2021-June-29 CTAB Public Minutes

CTAB call Tuesday, June 29, 2021

Attending

- David Bantz, University of Alaska (chair)
- Brett Bieber, University of Nebraska (vice chair)
- Rachana Ananthakrishnan, Globus, University of Chicago
- Ercan Elibol, Florida Polytechnic University
- Richard Frovarp, North Dakota State
- Meshna Koren, Elsevier
- Jon Miner, University of Wisc - Madison
- Andy Morgan, Oregon S tate University
- John Pfeifer, University of Maryland
- Robert Zybeck, Portland Community College
- Tom Barton, Internet2, ex-officio
- Johnny Lasker, Internet2
- Albert Wu, Internet2
- Emily Eisbruch, Internet2
- Ann West, Internet2
- Kevin Morooney, Internet2
- Netta Caligari, Internet2

Regrets

- Pål Axelsson, SUNET
- Eric Goodman, UCOP - InCommon TAC Representative to CTAB
- Dave Robinson, Grinnell College in Iowa, InCommon Steering Rep, ex-officio
- Chris Whalen, Research Data and Communication Technologies
- Jule Ziegler, Leibniz Supercomputing Centre

New Action Item

- AI Andy Morgan - document his approach to TLS endpoint issue and supporting older/legacy TLS versions

Discussion

Internet2 Intellectual Property reminder

Intro to Netta Caligari

- Netta Caligari is the new Internet2 Community Success Manager
- She is based in Fort Collins, Colorado
- Has recent experience working in a start-up around digital engagement
- Worked at Colorado State University previously
- Netta will be working to support Trust and Identity advisory committees
    - She will assist with recruitment of new members for CTAB, onboarding
- She will also be lead for IAM Online, CAMP and Advance CAMP

Responses to Baseline Expectations version 2 (BEv2) email to InCommon Execs & Site Admins

- Email sent out last week around BEv2
- We have received approximately 100 emails related to BE V2 since March 2021
- Each email from InCommon about BEv2 prompts more responses
- Comments include:
    - How do I know if I am compliant?
    - I am not going to meet the proposed deadline of July 19, so letting you know
    - Questions around SIRTFI, what do I need to do?
    - Some confusion around checking the box, email has been modified to clarify
- **Concerns about Qualys Testing Scores**
    - There have been questions about Qualys Testing scores
    - Scores are on dashboard upon sign in to InCommon Federation Manager
        - if you don't have Qualys testing score of A, you are shown as having an action pending
    - People are concerned about not meeting BEv2 because their Qualys score is not A
    - InCommon Ops is updating the flag in Federation manager so the score is not considered
    - Albert will
        - update the Baseline Expectations wiki to explain what the score means
        - continue to work with the community to reply to concerns and questions
- Excellent progress overall, encouraging
- SP adherence to BE jumped from 43% to 59%
    - Probably due to a few participants with a large number of SPs

- We have scores from around June 14
- Increase in number of Qualys scores of A
- Also increase in number of Qualys scores of F, (from a small number of organizations)
  - May be an anomaly
  - They all have a CDN
  - May have caused a false reading of F
  - InCommon staff will look into this
- July 19 is the official date to transition to BEv2
  - https://incommon.org/news/federation-site-admins-receive-baseline-expectations-notices/
  - https://spaces.at.internet2.edu/display/federation/meet-baseline-expectation
- CTAB needs to think about an extension process, in the fall, for those not able to meet Baseline Expectations
- Graph on wiki does not include the Qualys score, so it excludes what's perhaps the hardest part of BE v2
- https://spaces.at.internet2.edu/display/be/
- Score of A is not included in main Baseline Expectations text as being required, it's in implementation guidelines
- We can use discretion, but equity and fairness are important
- The message that "CTAB/the community cares about your encryption" is having an impact
  - organizations are patching servers
- Suggestion to provide more details on when the scan was performed
- Johnny: there is a date linked to when the scan was performed
- Desire for orgs to be able to initiate their own scan
- Suggestion for a **checkbox for those who have performed their own scan**
  - Not now, because of work going on around eduroam, InCommon operations does not have such bandwidth
  - Infrastructure for testing is not set up for one off testing
  - Concern self attestation would create more confusion
  - Need to keep this simple for the site admins who don't pay attention often
  - Any Federation Manager element we change creates some confusion
  - Self attestation around Qualys scan and score could impact how we drive the email campaigns
  - Can IDPs and SPs request a new test when they make changes?
  - Earliest we have InCommon staff availability to change InCommon Federation Manager is 2022
- Suggestion to document how the scan can be performed by the institution to check their infrastructure
- Suggestion for chart on the wiki to represent Qualys scores over time, April 15 and June 23 data points (DONE)
  - https://spaces.at.internet2.edu/display/be/
- Some orgs are intentionally **supporting older/legacy TLS versions because of their use cases**
  - Would be helpful to have a collection of use cases and solutions
  - UCOP system is a reason for a lot of N/As
  - The TLS part, the IDP would get an A if you could get to it, but the WOF in front of it is supporting legacy
  - One issue is concern about making a change and breaking things
  - Trying to come up with a target date, likely won't be as soon as July
  - We should focus on this use case and ways to solve the problem
  - We need to provide more examples of how to address need to support legacy
  - Andy Morgan has use case of needing to support older system, integrating w CAS, need to convince some other organization to update
  - Richard F has a CAS use case
  - John P has a use case, involving load balancer
  - Eric G talking to security team about the adverse security issues in supporting these old protocols
- Next step: Identification of use cases
- Document some of the solutions
- Start with collecting BEv2 solutions in google doc that Albert will share
- AI Andy Morgan - document his approach to TLS endpoint issue and supporting older/legacy TLS versions
- Ann: suggestion for office hours or survey
  - In past office hours, discussion was very general
  - Perhaps ask community members to share their solutions

Did not cover the remaining items on this call

Federation / Operations update (Albert, Johnny)
NIH Assurance work update; AAWG update

- Consultation period has ended
- Next steps: Brett will schedule meeting of the AAWG
- Produce final version of the document

Working Group updates

- REFEDS Assurance
- REFEDS MFA sub-grou

- Schema updates (R&S category ; eduPersonAnalyticsTag
- Others?

NIH Assurance updates
Deployment dive (1st of many) (Albert)

Next CTAB Call: Tuesday July 13, 2021