

Outlining the NIST Privacy Framework

3.14.2019

Session Overview

- Background and status of the NIST Privacy Framework
- Review of the NIST Privacy Framework outline and Request for Information (RFI) analysis
- Resources for engagement

NIST Privacy Framework: Background and Status

Why NIST?

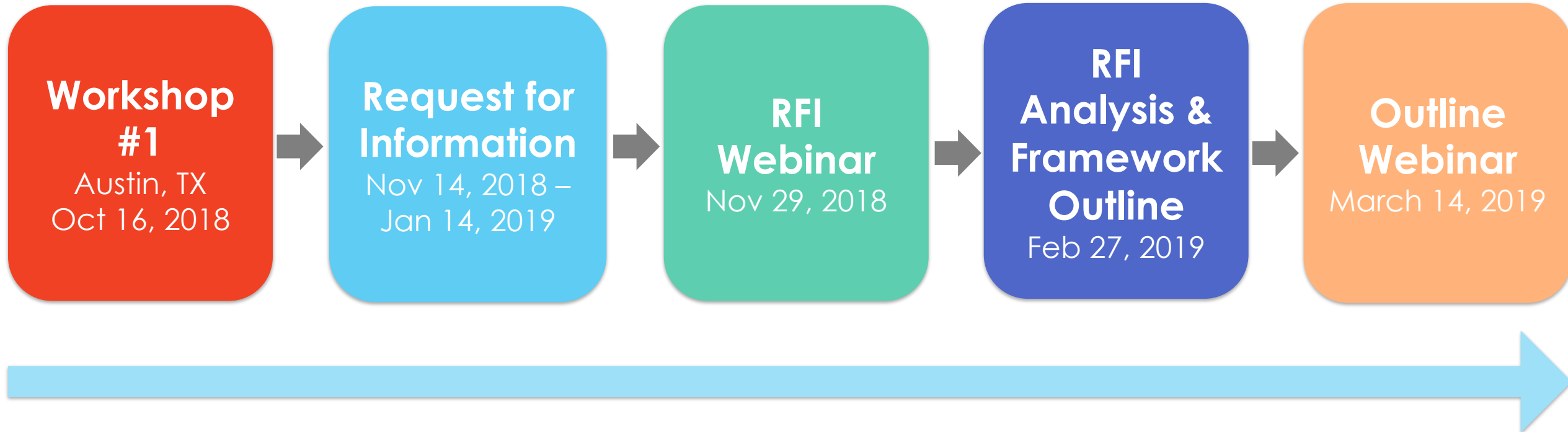
- Long track record of successfully, collaboratively working with public and private sectors
- Experience developing the Cybersecurity Framework
- Extensive privacy expertise



