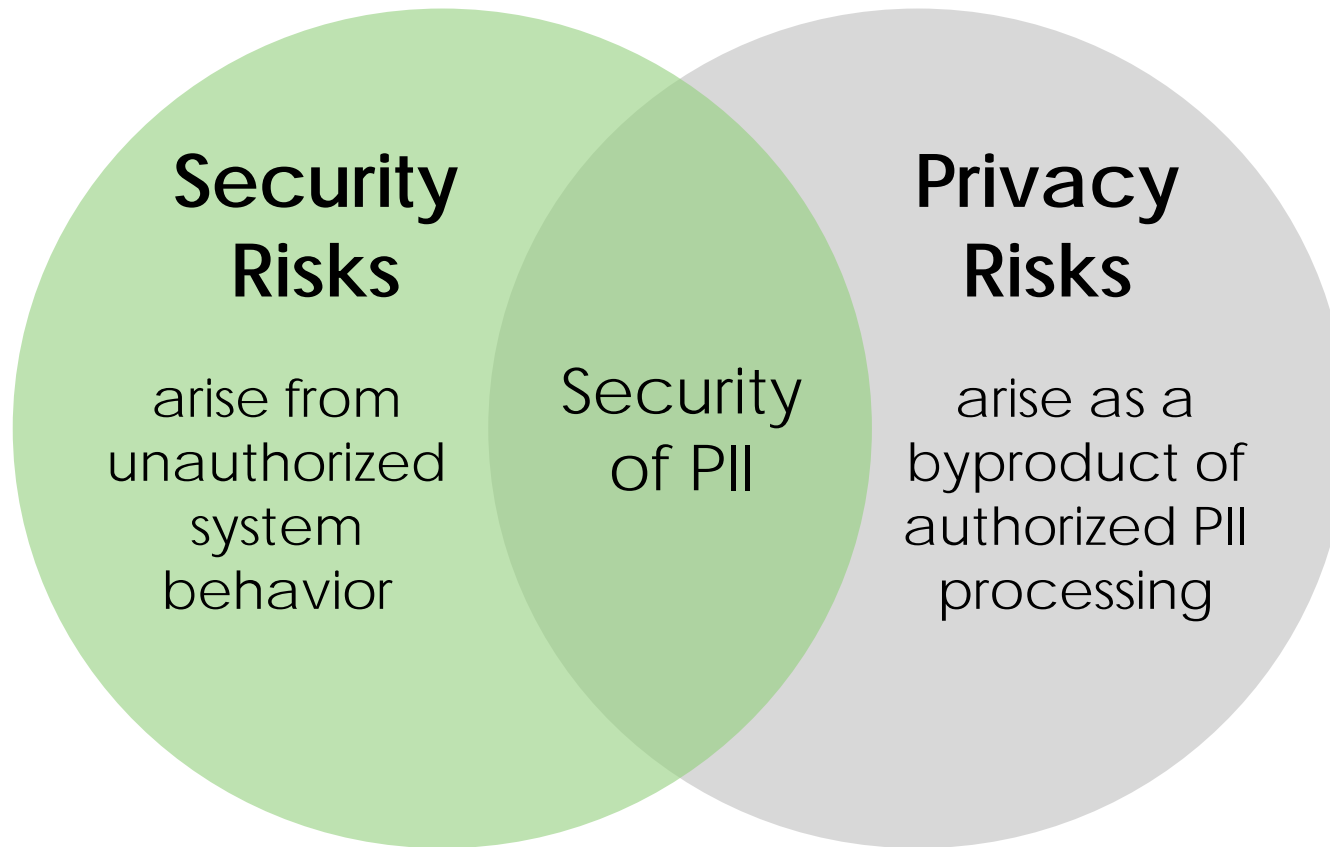# Why NIST?

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

- Experience developing the Cybersecurity Framework

- Extensive privacy expertise

National Institute of Standards and Technology
U.S. Department of Commerce

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 these challenges inside and outside the U.S.

