Baseline Expectations:
Keeping 100s of Organizations On Track

Tom Barton

UChicago & Internet2

Sources of federation's value to a research SP

- 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

- International standards
  - REFEDS Research & Scholarship attribute release
  - 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
- Sustain key FIM elements and evolve others
- Baseline Expectations
  - Ensure metadata quality
  - Ensure adoption of key standards

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 skills in-house at Higher Eds
- "Cloud-first" approach to campus IT is common

InCommon 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

InCommon 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
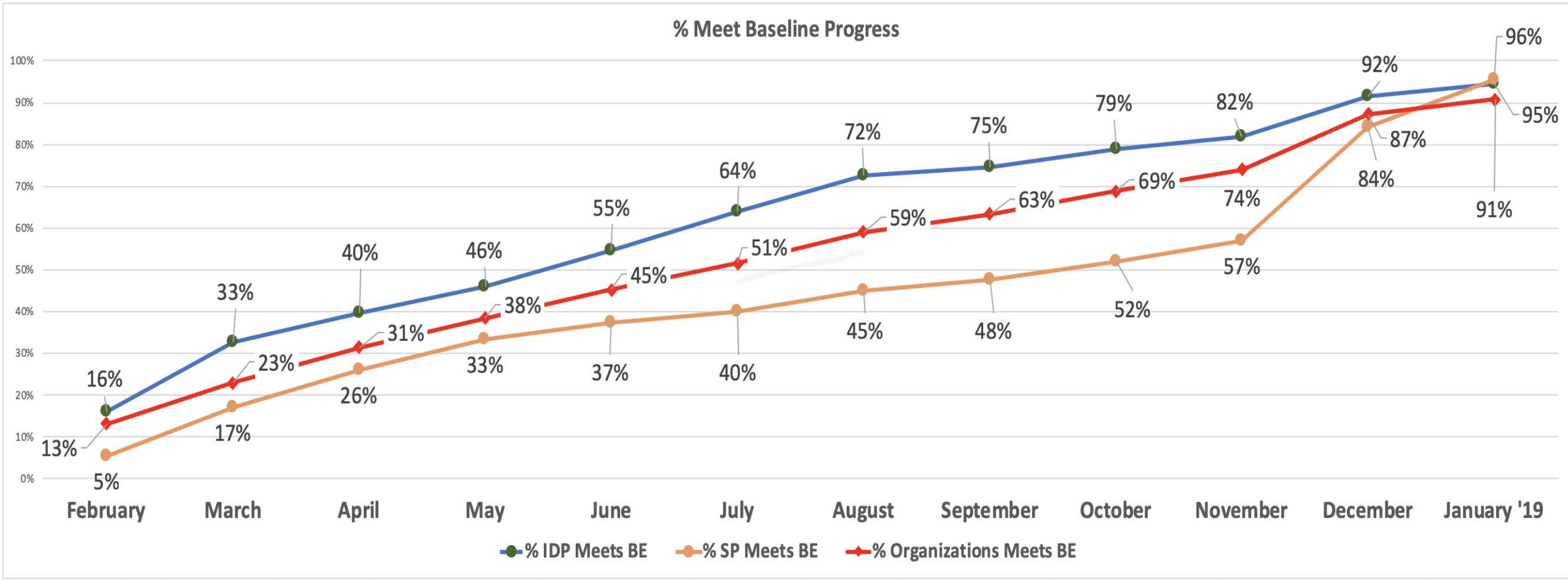
InCommon Baseline Expectations: Service Providers

