InCommon Assurance Call
November 4, 2015

Topics:

- Preliminary Proposal of Federation Baseline Practices to replace the InCommon Participant Operating Practices (POP)
- Results from the Assurance Survey conducted in September 2015

Presenters:

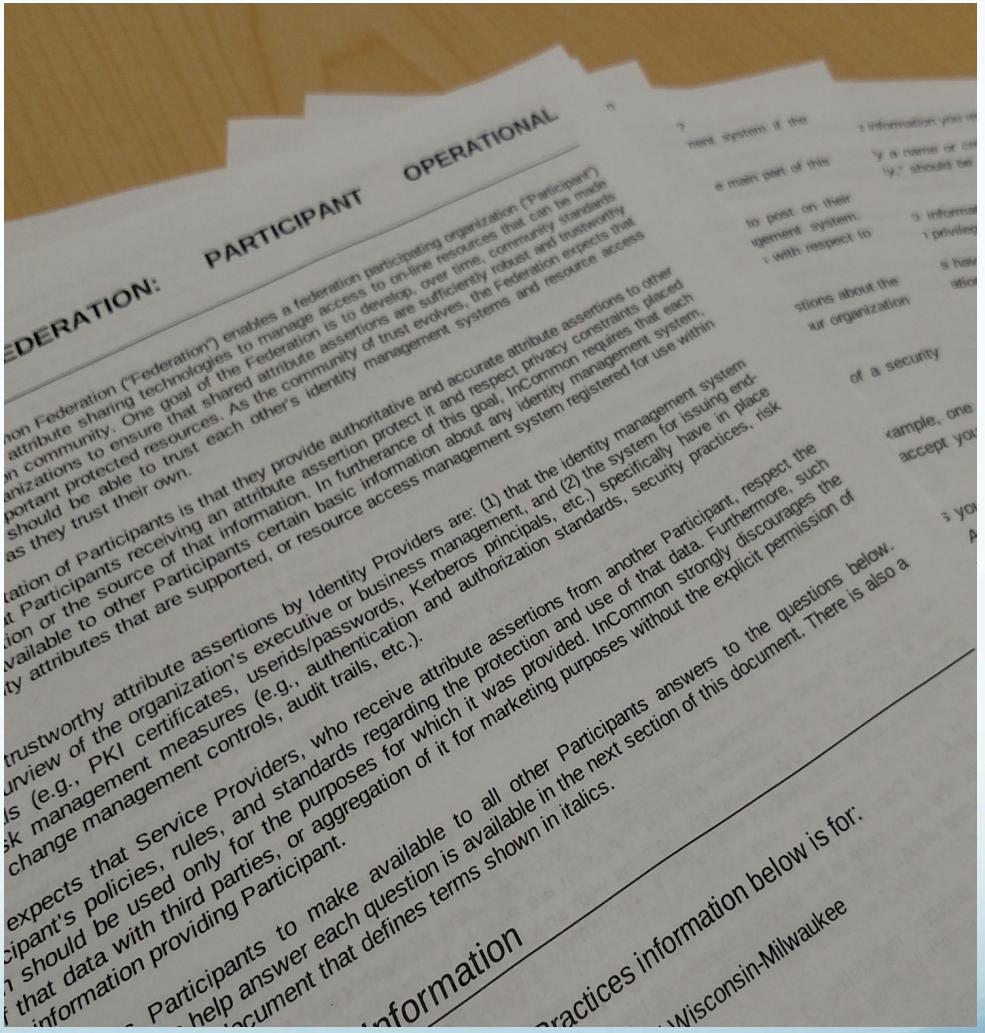
Jacob Farmer, Indiana University, InCommon Assurance Advisory Committee, Chair

Chris Spadanuda, University of Wisconsin-Milwaukee, InCommon Assurance Advisory Committee, Vice-Chair

Paul Caskey, Internet2, Moderator

Participant Operating Practices (POP)

- Community Standard and Expectation
- Self developed
- Not machine readable
- Some do not have
- Some have not updated
- Difficult to verify



Assurance Advisory Committee

- Discussions regarding the POP go back several years
- Break through at a recent AAC face to face meeting
  - Vision - Increasing the trust within the federation in a way that allows us to incrementally implement improvements, while leveraging data to measure the trust in the federation.
  - Using the Trustmark model we set a goal to have 5 questions for IdPs, 5 for SPs
  - Incorporate this in the federation management process
  - Discussing steps leading up to what a sanction might look like

More discussion at ACAMP 2015 in Cleveland

- Jacob Farmer lead a session called “POP Killers Anonymous”
- We saw pretty good community buy-in on replacing the POP
- Administrative/business processes around the sanction of and removal from metadata need to be developed
- Proposing the concept

What are we proposing?

