SCS
SECURE COMPLIANCE
SOLUTIONS

January 14, 2019

Katie MacFarland,
National Institute of Standards and Technology
100 Bureau Drive, Stop 2000
Gaithersburg, MD 20899
privacyframework@nist.gov

Re: Developing a Privacy Framework: The NIST Privacy Framework: An Enterprise Risk Management Tool ("Privacy Framework") Request for Information

To Whom it may Concern:

We at Secure Compliance Solutions applaud NIST's efforts to create a Privacy Framework akin to the widely adopted Cybersecurity Framework. The consensus approach to developing the framework will allow Privacy and Security professionals, Privacy activists, technologists, commercial enterprise stakeholders and government officials to participate in a much-needed privacy framework. The General Data Protection Regulation (GDPR) has modernized the legal landscape for data privacy on a global scale, but more importantly, along with a series of high-profile data breaches, public awareness of their privacy rights and risks has increased.

American enterprise faces a complicated future. As a country, we have developed a rich history and mastery of marketing. Data scientists have always tried to collect viewing, reading and usage habits of individuals to help companies reach those consumers. The introduction of an interconnected network of systems that could extrapolate more and better data, coupled with Big Data analysis techniques and Artificial Intelligence allows enterprise to reach many millions of people, at a micro level – the Individual level.

- What risks does that power pose to the Data Subjects?
- Is having all of that data even necessary? Do the benefits actually outweigh the Breach risk?
- What sorts of nefarious use could a group of smart scientists with mass amounts of computing power at their disposal dream up?
- What sorts of nefarious use could a single person with mass amounts of computing power at his/her disposal dream up?

The time is now for business and government to accept a new reality - that individual privacy rights matter, and loose management of Privacy Information (PI) is no longer acceptable. The onus to alter our business models is on us. We can no longer operate in a piecemeal approach, based on a function (payment processing) OR a service (healthcare). We need a comprehensive approach to managing the comprehensive set of PI elements that any one organization may process.

In the pages that follow, we offer response to your RFI, where we feel we can contribute valuable feedback or perspective. Secure Compliance Solutions is an Information Security and Data Privacy Consultant and Managed Security Services Provider (MSSP), serving the Small-Medium Business (SMB) community. Our responses are based on our experiences assessing SMB client privacy and security risks and guiding those clients through design and implementation of strategic security and data privacy programs. Most new customers with whom we work are just dipping their toes into Cybersecurity and/or Data Privacy waters.

Organizational Challenges to Privacy Protection Improvements

Organizational Resistance

While Privacy Officers, CISOs and CIOs may understand the need to invest in security controls and privacy risk mitigation activities, CEOs, COOs and CFOs are often harder to persuade. Obtaining senior sponsorship to invest the necessary resources to implement a Privacy program that they didn't even know they needed until recently, is a huge challenge, even with the looming threat of penalties for regulatory infractions.

Even with a solid business case to support the introduction of a privacy program as strategic imperative, the reality is that management in most SMBs will be shell shocked by the cost of investment necessary to:

1. Educate the organization on Privacy,
2. Inventory Privacy assets,
3. Identify legal and regulatory obligations,
4. Assess Privacy Risk (include vendor/partner assessment),
5. Design data protection strategy, which ultimately changes an organization's core business strategy and operating model,
6. Develop Privacy Policies and Public Disclosures,
7. Implement protective technologies (encryption, SIEM, File Integrity Monitoring),
8. Design Privacy controls and processing tactics,
9. Reengineer business processes to protect individuals' Privacy
10. Implement processes and controls,
11. Assess vendor / business partner Privacy practices,
12. Continuously Account,
13. Test, Assess, Attest, Certify
14. Repeat

Senior managers make risk-based decisions all the time. For an organization that has never been breached before, it is difficult to convince senior management that a security Incident or data Breach isn't a matter of "if," but "when."

Eliminating Barriers to Entry

A big challenge for NIST should be figuring out how to eliminate cost as a barrier to entry for small business. Small organizations typically don't have time, money or resources to dedicate to implementing privacy protections.

- Could NIST explore programs to encourage technological innovation in the area of privacy controls automation that can be delivered to the SMB market at reasonable price points?
- Develop education and awareness programs to help SMBs integrate responsible privacy practices into business operations.

