Getting to V1.0 of the NIST Privacy Framework: Workshop #3
July 8, 2019
Process to Date

<table>
<thead>
<tr>
<th>Workshop #1</th>
<th>Request for Information (RFI)</th>
<th>RFI Analysis &amp; Framework Outline</th>
<th>Framework Discussion Draft</th>
<th>Workshop #2</th>
<th>Supplemental Materials</th>
<th>Workshop #3</th>
</tr>
</thead>
</table>

ONGOING ENGAGEMENT

Feedback encouraged and promoted throughout the process
Materials for Working Sessions

Sessions 1-3 and 6
- Draft Executive Summary
- Updated Cores

Sessions 4-5
- Roadmap Topics
- Hypothetical Profiles

- Integrated version
- Separated version
WORKSHOP OBJECTIVE #1
Material: Draft Executive Summary

Purpose, value, & scope
Value

The Privacy Framework provides a shared lexicon and is a practical tool that can assist organizations—even those fully compliant with relevant laws or regulations—in making ethical decisions when designing or deploying their products and services and avoiding losses of trust that damage their reputations and can slow adoption or cause abandonment of these products and services.
Relationship Between Cybersecurity and Privacy Risk

Cybersecurity Risks
arise from unauthorized activity

Privacy Risks
arise as a byproduct of authorized data processing

data security (including unauthorized use & disclosure)

Data: A representation of information, including digital and non-digital formats, with the potential for adverse consequences for individuals when processed

Data Action: A system/product/service operation that processes data

Data Processing: An operation or set of operations performed upon data across the full data life cycle, including but not limited to collection, retention, logging, generation, transformation, use, disclosure, transfer, and disposal

Privacy Risk: The likelihood that individuals will experience problems resulting from data processing, and the impact should they occur
Privacy Risk and Organizational Risk

Problem
- arises from data processing

Individual
- experiences direct impact
  - (e.g., embarrassment, economic loss)

Organization
- experiences secondary impact
  - (e.g., customer abandonment, noncompliance costs, harm to reputation)
WORKSHOP OBJECTIVE #2
Material: Updated Cores
Risk-based & flexible
Privacy & Cybersecurity Framework Alignment

Core: a set of protection activities & desired outcomes that enables communication across the organization.

Profiles: representation of the current and target outcomes the organization is focused on.

Tiers: how an organization views risk and whether it has adequate processes & resources in place to manage that risk.
Two Proposed Cores

Integrated Core

- **IDENTIFY**
- **GOVERN**
- **PROTECT**
- **CONTROL**
- **COMMUNICATE**
- **DETECT**
- **RESPOND**
- **RECOVER**

Separated Core

- **IDENTIFY**
- **GOVERN**
- **PROTECT**
- **CONTROL**
- **COMMUNICATE**
- **DETECT**
- **RESPOND**
- **RECOVER**
Flexible Implementation

Not a checklist: organizations may not need to achieve every outcome or activity reflected in the Core

Partial achievement: organizations are not obligated to achieve an outcome in its entirety

Bundling: organizations may need to consider multiple outcomes in combination to appropriately manage privacy risk

Order: table format of Core is not intended to suggest an implementation order or degree of importance
WORKSHOP OBJECTIVE #3
Material: Hypothetical Profiles

Accessibility & efficacy for bridging communication gaps
Finding Yourself in the Core
Collaboration & Profile Development

- organizational or industry sector goals
- legal/regulatory requirements & industry best practices
- organization’s risk management priorities
  - the privacy needs of individuals

Current Profile

- Identify
- Govern
- Protect
- Control
- Communicate

Target Profile

- Identify
- Govern
- Protect
- Control
- Communicate
- Respond

Cross-functional collaboration
Hypothetical Partial Profile

- **Govern**: Governance Processes and Procedures
  - GV.PP-P5: Legal, regulatory, and contractual requirements...

- **Identify**: Inventory and Mapping
  - ID.IM-P8: Data processing is mapped...

- **Risk Assessment**: PR.PP-P1: Data are processed in an unobservable or unlinkable manner.

- **CT.DM-P1**: Data elements can be accessed for review.

- **CT.DM-P4**: Data elements can be accessed for deletion.

- **CT.DM-P6**: Metadata containing processing permissions...

- **ID.DE-P3**: Contracts with data processing ecosystem parties are used...

**Key:**
- Current Profile
- Target Profile
WORKSHOP OBJECTIVE #4
Material: Roadmap Topics

Gap areas & needs
Laying the Groundwork for the Future

Seeking to improve and overcome challenges around:

- Mechanisms to provide confidence
- Emerging technologies
- Privacy risk assessment
- Privacy workforce
- Re-identification risk
- Technical standards
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