The Federation Doctor Will See You Now: Metadata Health Checks are Here

Brett Bieber, University of Nebraska, Chair, InCommon CTAB

Nick Roy, Director of Technology and Strategy, InCommon

February 21, 2018

Three-Part Series

Baseline Expectations Impact — Wednesday, January 24, 2018

Metadata Health Checks — Wednesday, February 21, 2018

Policy Aspects & Legal Changes — Wednesday, March 7, 2018

Some Quick Polls

Covering a Lot Today

You can always find all this, and more, at:

https://www.incommon.org/federation/baseline

Identity Provider Baseline Expectations

IdP is operated with organizational-level authority

IdP is trusted enough to be used to access the organization's own systems

Generally-accepted security practices are applied to the IdP

Federation metadata is accurate and complete, and includes site technical, admin, and security contacts, MDUI information and privacy policy URL

Service Provider Baseline Expectations

Controls are in place to reasonably secure information and maintain user privacy

Information received from IdPs is not shared with third parties without permission and is stored only when necessary for SP's purpose

Generally-accepted security practices are applied to the SP

Federation metadata is accurate, complete, and includes site technical, admin, and security contacts, MDUI information, and privacy policy URL

Unless governed by an applicable contract, attributes required to obtain service are appropriate and made known publicly

Federation Operator Baseline Expectations

Focus on trustworthiness of their Federation as a primary objective and be transparent about such efforts

Generally-accepted security practices are applied to the Federation's operational systems

Good practices are followed to ensure accuracy and authenticity of metadata to enable secure and trustworthy federated transactions

Frameworks that improve trustworthy use of Federation, such as entity categories, are implemented and adoption by Members is promoted

Work with relevant Federation Operators to promote realization of baseline expectations

What Does That All Mean?

There are things you are on your honor to do as a Federation Participant

There are things InCommon is on its honor to do as a Federation Operator

There are some things we can easily check for in your metadata

We will check those things and report out to you about them

You are supposed to fix any problems identified in your metadata, and address other areas of baseline expectations that you may not meet

The things the community expects you to do will evolve over time – stay connected and informed.

Stuff We (InCommon, “The Federation Operator”) Will Check Automatically

Privacy Policy URL

Logo URL

mdui:DisplayName

Contacts:

- Technical
- Administrative
- Security

Why Is This Stuff Important?

Metadata User Interface (MDUI) elements are used by your federation partners to show users information about the systems the users are trying to use

- Name of the system - something users will recognize
- Logo - again, something users will recognize
- Privacy policy URL - where a user can go to learn more about how their information is handled
- Contact information - something federation partners can use to get in contact with the right people in various situations

Different Levels of Checking are Possible

- Does it exist in metadata? (what we will start off with)
- Do the URLs resolve? Are email addresses deliverable? (target for future checking)
- Prevention of submission of metadata that does not meet expectations
  - Input validation and a warning message
  - Input validation and prevention of submission of metadata that does not meet expectations
- Checking of ‘nice-to-haves’ like logo dimensions and file type, alpha channel, possible SSL grading/etc.

