

# Q&A on the NIST Privacy Framework

November 29, 2018

# Today's Webinar

- Background
- Process
- Request for Information (RFI)
  - Organizational Considerations
  - Structure
  - Practices
- Q&A

# Why NIST?

- Long track record of successfully, collaboratively working with public and private sectors
- Experience developing the Cybersecurity Framework
- Extensive privacy expertise

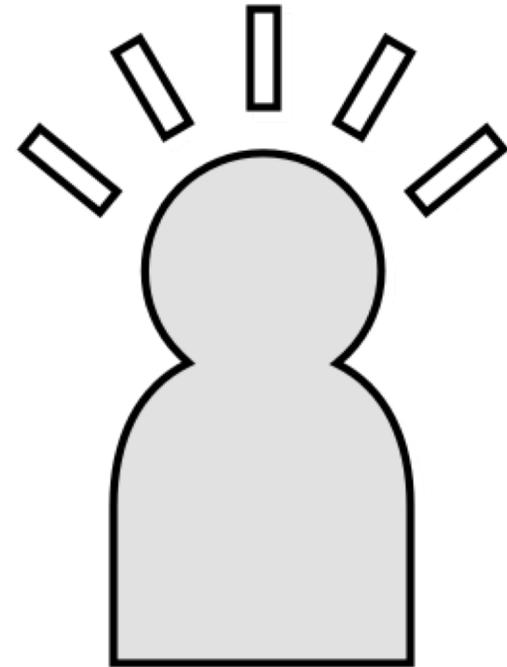


# Why a privacy framework?

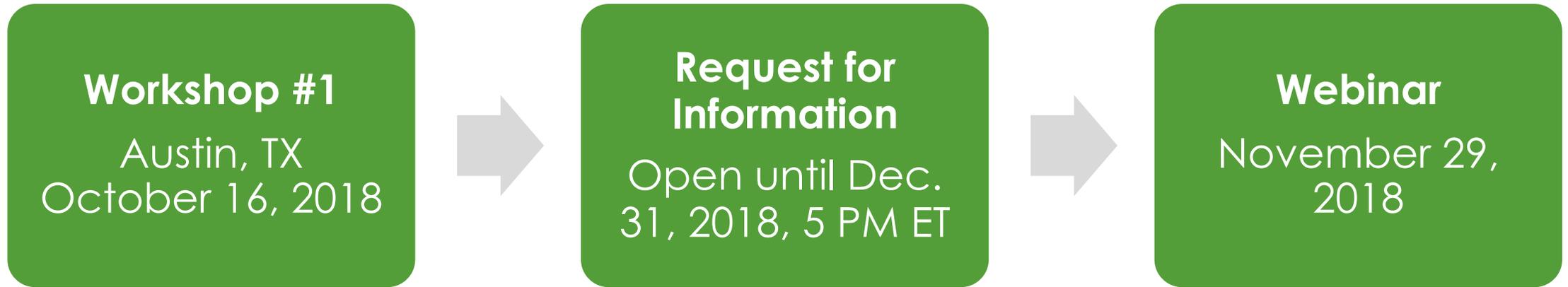
- Designing, operating, or using technologies in ways that are mindful of diverse privacy needs in an increasingly connected and complex environment
- Multiplying visions for how to address privacy challenges inside and outside the U.S.
- Good cybersecurity doesn't solve it all

What will the framework look like?