- Five minimum requirements for IDP's
- Five minimum requirements for SP's
- Minimum's communicated in a machine readable format.
- Creation of a business and technical processes to hold IDP's and SP's accountable for the five minimum standards

Identity Providers

1. The identity management system including the credential store is operated under the authority of the organization's InCommon executive contact, or their designee.
2. IdP only presents assertions believed to contain accurate information.
3. The institution’s identity data and systems are considered trustworthy enough to access enterprise systems on your campus.
4. Metadata is accurate, complete, and reviewed annually, including site contacts and all MDUI information, such as the privacy policy.
5. Documented security or incident response plan covers identity provider operations.

Service Providers

1. Controls are in place to reasonably secure information and maintain user privacy.
2. Information received from the identity provider about users and transactions is stored only when absolutely necessary.
3. Metadata is accurate, complete, and reviewed annually, including site contacts and all MDUI information, such as the privacy policy.
4. Documented attribute requirements are available upon request.
5. Documented security or incident response plan covers service provider operations.

Next Steps for Proposal on Baseline Practices to Replace the POP

- Community Feedback assurance@incommon.org
- Development of intent paper: context (history, rationale, thought process, roadmap, etc.)
- Conversations with IAM Steering Committee
- Sharing with community
- Concept approval
- Technical design
- Business process design