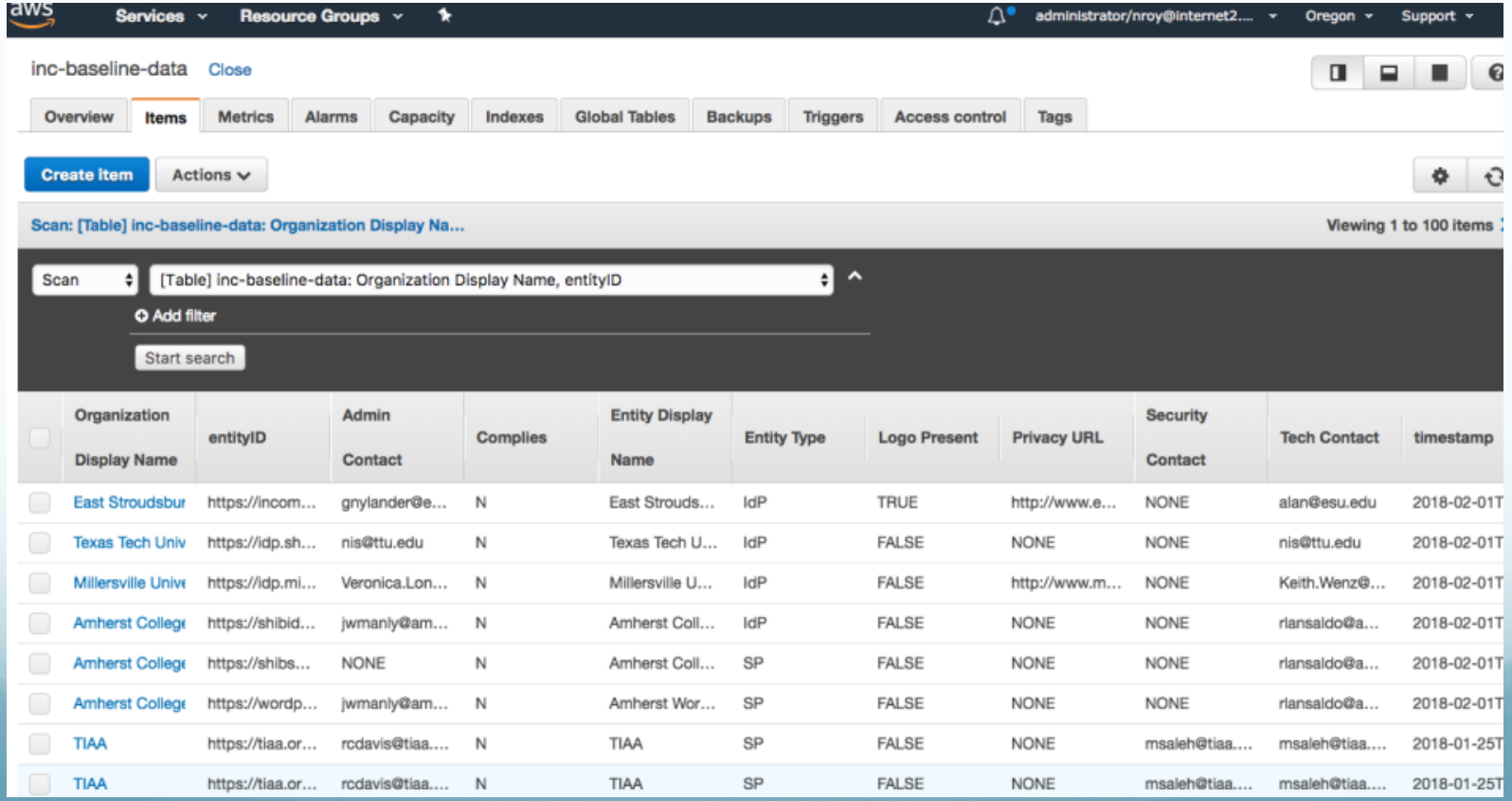
The Process

Initial implementation: metadata -> XSLT -> batch data + contacts from the Federation Manager -> mail merge (probably something like monthly)

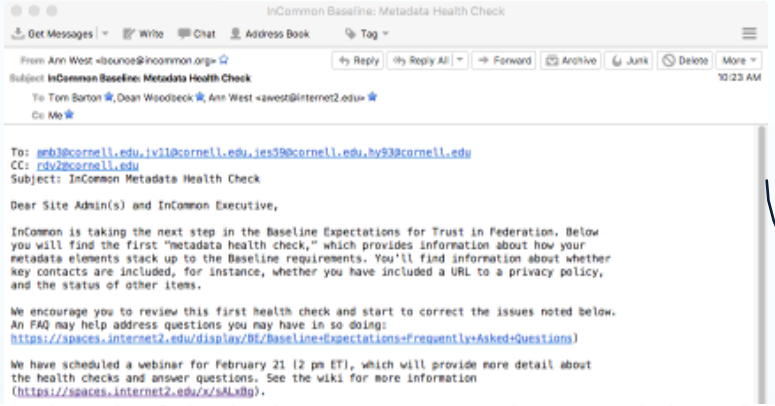
Later: Automated mailings on a periodic basis, notification to the Community Trust and Assurance Board (CTAB) on repeatedly problematic metadata, with escalations to InCommon Steering if needed

Later: Warnings and reporting in the Federation Manager

What Does The Data Look Like?



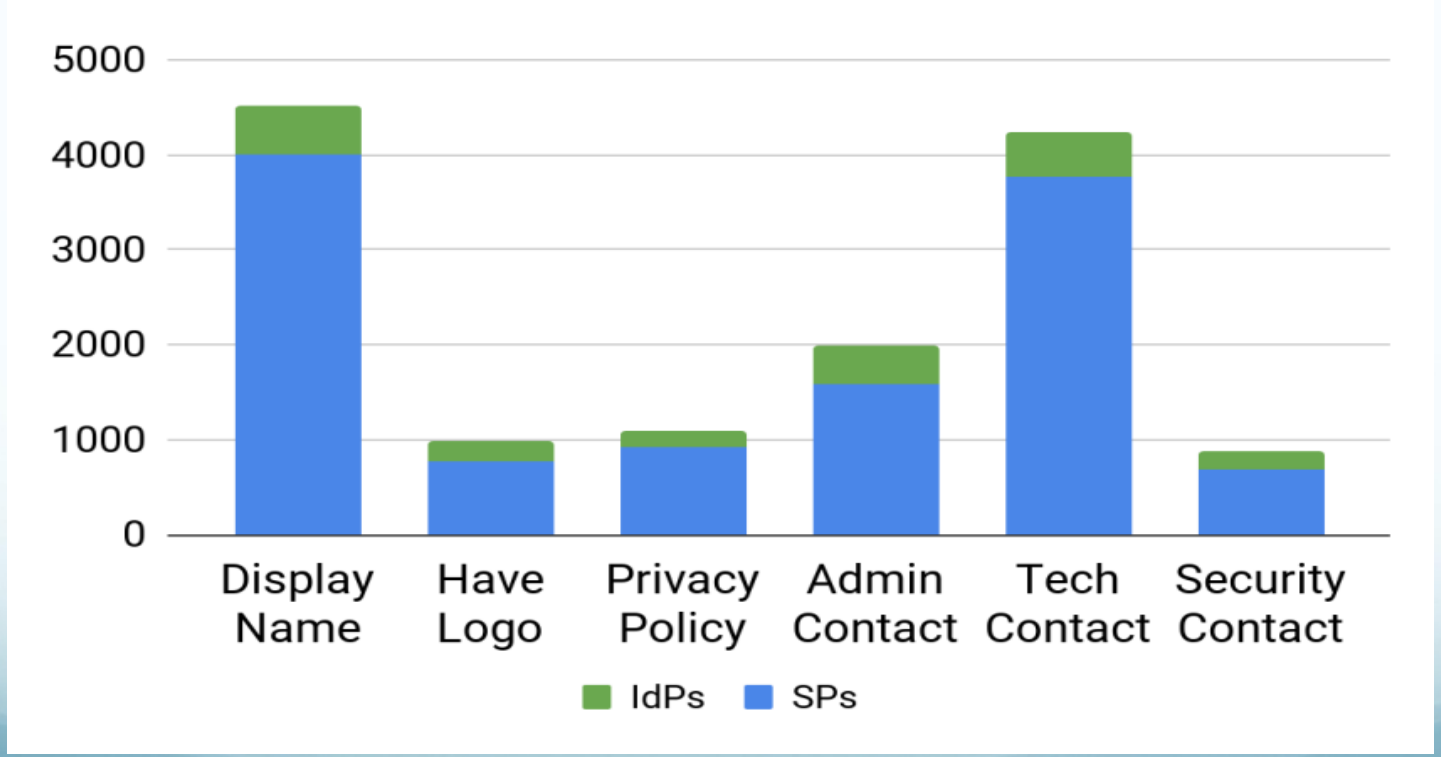
What Will The Notifications Look Like?



