework. The oil and natural gas industry commends NIST for its leadership.

API is the only national trade association representing all facets of the natural gas and oil industry, which supports 10.3 million U.S. jobs and nearly 8 percent of the U.S. economy. API's more than 600 members include large integrated companies, as well as exploration and production, refining, marketing, pipeline, marine businesses, and service and supply firms. They provide most of the nation's energy and are backed by a growing grassroots movement of more than 47 million Americans. API was formed in 1919 as a standards-setting organization. In its first 100 years, API has developed more than 700 standards to enhance operational and environmental safety, efficiency and sustainability.

API believes the Privacy Framework draft does not focus enough on individual requests. Many privacy regulations enable an individual to request a company to provide any personal information about that individual within a reasonable time frame. The individual has the right to request alterations to correct errors found within the data. The CT.PO-P2 and CT.PO-P3 subcategories could be interpreted and implemented from the perspective of the company holding the data and would completely neglect the perspective of the individual. NIST should explicitly mention, either by altering the two subcategories or by insertion of a new subcategory that covers individual access request for his/her personal data.

The Privacy Framework draft co-opts much of the Cybersecurity Framework (CSF) "Protect" function because many of the subcategories have privacy-specific considerations. The Privacy Framework states that "…Detect, Respond, and Recover are cybersecurity incident-related…" and therefore are not included within the Privacy Framework. That clause, though, is not factual as because of data breach notification requirements, there are privacy specific actions required within "Respond" and "Recover." One might be able to argue that the text within these Cybersecurity Framework subcategories is enough to cover the following four situations:

- RS.CO-4: Coordination with stakeholders occurs consistent with response plans
- RC.CO-1: Public relations are managed
- RC.CO-2: Reputation is repaired after an incident

- RC.CO.3: Recovery activities are communicated to internal and external stakeholders as well as executive and management team

However, this is not explicit in the Cybersecurity Framework. The informative references in the Cybersecurity Framework do not have privacy components and one can execute these functions without necessarily contacting impacted individuals as required by many jurisdictions.

The other argument for including privacy-specific text within the Privacy Framework is that if one can interpret these Cybersecurity Framework subcategories to apply to privacy as written, then there is little reason to co-opt and update the subcategories from "Protect" with privacy ramifications.

The Privacy Framework draft states that the "…Privacy Framework follows the structure of the Framework for Improving Critical Infrastructure Cybersecurity (Cybersecurity Framework) to facilitate the use of both frameworks together." While the organization of the document facilitates using both frameworks, other text within the Privacy Framework draft states that doing so is optional (i.e. lines 177-179). The Privacy Framework draft pulls out the "Detect", "Respond", and "Recover" functions from the Cybersecurity Framework. However, the draft explicitly states that these functions are not part of the privacy framework and the reader is left with incomplete guidance.

API recommends making the privacy framework a standalone document. API has commented previously that the requirement of using both the CSF and the Privacy Framework runs the risk of misalignment when the CSF is changed. Adding the CSF "Detect", "Respond", and "Recover" functions and categories to the Privacy Framework exacerbates this risk. The Privacy Framework draft seems to be positioned to be more of a starter guide to privacy implementation. (The "ready, set, go" model in section 3.3 is the basis for this assumption.) If this is correct, then a company starting out does not need to ingest two documents to implement their privacy program. It would be better to make the privacy framework a standalone document so that one would only have it use it to implement a privacy program. The organization of the privacy framework in core, profile, and tier could be maintained to allow those who wanted to delve into cybersecurity more deeply to do so but this should not be a requirement.

If the privacy framework is a standalone document, then those cybersecurity elements required for privacy should be moved into the document. The "PROTECT-P" function should be renamed "SECURITY-P" or "CYBERSECURITY-P" and should consist of subfunctions of "PROTECT", "DETECT", "RESPOND", and "RECOVER." If subfunctions are not allowed, then categories within each of these CSF functions should be included.

API encourages NIST to map the Privacy Framework to key privacy legislation like GDPR and CCPA. Many companies approach privacy as a compliance activity driven by applicable law. This differs from approach to cybersecurity is based on good business practice and cybersecurity is not explicitly regulated. This is not the case with privacy as even where there is a lack of regulation on managing data, there are breach notification laws to which all business must comply.

Conclusion

The American Petroleum Institute (API) welcomes the opportunity to comment upon NIST's preliminary draft of the Privacy Framework. The oil and natural gas industry commends NIST for its leadership on this effort.

Respectfully submitted,

/S/

James Crandall
API