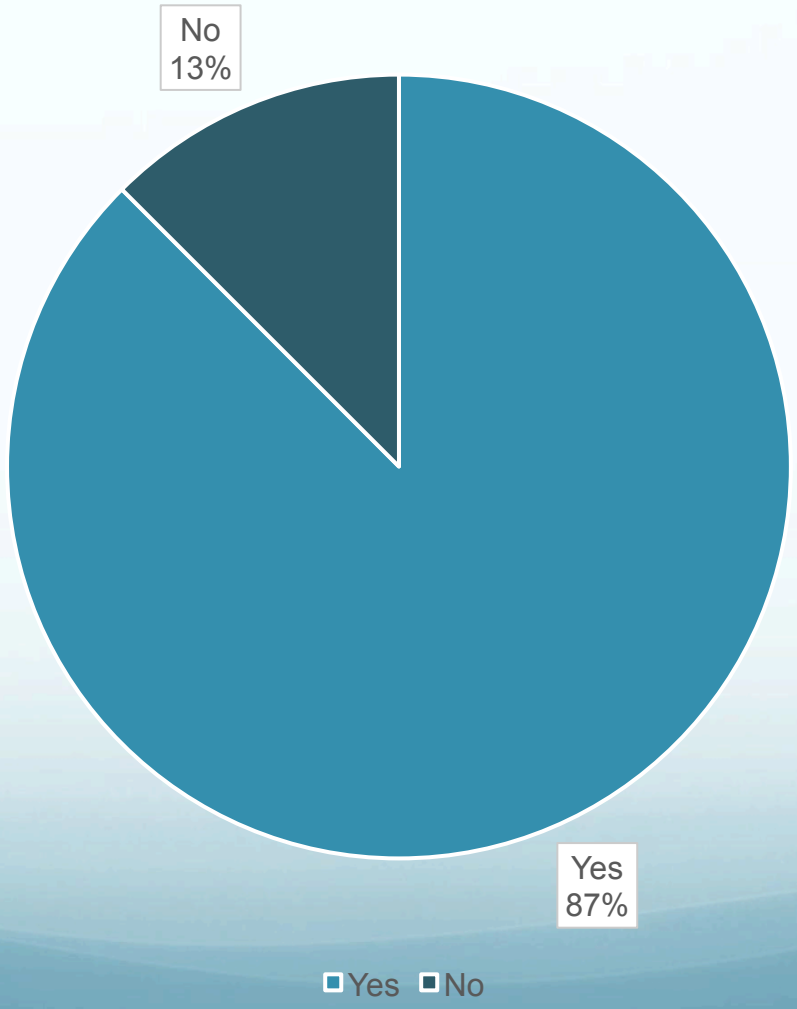
Comments
Questions

InCommon Assurance Survey, Sept 2015

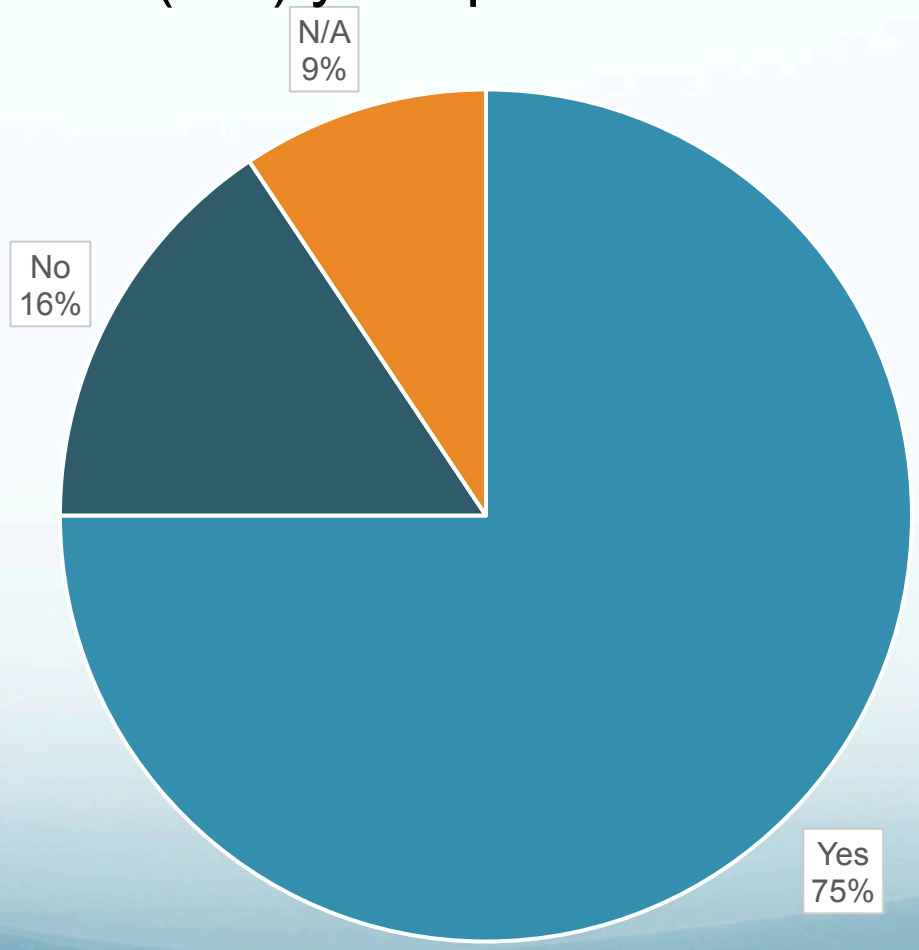
Overall Response Rate

33 Responses spread over two weeks

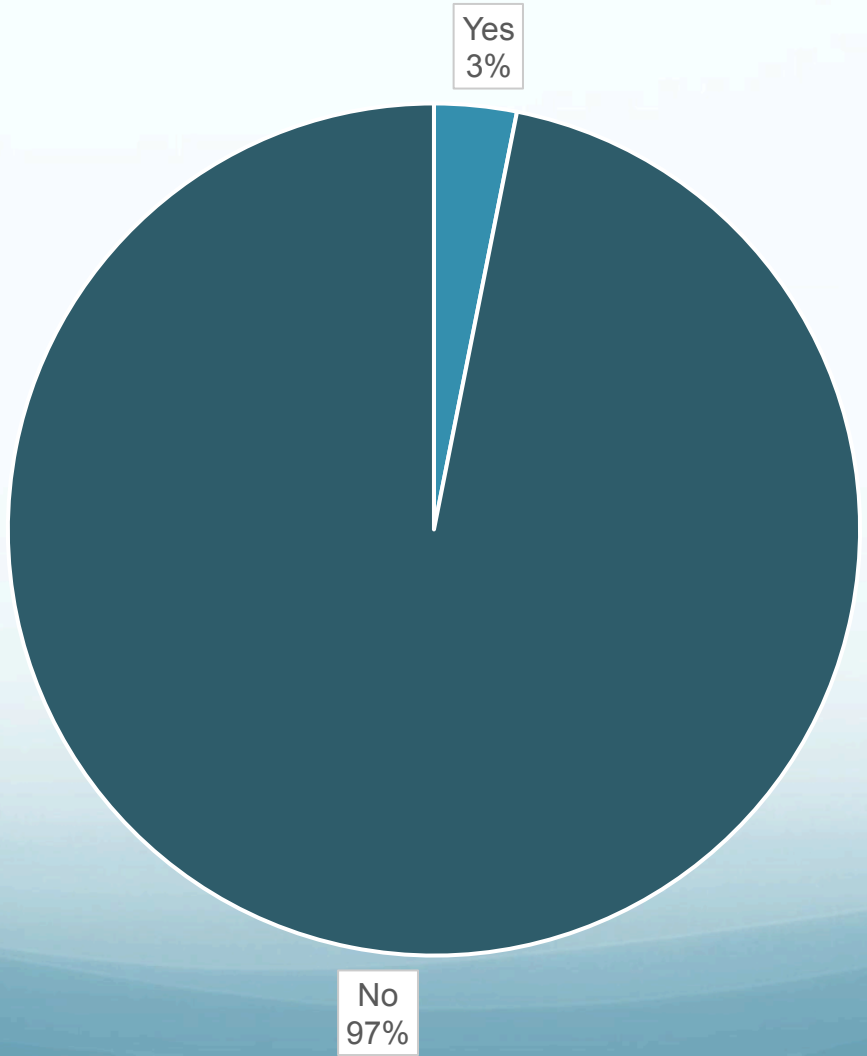
Are you aware of the InCommon Bronze and Silver Assurance Profiles?