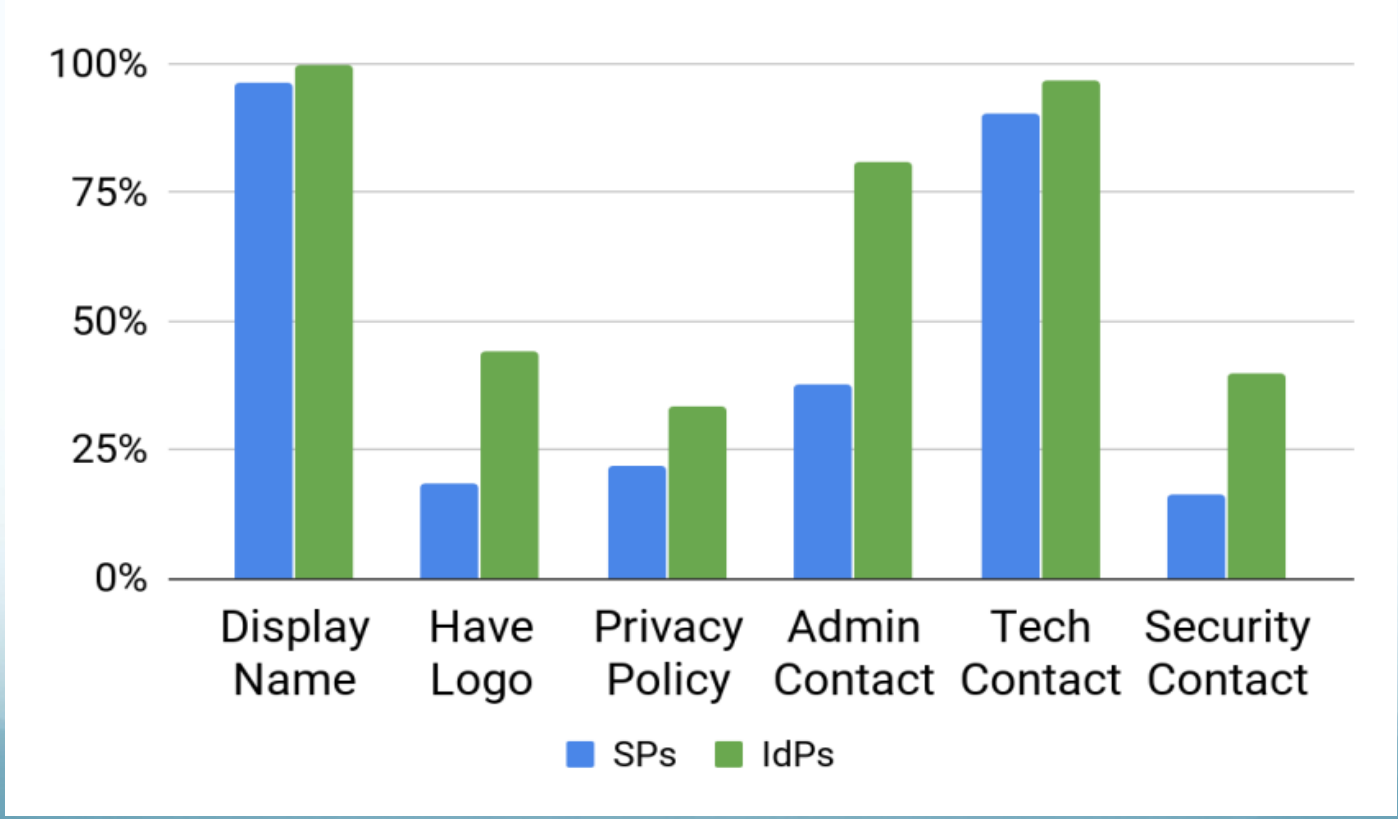
Metadata health check on 2018-02-12 for 9 entities of Cornell University.
M means corresponding required metadata element is missing.

