# NIST's Privacy Engineering Program

Privacy Engineering activities at NIST aim to further the field of privacy engineering. Currently, they're focused on providing guidance for federal agencies to manage privacy risks in their information systems, bringing privacy discussions into parity with the conversations agencies are already having around risks in other disciplines (e.g., security).

## Vision Statement:

*Privacy engineering is integral to establishing trustworthiness in information systems that support the growth of the digital economy and improve quality of life.*

## Mission Statement:

*To promote trustworthiness in information systems, the NIST Privacy Engineering program applies systems engineering principles in creating privacy frameworks, risk models, guidance on best practices, and other tools, and supporting the development of relevant standards.*

# Current Drivers

OMB update in July 2016 to Circular A-130 clarified that federal agencies' obligations with respect to managing privacy risk and information resources extends beyond compliance with privacy laws, regulations, and policies, and that agencies must **apply the NIST Risk Management Framework (NIST RMF)** to their privacy programs and Information Systems.

NIST Special Publication (SP) 800-53 Security and Privacy Controls for Federal Information Systems and Organizations is **scheduled to be updated in 2017**.

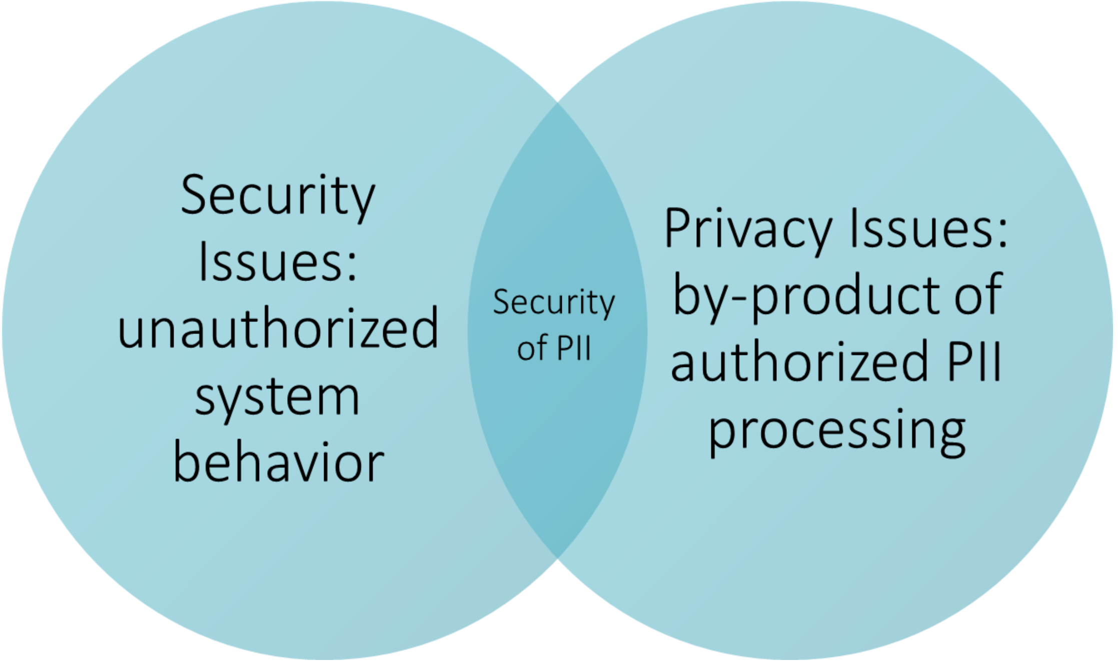
There is an opportunity to improve the way that privacy controls are expressed and organized in NIST SP 800-53 in a way that better enables agencies to **optimize security and privacy benefits**.

# Framing Questions

a. Is the current organization of Appendix J around the Fair Information Practice Principles (FIPPs) sufficient for addressing agencies’ increased privacy risk management responsibilities?

b. If changes are needed, what amendments would help agencies move beyond simply assessing compliance with privacy laws and regulations?

