Repository ID: TI.35.1 (note this document has a Repository ID assigned but it will not be placed in the Trust and Identity Document Repository until final and approved)
Authors: Tom Barton and members of the InCommon AAC
Sponsor: InCommon Assurance Advisory Committee (AAC)
Superseded documents: (none)
Proposed future review date: TBD
Subject tags: InCommon, federation, assurance, trust, framework

(DRAFT) Processes to Implement and Maintain Baseline Expectations of InCommon Participants

In recognition of the importance of the on-going and gradually increasing level of trustworthiness needed in federation transactions, InCommon Participants have established Baseline Expectations as one means to define what they expect of each other, and of InCommon Operations. As a baseline, federation members must meet or exceed this level of trustworthiness. The processes defined below are the means by which InCommon and InCommon members can hold each other accountable for meeting these expectations, and to establish rough consensus on how these expectations should be observed in specific operational circumstances.

The processes defined below fall into several categories. Some are mostly automated processes undertaken by InCommon Operations that are designed to help members keep their federation metadata aligned with Baseline Expectations. Another defines how the member community can establish their consensus on how Baseline Expectations should be observed in specific operational circumstances, e.g., whether security practice XYZ meets the expectation that “Generally-accepted security practices are applied” to an IdP or SP. There is also a process by which a member’s potentially non-compliant practice can be assessed and any needed mitigation agreed by peer members.

These processes all aim to help members understand when and how they deviate from meeting Baseline Expectations and provide help to get them back on track. But in the worst case, when a member is not meeting expectations and no remedial course of action is available, their non-compliant entities are altered or removed from federation metadata under authority given to InCommon in the Participation Agreement and in accord with its Federation Operating Policies and Practices.

The overall result of operating these processes is that all InCommon entities meet Baseline Expectations - not 100% perfectly 100% of the time, but deficiencies are diligently identified and corrected in a reasonable period of time.

I. Community Consensus Process for Interpreting Baseline Expectations and Acceptable Operations

Baseline Expectations contain requirements that are expressed at a high level and need interpretation to determine how they apply to specific operational circumstances. This section describes how the community develops guidance for how to interpret these statements.

1. A question is raised on technical-discuss@incommon.org or on participants@incommon.org.
2. Assurance Advisory Committee (AAC) members facilitate discussion as needed to reflect points of agreement and disagreement. They may also
    a. Invite other parties to the discussion (such as Executive Contacts or other subject matter experts that may help the discussion to reach consensus), and
    b. Generally move the discussion towards consensus.
3. As a result of the discussion, the AAC may
    a. Provide provisional interpretative guidance for the community on a related web page, and a Consultation Process is conducted to finalize the provisional guidance. The result is published in the InCommon Newsletter.
    b. Identify suggestions that would materially change Baseline Expectations and add them to a public Baseline Expectations changelog to be considered in the next Baseline Expectations revision process.
    c. Determine that a matter is better approached as a potential assurance profile or by other means and add it to a public list of prospective work items for InCommon and its community.

II. Community Dispute Resolution Process

The Community Dispute Resolution Process is used to address concerns that may arise about some aspect of an entity's operation from the perspective of meeting Baseline Expectations. Items that can be automatically checked or verified are detailed in Appendix A and supported by InCommon Operations to ensure accuracy of metadata in conformance with Baseline Expectations.

Dispute resolution proceeds by stages, using an informal and lightweight method at first, and progressing to further formality and rigor only if needed.

First Stage

When a Concerned Party believes they have noticed something about a Participant's operation that may not meet Baseline Expectations, they should use published contact information to try to resolve the concern with Participant informally and directly. InCommon need not be made aware of the concern or its successful resolution.

Second Stage

If the First Stage does not produce a successful resolution, the Concerned Party may elect to email InCommon Support (admin@incommon.org) with a description of the concern and request that InCommon try to address the concern with the Participant. InCommon Operations make an initial determination if the concern may constitute a violation of Baseline Expectations or if it should be treated as a Security Incident, in which case the Computer Security Incident Response Team will be notified and the issue will be tracked according to that process. If neither, they reply to the Concerned Party to that effect and try to advise an alternate course to address their concern.

