The NIST Privacy Framework: What It Is And What It Means For You

Session CYB5, February 11, 2019

Kevin Stine, Chief, Applied Cybersecurity Division, NIST

Ellen Nadeau, Deputy Manager, Privacy Framework, NIST

www.himssconference.org #HIMSS19

Conflict of Interest

Kevin Stine, Chief, Applied Cybersecurity Division, NIST

AND

Ellen Nadeau, Deputy Manager, Privacy Framework,
Privacy Risk Strategist, Privacy Engineering Program, NIST

Have no real or apparent conflicts of interest to report.

Agenda

- Background
- Process
- Organizational Considerations
- Structure and Practices

Learning Objectives

- Identify what to expect from the Privacy Framework and how it could benefit your organization

- Discuss the current state of the Privacy Framework and its timeline for publication

- Outline NIST's process for developing a privacy framework and how you can contribute

Why NIST?

- Long track record of successfully, collaboratively working with public and private sectors

- Experience developing the Cybersecurity Framework
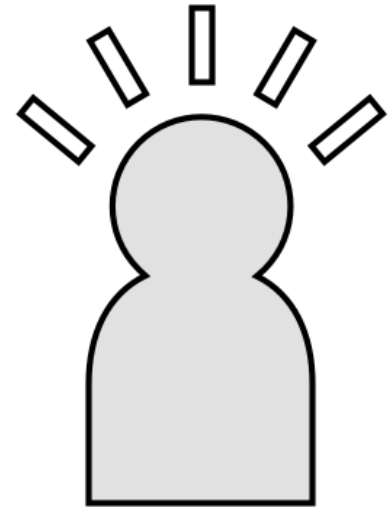
- Extensive privacy expertise

Why a privacy framework?

- Designing, operating, or using technologies in ways that are mindful of diverse privacy needs in an increasingly connected and complex environment

- Multiplying visions for how to address privacy challenges inside and outside the U.S.
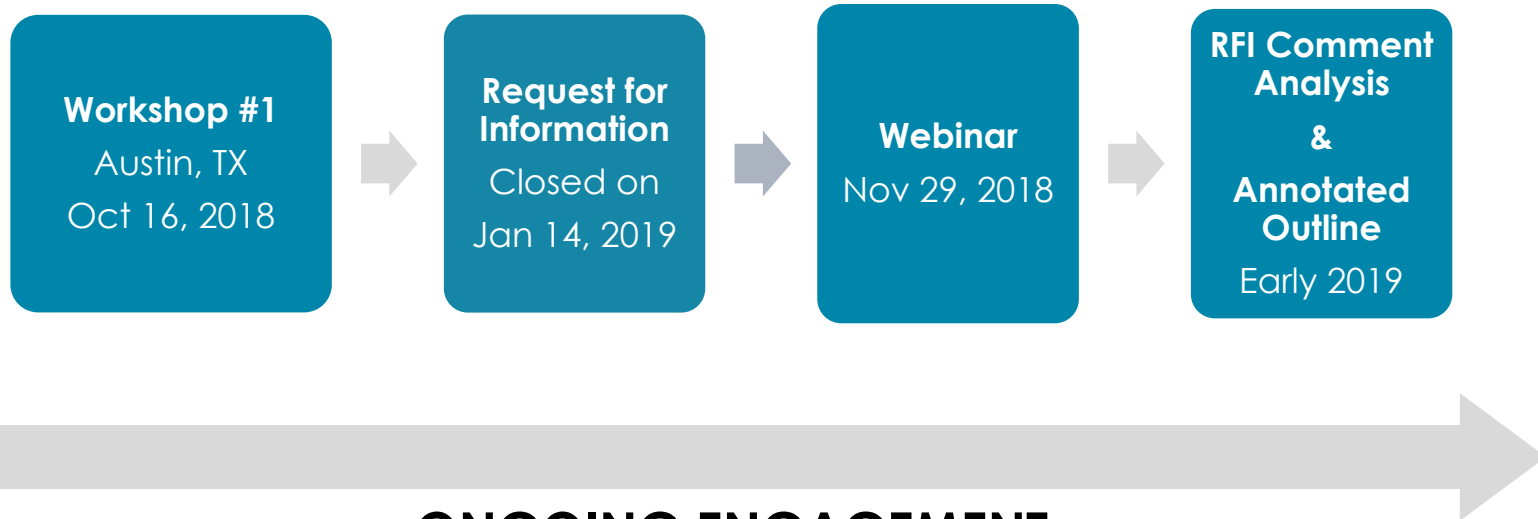
- Good cybersecurity doesn't solve it all

What will the framework look like?

Collaborative Effort

The Process

| **Workshop #1** Austin, TX Oct 16, 2018 | → | **Request for Information** Closed on Jan 14, 2019 | → | **Webinar** Nov 29, 2018 | → | **RFI Comment Analysis & Annotated Outline** Early 2019 |

ONGOING ENGAGEMENT
Feedback encouraged and promoted
throughout the process

Organizational Considerations

What need will the framework address?

