January 14, 2019

Security Industry Association
8405 Colesville Road
Suite 500
Silver Spring, MD 20910
(301) 804-4700

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

RE: Docket No. 181101997-8997-01

Introduction

The Security Industry Association (SIA) is pleased to submit the following comments in response to Docket No. 181101997-8997-01, the request for information regarding "The NIST Privacy Framework: An Enterprise Risk Management Tool."

SIA is a U.S. trade association representing more than 900 security solutions providers, ranging from large global technology firms to locally owned and operated small businesses. Our membership includes manufacturers, software developers and systems integrators that install and maintain security technology for end users in the government, institutional, commercial and residential sectors.

We address the data privacy needs and concerns of our members primarily through the SIA Data Privacy Advisory Board.

The comments are listed according to the section of the RFI to which they refer.

Privacy Framework Development and Attributes

NIST states that it "seeks to understand whether organizations would be better able to address the full scope of privacy risk with more tools to support better implementation of privacy protections." There is an opportunity here to create business incentives whereby value is generated as a result of increased privacy protections and controls. This is something the security industry has recognized and made progress with by representing the value inherent in security

services to protecting brand, personnel and intellectual property. The sensitive information involved in these circumstances has significant overlap with the sensitive information that is identified with privacy risk. Security systems add value in numerous ways that should be included in the framework.

The requirements for innovation, as called for in the RFI, cover not only technology innovation but also innovation in business models, incentives and regulations. NIST should work with trade associations such as SIA to explore and promote activities in these areas. SIA has developed a privacy framework for the manufacture and deployment of security and surveillance systems (https://www.securityindustry.org/wp-content/uploads/2017/11/gr-privacy-framework.pdf) and would welcome the opportunity to partner with NIST in creating the Institute's Privacy Framework, as well as developing a code of conduct related to privacy protections.

The RFI identifies several minimum attributes for the Privacy Framework, including:

"Common and accessible language."

> SIA is particularly aware of the challenges that small businesses face with regard to protecting privacy and would be willing to work jointly with NIST to develop a Privacy Framework that addresses the unique needs of small businesses.

"Risk-based, outcome-based, voluntary and non-prescriptive."

> Most security solutions are risk-based, and SIA and its member companies would be happy to work with NIST to apply their expertise in helping to develop a risk-based privacy protective framework.

Risk Management

NIST asks for information to help understand the use of frameworks, standards, guidelines and/or best practices related to legal or regulatory requirements. In terms of best practices, there are numerous examples, including efforts by the physical security industry to address secure communication channels between card readers and door controllers, as they can often be a conduit for personal information in the form of personal identifiers and/or biometric information. The SIA Open Supervised Device Protocol (OSDP), which is included in the International Electrotechnical Commission (IEC) standard as 60839-11-5. Additionally, since physical protection is critical to, among other things, the safeguarding of servers where personally identifiable information is processed and stored, ASIS International has developed a set of six risk management steps, referred to as the ITSC6, that covers cybersecurity, supply chain and privacy risk management.

Organizational Considerations

"The greatest challenge in improving organizations' privacy protections for individuals."

Silos of information and operations are a challenge that physical security professionals have taken on as physical, information and cybersecurity converge. Operational privacy faces the same challenges, and it will be critical that the privacy risk interdependencies among different parts of organizations and the supply chain be understood.

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

One challenge is that requirements and risk are very much based on legal jurisdiction. There are state-to-state variations in the United States, as well as international differences. Another challenge is allowing for the responsible use of anonymized data to further innovation while protecting the integrity and privacy of the data during initial collection. We should not stymie innovation to meet the demands of privacy, nor can we give up privacy in the name of innovation. Assurances and standards must be adhered to in order to protect both. A third challenge will be that, in anticipating the future of digital technologies, the framework must be flexible and broad enough to help guide innovation in all sectors without having to be rewritten. The line between privacy rights and expectations in all aspects of consumption and business needs to be clear.

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

The physical security industry has experience working with other teams in an organization to manage enterprise risk. This experience points to the need to manage risk, in this case privacy risk, across the enterprise.

"Current policies and procedures for managing privacy risk."

SIA has developed a set of references (https://www.securityindustry.org/wp-content/uploads/2018/07/Privacy-Profile-References-FINAL.pdf; https://www.securityindustry.org/2018/06/01/gdpr-and-the-security-industry) for its members that consolidated other privacy materials to provide a better understanding of the issue. We look forward to doing the same with the NIST Privacy Framework as it evolves.

"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."

The NIST Cybersecurity Framework and related NIST Special Publications such as 800-37 and 800-53 are relevant here. On occasion, the use of repositories such as Github has proven helpful in achieving minimum attribute 7 for these to be living documents. For example, the process with the SP 800-63 update very effectively leveraged this approach.

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

With regard to the security industry and surveillance systems, there do exist surveillance codes of conduct such as those put forward by the United Kingdom Surveillance Commissioner for a range of video and machine vision applications, including "Surveillance Camera Code of Practice" and, more recently, "In the picture: A data protection code of practice for surveillance cameras and personal information" (https://ico.org.uk/media/1542/cctv-code-of-practice.pdf). These documents cover uses including license plate reading, body-worn cameras, unmanned aerial vehicles and other systems. SIA has put together a set of global references to drive codes of practice and codes of conduct with regard to security and privacy best practices.

"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."

SIA is an ANSI-accredited standards developing organization and is currently engaging with ISO/IEC to create global standards for the security industry.

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

A Privacy Framework should ideally work across global contexts, only introducing unique requirements as a last resort or in pursuit of a specific profile or use case. To the extent that companies interact globally once a framework is adopted, it will have a global impact as users and organizations that interchange data interoperate with individuals and organizations across jurisdictions and sectors throughout information and service lifecycles. In particular, many organizations look to NIST as a source of best practices to help them address the challenge of operating globally, so the Privacy Framework needs to be sensitive to this. NIST often provides a mapping across other frameworks in its publications, such as in the CSF 800-53 and 800-63, which would be a useful appendix for the Privacy Framework.

"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."

Curriculum, workshops, training, and codes of practice and certifications all can build and be part of the development of a Privacy Framework. NIST should look to leverage industry, trade organizations, other standards developing organizations, subject matter experts, and users across use cases to develop a Privacy Framework that, in addition to enhancing data privacy, also supports workforce development.

Specific Privacy Practices

"How standards or guidelines are used by organizations in implementing these practices"

There are a wide range of standards efforts specific to AI and IoT, and SIA has conducted interoperability and conformance events and other activities to bring the security industry together, have end users share their experiences, and show the benefits of standards. SIA continues to work to ensure that standards evolve to meet the challenges of privacy and security risk in both the physical and cyber domains.

Conclusion

Many of the challenges that will arise during the development of the NIST Privacy Framework are already well known to the members of the physical security industry. For example, security professionals regularly manage risk, remove silos between traditionally separate but converging areas such as physical security and cybersecurity, develop standards and best practices to enhance efficiency and interoperability, and work across jurisdictions that have varying legislative and regulatory mandates, all to protect personnel and property while also ensuring the security and privacy of personally identifiable information and other sensitive data. SIA and its members would welcome the opportunity to share their experiences, expertise and lessons learned with NIST as it works to address the critical issue of data privacy.