SESSION IV: NIST'S ROLE IN A RAPIDLY CHANGING TECHNOLOGY WORLD

THE NIST PRIVACY FRAMEWORK—*Naomi Lefkovitz, Senior Privacy Policy Advisor and Lead for the Privacy Framework, Information Technology Laboratory*

Ms. Lefkovitz leads the efforts to develop the Privacy Framework through the Privacy Engineering program. The Privacy Framework was modeled after the Cybersecurity Framework. The collaborative development began last fall. All the attributes that contributed to the success of the Cybersecurity Framework were utilized in the collaborative development of the Privacy Framework.

There have been two public comment periods, three public workshops, five seminars to date. The goal is to refine the comments and get to Version 1.0 by the end of the year.

One of the biggest issues was asking about practices for privacy risk management and how organizations defined it. The Cybersecurity Framework helped with the genesis of the Privacy Engineering program and led to the development of standards, though the meaning of privacy was debated.

Cybersecurity risk can be associated with loss of confidentiality, integrity, and availability, and the privacy risks were associated with unintended consequences of data processing. One big discussion was the relationship between privacy risk and organizational risk. If privacy risk creates a problem arising from data processing, then it is the individuals who are going to experience those problems directly. Helping organizations understand managing privacy risk better will lead to them being able to manage other risks, resulting in better decisions and resource allocations to help strengthen privacy programs.

On how to frame value propositions, the Privacy Framework supports building customer trust, fulfilling current compliance obligations, and facilitating communication. Doing the privacy risk assessment helps organizations to figure out how to get beneficial uses while minimizing adverse consequences. The Privacy Framework can help organizations demonstrate how they may be fulfilling compliance obligations. Facilitation of communication of privacy practices are important to customers, as they could be individual direct customers or business customers.

How to structure the components in the Privacy Framework was requested through a Request for Information. Some suggested to structure it like the Cybersecurity Framework, using the concepts of the Core to provide an increasingly granular set of activities and outcomes that enable an organizational dialogue about managing privacy risk. Profiles are a selection of specific functions, categories, and subcategories from the Core that the organization has prioritized to help it manage privacy risk. Also, implementation tiers will help an organization communicate about whether it has enough processes and resources in place to manage privacy risk and achieve its target profile. The profiles, like the Cybersecurity Framework are a key part of the risk-based approach.

There are five Core functions of the Privacy Framework; identify, govern, control, communicate, and protect. These were based on stakeholder feedback, but there have been adjustments. Govern was added to the functions as well as monitoring and review categories. The two new categories are control and communicate, which focus on the data processing aspect. There is a continuing discussion about how to maintain flexibility and simplify the approaches to the different frameworks.

The informative references provide specific sections of standards, guidance, and practices that can be mapped to the Core subcategories and support achievement of the subcategory outcomes. NIST has provided a mapping of subcategories to relevant NIST guidance. NIST will develop a process for accepting external informative resources.

Laying the groundwork for the future, the Privacy Framework seeks to improve and overcome challenges around mechanisms to provide confidence, emerging technologies, privacy risk assessment, privacy workforce, re-identification risk, and technical standards.

Ms. Lefkovitz said the framework needs to be adopted by all stakeholders. Sharing insights as feedback will help to socialize the Privacy Framework. The program is in the process of gathering quotes to use in the Version 1.0, which was important in the development of the Cybersecurity Framework. The program is looking for organizations who want to submit informative references or use cases to help develop the framework. Moving the stakeholder engagement on adopting use and implementation is an area that will be developed in the coming year.

Discussion

The group discussed the following topics:

- Simplifying the control for existing privacy standards within the framework with effective solutions;
- Broaden the best means of managing privacy risk that individuals may be experiencing;
- Clarity around objectives and definition of what privacy harm is;
- Providing guidelines on what a risk management framework is and how it should be applied;
- Congressional concern made to VCAT members about what NIST is doing about privacy;
- Engagement on the Hill will be more important than ever when Version 1.0 is completed; and
- NIST consulting with Europeans on their findings relating to privacy and how it's handled in the European Union.

