Update on Internet2/InCommon Trust & Identity Program

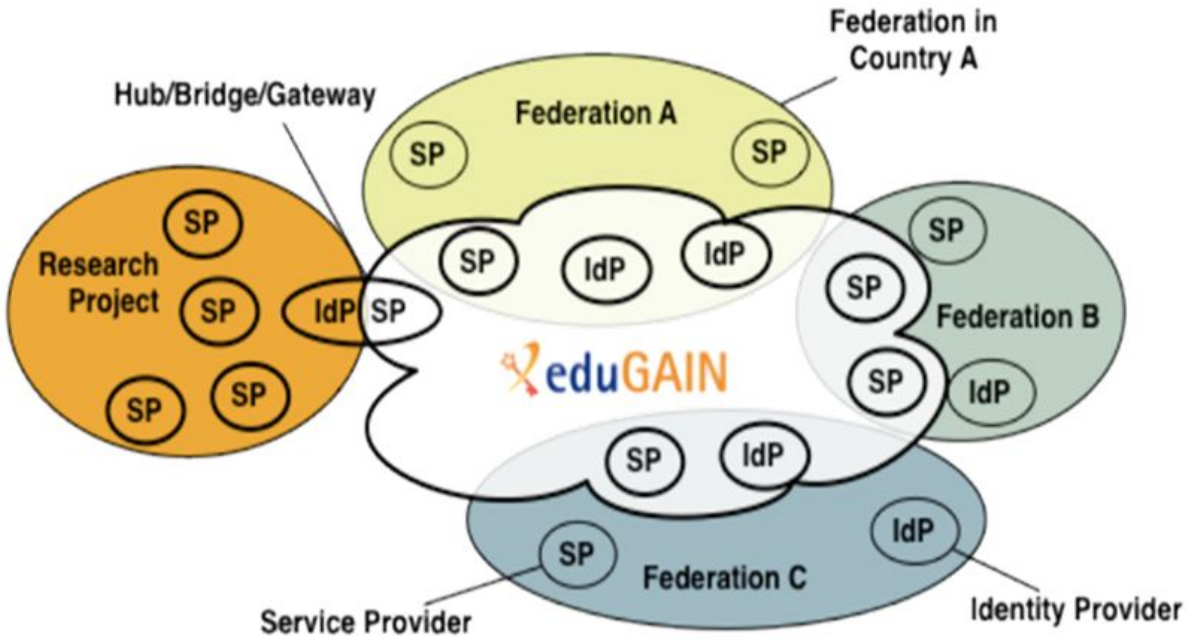
Tom Barton

University of Chicago & Internet2

Trust & Identity program areas

- ➢ InCommon Federation (focus for today)
- InCommon Trusted Access Platform
  - Software tools that make R&E federation work well for
    - Campus Identity & Access Management
    - Research and academic collaborations
- InCommon Certificate Service
- eduroam
- Engagement
  - NB: new InCommon Ecosystem meeting Summer 2019

Global R&E federated access ecosystem



eduGAIN stats:

58 countries

>5,000 entities

O(10^8) users

Federation's value to research collaborations

- Ubiquity – federated access for users at all Higher Eds
- Attribute release – "Research & Scholarship bundle"
- Interop
  - Accurate, complete, fresh federation metadata
  - Works no matter where user and service are located
  - Multi-protocol
- Trustworthiness
  - I'm ok relying on your credentials if you do too!
  - Security
  - Participation in federation governance

Increasing the value

- Baseline Expectations
- International standards
  - SIRTFI (Security Incident Response Trust Framework for Federated Identity)
  - REFEDS Assurance Framework, including MFA and SFA profiles
- IdP aaS to address long tail of Higher Eds
- Deep engagements
  - Science Gateways Community Institute Partner
  - Collaboration Success Partners (~10 collaborations to begin)
  - Campus Success Program (11 campuses just completed)

Baseline Expectations

#1 impedance to achieving full value of federation:

IdP and SP operators who don't pay attention, and Federation operators who aren't effective at managing that

- Falls off radar when key staff or management changes
- Decreasing IT skills in-house at Higher Eds
- "Cloud-first" approach to campus IT is common

Baseline Expectations: Identity Providers

1. The IdP is operated with **organizational-level authority**
2. The IdP is **trusted enough to be used to access the organization's own systems**
3. **Generally-accepted security practices** are applied to the IdP
4. Federation **metadata is accurate, complete**, and includes site technical, admin, and security contacts, MDUI information, and privacy policy URL

Baseline Expectations: Service Providers

1. Controls are in place to **reasonably secure information and maintain user privacy**
2. Information received from IdPs is n**ot shared with third parties without permission** and is stored only when necessary for SP's purpose
3. **Generally-accepted security practices** are applied to the SP
4. Federation **metadata is accurate, complete**, and includes site technical, admin, and security contacts, MDUI information, and privacy policy URL
5. Unless governed by an applicable contract, **attributes required to obtain service are appropriate and made known publicly**

