ISACA Response to Request for Information from the National Institute of Standards and Technology (NIST) for Developing a Privacy Framework

Document: 83 FR 56824
Document Number: 2018-24714
Agency/Docket Number: 181101997-8997-01

ISACA, on behalf of its nearly 60,000 information and cyber security professionals in the United States and its global community of nearly 140,000 professionals, is grateful for the opportunity to provide information for use in the continuing development of the NIST Privacy Framework.

This request for information is both timely and welcome. The development efforts for the NIST Privacy Framework have been exception thus far. ISACA believes that, while the information requested in these consultation's questions will provide valuable information to aid the ongoing development of the NIST Privacy Framework, our organization can best provide insights and information on the following questions:

Risk Management

Organizational Considerations

NIST is requesting information related to the following topics:

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

The greatest challenge is to fundamentally change the mindset of the organization regarding privacy. At all levels of the organization, employees need to understand why they are collecting personal data from their customers, how they use and store personal data, and how they dispose of personal data. This will require organizational change management and business process change to execute this transformation. It's also important for organizations to identify and maintain personal data inventories and data maps and build Privacy-by-Design and Privacy-by-Default into their product development lifecycle and software development lifecycle. Privacy risks should always be considered with new products or new technologies, from early conceptualizing, throughout the development process, and after deployment.

Finally, it's important for organizations to consider additional safeguards when collecting, using, storing, and disposing of personal data. Unfortunately, there can be reluctance by organizations to destroy data they have worked hard to obtain; some organizations, regrettably, might even go so far as to not abide by their data retention standards. Doing so benefits only one cohort: those looking to benefit from a data breach. Additional safeguards, including risk assessments, should be independently evaluated by Internal Audit or a third-party organization. The outcome of these reviews should be communicated to highest levels of senior leadership including the board.

2. The greatest challenges in developing a cross-sector standards-based framework for privacy;

The greatest challenge is data classification for personal data as some types of personal data are more sensitive than others. Data classification would need to consider these differences and then describe reasonable assurance to protect these differences. A federal data protection regulation could be the driver to enforce the protection of personal data especially if there are fines that are applicable for each level.

Another challenge is for organizations that are not heavily regulated to adopt a framework to protect personal data. Highly regulated organizations (i.e., healthcare, financial services, publicly traded) will be better positioned to adopt a privacy framework while other organizations will be more reluctant. Different organizations have different needs for the personal data they obtain, from different types of consumers (i.e., B2B businesses vs. B2C businesses, etc.), and this leads to different organizational mindsets regarding privacy. Again, a federal data protection act with fines provides a standard, level playing field, and will drive organizations to become more responsible for protecting personal data.

3. How organizations define and assess risk generally, and privacy risk specifically;

Organizations should consider a standard framework to assess and manage both cybersecurity and privacy risks within their organization. It would be imperative for organizations to adopt the NIST RMF 2.0 since it includes both cybersecurity and privacy risks.

4. The extent to which privacy risk is incorporated into different organizations' overarching enterprise risk management;

Both cybersecurity and privacy risks should be considered business risks for an organization. The extent should be high for incorporating these risks into the enterprise risk management framework; while this has been improving in recent years, it is not yet prevalent. The FAIR methodology should be considered to quantify the impact to the organization.

5. Current policies and procedures for managing privacy risk;

Current policies and procedures for managing privacy risk should be reviewed and approved annually by senior management. The creation and maintenance for privacy policies and procedures require a multidisciplinary approach including, but not limited to, the leadership of departments such as Legal, HR, Business Operations, Information Security, and IT.

6. How senior management communicates and oversees policies and procedures for managing privacy risk;

Data Protection Officers (DPOs) should, ideally, be present within all organizations to provide oversight on how an organization addresses policies and procedures for managing privacy risk. Privacy policies, apart from the healthcare sector, are not as pronounced as policies within cybersecurity, and they should be. The DPO should be a senior leader in the organization and should have enough knowledge and skills to protect personal data.

7. Formal processes within organizations to address privacy risks that suddenly increase in severity;

Formal processes should be implemented to protect personal data and address privacy risks. While these may currently be built into incident response plans, it may be of benefit to widen their reach, giving greater attention toward prevention as well (i.e., investments in encryption; centralized key systems, etc.).

The requirements for these formal processes should be like the requirements of GDPR as well as the consequences. An exceptional Privacy Framework would benefit greatly from a comprehensive and complementary Federal data protection act that enforces the protection of personal data.

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;

The Attributes section could benefit from the addition of an attribute related to accountability and responsibility. This would include governance by senior leadership within the organization and oversight and management by a senior leader within the organization—such as a Data Protection Officer.

9. What an outcome-based approach to privacy would look like;

An outcome-based approach to privacy would be scalable framework for any type of organization to address privacy risks and protect personal data within their organization. Organizations can no longer state that they are not accountable to address privacy risks and protect personal data.

While this could take many forms, it should include (at a minimum):

- The protection of privacy data (even though the data was accessed in an unauthorized manner), using encryption/tokenization, with centralized key management in place
- Providing audit and logging capability to inform Incident and Breach Response Plans
- Providing reports to Regulatory Authorities following a breach that show that encryption was in place

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;

All organizations should consider the NIST RMF 2.0 as well as NIST CSF and this future NIST Privacy Framework if they have not adopted an international standard (i.e., IS02700 series). In order to drive this adoption, we will need a skilled workforce with cybersecurity and privacy risk management knowledge and experience. This workforce will also need to understand the industry (i.e., healthcare, financial services, etc.) in order to understand how and where personal data is used within the organization.