U.S. Government and Emerging Technology Standardization—Implications for NIST's Roles—*Dr. Ajit Jillavenkatesa, Senior Policy Advisor, Standards and Digitalization*

Dr. Jillavenkatesa outlined the next portion of the meeting as consisting of three parts for discussion. His presentation providing the NIST perspective, a private-sector representative providing the private-sector perspectives around the dynamics of standardization, and then a panel discussion including three subject-matter experts from the private sector providing different perspective.

NIST uses standards in different contexts. Documentary standards provide common and repeated use, rules, guidelines, or characteristics for activities or their results, such as if things do not work out, there is a standard available for that. These are developed through processes with specific process attributes such as consensus, openness, and balance. Consensus, however, does not represent unanimity. It is what a group of experts can agree on, so they are developed in an open process. It is a balance of interests to avoid only one outcome.

Standards are pervasive and ubiquitous and impact every aspect of modern life. The widespread use of standards helps to realize the economies of scale e.g. in manufacturing. Looking at the competitiveness aspect, it gets to the issue of global adoption of standards, international relevance, and this is when manufacturers have a strong ability to drive innovation when they're not competing with regards to establishing a baseline. The competition is really around the value-add in the services.

There is an increase in complexity around standards for connectivity of devices and systems. This gets into the issue of interoperability. An effective standard system is one that looks for speed, agility, and solutions that are fit-for- purpose. This is evident in the US approach which is a decentralized system, one which includes private sector and government participation. This enables responsiveness in the system to meet stakeholder needs. Having an agile, fit-for-purpose solutions development process has contributed to U.S. leadership in technology and innovation.

NIST's role is defined by statute and policy in two key areas. The technical aspects are at the heart of the NIST measurements and technology mission. The standards development processes are a logical extension by which knowledge transfer from NIST laboratories happens into the world at large. It is a cost-effective means to get information and expertise from the NIST labs to the world outside. Another advantage is the ability to understand firsthand the emerging market needs and trends when NIST sits at the same table with private-sector colleagues and gains a better understanding of what are the issues and solutions. NIST is often called upon to be a technical advisor by federal agency colleagues who are also looking at many of these same issues. The NIST policy role is defined by statute and long-established policy. NIST is a facilitator of the information exchange between the federal agencies and the private sector.

NIST is in an ideal position to see global trends and changes due to innovations emerging in digital technology spaces. The extension of this role positions NIST to be a technology resource and technical expert to agencies such as the Office of the US Trade Representative, State Department and other agencies, that have responsibilities relating to trade negotiations. Our roles have included providing expertise that has shaped language around cybersecurity, aspects of digital trade, etc.

In standards development, there has been increased participation in the role of non-traditional participants, countries like China, Vietnam, Korea, Sub-Saharan Africa, and the Middle East, which is because of the shift in manufacturing to countries for the value chain that drive some of the standardization efforts. As well, the growth of R&D centers in other countries is driving this interest.

There is a high level of interest from executive and legislative branches of the U.S. government driven through a combination of national security and economic security considerations in a changing landscape. Success in standards development is tied to longevity of participation and the ability to invest into the future, and this can be challenging in constrained budgetary environment. NIST wants to raise awareness within the larger federal enterprise about why the standards development issues are important.

Areas that NIST is highlighting include changes in the standardization landscape that present new opportunities and challenges, stepped-up efforts to raise awareness among federal staff and leadership, increased federal interagency engagement and information exchange, enhancing standards and conformity assessment competence of federal staff, and facilitating greater engagement between U.S. private sector and federal agencies.

There are significant impacts and considerations for NIST to examine. A higher profile and understanding of NIST's role and responsibilities, increased expectations and interest in NIST engagement, filling in the gaps in standards development, reprioritization of limited financial resources, diversion of technical resources away from research, and awareness of the risk of mission creep and impact on effectiveness.

Key takeaways are that NIST is a valued player in the documentary standards ecosystem. Changes and trends in standards development reflect broader economic and geopolitical changes. Greater awareness about the need for effective and strong U.S. engagement is needed in standards development and how to best meet expectations.

Discussion

The group discussed the following topics:

- Raising awareness policy leaders about what works and what doesn't work;
- Standards development for emerging technologies such as artificial intelligence, quantum information science, and 5G; and
- Balancing NIST activities to create a more even playing field on a global scale.