Type	Privacy URL	Logo	Admin Contact	Tech Contact	Security Contact	EntityID
SP					M	https://beta.projecteuclid.org/shibboleth-sp
SP			M		M	https://blackboard.cornell.edu/shibboleth-sp
SP	M	M				https://cvw.cac.cornell.edu/shibboleth
SP	M	M			M	https://dibbs17.org/shibboleth
SP	M	M			M	https://federatedcloud.org/shibboleth
SP				M	M	https://projecteuclid.org/shibboleth
IdP	M	M				https://shibidp.cit.cornell.edu/idp/shibboleth

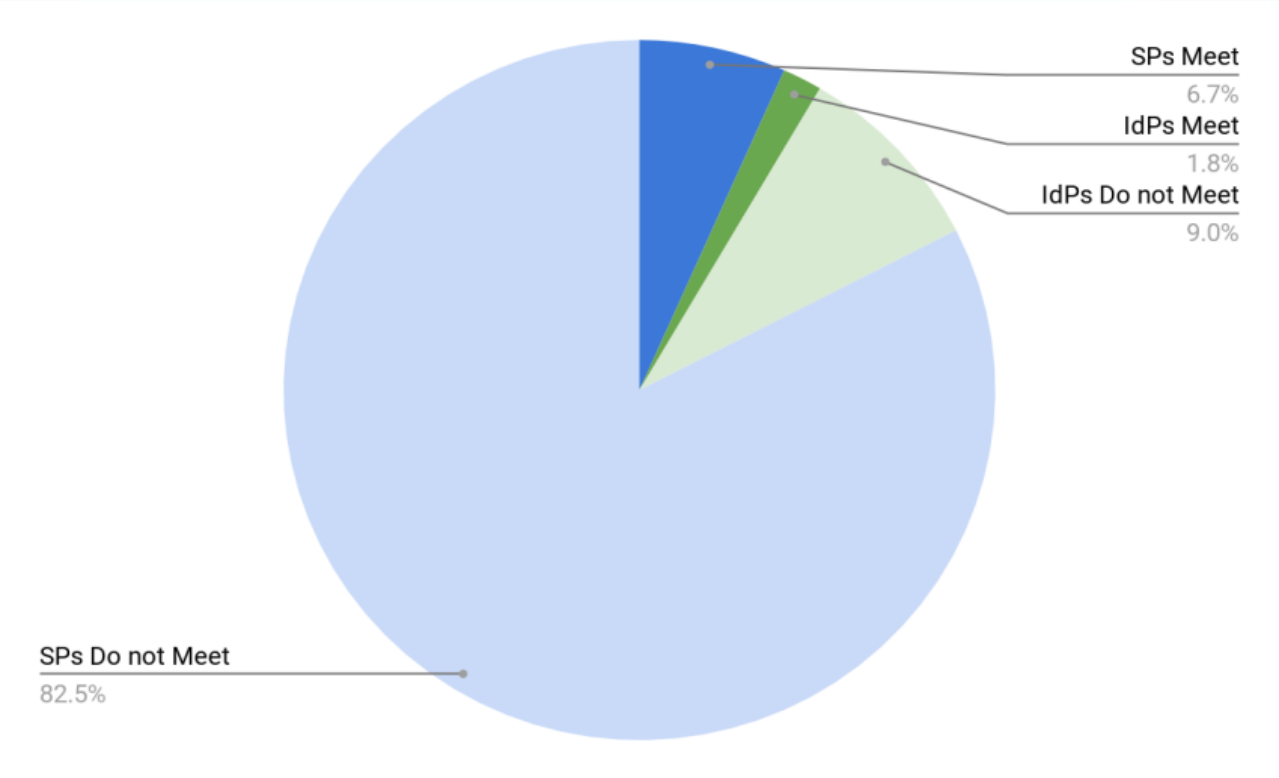
How Many InCommon Entities Currently Meet Expectations?