Risk Management

Unfortunately, many SMBs lack the capacity and capability to effectively adequately manage their own business risks. With Privacy, organizations now have to assess Privacy risks of their customers, data subjects, users and business partner contacts, which has never been in scope before. We should expect a learning curve for many organizations, who don't necessarily have experience conducting this Privacy Impact Analysis (PIA). These organizations haven't had to focus on risk identification that isn't directly tied to company assets, revenues, etc. Consideration of an individual's Privacy Risk is very different than assessing an organization's business, or even security risk.

As we have stated before, the biggest issue is convincing senior management to change the organization's strategic mindset to honor Privacy, particularly when obvious revenue generation opportunities present themselves that depend on the unforeseen use of Privacy data. Organizations must consciously decide that their long-term success will be based on a data protection strategy designed to avoid data breaches and a customer retention strategy based on mutual trust. Management of organizations across the country need to be trained that Privacy risk is a **business concern.** Business processes and communications protocols must change. Technology merely enables protection, but the organization must make business decisions every day that impact or are impacted by Privacy data, regulations, or internally implemented Privacy controls.

Aging Policies – Across SMBs, we routinely witness Privacy Policies that haven't been updated for 2-3 years. When older Privacy Polices were written, they didn't anticipate the legal changes that have occurred since across the globe in recent years. Very often, SMBs may consent to a project to update their Privacy Policies, because they are public-facing, and management wants to appear to comply with reasonable Privacy practices.

Privacy Governance

One big challenge here will be the education of senior managers to make them understand that Privacy is an ongoing business issue that they can no longer leave to the CIO. Security and privacy are not "set it and forget it" activities.

How much time and/or resource must the management team commit to oversight of Privacy? How does senior management justify the time spent governing Privacy vs. tending to other business concerns? Where should Privacy protection lie in the prioritization of business objectives?

The 'Privacy Owner' should be a mandated business role, who shall be responsible for implementation of a privacy program, ongoing enforcement of Privacy requirements across the business and throughout the supply chain. This role should have responsibility for Policy maintenance, and oversight of procedure development.

Organizational Governance Committee - Data Privacy issues should require the involvement of an organizational information security and data privacy governance committee. Like other NIST documentation, please provide objectives and recommendations for good practice. Because each organization is different, governance structures may vary. Can we establish recommended roles on the Governance Committee? Initial participation may include:

- Privacy Owner/Officer
- Authorizing Official
- System Owner
- Senior Information Security Officer
- Data Owner (If different from Privacy Owner)
- Counsel
- Chief Operations Officer
- Chief Financial Officer
- Human Resources Officer

Optional participants may include:

- Security Analysts, SOC Analysts, Security Engineers
- IT Administrators
- Critical Service Providers (IT Information Security)
- Quality Control Personnel

Cross-Applicability Objectives of NIST Privacy Framework

We would like to see the application of Privacy principles across US government and enterprise to match the rigorous implementation in other parts of the world.

- Ideally, Federal legislators will eventually pass a comprehensive Privacy law mandating further Privacy awareness and protection, approaching the protection requirements in the GDPR.
- At the very least, a Federal omnibus law must meet EU-US Privacy Shield requirements.
- Unfortunately, we anticipate that any future Federal privacy law may be susceptible to special interests, which could potentially skew the language in many different ways and result in uneven enforcement of the law across industry sectors.

Nevertheless, the NIST Privacy Framework must be able to support organizational objectives that may range from basic data security to the most stringent privacy protections, in line with business obligations, regulatory requirements and privacy risk.

Competing Regulations

Negotiating competing framework/regulation requirements can be a difficult proposition for organizations of all sizes. In our experience, PCI DSS' requirements are much more prescriptive than HIPAA's, but also much more narrowly focused. We routinely observe medical practices who urge patients to renew their HIPAA consent forms, but who refuse to implement Chip and PIN protection for the payment of fees.

Despite these challenges, a single, consistent Privacy framework, which hopefully supports future comprehensive Privacy legislation should be more readily accepted by most organizations, than the inconsistently implemented and enforced, piecemeal approach to Privacy we have now. Ideally, the NIST Privacy Framework will include a detailed Category (Principle) /Subcategory (Objective) / Control mapping to other Privacy Frameworks' controls (ISO 2700x) as well as laws comprised of very specific requirements (GDPR).

- Subsequent guidance documents (NIST IR) may establish minimal acceptable standards of practice to tailor the Privacy Framework to meet specific legal and regulatory obligations.