Changing Dynamics in International Standards Development—*Jeffrey Weiss, Esq., Venable LLP*

Mr. Weiss shared his extensive U.S. government background, spending more than 15 years, which consisted mainly working on standards, as the standards negotiator at the Office of the United States Trade Representative (USTR), Office of Management and Budget (OMB), Office of Information and Regulatory Affairs (OIRA), and Secretary of Commerce Office of Standards. While at OIRA he led the revision of OMB Circular A-119, the U.S. government policy on standards and conformity assessment to ensure that it is current with the evolving standards landscape.

The reason why A-119 had to be rewritten was that it did not say anything about international standards, and there was a need for consistency. This had to be put into guidance for agencies to follow. Clarifications address that an international standard is a voluntary consensus standard and complies with WTO Committee principles for international standards development: openness, transparency, effectiveness and relevance, impartiality and consensus, coherence, and a development dimension.

Noteworthy is that a policy was put in place for the technology space, a provision that does not preclude the use of non-voluntary consensus standards. To ensure adherence, a provision encouraged the use of more than one standard to meet an agency's objective to provide greater flexibility, enhance customer choice, enhance competition and innovation, while making it easier for a company to do business in multiple markets.

Distinct from the revision of OMB Circular A-119, but consistent with the focus on the federal government's use of consensus standards, a working group on international cybersecurity standards was put together at Commerce. Mr. Weiss assisted with developing a standardization strategy for international cybersecurity standards, which became sort of an embodiment of A-119 in the cybersecurity space. This document mapped the cybersecurity standards space looking at core areas and applications where standards were and were not available.

Recently, the USTR and interagency put more content reflecting the approaches in A-119 into the technical barriers to trade (TBT) chapter of the U.S.-Mexico-Canada Trade Agreement. An important provision encourages the use of multiple international standards by regulators when all standards fulfill an agency's objectives.

Mr. Weiss is working on a Standards Alliance project with the American National Standards Institute (ANSI) and the U.S. Chamber of Commerce and others. He went to South and Latin America looking at standards policies from different countries. It was discovered that there was a hierarchy of standards in some of those countries, some of which were below European standards. Phase two of this endeavor with the Standards Alliance is going to be a 5-year project.

Mr. Weiss also shared his experiences as a G20 digital economy negotiator for the U.S. Government and the challenges working on issues of cybersecurity, the free flow of data, and privacy.

An important trend to be aware of is the use of justifying measures based on national security grounds in the trade and other contexts. Another trend is the intersection between standards and national security that needs to be examined.

The rise of frameworks, specifically NIST frameworks, is something that the private sector likes to use as these frameworks extensively leverage the use of international standards. In the international space, it is not mandatory but, there are commitments for regulations and standards.

Industry Stakeholder Panel—*Jonathan Kallmer, Esq., Information Technology Industry Council; Mike Nawrocki, Technology Solutions, ATIS; and Sean Heather, International Regulatory Affairs, U.S. Chamber of Commerce*

Presentation by Jonathan Kallmer:

Mr. Kallmer described the Information Technology Industry Council (ITI) as a trade association consisting of over 70 large global technology companies. These companies depend on an open global industry-led approach to standards. The Standards Committee is one of 37 committees of ITI and is the most popular. ITI devotes resources and technical experts to support the work of advocating in an open industry-led system. It is an open interoperable system that supports the company's businesses from a commercial standpoint and supports U.S. national security, innovation, and national interests. In this regard, there is no conflict between having a global mandate and pursuing it in a way that furthers U.S. objectives.

One area of concern in the standards arena is the approach to standardization has been different in Europe than the one pursued in the United States, which desires an open forum for discussing standards rather than government prescribing standards. Another area of focus is China continuing to move up the innovation value chain, pursuing a more concerted strategy to become more technologically advanced and be the leader in innovation and technology development. It has pursued unique standards and created an environment where it is imperative for markets to operate under Chinese legal prescriptions, and setting those standards is not open to those outside of China. China is sending more representatives to international standard-setting discussions in its effort to achieve the leadership position.

