2016-07-11

InCommon Steering Committee Meeting - July 11, 2016

Minutes

Attending: Ann West, Michael Gettes, Von Welch, Susan Kelley, Pankaj Shah, Melissa Woo, Steve Carmody, Sean Reynolds, Ted Hanss

With: Nick Roy, Dean Woodbeck, Ken Klingenstein, Kevin Morooney

Action Items

(AI) Ann West will distribute a proposed resolution for the development of the InCommon Incident Response Policy and Procedures and Reporting Document for a vote via Wisegate.

June Minutes

Approved via Wisegate

InCommon Ops Review

Nick Roy provided an update on the InCommon Ops Review, an extensive process conducted in the summer of 2015, reviewing and prioritizing all of the aspects of InCommon operations. Steering has previously reviewed and voted on these priorities; this is a review and update.

Guiding principles for the review:

1. Trust and security of InC operations
2. Availability
3. Responsiveness
4. Adequate change management
5. Balance agility with formalism in project planning

Seven core recommendations coming out of the review (see the slides for details)

1. Adopt ServiceNow (ticketing)
2. Set SLAs/OLAs and measure against them
3. Address staffing shortfalls
4. Document the trust model
5. Engage a security officer for InCommon
6. Adopt lightweight change management activities
7. Update DR-BC plans

After reviewing these seven areas, there were some questions.

Q - Could we use ServiceNow instead of JIRA for issue tracking for software? A - Yes, but JIRA is what we have today and it's seen as best of breed by parties within Internet2. It also aligns with Confluence.

Q - Is there an opportunity as we review/revise onboarding operations to promote attribute release policies that align with the Research & Scholarship Category? A - Yes, there are discussions in the works. In addition, Internet2 community engagement staff are interviewing several InCommon participants about the attribute release policies current used. They are asking about three broad scenarios:

1. B2B - campuses accessing services is in the cloud (generally with a contract with a provider)
2. Individual-to-organization - this is the collaboration use case. We know we have some participants releasing the necessary R&S attributes to InCommon participants but not eduGAIN.
3. Blanket release - releasing a set of attributes to all services

This will result in a report for Steering, and will also be shared with key registrars in the AACRAO community to determine next steps. The purpose of this first step is discovering what people do; not promoting any particular policy.

InCommon Path Forward

Kevin provided background on the "deep dive" and "path forward" meetings which will wrap up this month. In May, a few community members reviewed all of the issues facing Trust and Identity in Internet2. Meetings in July are focusing on TIER (already completed) and InCommon (to be completed this week). Among other issues, the InCommon meeting will touch on:

1. What is needed by the Shibboleth Consortium, as InCommon and participants have a profound dependency on Shibboleth.
2. The prospect of Increasing InCommon participation fees.
3. Thoughts on the growth and changing demographics of InCommon and how that will affect the demand for support and scoping of services

InCommon management will combine the assets from all of these meetings and prepare the findings, to be shared with InCommon Steering and the TIER Community Investors Council at the September 26 meeting at TechEx.

Proposed Change - Federation Operation Policies and Practices (FOPP)

Steve Carmody brought forward a proposal from the InCommon TAC for a change in section 10.3.1 of the FOPP, giving InCommon management the authority and scope to act when the security of Federation services or the trustworthiness of the published metadata file might be impacted. One concern is with the large number (about 70%) of identity providers still operating Shibboleth IdPv2, which goes end of life on July 31, 2016. After that time, there will be no security updates. While there have been no problems to date, it seems prudent to be prepared.

TAC recommends changing the FOPP section 10.3.1 as follows:

> **Current 10.3.1 Suspension for reasons of security**
>
> A Participant may request the suspension of any Federation services in the case of Administrator credential compromise, participant key compromise, or other security compromise within the Participant's systems. This request may be made via e-mail or telephone from the Executive or Administrator and will be verified by InCommon using trusted communication channels. Suspension may include processes such as revoking credentials, or removing or modifying Metadata.
>
> If InCommon suspects any compromise or negligence on the part of a Participant, it will make reasonable efforts to contact Participant to verify Participant's status. For example, a non-responsive Administrator's account may be suspended for the security and safety of Participant's Metadata if InCommon suspects an Administrator is no longer active and its repeated attempts at contact go unanswered.
>
> **Recommended new second paragraph of 10.3.1:**
>
> If InCommon suspects any compromise or negligence on the part of a Participant, it will make reasonable efforts to contact Participant to resolve the issue. In the case of a significant security incident that poses an unacceptable risk to InCommon or other federation participants, InCommon may take immediate remediation actions commensurate with the impact of the incident.

TAC also recommends that InCommon Steering direct management to move quickly to develop, obtain community consensus around, and promulgate an InCommon Incident Response Policy and Procedures and Reporting Document. This could be done with the help of one or more campus security officers (and others as needed).

Steve pointed out that removing an IdP from the metadata, the ultimate remediation action, would be a huge step and one which would break a lot of services for many campuses. InCommon would take multiple steps to work with a campus to resolve problems before taking the step of removing from metadata. However, this language is needed in order to create the needed pressure on campuses.

In addition to the incident response policy, InCommon will also develop a document that outlines the most likely scenarios and actions that would be taken; a playbook to use if necessary.

There was discussion about setting a deadline for the development of the Incident Response Policy and Procedures and Reporting Document. It is likely that an interim policy could be developed in a fairly short time frame, but the playbook would take longer. TAC did not discuss a deadline. It would be helpful, though, to have this completed in November, before the membership in Steering changes for the 2017 year.

> **Resolution: Change in FOPP**
>
> Michael Gettes moved and Melissa Woo seconded approving the proposed change to the second paragraph of section 10.3.1 of the FOPP. The motion passed unanimously. The second paragraph of Section 10.3.1 now reads:
>
> *If InCommon suspects any compromise or negligence on the part of a Participant, it will make reasonable efforts to contact Participant to resolve the issue. In the case of a significant security incident that poses an unacceptable risk to InCommon or other federation participants, InCommon may take immediate remediation actions commensurate with the impact of the incident.*

(AI) Ann West will distribute a proposed resolution for the development of the InCommon Incident Response Policy and Procedures and Reporting Document, distribute that by email to InCommon Steering, for a vote via Wisegate.

Next Meeting

August 1, 2016 - 4 pm ET