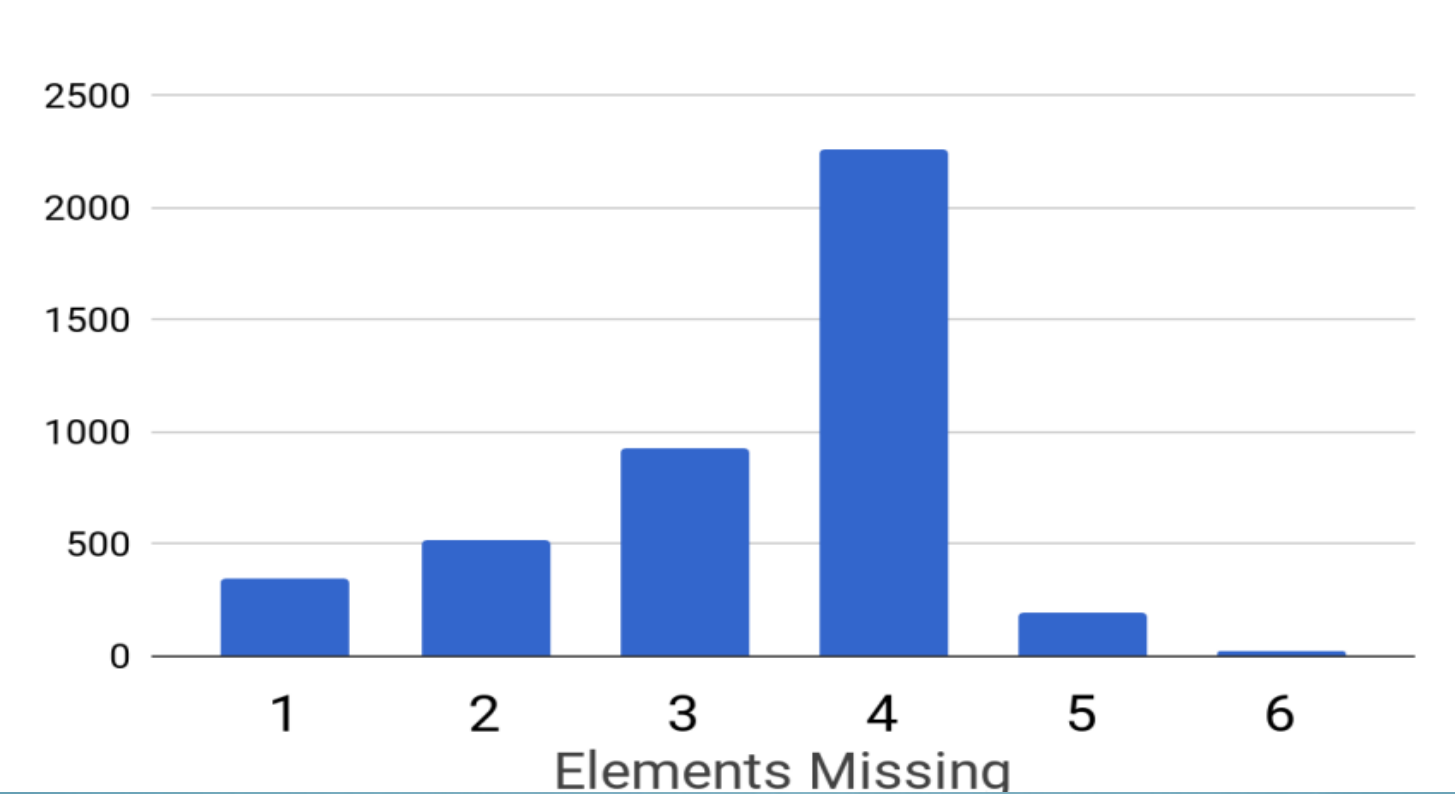
How Many InCommon Entities Currently Meet Expectations?



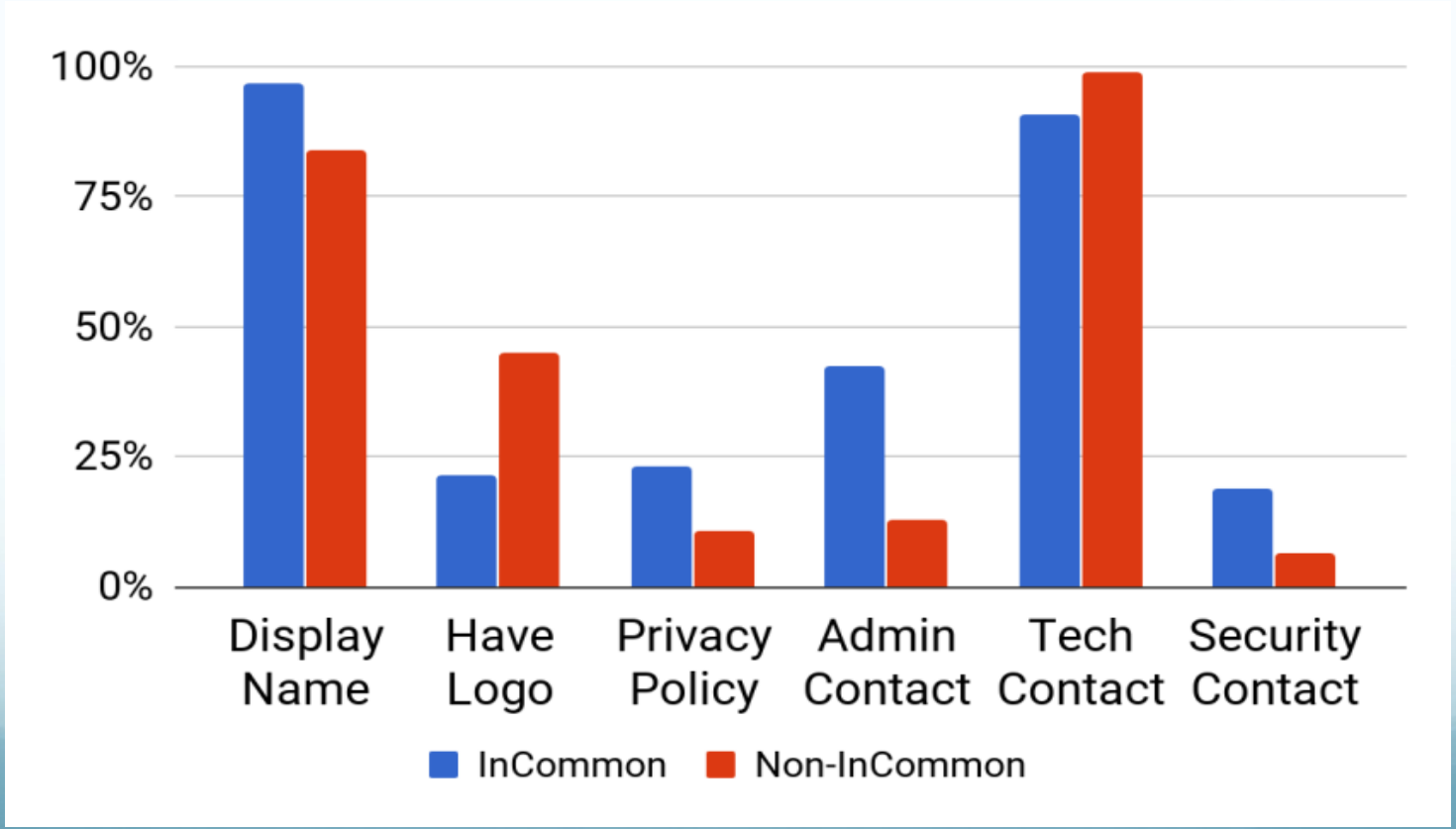
Overall?