The recent addition of Huawei and other Chinese entities to the Commerce Department Entity List, which imposes significant restrictions and export controls on the outflow of goods or technology outside of the United States to the entities listed is now intersecting with standards development. There is confusion about whether Huawei needs to cease participation in standards developing organizations (SDO's), or whether US participants can engage with Huawei experts in standards development and so clarification is needed from the Commerce Department. The desired result is for U.S., European, and Chinese companies to be in the same room in a voluntary industry-led environment and letting the market and best ideas prevail. The ITI is looking forward to working with NIST to help achieve this goal. NIST involvement can help make the United States a more appealing place and host international standards discussions.

Presentation by Mike Nawrocki:

The Alliance for Telecommunications Industry Solutions (ATIS) has about 150 members in the communications and information ecosystem. It is an ANSI-accredited SDO with concentration on business, technology, and policy standards.

When 5G specifications were being developed in 2018, ATIS was a North American regional partner for industry and government. ATIS was involved in developing protocols for mitigation of robocalling for the Federal Communications Commission. They have several strategic initiatives around artificial intelligence, 5G, blockchain, context-aware identity management when it comes to the future of standards. They are in the process of launching a 5G supply chain working group utilizing the work that NIST and other organizations have done around guidelines and best practices and to operationalize those into standards.

More recently, there has been more of a focus on integrating open-source solutions into something more stable in the communications industry. Standards have always been focused on interoperability, but there seems to be this growing understanding of stability. NIST can help in this area with activities focused on foundations, platforms, and frameworks, providing a sense of stability that can then promote innovation. Innovation needs a level of stability to be operable. On the future of standards as it pertains to communication, there will always be a balance that has to happen between regional and global standards. The U.S. must not be outpaced by other regions when it comes to communications technology and should continue to attend global development meetings.

Presentation by Sean Heather:

Mr. Heather represents the U.S. Chamber of Commerce, which consists of every sector as members, from self-employed individuals to large corporation employers. He runs the Center for Global Regulatory Cooperation at the Chamber, which was started about 10 years ago, and deals with trade barriers and cross-border business. Trade agreements and international standards are needed to promote the private-sector voluntary approach. The goal is to advance U.S. commercial interests at the same time as advancing the primary interest by regulating the market.

Mr. Heather gave an example, at an airport, someone can bring either 3 ounces or 100 milliliters of liquid on a plane; however, these measurements at not the same. This is an area where standards-setting needs to be examined more closely. The Europeans do not want to find constructive ways to work with the Chamber on third-country concerns, and they fight over definitions of what an "international standard" is. They do not want to take a multipath approach to standard setting. China is very effective in getting countries to increasingly follow their approach and have been more effective than the Europeans have been.

Another area of concern for the Chamber is the Chinese are buying into companies, going around the CFIUS (Committee on Foreign Investment in the United States) process, to get access to U.S. technology. It is difficult to define what parts of AI are national security concerns. There has been an active debate ongoing about antitrust issues surrounding places like Korea and China. The Chamber is enthusiastic about the U.S. to be the lead in taking Cybersecurity Framework internationally and promoting it. Mr. Heather believes the Privacy Framework is too late for the international arena.

Discussion

The group discussed the following topics:

- Privacy and data protection norms and rules are still in play globally;
- Importance of frameworks and future of standards driving interoperability;
- 5G supply chain standards and West Coast port IT systems;
- Being the hosting country for standards development meetings has economic advantages;
- NIST helping to advance standards can create an even playing field;
- Lessons learned in the influence of 3GPP standardization;
- U.S. efforts to elicit cooperation from European Commission on good practice in standard setting;
- China economic incentives to others give them market advantage on an international scale;
- NIST education and awareness efforts with executive and legislative branches on good practices;
- More focus by NIST needed on trade negotiation side to strengthen competitiveness;
- A role for NIST to play on data portability;
- Aligned policy around government, industry, and academia on a set of common objectives; and
- New position of Associate Director of ITL for IT standardization to help elevate ITL engagement in standards development arena.

SESSION V: NIST AND EQUITY

NIST Actions on Equity and Career Advancement for Women and Minorities—*Dr. Heather Evans, Senior Program Analyst, Program Coordination Office*

Dr. Evans stated a high-priority area of the administration is safe and inclusive research environments, as evidenced by the creation of the Safe and Inclusive Research Environments Subcommittee of the National Science and Technology Council and the inclusion of this topic in the FY 2021 R&D budget priorities memorandum. Within NIST, inclusivity is one of the four NIST core values. Evans explained that her presentation would cover a number of recent actions toward achieving this NIST core value by pursuing equity in career advancement.

