This document is scheduled to be published in the
Federal Register on 11/14/2018 and available online at
https://federalregister.gov/d/2018-24714, and on **govinfo.gov**

Billing Code: 3510-13

DEPARTMENT OF COMMERCE

National Institute of Standards and Technology

[Docket Number 181101997-8997-01]

Developing a Privacy Framework

AGENCY: National Institute of Standards and Technology, U.S. Department of Commerce.

ACTION: Notice; Request for Information (RFI)

SUMMARY: The National Institute of Standards and Technology (NIST) is developing a framework that can be used to improve organizations' management of privacy risk for individuals arising from the collection, storage, use, and sharing of their information.[1] The NIST Privacy Framework: An Enterprise Risk Management Tool ("Privacy Framework"), is intended for voluntary use and is envisioned to consist of outcomes and approaches that align policy, business, technological, and legal approaches to improve organizations' management of processes for incorporating privacy protections into products and services. This notice requests information to help identify, understand, refine, and guide development of the Privacy Framework. The Privacy Framework will

[1] While NIST requests information about how organizations define privacy risk in topic #3 below, for the purposes of this RFI, NIST references the privacy risk model set forth in NISTIR 8062, *An Introduction to Privacy Engineering and Risk Management in Federal Systems* at https://csrc.nist.gov/publications/detail/nistir/8062/final, which analyzes the problems that individuals might experience as a result of the processing of their information, and the impact if they were to occur.

be developed through a consensus-driven, open, and collaborative process that will include workshops and other opportunities to provide input.

DATES: Comments in response to this notice must be received by 5:00 PM Eastern time on [PLEASE INSERT DATE 45 DAYS AFTER DATE OF PUBLICATION IN THE *FEDERAL REGISTER*].

ADDRESSES: Written comments may be submitted by mail to Katie MacFarland, National Institute of Standards and Technology, 100 Bureau Drive, Stop 2000, Gaithersburg, MD 20899. Electronic submissions may be sent to privacyframework@nist.gov, and may be in any of the following formats: HTML, ASCII, Word, RTF, or PDF. Please cite "Developing a Privacy Framework" in all correspondence. Comments received by the deadline will be posted at http://www.nist.gov/privacyframework without change or redaction, so commenters should not include information they do not wish to be posted (e.g., personal or confidential business information). Comments that contain profanity, vulgarity, threats, or other inappropriate language or content will not be posted or considered.

FOR FURTHER INFORMATION CONTACT: For questions about this RFI contact: Naomi Lefkovitz, U.S. Department of Commerce, NIST, MS 2000, 100 Bureau Drive, Gaithersburg, MD 20899, telephone (301) 975-2924, e-mail privacyframework@nist.gov. Please direct media inquiries to NIST's Public Affairs Office at (301) 975-NIST.

SUPPLEMENTARY INFORMATION:

Genesis for the Privacy Framework's Development

It is a challenge to design, operate, or use technologies in ways that are mindful of diverse privacy needs in an increasingly connected and complex environment. Current and cutting-edge technologies such as mobile devices, social media, the Internet of Things and artificial intelligence are giving rise to increased concerns about their impacts on individuals' privacy. Inside and outside the U.S., there are multiple visions for how to address these concerns. Accordingly, the U.S. Department of Commerce (DOC) is developing a forward-thinking approach that supports both business innovation and strong privacy protections. As part of this effort, NIST is developing a voluntary Privacy Framework to help organizations: better identify, assess, manage, and communicate privacy risks; foster the development of innovative approaches to protecting individuals' privacy; and increase trust in products and services.[2] The Privacy Framework is intended to be a tool that would assist with enterprise risk management.

Privacy Framework Development and Attributes

While good cybersecurity practices help manage privacy risk through the protection of personally identifiable information (PII),[3] privacy risks also can arise from how organizations collect, store, use, and share PII to meet their mission or business objective, as well as how individuals interact with products and services. NIST seeks to understand whether organizations that design, operate, or use these products and services would be better able to address the full scope of privacy risk with more tools to support better implementation of privacy protections.