How Many Missing Elements?



How Many Global Entities Currently Meet Expectations?



Who Will Receive Notification?

InCommon Executives & Site Admins

These are named roles, defined in your Participation Agreement (Executive) or by your Executive (Site Admins)

The communication asks Site Admins and Execs to review the reports and take action on them - we recommend Site Admins and Execs take this opportunity to discuss with each other

If you need to change a site admin, ask your Exec to visit:
https://www.incommon.org/roles.html

Contacts: What should I put in the contacts?

Contacts should include an address that can handle:

- Administrative - Administrative requests related to the IdP or SP
- Technical - Technical requests related to the IdP or SP
- Security - Security requests related to the IdP or SP

Mail groups or lists are critical - don't use a single person's address

Preserve the ability to receive email even when people change roles

URLs

Logo - A URL for a (preferably) PNG-formatted roughly square logo. You should also specify the dimensions of the logo in pixels width x height in the interface.

> NOTE: This URL MUST be HTTPS in order to prevent issues displaying it on HTTPS-protected interfaces.

Privacy Statement - A URL for an institutional or service-specific privacy statement (it's likely your organization already has such a document, if so, you can probably use that)

DisplayName

Each IdP or SP must have an mdui:DisplayName element set in the User Interface Elements section of the Federation Manager.

This DisplayName should meet the guidelines set forth under the relevant (SP or IdP) User Interface Elements section of the InCommon Metadata Administration wiki page (see next slide)