Early analysis by NIST staff indicated two troubling trends: first, a lack of representation of women and minorities among senior scientific and engineering leadership positions, and second, and STEM (Science, Technology, Engineering, and Mathematics) women and minorities were being promoted at a lower rate compared to their peers. Evans showed data on gender diversity and minority representation in NIST's S&T (Science and Technology) workforce illustrating these findings, noting that at all points in time, women and minorities make up a smaller share of the higher pay bands in the dataset which covered the years 2000 – 2015..

This preliminary data resulted in a call to action. In January of 2018, scientists and managers delivered a memo to the Associate Director for Laboratory Programs (ADLP). In March of 2018, ADLP established a Steering Group for Equity in Career Advancement (SGECA) and in June 2018, the steering group held a kickoff event featuring outside experts. Data gathering and analysis continues today and is ongoing. The mission of the SGECA is to identify causes of apparent inequities in promotions at NIST for women and minority researchers and make recommendations. The steering group consists of representatives from across NIST—career laboratory staff, managers, Human Resources, and Civil Rights and Diversity Office. SGECA actions to date have been to create additional training and staff engagement opportunities, develop and share new data analysis tools and other best practices, advise NIST Director and ADLP on promotion criteria, and establish externa contract and internal detailees to conduct data-driven investigations.

In terms of training, the SGECA partnered with the Office of Human Resources Management and Civil Rights and Diversity Office to offer additional courses such as Unconscious Bias, Generations in the Workplace, Recruiting Through a Diversity Lens, What's Your Micro Trigger, Building Trust in the Workplace, and Assertiveness and Influencing Skills.

Borrowing from the World Café format, the steering group held informal equity cafes, which were structured staff discussions of challenges and opportunities for promoting equity and inclusion. One was held at the Gaithersburg campus in December 2018, and another was held in Boulder in March 2019. There was a full house at both equity cafes, showing that staff are interested in this topic and want to see improvements in this area.

The steering group supported an Inclusivity Summit for all managers and supervisors at NIST on April 30, 2019. At the event, Dr. Copan reinforced the importance of inclusivity and the critical role of managers and supervisors in achieving this core value. The event featured speaker was Dr. Freeman Hrabowski, President of University of Maryland Baltimore County, and an interactive panel discussion with leaders of a variety of NIST affinity and community groups.

Evans described several ongoing data-driven efforts continue to advance equity. One of the original commitments of the SGECA was to commission a study to examine the source of apparent inequities in the career advancement of women and minority STEM workers at NIST. In September, NIST awarded a contract to the University of Oregon (COACh program) to conduct this study. The team is led by Dr. Geraldine Richmond, a renowned scientist and founder of COACh, a grassroots organization with the mission to increase representation of women and underrepresented groups in science and engineering. They will analyze career advancement process for STEM disciplines, identify critical factors in promotion disparity, and develop sustainable approaches and methods that NIST can build upon. This work is anticipated to be completed by April 2021. In addition, two NIST staff were selected by the ADLP for one-year detail assignments to work on their proposed projects to study equity, diversity, and inclusion among NIST staff. Selected through an open competition, the individuals are computer scientist Mary Theofanos and materials scientist Laura Espinal.

Evans described several next steps including follow-up on issues raised by staff during the equity cafes; sharing best practices and infusing knowledge throughout NIST; continuing data gathering and analysis; and providing additional training opportunities for staff engagement.

Additional members from the steering group joined Evans for the discussion: Dr. Joannie Chin, Deputy Director of the Engineering Laboratory; Ms. Teresa Whiteside, Chief, Operations and Strategic Programs

Division, Office of Human Resources Management; and Mr. Jeremy Lawson, Deputy Director of the Civil Rights and Diversity Office.

Discussion

The VCAT thanked the steering group for their progress to date and encouraged them to continue their efforts. The group discussed the following topics with VCAT:

- The importance of aspiring to having diverse finalist candidate pools;
- How gender balance changes the dynamic of research in organizations;
- The importance of being available and on-site at Career Days and Conferences for recruiting to answer questions;
- How issues of diversity may affect attrition statistics; and
- The importance of transparent, unbiased, and clearly communicated recruiting materials and practices.