# InCommon Service Provider Onboarding - Final Report

DRAFT v2, July 2018

**Document Title:** InCommon Service Provider Onboarding - Final Report
**Document Repository ID:** TI.98.1
**DOI:** 10.26869/TI.98.1
**Persistent URL:** http://doi.org/10.26869/TI.98.1
**Authors:** InCommon Streamlining SP Onboarding Working Group
**Publication Date:** April 2018
**Sponsor:** InCommon TAC

# Table of Contents

# 1. Executive Summary

This final report reviews and summarizes the three deliverables of this working group:

- InCommon Service Provider Onboarding - Criteria Document
- InCommon Service Provider Onboarding - Questionnaire
- InCommon Service Provider Onboarding - Primer Document

The 'Criteria Document' gives a Service Provider (SP) a high level overview of existing principles and standards, that when reviewed and followed as part of their onboarding process into InCommon, will ensure their application is able to maximize interoperability, user experience, and security within the InCommon federation.

For those SPs that need additional assistance or guidance with the 'Criteria Document', the 'Questionnaire' can be used as an interactive guide that walks the SP through the adoption of the material. This walkthrough style guide provides context, tips, and helpful resources to help an SP develop a better understanding of the criteria and assist them with criteria adoption.

As a backdrop to the 'Criteria Document' and the 'Questionnaire', the 'Primer Document' was created to help onboarding Service Providers understand core concepts such as 'SAML', 'InCommon Aggregate', 'Shibboleth', and 'Metadata Exchange'. Giving the SP the prerequisite knowledge they need to better understand the terminology, concepts, and best practices within the 'Criteria Document' and 'Questionnaire'.

Given these three deliverables, the Looking to the Future section of this report contains the working group's recommended next steps for advancing this material further, along with those items that fell out of scope but are recommended for further discussion and review.

# 2. Introduction

A summary of the working group's mission is as follows:

"The Streamlining SP Onboarding Working Group will **identify and document standards** for Service Provider operation within the InCommon Federation using the CIC Cloud Services Cookbook as a starting point. Having **standards available that help SPs onboard** will add to the value proposition for SPs in the InCommon Federation and reduce variance in configuration and increase interoperability."

With that mission, the working group set out to gather and review existing standards that are documented for both Service Providers (SP) and Identity Provider Organizations (IDPO); starting with the 'CIC Cloud Services Cookbook'. Drawing on several dozen different standards and criteria, the working group then set out to narrow these standards down to a set of criteria that we felt were most applicable to the SP onboarding process.  Specifically selecting those criteria, that if followed and applied correctly, would streamline the SP onboarding process while providing the SP with optimal levels of interoperability and security.  Lastly, to narrow the criteria down further, we grouped them into two categories: minimum and recommended.  'Minimum' criteria defined as those criteria that should be met by all SPs regardless of their setup. 'Recommended' criteria being those criteria that would be strongly encouraged, but depending on various factors, not always necessary.

In conjunction with identifying and documenting these core set of SP standards, the working group also set out to help clarify what the value adds were for meeting these standards with respect to becoming an InCommon participant and leveraging the InCommon federation.

- For the complete list of criteria, please see 'InCommon Service Provider Onboarding - Criteria Document'.

## 3. Using the Criteria as the Foundation for a Questionnaire

The 'InCommon Service Provider Onboarding - Criteria Document' provides a foundation, built on a set of consistent standards, for Service Providers (SP) in InCommon to follow.  A set of standards that would apply equally to vendor (commercial), education, and research SPs.

- For more details on the Service Providers that are targeted by this material, please see Targeted Service Providers

However in many cases, a standalone criteria document may provide too steep of a learning curve for new or inexperienced SPs to follow.  For example, SPs that are interested in joining InCommon but need pointers on where to start and what standards they need to get started with.  Or SPs that need help understanding the terminology that make up the criteria or need technical assistance with implementing the criteria.  Therefore, as a complement to the criteria document, a self-assessment (questionnaire) style approach was developed.  An approach that would "walk" the SP through standards adoption and the overall onboarding process into InCommon; providing the opportunity to self-assess against the criteria while also interweaving helper material, online references, and appropriate guidance every step of the way.

- For more information on when to surface the questionnaire to Service Providers, please see Opportunities to Surface the Questionnaire

With the end result being, the centralization of a core set of standards and best practices that are more readable, easier to follow, and accessible to a much wider experience spectrum of InCommon Service Providers.  And for those Service Providers that are more experienced and have already designed and deployed their applications, the self-assessment questionnaire will give them the opportunity to reassess their current setup against the latest set of SP criteria and best practices.