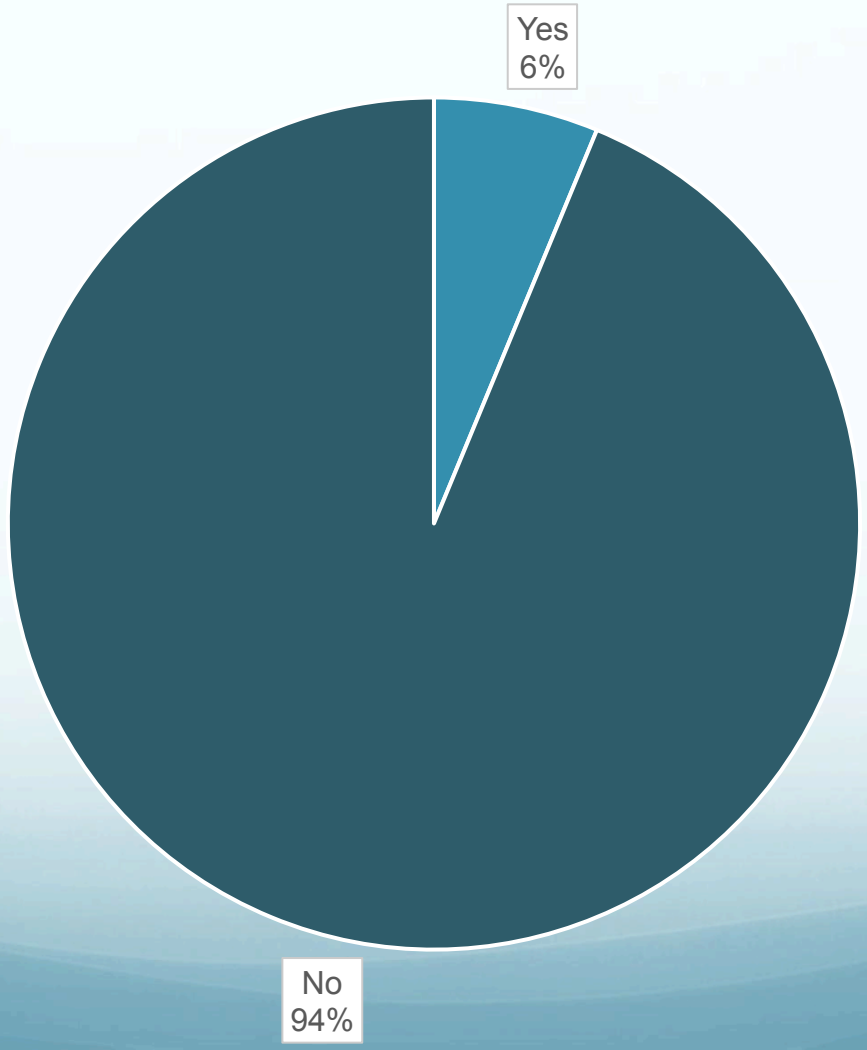
Is your institution interested in implementing either the InCommon Bronze or Silver Assurance Profile for any Identity Provider (IdP) you operate?