NIST will develop the Privacy Framework in a manner consistent with its mission to promote U.S. innovation and industrial competitiveness, and is seeking input from all interested stakeholders. NIST intends for the Framework to provide a prioritized, flexible, risk-based, outcome-based, and cost-effective approach that can be compatible with existing legal and regulatory regimes in order to be the most useful to organizations and

[2] In parallel with this effort, the DOC's National Telecommunications and Information Administration is developing a set of privacy principles in support of a domestic policy approach that advances consumer privacy protections while protecting prosperity and innovation, in coordination with DOC's International Trade Administration to ensure consistency with international policy objectives: https://www.ntia.doc.gov/federal-register-notice/2018/request-comments-developing-administration-s-approach-consumer-privacy.

[3] For the purposes of this RFI, NIST is using the definition from the Office of Management and Budget Circular A-130. PII is defined as "information that can be used to distinguish or trace an individual's identity, either alone or when combined with other information that is linked or linkable to a specific individual."

enable widespread adoption. NIST expects that the Privacy Framework development process will involve several iterations to allow for continuing engagement with interested stakeholders. This will include interactive workshops, along with other forms of outreach.

On October 16, 2018, NIST held its first workshop in Austin, Texas to launch the framework development process.[4] NIST heard from panelists from industry, civil society and academia, as well as audience participants about the needs the Privacy Framework should address and some key desired characteristics. As a consequence, NIST believes that in order to be effective, the Privacy Framework should have the following minimum attributes:

1. **Consensus-driven and developed and updated through an open, transparent process.** All stakeholders should have the opportunity to contribute to the Privacy Framework's development. NIST has a long track record of successfully and collaboratively working with stakeholders to develop guidelines and standards. NIST will model the approach for the Privacy Framework on the successful, open, transparent, and collaborative approach used to develop the Framework for Improving Critical Infrastructure Cybersecurity ("Cybersecurity Framework").[5]
2. **Common and accessible language.** The Privacy Framework should be understandable by a broad audience, including senior executives and those who are not privacy professionals. The Privacy Framework can then facilitate communications among various stakeholders by promoting use of this common language.
3. **Adaptable to many different organizations, technologies, lifecycle phases, sectors, and uses.** The Privacy Framework should be scalable to organizations of all sizes, public or private, in any sector, and operating within or across domestic borders. It should be platform- and technology- agnostic and customizable.

[4] https://www.nist.gov/news-events/events/2018/10/kicking-nist-privacy-framework-workshop-1.

[5] https://www.nist.gov/cyberframework/framework.

4. **Risk-based, outcome-based, voluntary, and non-prescriptive.** The Privacy Framework should provide a catalog of privacy outcomes and approaches to be used voluntarily, rather than a set of one-size-fits-all requirements, in order to: foster innovation in products and services; inform education and workforce development; and promote research on and adoption of effective privacy solutions. The Privacy Framework should assist organizations to better manage privacy risks within their diverse environments without prescribing the methods for managing privacy risk.
5. **Readily usable as part of any enterprise's broader risk management strategy and processes.** The Privacy Framework should be consistent with, or reinforce, other risk management efforts within the enterprise, recognizing that privacy is one of several major areas of risk that an organization needs to manage.
6. **Compatible with or may be paired with other privacy approaches.** The Privacy Framework should take advantage of existing privacy standards, methodologies, and guidance. It should be compatible with and support organizations' ability to operate under applicable domestic and international legal or regulatory regimes.
7. **A living document.** The Privacy Framework should be updated as technology and approaches to privacy protection change and as stakeholders learn from implementation.

Although the goal of the Privacy Framework is to help organizations better identify, assess, manage, and communicate privacy risks, NIST expects there may be aspects of privacy practices that are not sufficiently developed for inclusion in the Privacy Framework. When developing the Cybersecurity Framework, NIST produced a related roadmap that identified focus areas that still needed more research and understanding before they were mature enough for widespread adoption, but that could potentially inform future revisions of the Cybersecurity Framework. With respect to the Privacy Framework, NIST anticipates that a roadmap may be needed for similar reasons.