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

Process to Date



ONGOING ENGAGEMENT

Feedback encouraged and promoted throughout the process

Compatible and Interoperable



Benefits of Framework Attributes



Upcoming Opportunities to Engage



Drafting the NIST Privacy Framework: Workshop #2

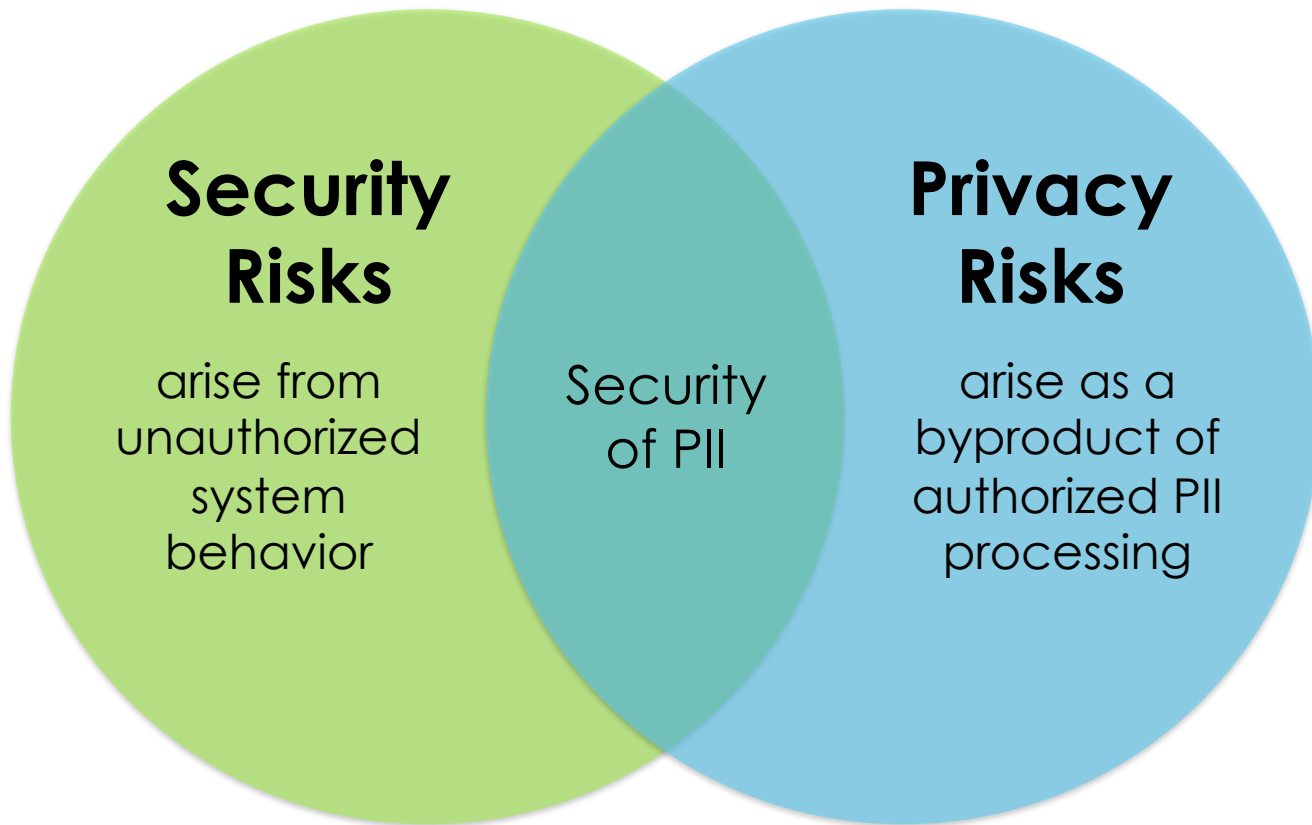
Monday, May 13 - Tuesday, May 14, 2019

Hosted by Georgia Tech Scheller College of Business
Atlanta, Georgia

NIST Privacy Framework: Review of Outline and RFI Analysis

Privacy Risk Management

Information Security and Privacy 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