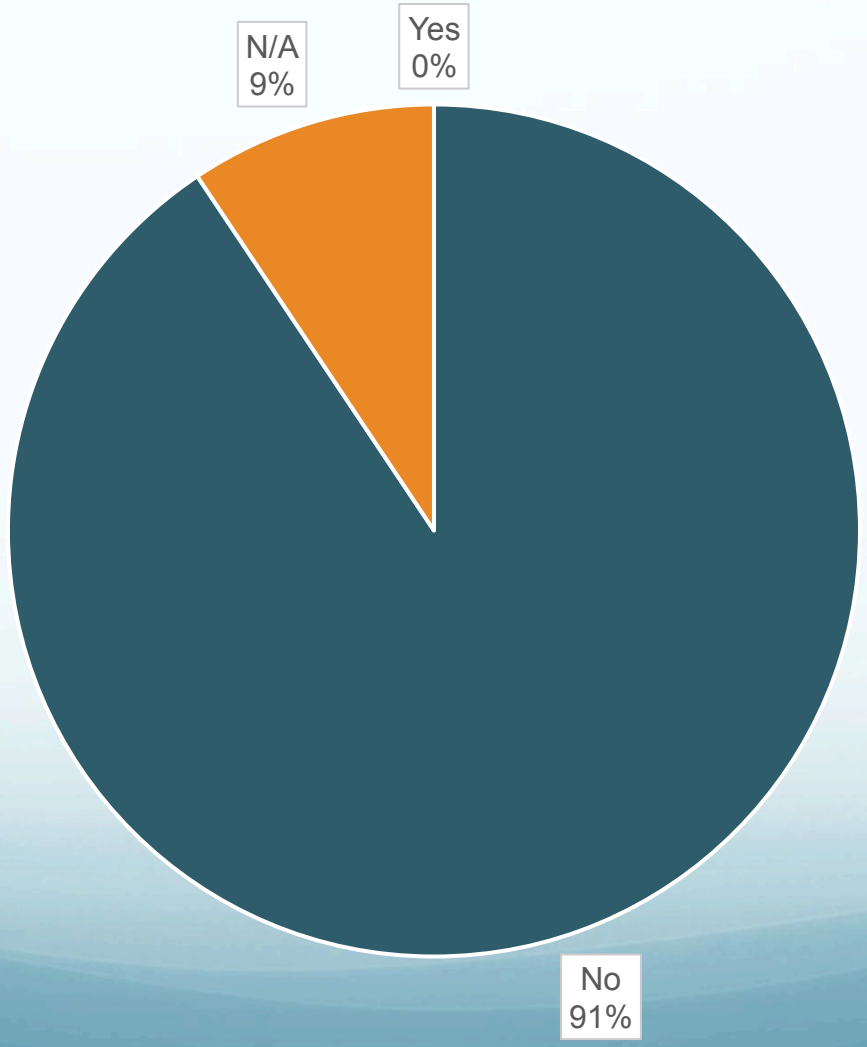
Are you aware of any SPs that require InCommon Bronze or Silver Assurance Profiles for authentication?



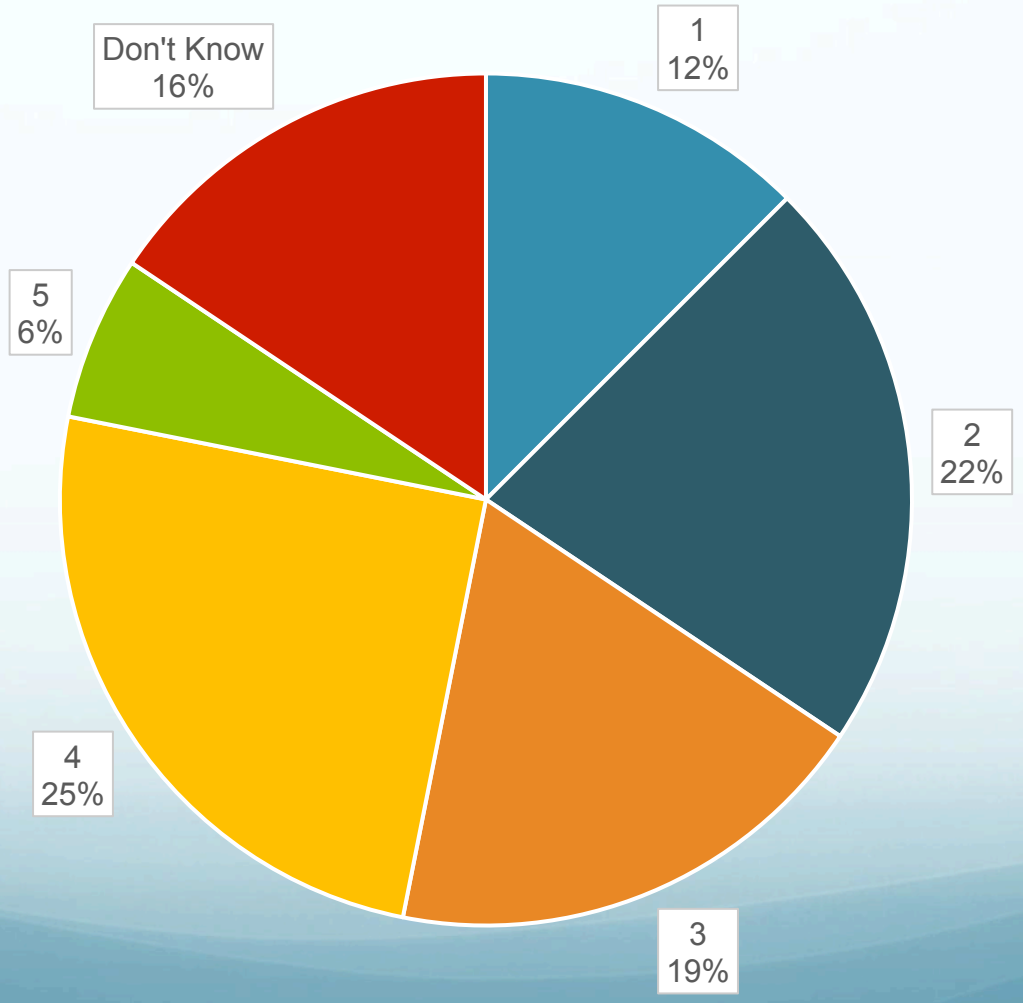
Does your institution have any users that need access to any Service Provider (SP) that requires an InCommon Bronze or Silver Assurance Profile?