As noted below, NIST solicits comments on the desired attributes of a Privacy Framework, as well as high-priority gaps in organizations' ability to manage privacy risk, as part of this RFI.

Goals of this Request for Information

Based upon discussions that took place during the October 16, 2018 workshop, this RFI seeks further information about the topics discussed by stakeholders, as elaborated in the sections below. The RFI invites stakeholders to submit ideas, based on their experience as well as their mission and business needs, to assist in prioritizing elements and development of the Privacy Framework. NIST invites industry, civil society groups, academic institutions, Federal agencies, state, local, territorial, tribal, and foreign governments, standard-setting organizations, and other interested stakeholders to respond.

The goals of the Privacy Framework development process, generally, and this RFI, specifically, are:
(i) to better understand common privacy challenges in the design, operation, and use of products and services that might be addressed through a voluntary Privacy Framework,
(ii) to gain a greater awareness about the extent to which organizations are identifying and communicating privacy risk or have incorporated privacy risk management standards, guidelines, and best practices, into their policies and practices; and
(iii) to specify high-priority gaps for which privacy guidelines, best practices, and new or revised standards are needed and that could be addressed by the Privacy Framework or a related roadmap.

Details About Responses to This Request for Information

When addressing the topics below, commenters may address the practices of their organization or a group of organizations with which they are familiar. If desired, commenters may provide information about the type, size, and location of the organization(s). Provision of such information is optional and will not affect NIST's full consideration of the comment.

Comments containing references, studies, research, and other empirical data that are not widely published (e.g., available on the Internet) should include copies of or electronic links to the referenced materials. Beyond that, responses should not include additional information. Do not include in comments or otherwise submit information deemed to be proprietary, private, or in any way confidential, as all comments relevant to this RFI topic area that are received by the deadline will be made available publicly at http://www.nist.gov/privacyframework.

Request for Information

The following list of topics covers the major areas about which NIST seeks information. The listed areas are not intended to limit the topics that may be addressed by respondents so long as they address privacy and how a useful Privacy Framework might be developed. Responses may include any topic believed to have implications for the development of the Privacy Framework, regardless of whether the topic is included in this document.

Risk Management

NIST solicits information about how organizations assess risk; how privacy considerations factor into that risk assessment; the current usage of existing privacy standards, frameworks, models, methodologies, tools, guidelines, and principles; and other risk management practices related to privacy. In addition, NIST is interested in understanding whether particular frameworks, standards, guidelines, and/or best practices are mandated by legal or regulatory requirements and the challenges organizations perceive in meeting such requirements. This will assist in achieving NIST's goal of developing a framework that includes and identifies common practices across contexts and environments and is structured to help organizations achieve positive privacy outcomes. Accordingly, NIST is requesting information related to the following topics:

Organizational Considerations

1. The greatest challenges in improving organizations' privacy protections for individuals;

2. The greatest challenges in developing a cross-sector standards-based framework for privacy;
3. How organizations define and assess risk generally, and privacy risk specifically;
4. The extent to which privacy risk is incorporated into different organizations' overarching enterprise risk management;
5. Current policies and procedures for managing privacy risk;
6. How senior management communicates and oversees policies and procedures for managing privacy risk;
7. Formal processes within organizations to address privacy risks that suddenly increase in severity;
8. The minimum set of attributes desired for the Privacy Framework, as described in the *Privacy Framework Development and Attributes* section of this RFI, and whether any attributes should be added, removed or clarified;
9. What an outcome-based approach to privacy would look like;
10. What standards, frameworks, models, methodologies, tools, guidelines and best practices, and principles organizations are aware of or using to identify, assess, manage, and communicate privacy risk at the management, operational, and technical levels, and whether any of them currently meet the minimum attributes described above;
11. How current regulatory or regulatory reporting requirements (e.g., local, state, national, international) relate to the use of standards, frameworks, models, methodologies, tools, guidelines and best practices, and principles;
12. Any mandates to use specific standards, frameworks, models, methodologies, tools, guidelines and best practices, and principles or conflicts between requirements and desired practices;
13. The role(s) national/international standards and organizations that develop national/international standards play or should play in providing confidence mechanisms for privacy standards, frameworks, models, methodologies, tools, guidelines, and principles;
14. The international implications of a Privacy Framework on global business or in policymaking in other countries; and