If the concern may constitute a violation of Baseline Expectations, InCommon Operations opens a ticket to track this matter. The ticket records details such as description of concern, dates, concerned parties and their contact info. InCommon Support contacts the Participant to bring the concern to their attention and requests that the Participant try to resolve the matter directly with the Concerned Party. If Participant agrees to this, InCommon Support updates the ticket accordingly and periodically checks with the Concerned Party and with the Participant to see if the matter is being addressed to their mutual satisfaction. This stage continues until either both parties agree that the matter is resolved, or either party wishes to use the Third Stage to continue addressing the concern.

Third Stage

InCommon Support notifies the Assurance Advisory Committee (AAC) of the issue and provides the ticket. AAC makes an initial determination if the concern may have merit as a Baseline Expectations violation. If not, it passes it back to InCommon Support to reply to the Concerned Party, as in the Second Stage. Otherwise the matter is added to the AAC Docket. A summary of matters pending in the AAC Docket is maintained in AAC's public space. Each docketed matter is processed as follows.

AAC notifies Participant of its intent to formally review the concern on behalf of the InCommon community, describes what is expected of the Participant and cycle times of the review process, and requests a reply that explains either why the concern does not constitute a violation of Baseline Expectations, or a plan to satisfactorily mitigate the basis for the concern. In parallel, AAC selects at random 3 peer reviewers from the set of Technical or Security contacts (depending on the nature of the concern) and 1 peer reviewer from the set of Executive contacts

and invites them to participate in this review. Process continues until a Review Board of 4 panelists is assembled. AAC + Review Board reviews materials submitted by Participant, further engages with the Participant or Concerned Party as they may wish to better understand the matter or to help Participant understand whether their proposed mitigation will be satisfactory.

If in the sole judgment of AAC + Review Board this process results, within 2 months, in either vacating of the concern by the Concerned Party or agreement by Participant to implement a satisfactory mitigation in a reasonable time frame, the AAC Docket is updated accordingly, InCommon Support is asked to update the ticket accordingly, and InCommon Support requests Participant to notify it when implementation is complete. The Review Board is discharged.

If this occurs within the agreed time frame, the ticket is updated with this information and then closed. If not, InCommon Support contacts the Participant to confirm whether the implementation has occurred.

If not, and if implementation is not imminent, InCommon Support notifies AAC of the lack of compliance. AAC updates the Docket to show lack of compliance, as does InCommon Support the ticket. The matter is referred to InCommon Steering with a recommendation to remove the Participant's infringing entity or entity attribute(s) from the federation until such time as the Participant demonstrates implementation of the agreed mitigation or otherwise demonstrates compliance with Baseline Expectations. Compliance is solely judged by the AAC. If InCommon Steering accepts AAC's recommendation, the Process to Notify InCommon Community of Intent to Alter Participant Metadata is followed. If InCommon Steering doesn't accept the recommendation, record the reason in the ticket and close it.

III. On-Going Federation Operational Processes

As the Federation Operator adhering to Baseline Expectations, InCommon Operations implements several processes to ensure that members' federation metadata is accurate. These help address the Baseline Expectation of IdPs and of SPs that "Federation metadata is accurate, complete, and includes site technical, admin, and security contacts, MDUI information, and privacy policy URL", and also partially fulfill the Baseline Expectations of InCommon Federation Operations "Focus on trustworthiness of their Federation as a primary objective and be transparent about such efforts", and "Good practices are followed to ensure accuracy and authenticity of metadata to enable secure and trustworthy federated transactions". For more information on this process, see Appendix A.

Process to Notify InCommon Community of Intent to Alter Participant Metadata

This process is a prerequisite for InCommon Operations removing or altering Participants' metadata due to lack of adherence to Baseline Expectations. Changes to metadata

necessitated by response to a security incident are handled through the InCommon Security Incident Handling Framework.

InCommon Operations will use this process under the following circumstances as a last attempt to notify a Participant organization of an identity provider or service provider that is out of compliance and that InCommon metadata will be altered to address the non-compliant entity:

1. InCommon Operations metadata checking, as described in Appendix A, has failed to elicit a required correction by the Participant to its entity metadata.
2. The InCommon Steering Committee, upon accepting the recommendation of the Assurance Advisory Committee (AAC), given after unsuccessfully exhausting all avenues of collaborative resolution of a compliance concern raised by a federation member, requests InCommon Operations to take this step towards altering federation metadata to remove or alter the Participant's non-compliant elements.