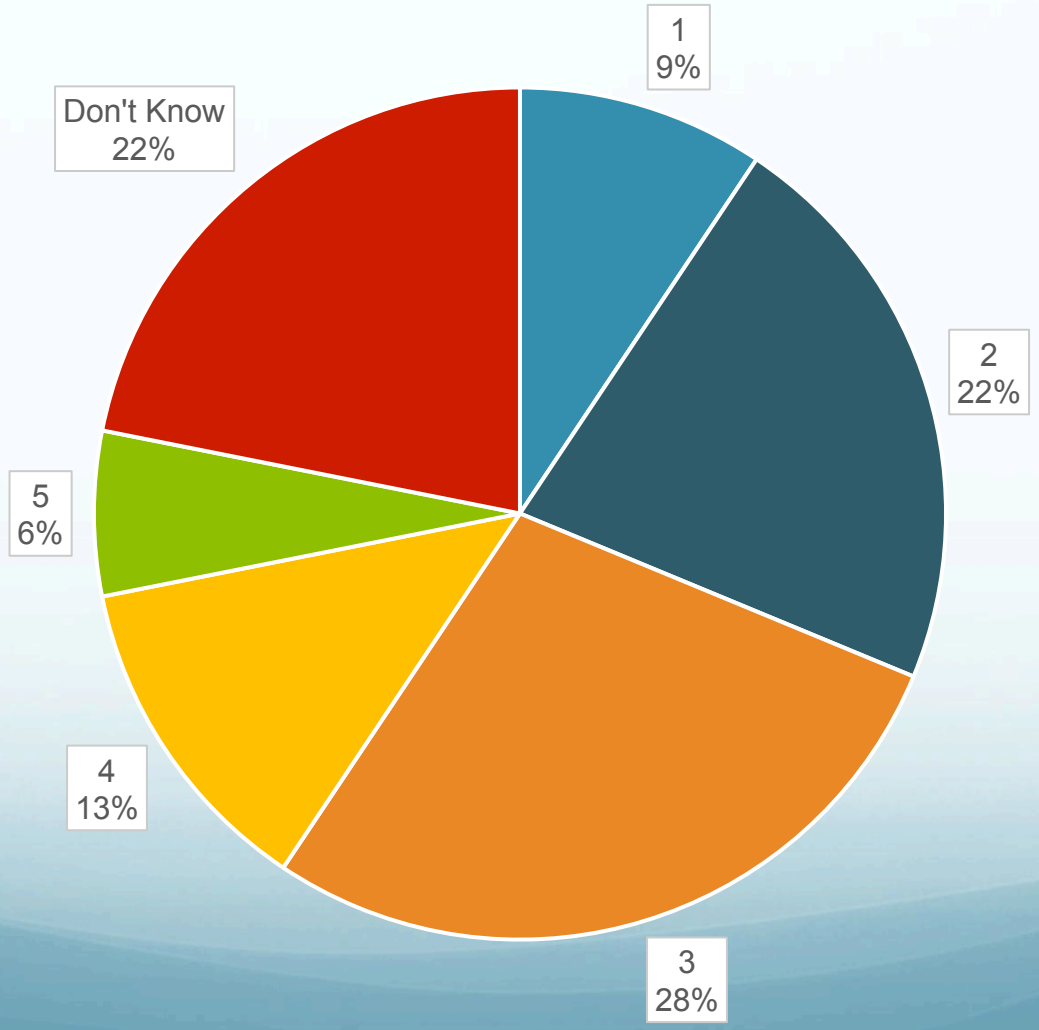
Are their services your institution would like to use, but cannot because your IdP lacks a required assurance profile?