Existing Privacy Tools

To facilitate interoperability with other Privacy regulations and frameworks, perhaps NIST may consider leveraging existing tools that may hasten the delivery of a mature Privacy Framework. At SCS, we champion the following tools and techniques, borrowed from multiple sources:

- We utilize the NIST CSF to assess most organizations on their information security practices. We focus on NIST SP 800-171 security controls. We add the NIST SP 800-53 Privacy controls, because 800-171 doesn't adequately cover Privacy.
- We follow NIST assessment and audit standards as defined in NIST SP 800-115.
- For organizations that must comply with GDPR and/or CCPA, we use the Microsoft GDPR Controls Framework.

PCI DSS Privacy Tools:

- We develop a security program for an organization that only has PCI DSS as a regulatory obligation, we design the program around the PCI DSS framework. We may add NIST SP 800-53 Privacy controls.

HIPAA Privacy

- We tailor the NIST CSF to assess most organizations on their information security practices. We focus on NIST SP 800-171 security controls. We add the NIST SP 800-53 Privacy controls, because 800-171 doesn't adequately cover Privacy.

Inclusion of Internet of Things (IoT) and Artificial Intelligence (AI)

The NIST Privacy Framework should promote privacy risk assessment throughout the Service Development Life Cycle. We need to impress upon entrepreneurs that products and services (particularly IoT device manufacturers) must be built with "Privacy designed in", so we can compete with similar products and services originating from countries, in which "Privacy designed in" is already mandated, or in other countries where that sort of control might be strictly forbidden.

- **Artificial Intelligence** - AI, and the associated computer processing power makes micro-level processing and analysis of an individual's habits, preferences, spending trends possible. Previously, organizations churn through de-identified data to extrapolate information about groups of people. Without regulatory controls, organizations have the potential to use AI for nefarious, or at least, unsolicited marketing purposes.
- **IoT** – The inclusion of addressable technologies in all manner of personal devices opens the door to potential Privacy risks on a major scale. The NIST Privacy Framework, and its supplementary documentation, should provide Privacy by Design guidance to protect consumers of the technology.
- **Privacy Engineering** - Please encourage the privacy engineering methods in system development.
  - Encourage *Privacy-By-Default* configurations.
  - Leave user data on the user's device as much as possible. There is no sense collecting the information, if it poses Risk to the Consumer/Service User, and the organization has not real need to collect the data.

We have already mentioned tailoring the NIST CSF to organizational needs. We anticipate tailoring a Privacy Framework for specific use cases, based on the stated objectives in *Privacy Framework Development and Attributes, # 3, "Adaptable to many different organizations, technologies, lifecycle phases, sectors, and uses."*

Structuring the Privacy Framework

Privacy Risk Assessments

While we follow an Information Lifecycle approach to look at risk throughout each of the lifecycle stages, we believe that Privacy protection begins from the moment that a Service concept moves into the Requirements phase. We want privacy protections developed and implemented before we collect the first data.

Organizations must consider ALL of the PI elements that will be:

- Collected,
- Retained and protected,
- Processed (and for what limited purposes), and
- Archived or deleted.

As Security and Privacy Consultants, we are often asked to conduct Data Privacy Impact Assessments (DPIA) on customer information systems. We identify, inventory and analyze an organization's privacy information, and associated risk to help determine a course of action to meet Privacy objectives. We examine:

- Privacy Risks, based on the nature of data elements collected,
- Geographic location of data subjects,
- Privacy data flows,
- Use limitation or processing specifications of the data, in accordance with stated Policy,
- Data subject rights,
- Data collection and protection controls,
- Supply chain Privacy protection practices,
- Record Retention Policy and justification for/adherence to the Policy's terms.

Data Privacy Impact Assessment Template: We have developed a DPIA Template, based on a similar document published by the UK Information Commissioner's Office. This is a simple tool that helps organizations assess their privacy risks. The ICO's template is available here.[i]

Emphasis on Privacy Awareness Training

Certainly, a widely adopted best practice that becomes a standard also becomes the vehicle by which we can educate Privacy and Security workers. Use of business risk terminology, rather than technical terms, helps us to educate the masses on Privacy concerns and controls.