# 4. InCommon Service Provider Onboarding - Questionnaire

This questionnaire style approach allows onboarding SPs to self-assess; using a series of yes/no questions that present guidance, recommendations, and criteria depending on the answers given. With each question representing a particular standard or criteria sourced from the ‘InCommon Service Provider Onboarding - Criteria Document’.

- For a **preview** of the questions in the questionnaire, please see the Questionnaire Outline
- For the **complete** experience, please see the InCommon SP Onboarding - Questionnaire.

Additionally, the questionnaire is able to provide appropriate context and helper material to each question being asked; allowing the SP to understand what the question is asking and make an informed decision on how to best answer the question. Taking this further, if the SP decides to answer a question a certain way that would imply they are not meeting a specific criteria item, then the questionnaire provides the associated risks along with recommended next steps. At which point, the SP has the information they need to make the proper decision on whether to proceed, given the associated risks, or not.

By the end of the questionnaire, the SP should understand the onboarding criteria, the fundamental concepts behind the criteria, the steps required to meet the criteria, and be able to find references to applicable online resources if further information or assistance is needed.

# 5. Summary

With the ‘Criteria Document’, ‘Questionnaire’, and ‘Primer Document’, Service Providers have resources they can follow that will guide them through standard adoption and help streamline their onboarding process into the InCommon Federation. While at the same time, providing clarity for how standard adoption along with being a participant in InCommon, can lead to improved interoperability with other SPs and more streamlined integrations with Identity Provider Organizations within InCommon.

# 6. Looking to the Future

We believe the effectiveness of the working group deliverables hinge on Service Provider maturity within the larger InCommon community:

- Service Provider (SP) maturity - their ability to locate and understand federation criteria and standards and the maturity and motivation to adopt those criteria and standards

We feel to continue to increase this maturity for SPs, there needs to be a common/de-facto web space dedicated for the sole initiative of surfacing the recommended standards and best practices for all stages of an SPs interaction with the federation.

Specifically for the purposes of this working group, the ‘Criteria Document’, ‘Questionnaire’, and ‘Primer Document’ would be hosted in this space and would specifically target those SPs that are onboarding to the InCommon federation.  Future work to be developed, for example, would touch on IDPO onboarding to the federation or SP and IDP operational best practices over the course of their service lifecycle within the federation.

Lastly, there are likely many different formats and approaches for the material within the ‘Criteria Document’, ‘Questionnaire’, and ‘Primer Document’ material.  For example, the working group went down the path of using a questionnaire (Google Forms) style approach for the ‘Questionnaire’.  However an alternate approach could have been collapsing the ‘Questionnaire’ into a one-page or quick start checklist.  But ultimately what we learned is that no matter what approach is taken with this material, **it needs to be grounded in the recommended technology standards of the federation, be produced in a way that’s accessible to a wide experience spectrum of SPs, and hosted in a web location that’s easy to find and can be centrally referenced by all InCommon participants.**

In summary, fundamentally landing on those standards the federation deems most important and agreeing on the official web home for this material, will open up the doors to be able to refine how this material is hosted and styled over time and continue to increase the baseline maturity of InCommon SPs.

- For additional information on a number of growth opportunities on taking the next step to expand this working group’s material further, please see Appendix E. Further Developments and Opportunities for this Material.

# Appendix A. Questionnaire Outline

A. **Establishing Trust**
   a. Is your organization a participant in the InCommon Federation??
   b. Has your organization registered your service's metadata with the InCommon federation?
   c. Has your organization defined a process for keeping your metadata up to date?
   d. Does your application consume, refresh, and verify the signature on InCommon metadata routinely?

B. **Technical Interoperability**
   a. Does your application implement SAML2 using the recommended software?
   b. Have you generated your SAML (X.509) certificate using the InCommon security and trust requirements?
   c. Will your application be authenticating users via more than one Identity Provider, either within a single institution or within a Federation?

C. **Identifiers and Attributes**
   a. Does your application support a relevant portion of the InCommon Attribute Set?
   b. Is your application able to support user identification using at least one of the eduPerson or SAML V2.0 Subject identifiers?
   c. Please specify those minimum attributes that your application requires from its user community?

D. **Authorization**
   a. Will your application be using authorization to allow or restrict access?
   b. How will your application be authorizing its user population?

