Processes to Maintain Baseline Expectations by InCommon and its Members

September 14, 2017

Repository ID: TI.35.1
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Superseded documents: (none)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

© 2017 Internet2
This work is licensed under a Creative Commons Attribution 4.0 International License.

Processes to Maintain Baseline Expectations by InCommon and its Members

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 Participants 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 that are designed to help Participants keep their federation metadata aligned with Baseline Expectations. Another defines how the Participant 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 specific Participant’s practice can be assessed against Baseline Expectations and any needed mitigation agreed by peers.

These processes all aim to help Participants 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 federation entity is not meeting expectations and no remedial course of action is available, the entity is altered or removed from federation metadata as recommended by the InCommon Assurance Advisory Committee (AAC) upon approval being given by the InCommon Steering Committee under authority given it by the Participation Agreement (PA) and in accord with InCommon’s Federation Operating Policies and Practices (FOPP).

The overall result of operating these processes is that all InCommon entities meet Baseline Expectations - not 100% perfectly 100% of the time, but variances 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 may 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 about how Baseline Expectations applies to a given operational circumstance is raised in a manner to be defined by the AAC.
2. 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, CIOs, or other subject matter experts that may help the discussion to reach consensus), and
    b. Generally try to 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 conduct a Consultation Process 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. This process is one means of fulfilling the requirements of the Dispute Resolution Procedure defined in Section 8 of the FOPP. Items that can be automatically checked or verified are detailed in Appendix A and supported by InCommon 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 the 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 (admin@incommon.org) with a description of the concern and request that InCommon address the concern with the Participant. InCommon staff make an initial determination if the concern relates to meeting Baseline Expectations or if it should be treated as a security incident, in which case the InCommon 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 relates to meeting Baseline Expectations, InCommon opens a ticket to track this matter. The ticket records details such as description of concern, dates, concerned parties and their contact info. InCommon staff contact the Participant and a Registered Contact from the Concerned Party's member organization 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 staff notify the AAC of the concern and provide the ticket. AAC makes an initial determination if the concern relates to meeting Baseline Expectations. If not, it passes the ticket back to InCommon staff to reply to the Concerned Party, as in the Second Stage. Otherwise the matter is added to the AAC's Docket. A summary of matters pending in the Docket is maintained in the Baseline Expectations website. 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 matter of concern does not contradict Baseline Expectations, or a plan to satisfactorily mitigate the basis for the concern. In parallel, AAC empanels a Review Board, if one is not already empaneled, by selecting 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 or Participant senior IT management 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 Docket is updated accordingly, InCommon is asked to update the ticket accordingly, and InCommon staff requests Participant to notify it when implementation is complete.

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

If implementation of the agreed mitigation has not been completed, or if it is not imminent, InCommon staff notify AAC of the lack of agreed implementation. AAC updates the Docket to reflect this status, as does InCommon the ticket. The matter is referred to InCommon Steering with a recommendation to remove the concerned entity or entity attribute(s) from federation metadata until such time as the Participant demonstrates implementation of the agreed mitigation or otherwise demonstrates that the entity meets Baseline Expectations. This is solely judged by the AAC. If the InCommon Steering Committee accepts AAC's recommendation, the Process to Notify InCommon Community of Intent to Alter Participant Metadata is followed. If the Steering Committee doesn't accept the recommendation, record the reason in the ticket and close it.

A Review Board is empaneled for a 4 month period, participates in any Third Stage matters in the Docket during this period, and then is discharged.

III. On-Going Federation Operational Processes

As a Federation Operator adhering to Baseline Expectations, InCommon implements several processes to ensure that Participants' 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 "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 followed when InCommon is required to remove or alter Participants' metadata as the last step in two of the processes described in this document, as noted below. Changes to metadata necessitated by response to a security incident are handled through the InCommon Security Incident Handling Framework.

InCommon 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 does not meet Baseline Expectations and that the entity will be altered or removed from InCommon metadata:

1. InCommon 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 AAC, given after unsuccessfully exhausting all avenues of collaborative resolution of a Baseline Expectations concern raised by a federation member, authorizes InCommon to take this step towards altering federation metadata to remove or alter the identified entity.

Process

1. InCommon updates the AAC's Docket (in circumstance #2) or adds to the Docket (in circumstance #1) describing why this entity has 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 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 the concerned Participant before their entity's metadata is 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 as authorized.

InCommon will ensure that appropriate controls are in place to mitigate the possibility of an unauthorized reinstatement of an entity altered or removed by this process.

IV. Reinstatement

An entity that was removed or altered per the above process can be reinstated to InCommon metadata as follows.

1. If the entity was altered or removed by the processes defined in Appendix A, then
    a. Either the Participant's Technical or Executive Contact or a Site Administrator may make a request to InCommon to reinstate the entity to its federation metadata. The request must contain a copy of the entity metadata proposed to be reinstated.
    b. InCommon staff will determine whether or not the entity metadata submitted with the request meets the criteria of the processes defined in Appendix A and

reinstates the metadata if it does. Either way, this outcome will be reported on the Baseline Expectations Website.

2. If the entity was altered or removed upon the recommendation of the AAC as the final outcome of the Community Dispute Resolution Process, then
    a. The Participant's Executive Contact must make a request to InCommon to reinstate the entity to its metadata. The request must contain a description of the mitigation that was implemented to address the concern that led to its entity being altered or removed.
    b. InCommon will refer the request to the AAC, who will review the mitigation and determine whether or not it results in the entity meeting Baseline Expectations.
    c. The AAC will communicate its decision to InCommon staff, who will reinstate if that is the AAC's recommendation. Either way, this outcome will be reported on the Baseline Expectations Website.

V. Publication of the Operation of These Maintenance Processes

A Baseline Expectations website makes all Baseline Expectations related information publicly available. The InCommon Newsletter is also used to publish some of this information. Between them, the following materials shall be published:

- The Baseline Expectations themselves. This is the page linked in the FOPP and 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 (this document) incorporating links to related Baseline Expectations website pages.
- Metrics on the "Maintain Accuracy of Contact Info, MDUI, Error and Privacy URLs in Metadata" process in Appendix A, 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.
- Metrics on the "Process to Notify InCommon Community of Intent to Alter Participant Metadata", such as when which entities were put on notice, ultimate disposition of those, date of next cycle.
- 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.
- Suggestions for future changes to the Baseline Expectations themselves.
- Activity of the "Community Dispute Resolution Process", i.e., the AAC's Docket, 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 the Steering Committee to alter or remove the entity from federation metadata, Steering Committee 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 information, Error and Privacy URLs in federation 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 information, Error and Privacy URLs for an acceptable response and if any fail continuously for 2 weeks, re-notify the associated contacts.
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 or a senior IT manager (which is not kept in metadata) of non-respondent Participants.
5. Send 2nd notice to Executive Contact or senior IT manager if no answer after 2 weeks.
6. Phone call to Executive Contact or senior IT manager. Repeat 3 tries over 2 weeks if necessary.
7. Use Process to Notify InCommon Community of Intent to Alter Participant Metadata.
    a. Notices due to unverified contact information or unacceptable MDUI information, 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.

Appendix B: Diagram of Community Dispute Resolution Process