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**
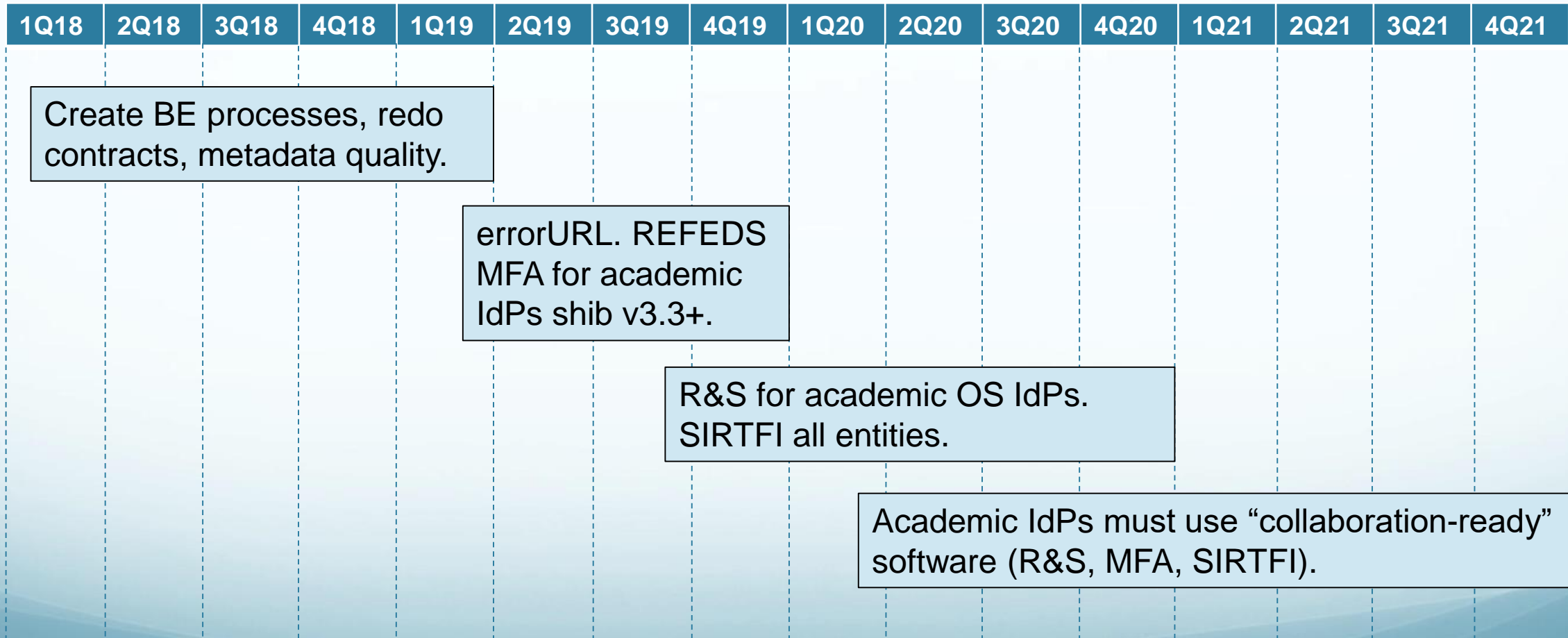
How the Baseline Expectations program works

Purpose	Process
Give specific, actionable info to the right people at the right time	Automated 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
Guided by InCommon's Community Trust and Assurance Board	

InCommon metadata health

% Meet Baseline Progress

Legend: % IDP Meets BE · % SP Meets BE · % Organizations Meets BE

Baseline Roadmap – In Development

1Q18	2Q18	3Q18	4Q18	1Q19	2Q19	3Q19	4Q19	1Q20	2Q20	3Q20	4Q20	1Q21	2Q21	3Q21	4Q21

Create BE processes, redo contracts, metadata quality.

errorURL. REFEDS MFA for academic IdPs shib v3.3+.

R&S for academic OS IdPs. SIRTFI all entities.

Academic IdPs must use "collaboration-ready" software (R&S, MFA, SIRTFI).

Baseline Expectations Beyond InCommon…

Is it improving trustworthiness, perception of value?

Who's up for trying something like this? Is there an analogous issue in some research communities?

Do we need a single, globally-agreed set of Baseline Expectations, or is it good enough for each federation or community to have their own version?