E. **User Experience**
   a. Checklist
      i. Login Experience - Is the login page accessible and easy to find? What's the experience if a user logs in but is not authorized?
      ii. Logout Experience - Does your application support a proper logout? Is the logout page accessible and easy to find?
      iii. User Information - How are the user attributes (UserID, display name, email) exposed, presented, or shared within your application?
      iv. Error Screens - Are error messages user friendly? (What happened, why it happened, what the user might do to remedy the situation)
      v. Federated Login Experience - Is your application able to support a discovery mechanism for federated login? Are direct resource URLs able to work with your discovery service?
      vi. Federated Login Experience - If your application will be authenticating users via more than one Identity Provider, does your application allow a user to login to the same account from multiple Identity Providers?

# Appendix B. Targeted Service Providers

The targeted audience for the 'InCommon Service Provider Onboarding - Criteria Document' and the 'InCommon Service Provider Onboarding - Questionnaire' material include the following class of Service Providers:

1. You are a vendor (commercial or third party), education, or research Service Provider and fall into one of the following categories:
    a. Have not yet joined InCommon but are interested; and need more information on the value adds for joining InCommon and what technical steps they will need to take to become an operational InCommon participant
    b. Have recently joined InCommon and need assistance and/or a jumpstart for getting started and becoming operational
    c. Have been an InCommon participant for quite some time, however need to self-assess and determine whether you are meeting the necessary standards and maximizing the potential of your InCommon partnership

Those audiences that are out of scope of this material include:

1. Service Providers, that are members of an Identity Provider Organization (IDPO), that are requesting assistance with bilateral registrations with the IDPO.

# Appendix C. Opportunities to Surface the Questionnaire

With the 'InCommon SP Onboarding - Criteria Document' and the 'InCommon SP Onboarding - Questionnaire', what may be the opportune times to surface this material?

1. During a home institution's procurement or RFP (request for proposal) process, the Service Provider (vendor) would be directed to the questionnaire and their response used as part of the institution's vendor evaluation
2. The questionnaire would be encouraged for Service Providers to follow as part of joining InCommon*
3. The questionnaire would be encouraged, generally by the Identity Provider Organization (IDPO), when sponsoring a Service Provider (https://www.incommon.org/sponsor.html).
4. For existing InCommon Service Provider participants, site administrators or executives would be encouraged to self-assess and review the criteria on a periodic basis**
5. When an SP is onboarding new employees; this material would be reviewed when these new employees are being added as Site Administrators/Executives
6. This material could be surfaced on a 'InCommon Technical Eligibility' page***
7. This material could be surfaced on a 'New InCommon Participant' landing page

*Following along the necessary steps for joining InCommon , once the organization's Executive and Administrator are named (step 5), these individuals could be tagged to follow (or delegate) the questionnaire for additional onboarding guidance. Note: This touchpoint being the first time the organization sees this material, however Identity Provider Organization's should still have the ability to resurface this same information during their engagements with SPs.

**Either regularly (yearly email to execs/admins) or as the documentation changes in a significant way.

***Any interested service owner or Service Provider could review the material as part of gaining a brief understanding of what InCommon is and the necessary technical requirements towards becoming an operational participant in the InCommon federation. This material serving as a baseline and a 'what to expect' before an SP decides to dive in and join InCommon.

# Appendix D. Working Group Consultation - FAQ

For a summary of the common questions that arose during the creation and consultation of the working group material:

1. Who should maintain the SP questionnaire over time, as the federation involves?

The working group envisions this material falling into the larger InCommon documentation repository; following the established lifecycle for documentation review and refreshes. Possibly tagging specific subject matter experts to speak to more specific/technical aspects of the material. And as a general approach with keeping this documentation fresh, establishing a consistent cycle for review (semi-annually or annually) that may vary in frequency depending on the technology trends or "disruptions" that happen over the course of the year.

2. Are Service Providers (SP) expected to follow the questionnaire once or on an recurring basis?

At a minimum, SPs should fill out the questionnaire at least once. And then generally speaking, the recommendation is for Service Providers to use their discretion for whether it would be advantageous for them to fill out the questionnaire more than once or on an annual basis. For example, if a Service Provider made a major upgrade to their application that impacts how they handle attributes, authorization, or metadata consumption, then revisiting the questionnaire could be very useful to ensure their application stays aligned with InCommon standards and recommendations. Or if InCommon finds the material changing substantially, then a formal email outreach to InCommon Administrators/Executives.

