

2020-Feb-11 CTAB Public Minutes

CTAB Tuesday Feb. 11, 2020

Attending

- David Bantz, University of Alaska (chair)
- Mary Catherine Martinez, InnoSoft (vice chair)
- Rachana Ananthakrishnan, Globus, University of Chicago
- Tom Barton, University Chicago and Internet2, ex-officio
- Brad Christ, Eastern Washington University, InCommon Steering Representative to CTAB, ex-officio
- Ercan Elibol, Florida Polytechnic University
- Richard Frovarp, North Dakota State
- Chris Hable, University of Michigan
- Chris Whalen, Research Data and Communication Technologies
- Jule Ziegler, Leibniz Supercomputing Centre
- Albert Wu, Internet2
- Emily Eisbruch, Internet2
- Kevin Moroney, Internet2

Regrets

- Pål Axelsson, SUNET
- Brett Bieber, University of Nebraska
- Eric Goodman, UCOP - TAC Representative to CTAB
- Jon Miner, University of Wisc - Madison
- John Pfeifer, University of Maryland
- Robert Zybeck, Portland Community College
- Ann West, Internet2

Action Items from Last Call

- AI - Chris W will conduct a doodle poll or other survey to find out what will work best for a 2020 CTAB F2F (DONE)
- AI - Albert work with a CTAB volunteers (Pal, perhaps DavidB and Brett and Jon) to create and present Global Summit lightning talk. Global Summit is March 29-April 1, 2020 in Indianapolis, IN

Discussion

Finalize the invitation to community consultation for BE v2

- Albert will handle adding links/references at end
- **Questions about SSL Labs grading A or B**

Suggested wording:

Popular security testing software such as the Qualys SSL Lab Server test [**SSLLab**] offers a convenient way to test your server against these criteria and identify weaknesses. If using the Qualys SSL Lab Server test, an overall rating of A or better is considered meeting the requirements of the InCommon Baseline Expectations

- We want trustworthiness in the federation where all connected to the Federation is in harmony on what constitutes a secure posture
 - Counterbalancing force is the community's desire that we make things easier to use
 - For baseline, what should the base standard be?
 - Concern that requiring everyone to have an A grade could alienate some
 - Some orgs need to provide legacy browser support and that forces them to allow compatibility mode.
 - That results in grade of B in SSL grading.
 - There may be a way to declare yourself an exception if you can't make the SSL Lab grade
 - we could require those who can't achieve A to file a notice that they can only achieve B
 - Even with an A+ you are not eliminating all risk of attacks
 - It is about diligence over time
 - Chris Whalen notes that all systems at NIH must be A+ and he believes baseline expectations should require A grade
 - Mary Catherine's organization, InnoSoft, requires A grade
 - Suggestion: set A as the bar
 - If during community consensus we learn that many can't make A, then maybe reconsider. Also have an exception process.
 - **Kevin:** We want InCommon Federation to be more trustworthy
 - Suggestion to require A or better and provide qualifications later
 - **DECISION: stick with requirement of Grade A**
- **Error URL**
 - Albert notes that REFEDS has included Pal's proposal to define additional errorURL syntax extension in its 2020 work plan
 - It's worth tracking along side this item.
 - <https://wiki.refeds.org/display/WOR/2020+Workplan>

- **Appendix A: Additional Expectations coming in 2021 and beyond**

- Include rationale for why we are not including the items for future (such as REFEDS MFA) in this round of Baseline Expectations but saving them for future round
- Albert and David will add this wording

Communications

- CTAB should have a communications plan around the **Invitation to Participate** document and community consensus process
- Reach out to Dean Woodbeck, Internet2 for development of communications plan.
- Suggestions:
 - Engage InCommon Steering in getting the community's attention
 - Suggestion: Invite 20 random IDPs and SPs to meet with CTAB to provide feedback
 - Suggestion: do targeted outreach to ask organizations to participate in the consensus process
 - A technique used for the InCommon Fee Increase conversation: there were 4 **open office hours** Zoom calls. There was fairly low participation in these open office hours Zoom calls.

Next CTAB call: Tuesday, Feb. 25, 2020