NSTIC Privacy Workshop

June 27, 2011

Privacy in Practice: A Case Study

Kellie Cosgrove Riley

Agenda

- Background
- TFPAP Privacy Criteria
- Draft Assessor Guidance

Background

- Federal Identity, Credential, and Access Management (FICAM)
- Trust Framework Provider Adoption Process (TFPAP)
- Trust Framework Evaluation Team (TFET)

Background

- Provisionally Approved TFPs
  - Open Identity Exchange (LOA 1)
  - Kantara Initiative (LOA 1, 2, non-crypto 3)
  - InCommon Federation (LOA 1 and 2)

- Certified Identity Providers
  - Google
  - Equifax
  - PayPal
  - VeriSign
  - Wave Systems

www.idmanagement.gov

TFPAP Privacy Criteria

- Non-compulsory
- Adequate Notice
- Opt-In
- Activity Tracking
- Minimalism
- Termination

TFPAP Privacy Criteria

Non Compulsory

- As an alternative to 3rd-party identity providers, agencies should provide alternative access such that the disclosure of End User PII to commercial partners must not be a condition of access to any Federal service.

TFPAP Privacy Criteria

Adequate Notice

- Identity Provider must provide End Users with adequate notice regarding federated authentication.
- Adequate Notice includes a general description of the authentication event, any transaction(s) with the RP, the purpose of the transaction(s), and a description of any disclosure or transmission of PII to any party.
- Adequate Notice should be incorporated into the Opt In process

TFPAP Privacy Criteria

Opt In

- Identity Provider must obtain positive confirmation from the End User before any End User information is transmitted to any government applications.
- The End User must be able to see each attribute that is to be transmitted as part of the Opt In process.
- Identity Provider should allow End Users to opt out of individual attributes for each transaction.

TFPAP Privacy Criteria

Activity Tracking

- Commercial Identity Provider must not disclose information on End User activities with the government to any party, or use the information for any purpose other than federated authentication.
- RP Application use of PII must be consistent with RP PIA as required by the E-Government Act of 2002.

TFPAP Privacy Criteria

Minimalism

- Identity Provider must transmit only those attributes that were explicitly requested by the RP application or required by the Federal profile.
- RP Application attribute requests must be consistent with the data contemplated in their Privacy Impact Assessment (PIA) as required by the E-Government Act of 2002.

TFPAP Privacy Criteria

Termination

- In the event an Identity Provider ceases to provide this service, the Provider shall continue to protect any sensitive data including PII.

Draft Assessor Guidance

- Assessor Guidance for Privacy is in development.
- Translates Privacy Criteria to something more concrete.
- Effort to show how to implement the Privacy Criteria in practice.

QUESTIONS?