# Information Security and Privacy Relationship



Security Issues: unauthorized system behavior

Security of PII

Privacy Issues: by-product of authorized PII processing

- There is a clear recognition that confidentiality of personal data plays an important role in the protection of privacy

- However, both privacy and security have issues that are unrelated to each other
  - Concerns about smart meters collecting energy usage from homes largely unrelated to how secure the data is, but rather the fact that the system is collecting this data in the first place, and what behaviors that data might reveal (example of authorized processing of PII producing a privacy issue)

- Appendix J controls address the right side of the diagram

# NIST SP 800-53 Current Organization

- Appendix F
  - Organization and system level security controls
- Appendix G
  - Program management controls
- Appendix J
  - Privacy Controls

Appendix J is organized around the FIPPs and contains less technical measures than Appendix F. This leads to the perception that privacy is the domain of policy and legal only.

# SP 800-53 organizational considerations

There may be existing security controls – or even families – that could also apply directly to privacy practices

- e.g. Audit and Accountability in Appendix F and Accountability, Audit, and Risk Management in Appendix J could be merged

Augment existing control families

- e.g. Awareness and Training could be augmented by adding privacy training

Control enhancements - provide additional language to clarify privacy controls

- e.g. Add pseudonymous authentication to the control enhancements in the Identification and Authentication security control

Supplemental Guidance

- Add text to clarify privacy benefits or risks associated with existing security controls

# BREAKOUT #1: CONTROL FAMILIES AND THEIR APPLICABILITY TO PRIVACY

# Questions in Discussion Draft

| Topic | Questions |
|---|---|
| Benefits and Challenges | What are some of the current benefits of Appendix J? In particular, what are some benefits of how privacy controls are currently integrated into SP 800-53? |
|  | What are some of the current challenges with Appendix J? In particular, what are some challenges with how privacy controls are currently integrated into SP 800-53? |
| Overlapping Controls | How should overlapping controls be managed in the next revision of SP 800-53? |
|  | Are there benefits to maintaining similar controls in distinct security and privacy families? |

# Questions in Discussion Draft

| Topic | Questions |
|---|---|
| Control Enhancements | Should control enhancements in the security control families be used to address risk mitigation for privacy? |
| Supplemental Guidance | Should supplemental guidance for the security controls be used to provide more detail about the potential privacy risks associated with the deployment of a given control? |
| | Should supplemental guidance for the security controls be used to provide more detail about the potential privacy benefits associated with the deployment of a given control? |

# Breakout 2: Privacy & Security Controls

# QUESTIONS IN DISCUSSION DRAFT

| Topic | Questions |
|---|---|
| Classification | Are there stand-alone privacy controls that should be classified as program management controls? Should they be integrated into Appendix G so that all program management controls are located in one place in 800-53? |
| | If security controls also contribute to protecting privacy, should the remaining stand-alone privacy controls in Appendix J be classified as “data governance” controls (or another label)? |

# QUESTIONS IN DISCUSSION DRAFT

| Topic | Questions |
|---|---|
| Additional Questions | On balance, should privacy controls and security controls continue to be integrated into one document? |
| | Should there be an independent process of Categorization for privacy aspects of Information Systems? |
| | Are there any other changes that should be considered? |

# Reference - List of Control Families

| Security Control Identifiers and Family Names | | | |
|---|---|---|---|
| ID | FAMILY | ID | FAMILY |
| AC | Access Control | MP | Media Protection |
| AT | Awareness and Training | PE | Physical and Environmental Protection |
| AU | Audit and Accountability | PL | Planning |
| CA | Security Assessment and Authorization | PS | Personnel Security |
| CM | Configuration Management | RA | Risk Assessment |
| CP | Contingency Planning | SA | System and Services Acquisition |
| IA | Identification and Authentication | SC | System and Communications Protection |
| IR | Incident Response | SI | System and Information Integrity |
| MA | Maintenance | PM | Program Management |

| Privacy Control Identifiers and Family Names | |
|---|---|
| ID | PRIVACY CONTROL FAMILIES |
| AP | Authority and Purpose |
| AR | Accountability, Audit, and Risk Management |
| DI | Data Quality and Integrity |
| DM | Data Minimization and Retention |
| IP | Individual Participation and Redress |
| SE | Security |
| TR | Transparency |
| UL | Use Limitation |

# Other considerations

- Does the proposed set of privacy engineering objectives in the draft NISTIR 8062 help to assess privacy risk and select appropriate controls?
  - Predictability, Manageability, and Disassociability
  - c.f. Confidentiality, Integrity, and Availability

- Comments are invited through September 30
  - privacyeng@nist.gov
  - Output from this workshop and the written comments will contribute to the process of the fifth revision of SP 800-53