# Collaborative Effort



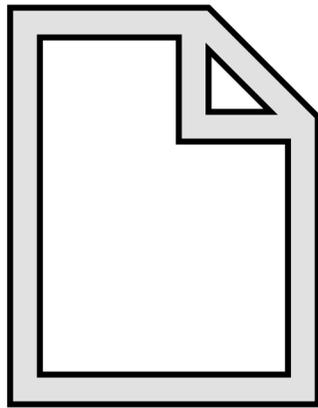
# The Process to Date



## ONGOING ENGAGEMENT

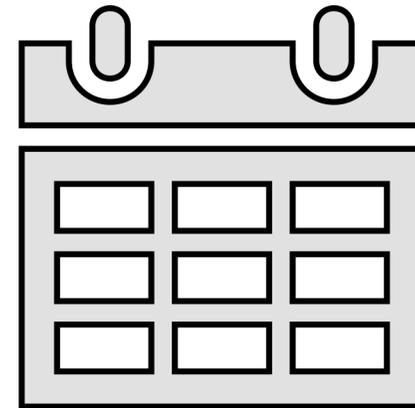
Open public comment and review encouraged and promoted throughout the process

# Upcoming Opportunities to Engage



## Framework Outline Release

Anticipated early 2019



## Outlining the Privacy Framework: Workshop #2

Anticipated early 2019

# 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.

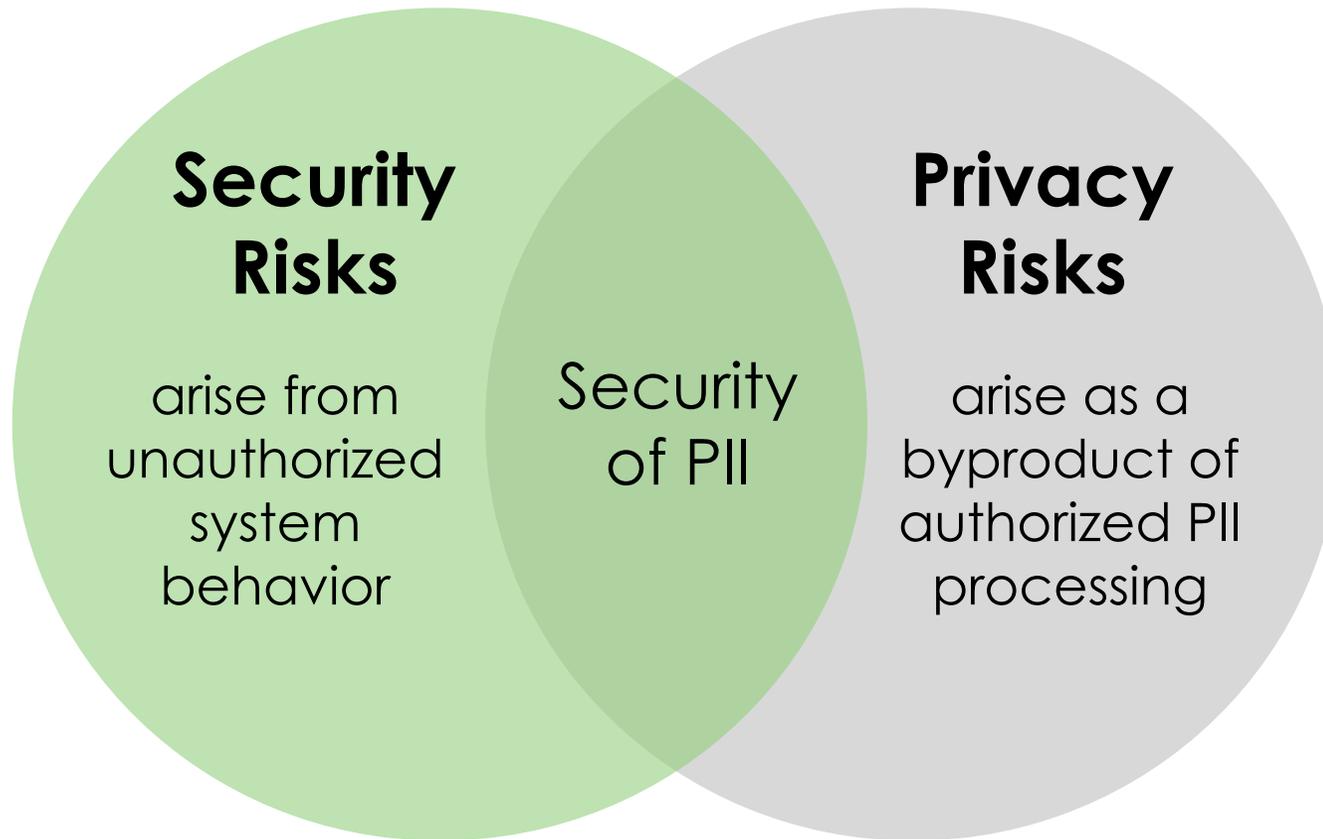