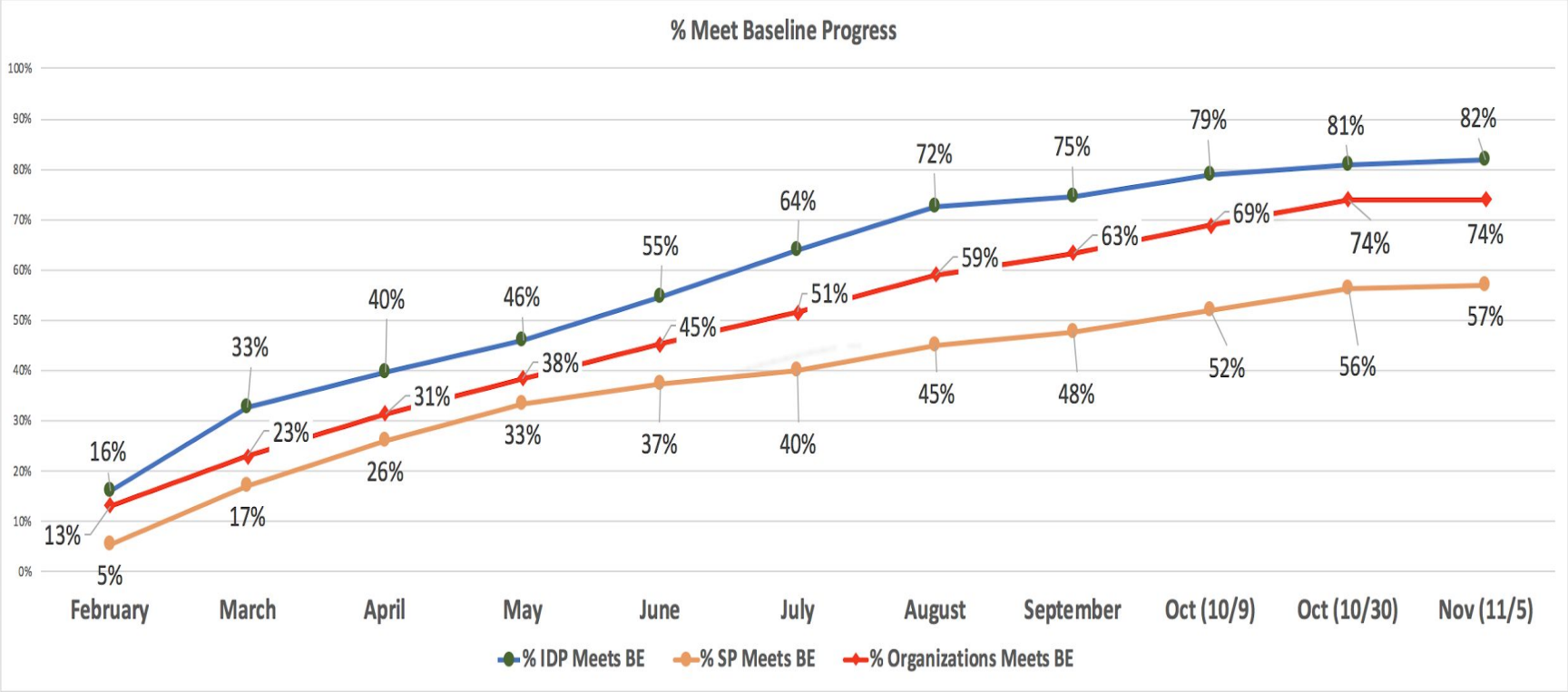
Baseline Expectations: Federation Operators

1. Focus on **trustworthiness** of their Federation as a primary objective and be **transparent** about such efforts
2. **Generally-accepted security practices** are applied to the Federation's operational systems
3. Good practices are followed to ensure **accuracy and authenticity of metadata** to enable secure and trustworthy federated transactions
4. **Frameworks that improve trustworthy use of Federation**, such as entity categories, are implemented and adoption by Members is promoted
5. **Work with relevant Federation Operators** to promote realization of baseline expectations

How the Baseline Expectations program helps

Purpose	Process
Give specific, actionable info to the right people at the right time	Metadata Health Check
Formal, transparent resolution of concerns about federation entities. Mitigate or remove.	Community Dispute Resolution
Enhance Baseline Expectations	Community Consensus
Make member obligations clear	Amend Participation Agreement
Tell people stuff!	All manner of outreach

InCommon metadata & Baseline Expectations



Attribute release

- Research & Scholarship Entity Category
  - International standard
  - Federation operators “tag” SPs serving R&S mission
  - Participating IdPs automatically release attributes to R&S SPs
    - Name, email, affiliation, persistent unique identifier
- Great idea and GDPR goodness, but insufficient uptake
- Community working group recommended adding R&S for IdPs to Baseline Expectations

Maturing federation

- Baseline Expectations needs to go global
- Not just SAML anymore
- More delegation in the trust chain as the ecosystem evolves
- People and processes are needed to leverage innovations in federation technology
- "Federated Identity Management for Research v2"
- International "Federation 2.0" WG about to start

Thank You!

tbarton@uchicago.edu

"Any opinions, findings, conclusions or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of the Networking and Information Technology Research and Development Program."

The Networking and Information Technology Research and Development (NITRD) Program

Mailing Address: NCO/NITRD, 2415 Eisenhower Avenue, Alexandria, VA 22314

Physical Address: 490 L'Enfant Plaza SW, Suite 8001, Washington, DC 20024, USA Tel: 202-459-9674, Fax: 202-459-9673, Email: nco@nitrd.gov, Website: https://www.nitrd.gov