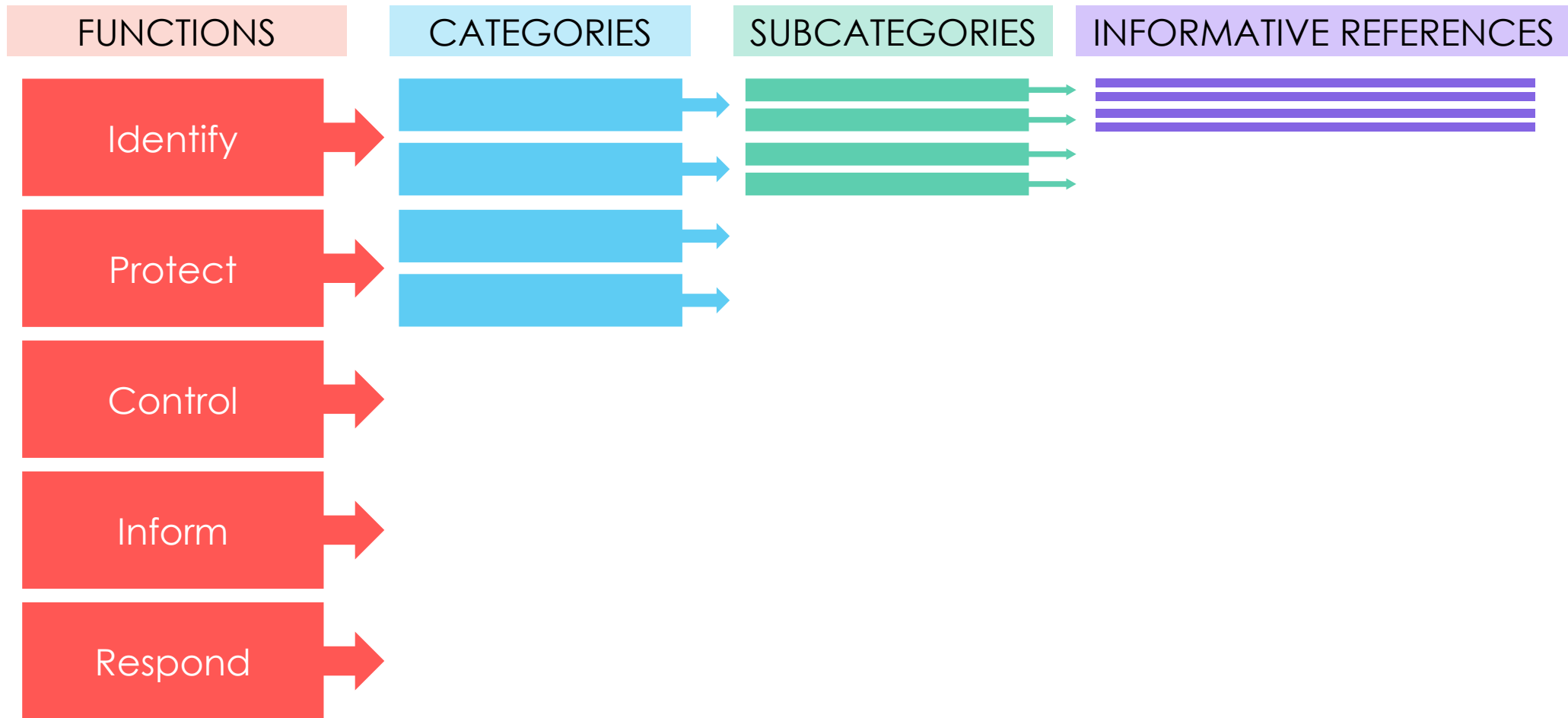
Privacy Risk Management

NIST Working Model: System Privacy Risk

Privacy Risk Factors:

Likelihood | Problematic Data Action | Impact

Alignment with the Cybersecurity Framework: Core



Alignment with the Cybersecurity Framework: Profiles



Alignment with the Cybersecurity Framework: Tiers

Tiers 1-4:

1. PARTIAL

2. RISK-INFORMED

3. REPEATABLE

4. ADAPTIVE

Elements per tier:

Risk Management Process

Informal, ad hoc privacy risk management processes → processes that enable continuous adaptation to changing technologies and data processing activities and incorporate the use of advanced privacy-enhancing technologies

Integrated Risk Management Program

A limited awareness of privacy risk at the organizational level → all levels of the organization being able to make decisions with a clear understanding of the relationship between privacy risk organizational objectives

Ecosystem Relationships

Entity does not understand its role in the larger ecosystem with respect to other entities → the entity understands its role in the larger ecosystem and contributes to the community's broader understanding and management of privacy risks

Workforce

A workforce that has little or no understanding of privacy risks → a workforce that includes specialized privacy skillsets throughout the organizational structure

Roadmap

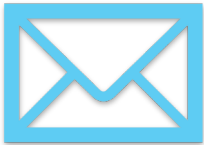


Resources



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](#)