Process

1. InCommon Operations updates the AAC Docket (in circumstance #2) or adds to the AAC Docket (in circumstance #1) describing why this Participant's entities have arrived at this process, e.g., non-responsive to Error URL being corrected.
2. The VP or AVP for Trust & Identity personally messages the Executive Contact at the Participant to notify them of the status of their identity or service provider under concern.
3. The AAC Docket is published in the InCommon Newsletter monthly along with contact information to enable other parties the opportunity to speak up or make any corresponding changes, and functions as *Last Call* to infringing Participants before their metadata is really removed or altered.
4. If the issue has not been addressed within 30 days of the newsletter having been distributed, the entity will be removed or altered.

IV. Baseline Expectations Website

A Baseline Expectations website makes all Baseline Expectations related information publicly available. Purposes of various website pages include:

- The Baseline Expectations themselves. This is the page linked in the Federation Operating Policies and Practices (FOPP) and Participant Agreement (PA) rather than inserting Baseline Expectations-specific wording into those agreements. It is referred to appropriately from the incommon.org website.
- Summary of the Baseline Expectations maintenance processes incorporating links to related Baseline Expectations website pages.
- Page reporting on the "Maintain Accuracy of Contact Info in Metadata" process, including stats and metrics such as date of completion of last cycle, date of next cycle, stats on #

updated addresses/cycle, # entities moved to “Process to Notify InCommon Community of Intent to Remove Entities from Metadata”/cycle.

- Page reporting on the “Process to Notify InCommon Community of Intent to Alter Participant Metadata”, including stats on when which entities were put on notice, ultimate disposition of those, date of next cycle.
- Page reporting on the “Maintain Accuracy of Contact Info, MDUI, Error and Privacy URLs in Metadata” process in Appendix A, similar to the above pages.
- Page publishing provisional and final statements of acceptable or unacceptable operations arising from the “Community Consensus Process for Interpreting Baseline Expectations and Acceptable Operations” process, with dates.
- Page publishing suggestions for future changes to the Baseline Expectations themselves.
- Page publishing activity of the “Community Dispute Resolution Process”, including parties, summary of the dispute/concern, dates of entry into Second and Third Stages, resolution and either date of remediation or date of recommendation to Steering to remove Entity or its infringing attribute(s) from metadata, Steering decision and date.

Appendices

Appendix A: Maintain Accuracy of Contact Info, MDUI, Error and Privacy URLs in Metadata

Following is a progression of steps taken to validate currency of each entity’s contact info, MDUI, Error and Privacy URLs in metadata. Steps 3 onwards are only taken if preceding ones do not conclude satisfactorily. Groups of entities may be put on different cycles to manage the effort required.

1. Send email to each email contact with an embedded code so that replying to the email will automatically update an associated database, eg, as commonly supported by listserv software. Do this every 6 months.
2. Monitor MDUI, Error and Privacy URLs for an acceptable response and if any fail continuously for 2 weeks, notify the participant.
3. Run a report on the database after the notification or reply has expired (2 weeks) and send a follow up to non-respondents.
4. Run another report after 2 weeks and send a follow up to executive contact (which is not kept in metadata) of non-respondent Participants.
5. Send 2nd notice to executive contact if no answer after 2 weeks.
6. Phone call to executive contact. At least 3 tries over 2 weeks.
7. Use Process to Notify InCommon Community of Intent to Alter Participant Metadata.
    a. Notices due to unverified contact information or unacceptable MDUI, Error or Privacy URLs should state clearly that (1) InCommon is using this means as a last resort to contact someone at Participant to resolve the issue, which is the

desired outcome, (2) if no contact can be made after 1 month, InCommon will have no choice but to remove or alter Participant's $Entity metadata on $Date, and (3) the specific basis in the FOPP or PA for that action, if no contact is made.

b. This should be a personal note from VP/AVP of T&I.

Appendix B: Diagram of Community Dispute Resolution Process