**Agree? Disagree?**

# Risk-Based Approach

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

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

# Security and Privacy Risk Relationship



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

# NIST Working Model: System Privacy Risk

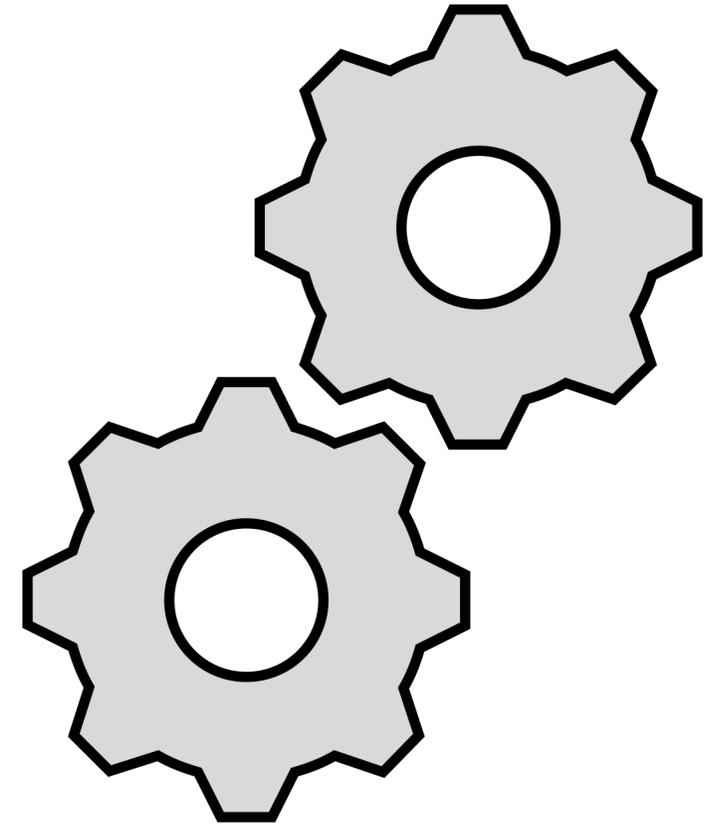
## **Privacy Risk Factors:**

Likelihood | Problematic Data Action | Impact

# Compatibility

Support organizations' obligations under different regimes

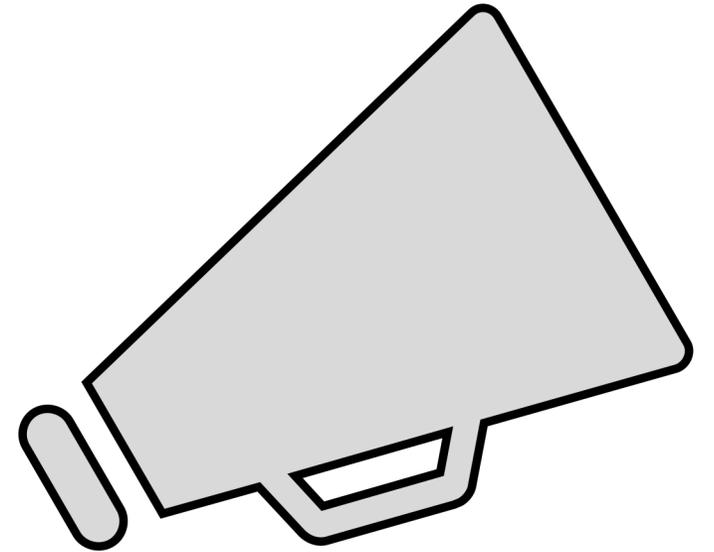
Align with other frameworks or standards



