Baseline Trust

- What assurances do members of R&E Feds need of each other to be comfortable transacting with each other?
- FICAM/Kantara assurance profiles
  - Requires formal audit, too heavy
- InCommon's Participant Operating Practices
  - Hard to verify, too light
- New approach:
  - Five expectations of IDPs
  - Five expectations of SPs
  - Attestation communicated in a machine readable format
  - Create InCommon business and technical processes to hold IdPs and SPs accountable for attesting to baseline expectations
- Trustworthiness emerges from organizational maturity and commonality of practice. Internet2 TIER project should help orgs with those.

Potential Participant Baseline Expectations

Expectations of IdPs

1. The IdP is operated under the authority of the organization's InCommon executive contact
2. The IdP only presents assertions believed to be accurate
3. The IdP is trustworthy enough to access the organization’s enterprise systems
4. Federation metadata is accurate, complete, and includes site contacts, MDUI information, and privacy policy
5. Security incident response plan covers IdP operations

Expectations of SPs

1. Controls are in place to reasonably secure information and maintain user privacy
2. Information received from IdPs is stored only when absolutely necessary for SP’s purpose
3. Federation metadata is accurate, complete, and includes site contacts, MDUI information, and privacy policy
4. Documented attribute requirements are published
5. Security incident response plan covers SP operations