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;

In addition to existing privacy laws and data protection regulations (i.e., HIPAA, GLBA, state laws), the current privacy landscape would benefit greatly from a comprehensive federal data protection act to cover the organizations that are impacted by existing regulatory requirements. Organizations need to disclose how they are addressing these risks; perhaps constructs like RMF 2.0 and the AICPA's SOC for cybersecurity report should be considered among the standard requirements for organizations.

12. Any mandates to use specific standards, frameworks, models, methodologies, tools, guidelines and best practices, and principles or conflicts between requirements and desired practices;

Organizations should demonstrate how they have considered privacy risks and have applied appropriate safeguards to protect personal data. Though mandating the use of a standard or framework takes time and marketplace-wide cooperation, it will eventually be likely that the marketplace becomes the mandator of standards and frameworks. Those companies adhering to standards and frameworks will be able to demonstrate to their constituencies their concern for privacy risks and the steps that have been taken to protect data. In the mind of their constituent consumers, this is an advantage their non-adherent competitor will not have. At this point, adoption of standards and frameworks becomes market-driven, and mandated because their competitor is already using them.

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;

If the AICPA's SOC for cybersecurity report become a mandatory report and include privacy risks, that could be an exceptional complement to an organization's financial reporting.

14. The international implications of a Privacy Framework on global business or in policymaking in other countries; and

Just like GDPR set an expectation that any organization must adopt compliance with the regulation, this should also apply to any organization operating in the US. There should be a minimum standard that global organizations adopt a privacy framework to protect personal data. This should be one of the foundational purposes for a privacy framework: to provide guidance to organizations to prepare a comprehensive privacy plan that will meet their internal needs, and those, generally, of countries in which they do business, or plan to do business.

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.

It's important that we address the skills, knowledge, and experience gap with the workforce to address cybersecurity and privacy risks. We need individuals with a combination of skills that include quantitative risk management (i.e., FAIR methodology, NIST RMF 2.0), cybersecurity, and privacy. In addition, this will hopefully inform and encourage 2- and 4-year educational institutions (as well as graduate programs) in preparing individuals in areas such as IT Risk Management, Privacy, and Cybersecurity.

Structuring the Privacy Framework

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?

Managing privacy risks should be a combination of managing information through a lifecycle (i.e., from collection to disposal) and FIPPs. It's important for organization to capture where they collect, use, store, and dispose of personal data using data inventories and maps.

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.

The NIST CSF would support security for privacy, incident response, and data sharing limitation. The two frameworks should be complementary and would be further supported by the RMF and/or FAIR.

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 or other objectives;

d. Use cases or design patterns;

Structuring a Privacy Framework that encompasses all the above elements is critical. In addition, future Privacy Framework drafts should include the following terms, as well as their standardized definitions:

consent
right/s
privacy-by-design
security-by-design
data lifecycle

Encryption
breach
notification
erase / erasure
delete
penalty
review
transfer

Specific Privacy Practices

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;

If these practices are not currently employed in most organizations, they should be considered. One of these items stood out from the rest: *Use of cryptographic technology to achieve privacy outcomes—for example, the disassociability privacy engineering objective*.

Encryption and centralized key management is the key (so to speak) to achieving compliance with Article 25 over Data Subjects' Rights, even though Privacy by Design to achieve Privacy by Default has occurred. Meaning, the Article 25 objective is to apply privacy principles and perform a risk assessment, utilize available technology, and prevent a breach of data subjects' rights. A way to assure that, in today's breach-prone environment, is to implement a centralized key management solution over encrypted data.

20. Whether, in addition to the practices noted above, there are other practices that should be considered for inclusion in the Privacy Framework;

RMF, NIST CSF, and the NIST Privacy Framework 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;

There is an opportunity to map the RMF, NIST CSF, and NIST Privacy Framework to the AICPA TSC for a SOC 2+ report.

22. Which of these practices you see as being the most critical for protecting individuals' privacy;

All these practices are critical to the protection of individuals' privacy, with centralized encryption key management and encryption or tokenization efforts being among the most critical.

23. Whether some of these practices are inapplicable for particular sectors or environments;

All sectors could benefit from these frameworks.

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;

n/a

25. Whether these practices are relevant for new technologies like the Internet of Things and artificial intelligence; and

Yes, these practices, including encryption and centralized key management, are relevant to the collection, usage and sharing of personal data.

26. How standards or guidelines are utilized by organizations in implementing these practices.

Standards and guidelines (particularly those put forth by NIST, especially in areas such as centralized key management and encryption) will be critical for the successful implementation and application of these practices.

Thank you again for this opportunity to assist NIST in the development of the NIST Privacy Framework. In the past, NIST had engaged in efforts around Privacy Engineering; we hope to see those efforts also built upon as

NIST continues to build its Privacy Framework. ISACA looks forward to continuing to work with NIST and the Federal government on privacy issues and concerns in the years ahead.