# Communication

Provide common language

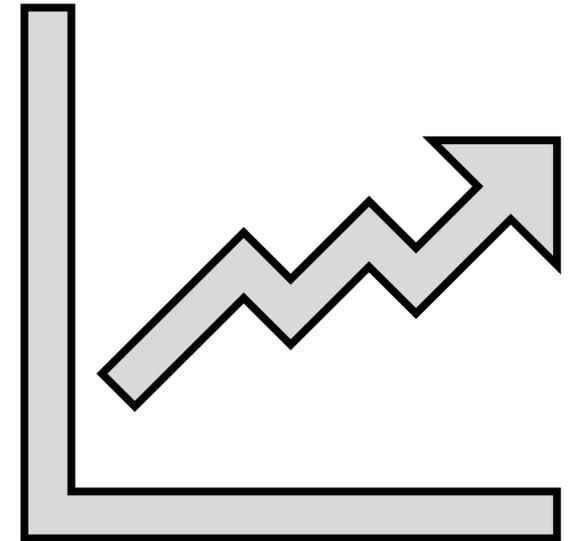
Serve broad audience



# Scalable

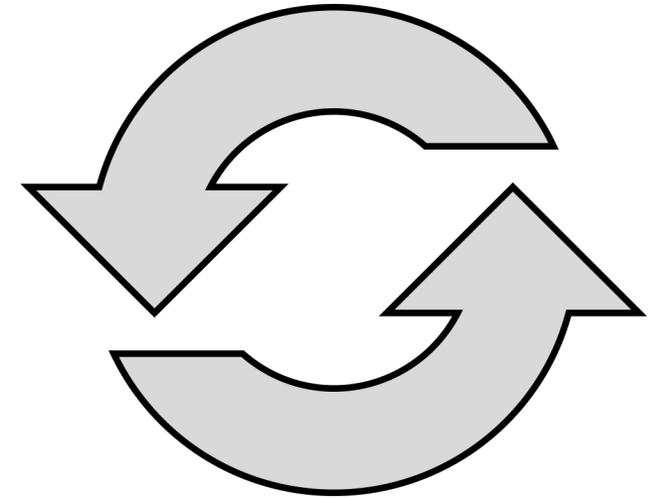
Various sectors

Small and medium-sized  
business



# Living Document

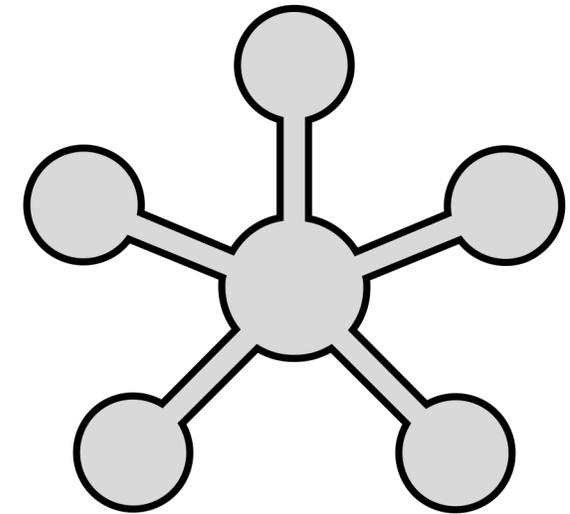
Able to be updated as technology and approaches to privacy protection change



# 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

## Website

<https://nist.gov/privacyframework>

## Mailing List

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

## Contact Us

[PrivacyFramework@nist.gov](mailto:PrivacyFramework@nist.gov)

@NISTcyber

#PrivacyFramework

Q&A