Privacy Awareness & Training (NIST SP 800-53: control: AR-5) must be emphasized to ensure organization-wide understanding of

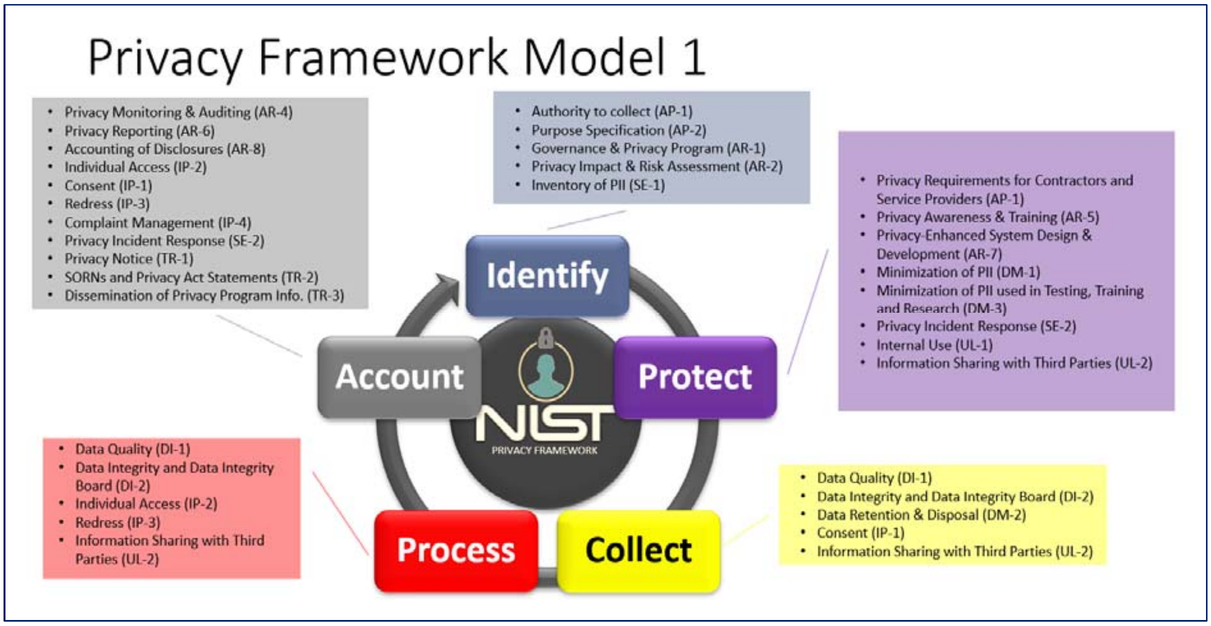
- Privacy Risks,
- Rights of Individuals,
- Roles and Responsibilities,
- Legal and regulatory requirements,
- Organizational Privacy Policies, Standards and governance,
- Incident Disclosure obligations and procedures, and
- Privacy Information Handling Do's and Don't's.

Framework Model

We would like to see the NIST Privacy Framework resemble the NIST CSF, from a structural standpoint. We believe there is a lot of crossover between the NIST Privacy and Cybersecurity Frameworks, particularly since Privacy depends on tight security.

The Privacy Framework should be similarly flexible, with myriad tailoring options available. In fact, it is an organization's ability to creatively implement a Data Privacy program, built on the CSF that makes it so easily adoptable. If we implement programs that **IDENTIFY** appropriate Privacy regulations and associated requirements, we should be able to build in regulation-specific tasks on the Privacy/Info Sec Roadmap and/or Action Plan.

To that end, we offer one perspective in the picture below. Unfortunately, we are not able to offer an image that easily shows the intersection between the two Frameworks, because the crossover occurs at many different points.



Privacy Framework Model 1

- Privacy Monitoring & Auditing (AR-4)
- Privacy Reporting (AR-6)
- Accounting of Disclosures (AR-8)
- Individual Access (IP-2)
- Consent (IP-1)
- Redress (IP-3)
- Complaint Management (IP-4)
- Privacy Incident Response (SE-2)
- Privacy Notice (TR-1)
- SORNs and Privacy Act Statements (TR-2)
- Dissemination of Privacy Program Info. (TR-3)

- Authority to collect (AP-1)
- Purpose Specification (AP-2)
- Governance & Privacy Program (AR-1)
- Privacy Impact & Risk Assessment (AR-2)
- Inventory of PII (SE-1)

- Privacy Requirements for Contractors and Service Providers (AP-1)
- Privacy Awareness & Training (AR-5)
- Privacy-Enhanced System Design & Development (AR-7)
- Minimization of PII (DM-1)
- Minimization of PII used in Testing, Training and Research (DM-3)
- Privacy Incident Response (SE-2)
- Internal Use (UL-1)
- Information Sharing with Third Parties (UL-2)