15. How the Privacy Framework could be developed to advance the recruitment, hiring, development, and retention of a knowledgeable and skilled workforce necessary to perform privacy functions within organizations.

Structuring the Privacy Framework

NIST is interested in understanding how to structure the Privacy Framework to achieve the desired set of attributes and improve integration of privacy risk management processes with the organizational processes for developing products and services for better privacy outcomes. NIST is seeking any input from the public regarding options for structuring the Privacy Framework, and is particularly interested in receiving comment on the following issues, if applicable:

16. Please describe how your organization currently manages privacy risk. For example, do you structure your program around the information life cycle (i.e., the different stages – from collection to disposal – through which PII is processed), around principles such as the fair information practice principles (FIPPs), or by some other construct?
17. Whether any aspects of the Cybersecurity Framework could be a model for this Privacy Framework, and what is the relationship between the two frameworks.
18. Please describe your preferred organizational construct for the Privacy Framework. For example, would you like to see a Privacy Framework that is structured around:
    a. The information life cycle;
    b. Principles such as FIPPs;
    c. The NIST privacy engineering objectives of predictability, manageability, and disassociability[6] or other objectives;
    d. Use cases or design patterns;
    e. A construct similar to the Cybersecurity Framework functions, categories, and subcategories; or
    f. Other organizing constructs?

[6] NISTIR 8062, *An Introduction to Privacy Engineering and Risk Management in Federal Systems* at https://csrc.nist.gov/publications/detail/nistir/8062/final.

Please elaborate on the benefits or challenges of your preferred approach with respect to integration with organizational processes for managing enterprise risk and developing products or services. If you provided information about topic 10 above, please identify any supporting examples of standards, frameworks, models, methodologies, tools, guidelines and best practices, and principles.

Specific Privacy Practices

In addition to the approaches above, NIST is interested in identifying core privacy practices that are broadly applicable across sectors and organizations. NIST is interested in information on the degree of adoption of the following practices regarding products and services:

- De-identification;
- Enabling users to have a reliable understanding about how information is being collected, stored, used, and shared;
- Enabling user preferences;
- Setting default privacy configurations;
- Use of cryptographic technology to achieve privacy outcomes – for example, the disassociability privacy engineering objective;
- Data management, including:
    - Tracking permissions or other types of data tracking tools,
    - Metadata,
    - Machine readability,
    - Data correction and deletion; and
- Usable design or requirements.

19. Whether the practices listed above are widely used by organizations;
20. Whether, in addition to the practices noted above, there are other practices that should be considered for inclusion in the Privacy Framework;
21. How the practices listed above or other proposed practices relate to existing international standards and best practices;

22. Which of these practices you see as being the most critical for protecting individuals' privacy;
23. Whether some of these practices are inapplicable for particular sectors or environments;
24. Which of these practices pose the most significant implementation challenge, and whether the challenges vary by technology or other factors such as size or workforce capability of the organization;
25. Whether these practices are relevant for new technologies like the Internet of Things and artificial intelligence; and
26. How standards or guidelines are utilized by organizations in implementing these practices.

Authority: 15 U.S.C. 272(b), (c), & (e); 15 U.S.C. 278g-3.

Kevin A. Kimball,
Chief of Staff.

[FR Doc. 2018-24714 Filed: 11/13/2018 8:45 am; Publication Date: 11/14/2018]