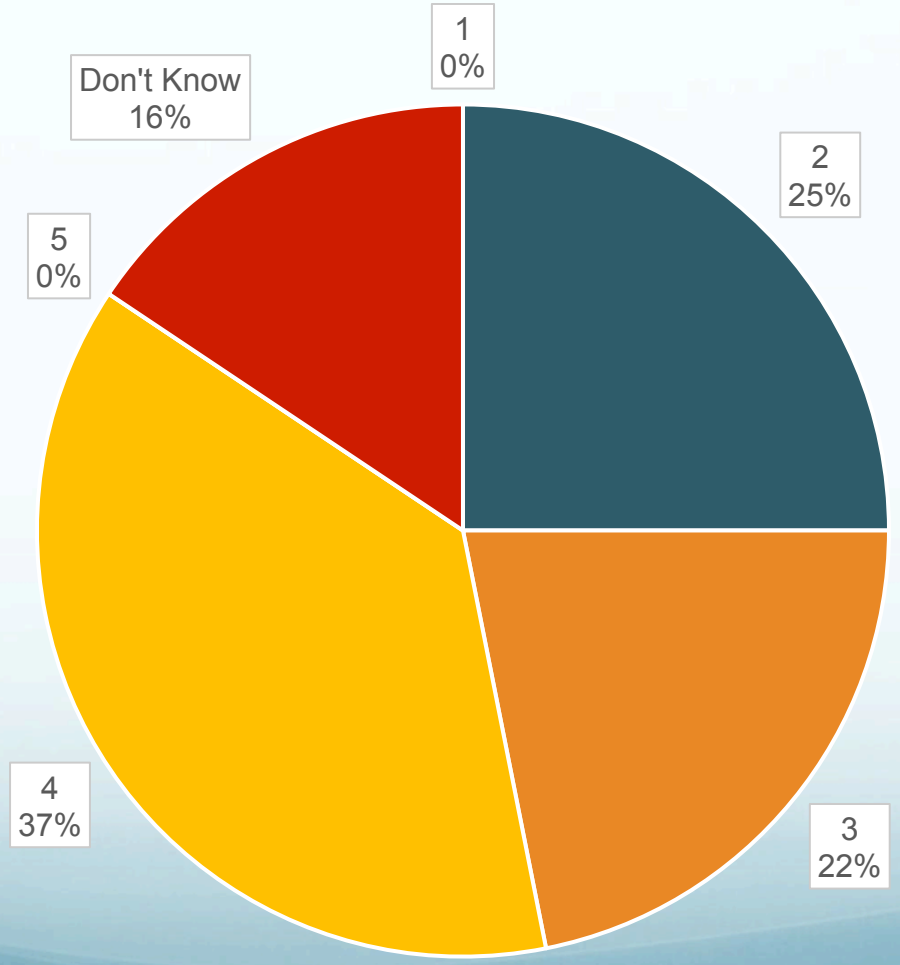
What is your perception of the VALUE of implementing a Bronze Assurance Profile? (Higher number means more value)



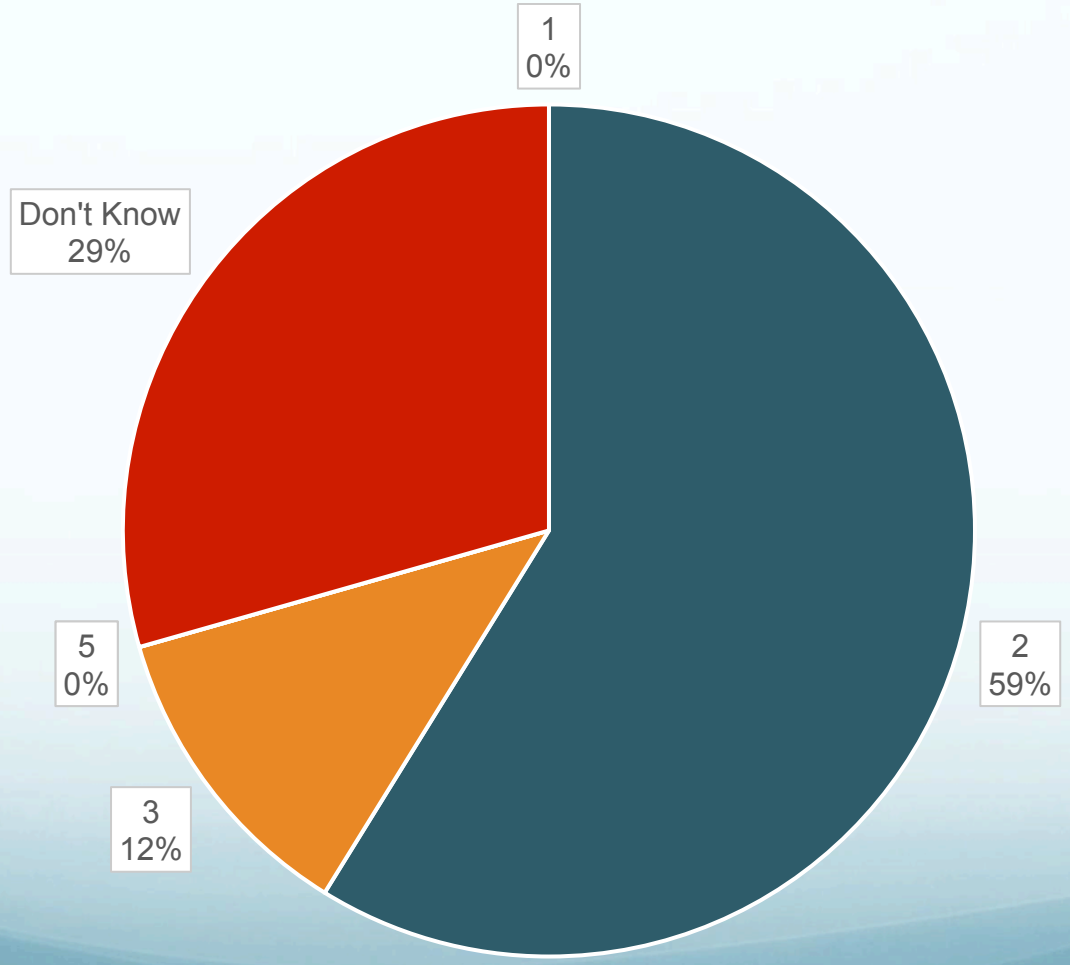
What is your perception of the VALUE of implementing a Silver Assurance Profile? (Higher number means more value)