NIST is proposing as a working assumption:

Organizations are challenged with bridging between policies or principles and implementation of effective privacy practices. NIST believes that organizations would be better able to address the full scope of privacy risk with more tools to support better implementation of privacy protections.
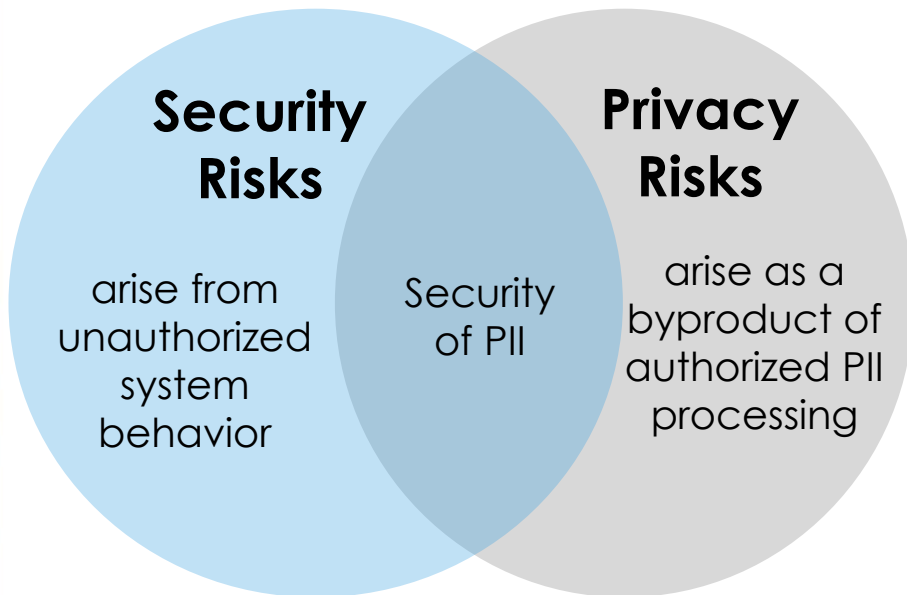
Agree? Disagree?

Risk-Based Approach

Managing **privacy risk**, not just compliance risk

It's a **framework**, not a prescription

Security and Privacy Risk Relationship

Security Risks

arise from unauthorized system behavior

Security of PII

Privacy Risks

arise as a byproduct of authorized PII processing

There is a clear recognition that security of PII plays an important role in the protection of privacy

Individual privacy cannot be achieved solely by securing PII

Authorized processing: system operations that handle PII (collection - disposal) to enable the system to achieve mission/business objectives
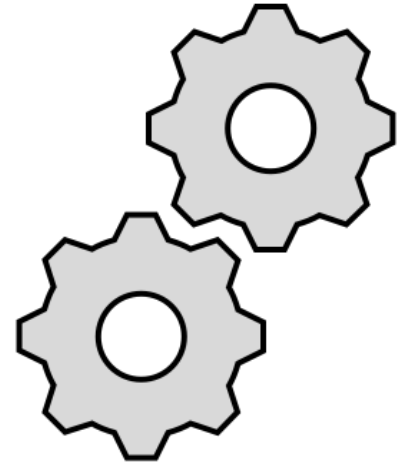
12

NIST Working Model:
System Privacy Risk

Privacy Risk Factors:
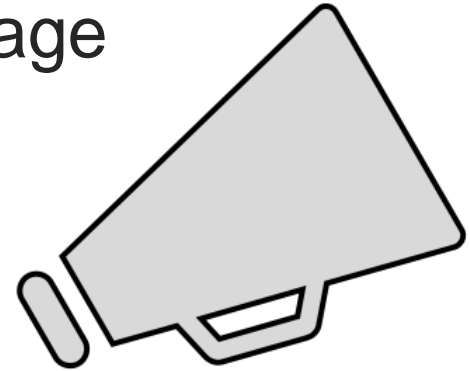Likelihood | Problematic Data Action | Impact

Compatibility

- Support organizations' obligations under different regimes

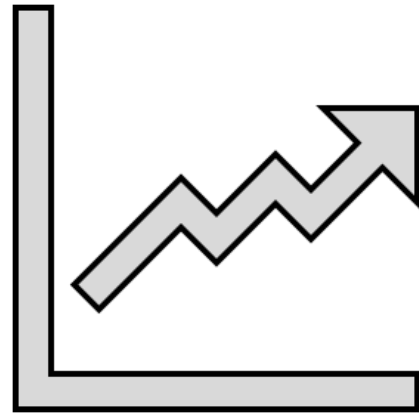- Align with other frameworks or standards

Communication

- Provide common language

- Serve broad audience

Scalable

- Various sectors
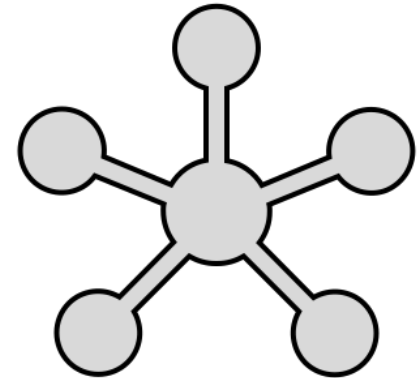
- Small and medium-sized business

Living Document

Able to be updated as technology and approaches to privacy protection change

Structure and Practices

Usable

Improving integration of privacy risk management process with product and service development processes

Specific Privacy Practices

- Practices that are widely used

- Relevant standards or guidance

- Implementation challenges

Resources & Questions

Website

https://nist.gov/privacyframework

Mailing List

https://groups.google.com/a/list.nist.gov/forum/#!forum/privacyframework

Contact Us

PrivacyFramework@nist.gov

@NISTcyber

#PrivacyFramework