Learning More About What Should Go In The Required Elements

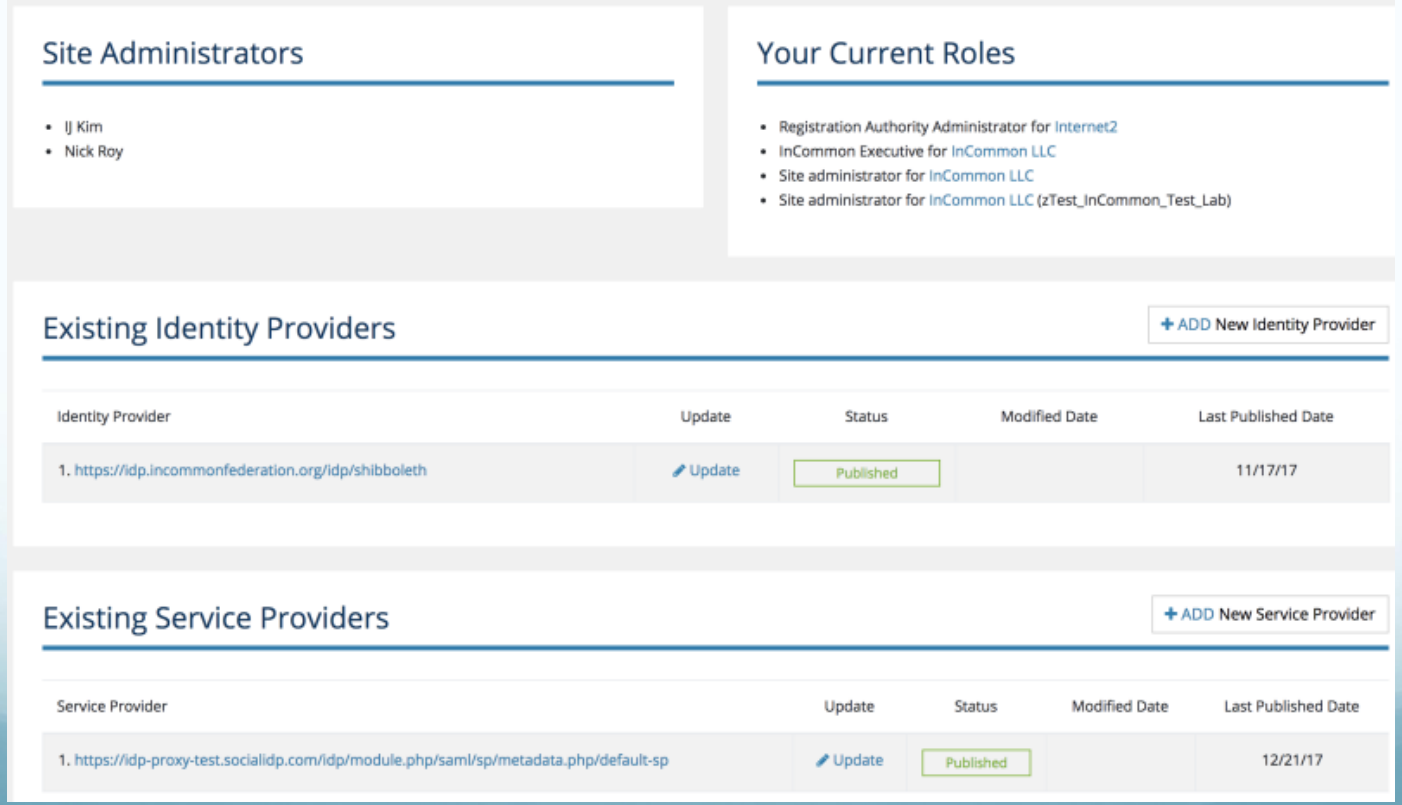
Please thoroughly review the InCommon Metadata Administration Wiki and its child pages: https://spaces.internet2.edu/x/5YKKAQ

What Can I Do Now?

Go to the Federation Manager:

https://service1.internet2.edu/siteadmin

What Can I Do Now?



Site Administrators

- IJ Kim
- Nick Roy

Your Current Roles

- Registration Authority Administrator for Internet2
- InCommon Executive for InCommon LLC
- Site administrator for InCommon LLC
- Site administrator for InCommon LLC (zTest_InCommon_Test_Lab)

Existing Identity Providers

+ ADD New Identity Provider

Identity Provider	Update	Status	Modified Date	Last Published Date
1. https://idp.incommonfederation.org/idp/shibboleth	Update	Published		11/17/17

Existing Service Providers

+ ADD New Service Provider

Service Provider	Update	Status	Modified Date	Last Published Date
1. https://idp-proxy-test.socialidp.com/idp/module.php/saml/sp/metadata.php/default-sp	Update	Published		12/21/17

What Can I Do Now?

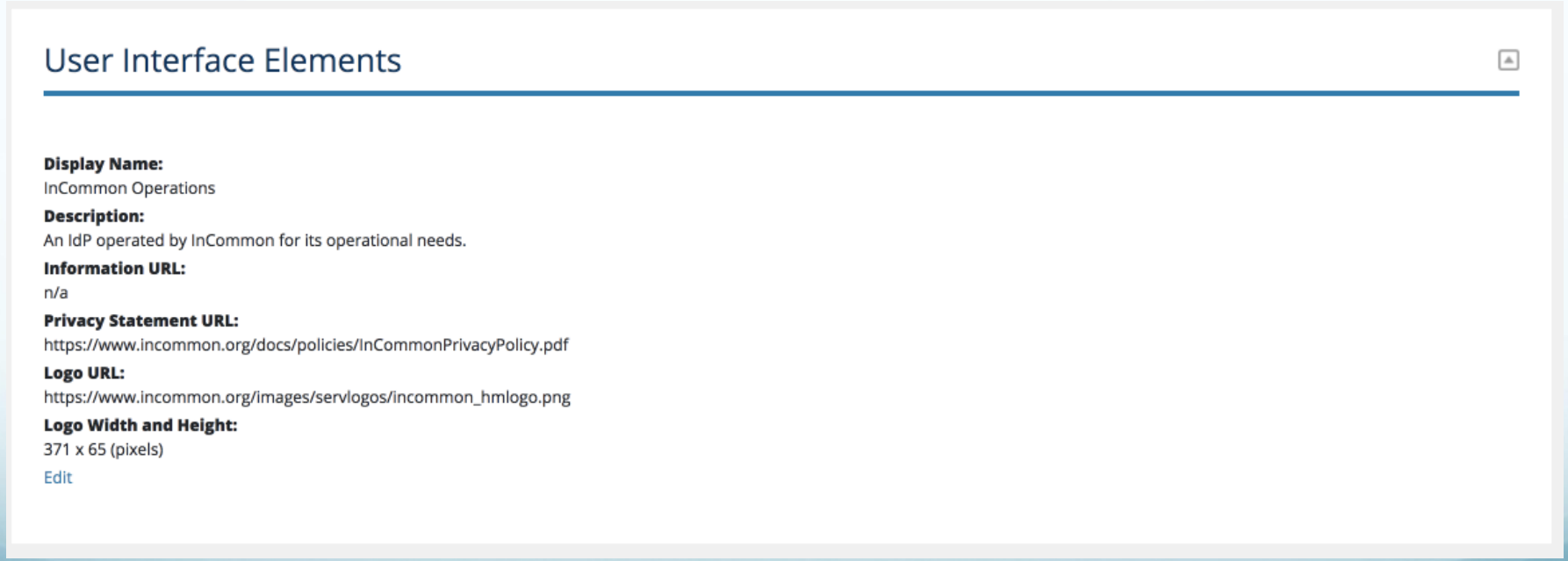
Click the “Update” link next to the entityID of your IdP (if you have one) and any SPs that you have