- Data Quality (DI-1)
- Data Integrity and Data Integrity Board (DI-2)
- Individual Access (IP-2)
- Redress (IP-3)
- Information Sharing with Third Parties (UL-2)

- Data Quality (DI-1)
- Data Integrity and Data Integrity Board (DI-2)
- Data Retention & Disposal (DM-2)
- Consent (IP-1)
- Information Sharing with Third Parties (UL-2)

<u>Outcome Based Approach</u>

Like the NIST CSF model, organizations would likely use the Privacy Framework model to establish privacy objectives and a roadmap of initiatives with timelines to ultimately achieve those objectives. To align with Instead of labeling *Functional* components as 'Categories' and 'Subcategories,' please use terms such as privacy "Principles" or functional "Objectives," which will:

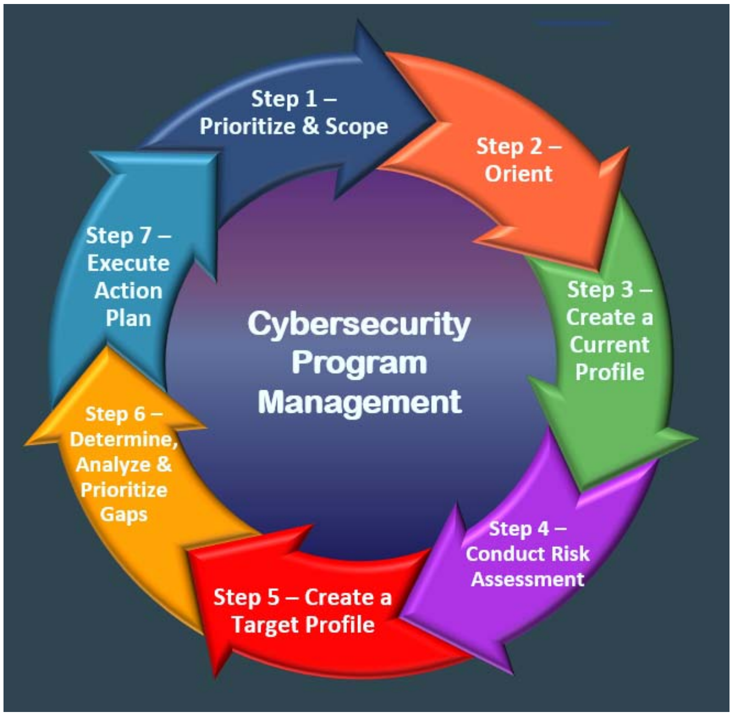
a) Acknowledge ongoing organizational efforts to respect and honor Privacy,
b) Align with the EU philosophy on Privacy that underlies GDPR, and
c) Speaks directly to 'business' decision makers, who are ultimately accountable for implementation and ongoing execution of operational practices that honor privacy.

<u>Implementation Tiers / Maturity Model</u>

We anticipate the introduction of additional state privacy laws, and hopefully, a Federal privacy law that homogenizes myriad efforts to govern privacy into a single set of requirements and objectives. We also anticipate different, state by state approaches to privacy law implementation and enforcement. Although an organization may not yet meet all requirements mandated by a certain state's privacy law, the organization's ability to demonstrate a pathway to compliance and privacy practice maturity save the organization from potential sanctions and fines.

<u>Focus on Program Management</u>

While many of us tend to overlook the PM family of controls in SP 800-53, there may be value in providing more instruction on the management of a Privacy Program. A clearly communicated, objective-driven Privacy program should facilitate organizational privacy practice maturity. We believe the framework may be able to offer program design guidance based NIST's Risk Management process:


Step 1 – Prioritize & Scope
Step 2 – Orient
Step 3 – Create a Current Profile
Step 4 – Conduct Risk Assessment
Step 5 – Create a Target Profile
Step 6 – Determine, Analyze & Prioritize Gaps
Step 7 – Execute Action Plan
Cybersecurity Program Management

Conclusion

In closing, we would like to thank the NIST committee leading the Privacy Framework development effort. We recognize the immense benefits that the CSF has brought to the business of information security. We have the same hope for the Privacy Framework, which the country greatly needs to bring our Privacy practices up to global standards.

Thank you again for allowing us to contribute.
Regards,

Andrew L Soodek
President
Secure Compliance Solutions LLC
asoodek@securecompliance.co

[i] https://ico.org.uk/media/about-the-ico/consultations/2258461/dpia-template-v04-post-comms-review-20180308.pdf