

# 2020-Feb-25 CTAB Public Minutes

## CTAB Tuesday, Feb. 25, 2020

### Attending

- David Bantz, University of Alaska (chair)
- Mary Catherine Martinez, InnoSoft (vice chair)
- Pål Axelsson, SUNET
- Brett Bieber, University of Nebraska
- Tom Barton, University Chicago and Internet2, ex-officio
- Brad Christ, Eastern Washington University, InCommon Steering Representative to CTAB, ex-officio
- Ercan Elibol, Florida Polytech Institute
- Richard Frovarp, North Dakota State
- Eric Goodman, UCOP - TAC Representative to CTAB
- Chris Hable, University of Michigan
- Jon Miner, University of Wisc - Madison
- Robert Zybeck, Portland Community College
- Ann West, Internet2
- Albert Wu, Internet2
- Emily Eisbruch, Internet2
- Nick Roy, Internet2
- Shannon Roddy, Internet2

### Regrets

- Rachana Ananthakrishnan, Globus, University of Chicago
- Chris Whalen, Research Data and Communication Technologies
- Jule Ziegler, Leibniz Supercomputing Centre
- John Pfeifer, University of Maryland

## DISCUSSION

### CTAB meeting time update

- “daylight savings time” (starts 8 March in US) (see options below)

### Ramping up Consensus Process (David)

- [Invitation to Participate in Baseline Expectations 2.0's Community Consensus Process](#) (DO NOT INCLUDE LINK IN PUBLIC NOTES)
- Decision: use **Baseline Expectations 2** instead of **Baseline Expectations 2.0**
- Suggestion to add mention of channel to communicate concerns confidentially, per the info in the Community Consensus doc. <https://www.incommon.org/federation/community-consensus/>
- Albert will handle adding more detail on how to sign up for the email list [be-consensus@internet2.edu](mailto:be-consensus@internet2.edu)
- For the appendices, the decision was to leave some of the details on future potential BE items (such as MFA), and workarounds, for the discussion rather than include in the document.
- One clarification around MFA is recommended (see Brett's note in the doc)
- Ann will help with editing/shortening the email that will be used with the Invitation to Participate
- Timeline for triggering Community Consensus on BE v2:
  - Set up:
    - Wiki for recording discussion
    - Use existing wiki with version control
    - Initially will contain the Invitation
    - Add health checks as available (from metadata)
    - Email discussion list
  - Advance notice to Steering (approval not required)
- Email to:
  - InCommon Participants list
  - TAC
  - CACTI
  - SiteAdmins
  - InCExs
  - International (REFEDS) powers that be

### Conversation on realistic risks around encrypting endpoints with less than perfect algorithms/cipher (Shannon)

- For the average participant it's OK to specify a required letter grade for Qualys SSL Lab Server test
- Unfortunately, currently there are endpoints that get grade of F

- Shannon's preliminary work in Dec 2019 showed 186 received a grade of F out of 11K endpoints; 1.62% had grade of F
- Some of those may have been resolved
- Raising those that are still at F will be progress
- For things like robot, Shannon is looking to find vulnerabilities
- No such thing as perfect security.
- Shannon notes it is possible to get an A grade on SSL labs test, but still be running an old and vulnerable version of Apache.
- What do we all decide is good enough?
- Some vulnerability items require state actor, others are trivial
- How will we handle exceptions, when an organization has a non A grade but wants to improve?
- Suggestion to have a remediation plan
- For example limiting access to the SP or limiting use of the IDP
- Albert: adherence will likely need to come from self attestation
- InCommon may not have resources to enforce all participants having A grade
- InCommon can provide guidance on how to improve grade on Qualys SSL Lab Server test
- Point to documentation by Apache, Jetty, Load Balancer, or others
- Link to consulting firms (such as Unicon) that can provide help

***Did not discuss this item on the Feb 25 CTAB call:***

- *Updates from REFEDS WGs - errorURL and Baseline (Pal and Tom?) (as time permits)*

**Next CTAB call: Tues., March 10, 2020**