Look at the “User Interface Elements” and “Contacts” sections

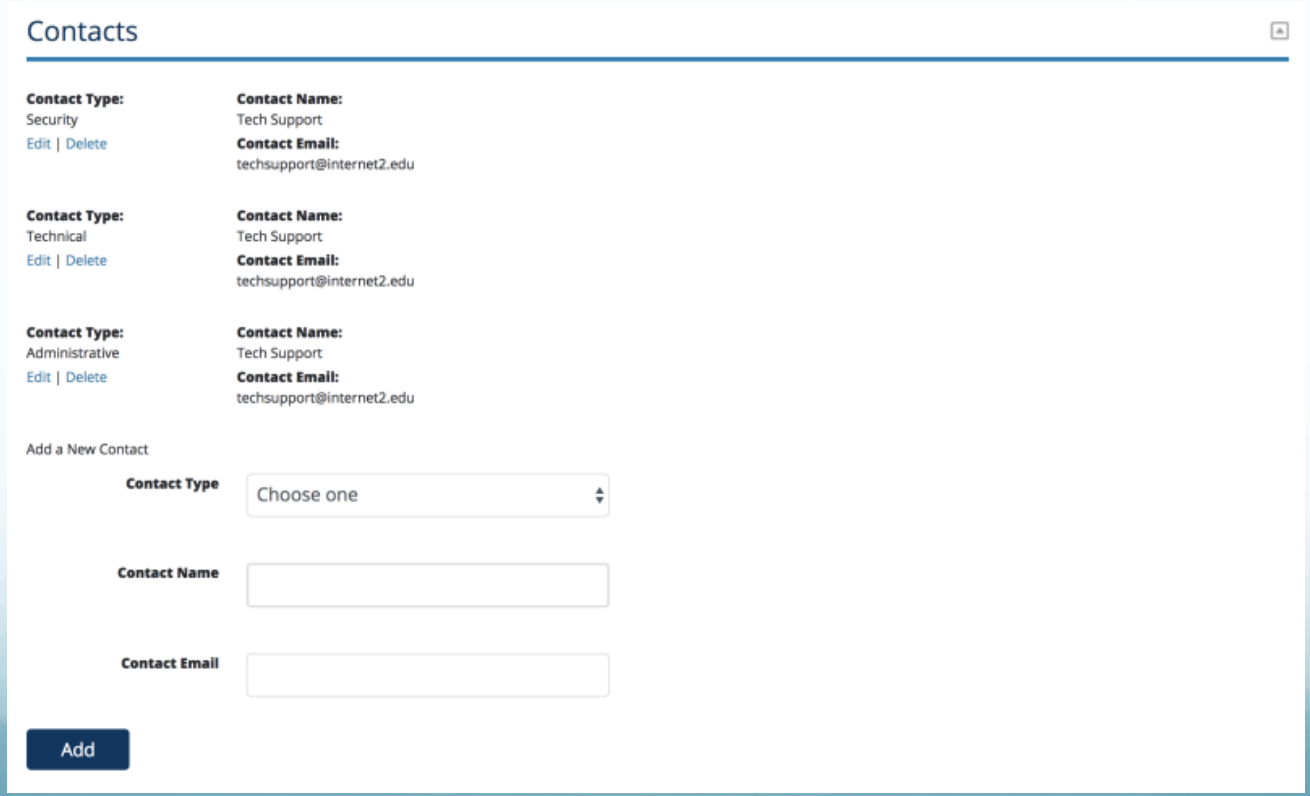
Make sure each IdP and/or SP contains the REQUIRED parts documented at: https://spaces.internet2.edu/x/4RL9Bg

If you need to, add the relevant information via the “Edit” link under the “User Interface Elements” section or by clicking “Add” after specifying missing contact info in the “Contacts” section

What Can I Do Now?



What Can I Do Now?



Questions/Discussion

And remember that one-stop shopping link:
https://www.incommon.org/federation/baseline
(for all your Baseline Expectations needs!)

Next Time: Policy Changes and the Participation Agreement: What Executives Need to Know

Baseline Expectations Impact — Wednesday, January 24, 2018

Metadata Health Checks — Wednesday, February 21, 2018

Policy Aspects & Legal Changes — Wednesday, March 7, 2018
2 pm ET | 1 pm CT | Noon MT | 11 am PT

For details, see the wiki: https://spaces.internet2.edu/x/sALxBg

Thanks!