2020-Aug-11 CTAB Public Minutes

Attending

Members

- David Bantz, University of Alaska (chair)
- Rachana Ananthakrishnan, Globus, University of Chicago
- Tom Barton, University Chicago and Internet2, ex-officio
- Ercan Elibol, Florida Polytechnic University
- Richard Frovarp, North Dakota State
- Eric Goodman, UCOP - TAC Representative to CTAB
- Jon Miner, University of Wisc - Madison
- Chris Whalen, Research Data and Communication Technologies
- Robert Zybeck, Portland Community College

Internet2

- Ann West, Internet2
- Albert Wu, Internet2
- Emily Eisbruch, Internet2
- Jessica Fink, Internet2
- Kevin Morooney, Internet2

Regrets

- Pål Axelsson, SUNET
- Brett Bieber, University of Nebraska
- Mary Catherine Martinez, InnoSoft (vice chair)
- Chris Hable, University of Michigan
- John Pfeifer, University of Maryland
- Marc Wallman, North Dakota State University, InCommon Steering Rep, ex-officio
- Jule Ziegler, Leibniz Supercomputing Centre

DISCUSSION

Next step on Baseline Expectations v2 - what do we need to have ready to move to the community consultation process?

- For Reference, Notes from July 28, 2020 office hours

- Finalized, proposed BE statement with BE2 changes. https://spaces.at.internet2.edu/display/be/ (?)

- Draft Implementation Plan

Secure Endpoints BEv2 Requirement Enforcement

- Rachana:
  - How to enforce the secure endpoints requirement?
  - Adding burden on endpoint owner, can we require owner to submit results to be reviewed?
  - As an SP operator, guidelines that are not enforceable are an issue

- Albert
  - Nick Roy and InCommon team are looking at automated testing
  - Could be a long delay if we hold up the BEv2 until automated testing by InCommon is in place
  - Proposed Guidelines suggest Qualys SSL Lab as a good way to do testing
  - Care around using the word scanning
    - Use the word "inspect" or "detect" when possible
  - The Guidance document expands on the Baseline Expectations
  - Organization attests that they have done due diligence
  - Guidance document suggests using the Open Web Application Security Project's (OWASP) cheat sheets
  - Guidance doc also includes a note about making the endpoints accessible
  - Indicates a 90 day period for addressing
  - Albert will add another paragraph about the InCommon testing plan process
- Summary of SSL Enforcement issue:
  - InCommon will work towards enforcement
  - InCommon is looking at how to record findings and how to do follow up around non compliant finding
  - We start at a certain level, with guidance, and then raise the bar when InCommon is able to do testing

- Should the guidance document state an A grade or a B grade is minimum required in Qualys SSL Lab Server Testing?
- Comment: If we go with requiring a grade of A, and there is pushback, even this might not be so bad, It would raise awareness.
- **Decision:** Guidance doc should state that requirement is for an “A” grade in Qualys SSL Lab Server Testing

- **SIRTFI BEv2 requirement**
    - Albert has added instructions for the federation operator in the guidance document
    - At BEv2 office hours, community member from Elsevier mentioned concerns about whether Elsevier could meet the proposed SIRTFI requirement for BEv2. There are many services in Elsevier. But it was explained that the BE v2 statements only apply to the federation facing aspects. On the BEV2 call, TomB offered to provide help where there are areas of concern around complying with the BE Sirtfi requirement.

- **ERROR URL BEv2 requirement**
    - Albert has added sentence in the guidance document about using the federation manager.
        - "Participant’s Site Administrator accomplishes this by entering the appropriate errorURL when registering the entity using Federation Manager."
    - In best practice for IDPs , Albert added text around legitimate reasons an SP might send back to error URL , and kind of conditions to be prepared for. Borrowed from REFEDs spec.
    - Added working about the REFEDs spec, and some other guidance

Comment about obligations under Baseline Expectations

- TomB: Need to be clear about Baseline Expresses requirements as being obligations and part of the InCommon Participation Agreement contract.
    - https://incommon.org/wp-content/uploads/2019/04/Participation-Agreement-20180312-Rvw-Copy1.pdf
- State at the top of the document the Baseline Expectations are an obligation
- Segment, clearly identify by section, what is guidance and what is required

Next Steps for Baseline Expectations V2

- This is final week of the consensus period according to plan, consensus period ends Aug 15, 2020.
    - as stated in this blog: https://incommon.org/news/baseline-expectations-office-hour-june-30/

- We have held several BEv2 office hours, time to move ahead with schedule.
- Albert will make the changes recommended today
- Will draft BEv2 implementation plan
- At the next CTAB call we will ready the docs for the consultation

Did not discuss on today's call

1. Sirtfi survey
2. Comments on NIST 800-63C

Next CTAB Call: Tuesday, Aug. 25, 2020