3. Should the questionnaire results be shared? And if so, how and to whom?

Until the adoption of the questionnaire reaches a critical mass, it's expected that an individual Service Provider's results will remain private and only be shared ad hoc on a per request/per engagement basis. In a later phase of this work, it's foreseeable that a Service Provider's questionnaire result (or "SP Onboarding Profile") would be uploaded to a central web space to then be selectively, or more broadly shared, to InCommon participants. For example, during an engagement, an IDPO could request access to an SP's questionnaire result; to jumpstart engagements, level set knowledge and capabilities, and quickly raise those red flags that can be addressed earlier in the onboarding process.

4. If a Service Provider (SP) is not meeting the standards or criteria within the 'Criteria Document' or 'Questionaire', who pushes for and/or owns the remediation steps?

The tone and direction of the questionnaire were meant to make this material as self-service as possible. Using this material, the Service Provider ideally has the information and resources they need to make adjustments to their application and realign with the standards completely on their own. IDPOs are not obligated to make these adjustments, directly or indirectly, on behalf of the SP.

For those SPs that insist on becoming an InCommon participant however are not meeting the minimum criteria, the decision falls onto InCommon as far as what level of enforcement should be made to restrict or deny InCommon participation. An interim strategy may be, using the Questionnaire results, InCommon may feel comfortable “flagging” those Service Providers for being at elevated risk; a dataset that may fuel security monitoring or followup outreach efforts. As the SP community and InCommon tooling maturity increases, automated checks and restrictions could be enforced as part of the SP onboarding process.

5. Is additional guidance needed for InCommon/federation operators on consulting with SPs regarding multiple endpoint registrations?

More discussions are needed for whether InCommon or federation operators should push back on SPs that are registering a new endpoint for every institution or campus engagement. At this time, this working group felt this would be a general recommendation, as opposed to a hard requirement, but would not be appropriate to be included in the ‘Criteria Document’ at this time.

# Appendix E. Further Developments and Opportunities for this Material

A couple of the items/topics that this working group felt were out of scope, but deserving of future consideration or possibly dedicated resources:

1. Establish the central web space to host this material. This web space should be surfaced as a landing page where prospective participants, newly joined, or existing participants would land to review and reference the material. The main InCommon Federation would likely be a starting point: https://incommon.org/federation/ This landing page can then be consistently called out and referenced by InCommon during SP onboarding and by IDPOs during SP engagements.

2. Coupling this central web space with a strong/clear value statement to help provide clarity around the ‘Why join InCommon?’ question and that would fuel the SP’s motivation to adopt InCommon standards and criteria. For example, the existing online material (https://www.incommon.org/federation/partners.html) should be updated to exemplify these value adds. Taking this further, more supporting documentation is needed for the visual representation of the caveats and overhead associated with 1-1 or bilateral metadata integrations as opposed to leveraging the multilateral federation for metadata exchange (see Primer Document for examples).

3. Establish a pilot to further vet the working group’s material. This pilot would tag select onboarding Service Providers to follow the questionnaire and report back on first impressions and feedback. Or otherwise, a ‘soft release’ to pilot the material by hosting on the InCommon web space and asking for SP volunteers to fill out and report back on the questionnaire.

4. Google Forms was chosen as the tool to implement the questionnaire in order to demonstrate the questionnaire style approach to this information. However if necessary, the current Google Forms questionnaire could be ported to another commercial or open source tool.

5. Automating Criteria Assessment - where an SP would be automatically validated against a set of criteria. For example, an SP's configuration or metadata could be exported and then be validated to conform to certificate and metadata best practices and standards.

6. This working group recommends the formalization of a testing federation that Service Providers could utilize to validate their configuration before entering into any engagements with Identity Provider Organizations. For example, does InCommon have a testing service they are creating or would they be backing an existing service (http://www.testshib.org/) for recommended use? For purposes of this working group, this material was deemed to be out of scope.

7. This working group felt that any best practices or criteria that fell too far outside of the SP onboarding process were out of scope. For example, as alluded to earlier in this report, once an SP is onboarded as a InCommon participant, there needs to be work to establish the operational standards and best practices for SPs to follow (i.e. security measures, user/access deprovisioning, etc) as part of their overall service lifecycle in the federation.

# Appendix F. InCommon Service Provider Onboarding - Questionnaire

Quick reference to the InCommon Service Provider Onboarding - Questionnaire

# Appendix G. InCommon Service Provider Onboarding - Criteria Document

Quick reference to the InCommon Service Provider Onboarding - Criteria Document

# Appendix H. InCommon Service Provider Onboarding - Primer Document

Quick reference to the InCommon Service Provider Onboarding - Primer Document