- Good cybersecurity doesn't solve it all

National Institute of Standards and Technology
U.S. Department of Commerce

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

National Institute of Standards and Technology
U.S. Department of Commerce

NIST Working Model: System Privacy Risk

Privacy Risk Factors:
Likelihood | Problematic Data Action | Impact

National Institute of
Standards and Technology
U.S. Department of Commerce

Potential Models: Key Attributes of the Cybersecurity Framework

It's a framework, not a prescription

It provides a common language and systematic methodology for managing cyber risk

The framework is a living document

It is intended to be updated over time as stakeholders learn from implementation, and as technology and risks change

NIST National Institute of Standards and Technology
U.S. Department of Commerce

What need will the framework address?
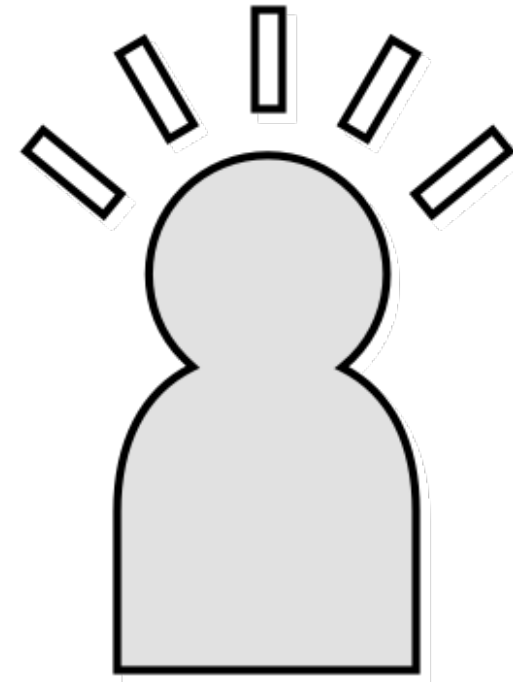
NIST is proposing as a working assumption:

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?

National Institute of
Standards and Technology
U.S. Department of Commerce

What will the framework look like?

Collaborative Effort

- Attributes
- Structure
- Practices

National Institute of
Standards and Technology
U.S. Department of Commerce

The Process

Over the coming year, NIST will:

- Issue framework drafts for feedback
- Hold a series of workshops
    Kickoff workshop: Oct.16, 2018
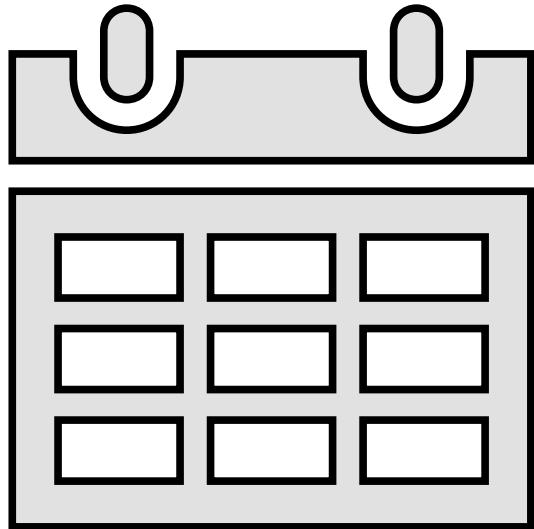- Host briefings, conference side events, etc.

Ongoing Engagement

Open public comment and review encouraged and promoted throughout the process

NIST
National Institute of Standards and Technology
U.S. Department of Commerce

Workshop #1: Overview

- Interoperability
- Common language/communication tool
- Risk-based approach

Upcoming Opportunities to Engage

Request for Information
Open until 12/31 @ 5pm ET

Live Webinar: Q&A on the NIST Privacy Framework
November 29, 2018

Framework Outline: Workshop #2
Anticipated early 2019

NIST
National Institute of Standards and Technology
U.S. Department of Commerce

Resources

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

National Institute of Standards and Technology
U.S. Department of Commerce