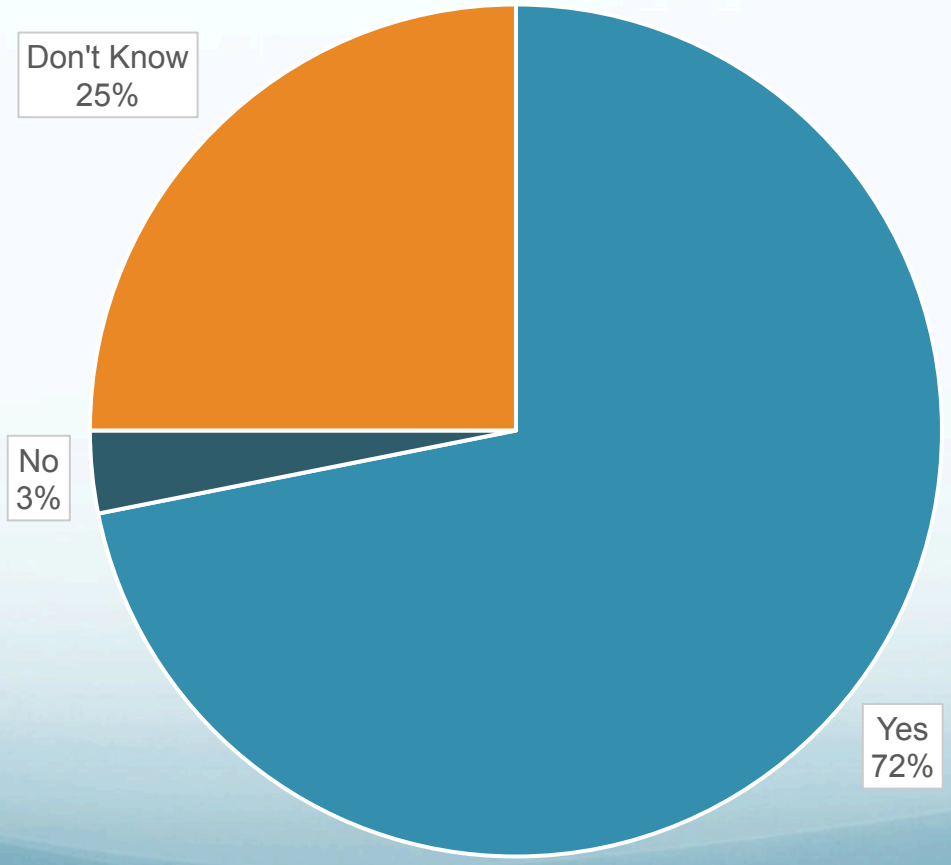
What is your perception of the EASE of implementing a Bronze Assurance Profile? (Lower number means more difficult)



What is your perception of the EASE of implementing a Silver Assurance Profile? (Lower number means more difficult)



If there existed an InCommon Multi-Factor Authentication Assurance Profile that asserted compliance with certain community standards in implementing multi-factor authentication, would you be interested in attaining such a profile?



Comments
Questions

Thank you for participating in today's InCommon Assurance call