

SECURITY COMMITTEE MEETING NOTES

Attendees:

Steve Orrin
Adam Madlin
Adam Migus
Paul Knight
Ryan Galluzzo
Sal D'Agostino
Linda Braun, Global Inventures

Meeting Notes:

Steve Orrin led the call. Notes taken by Linda Braun.

Agenda Review – as distributed by Mary Ellen in advance of the call (approved)

Roll call; Quorum determination. Quorum was met.

IPR policy reminder –

<https://www.idecosystem.org/system/files/filedepot/103/IDESG%20IPR%20Policy.pdf>

Notes taken for September 21, 2015 and October 1, 2015 meetings approved.

Minutes:

- SALS Overview Birds of a Feather discussion:
 - Comments: Open discussion for those who did not see the presentation at the Tampa Plenary. The presentation was sent earlier by Mary Ellen along with the agenda. This is a self-assessment; we are not validating their assessment. When an organization says they have done “xyz” as far as the self-assessment goes, they are done. The organization is also agreeing to the terms that are included.
 - Path A and Path B – not quite seen as black and white. Pilots have shown us that we aren’t going to get entities that are going to fully attest. Could everyone attest to what they feel comfortable with? Path B is ongoing process on way to Path A. Path A – meets conformance.
 - Concern with number of things entities agree to – if they only attest to all Security versus none for Interop as an example. If we find that some requirements are not being attested to across the board that means there is a problem with the requirement.
 - These are recommendations from TFTM to leadership as to what we might do and the recommendations have been accepted. What we are doing is not going to be black and white. Sal shared a presentation with the rest of the Security Committee that was used at the Plenary; it uses Harvey Balls to rank categories. There will be multiple ways that the information is presented in order to get feedback from users so we can learn if we are providing the information in a helpful way. Wants to see visual representation as to how well people did.
 - As we roll this out and get familiarity with participants, it is going to be an evolving process. Someone thought there was a Path A and Path B also clearly identified from an end user perspective. This is going to be difficult to understand. How do they use it and how do they decide to participate? We need to get to a future version where we make it easier for participants. Ease to use is a goal.
 - Graphics is a good way to visually represent the rankings. From an end user perspective, if we start off with “you conform” or “you don’t” is a good way to go. If you don’t achieve all 42 requirements, you are not in conformance right out of the gate. There will likely be a category on conforming. Ranking them would be a good thing to do as well. People can try to get their score up overtime when they go to the list. This might create competition to be fully conformant.
 - Audience is important to discuss which we are not doing right now. AV-TEST.org example cited by Adam Migus. It scores in a way that is similar to the way Sal’s diagram does – using Harvey Balls. It produces a matrix and shows categories that are important to the individual. Maybe someone is concerned about security versus something else.

- Need matrix for end user and one for professionals who want to use. There will be multiple ways the information is presented. A big web would be a good way to do it. At this phase we are trying to get feedback on baseline and people's reaction to it.
- We are assuming no one will meet 100 percent conformance at the first round. We should not take that approach since we have requirements versus best practices. That is taking a defeatist approach.
- Our expectation is that we are setting a high bar and we will highlight people who have gone over the bar.
- In an ideal state, users who are evaluating the matrix should look at those who have gone over the bar.
- Not reaching 100 percent conformance shouldn't be considered defeatist.
- We need to factor this in the future roll out. Reality is, we have a long way to go and we need to move the ecosystem along. Right now, both points are valid in this discussion.
- Value of IDESG is the breath of what we are doing. We do both soft and hard requirements.
- Steve went to AV-TEST.org and showed the matrix. There is no one best vendor. It's based on what's important to you.
- ID operational security discussion
 - Agreed that the Security Committee should not be doing that work. Role of IDESG organization is to hire someone to do this work. There are conversations taking place as to the staffing needed. As we move to an operation phase, there are a number of things that need to be done and Sal indicated that the management council is putting together a list. Comment was made that the identity provider chosen should be in 100 percent conformance of the IDEF requirements.
 - Paul Knight - one of Security Committee's deliverables, listed on the dashboard, is to create a security guideline document.
 - Steve commented that it would be a good idea to report back the feedback from today's discussion on the SALS.
- Strategic Plan Update (Adam Madlin)
 - Adam wants to have an interactive discussion about the strategic plan that the Security Committee is responsible for. Adam asked that we hold off until next week to discuss given there was only 10 minutes left in today's meeting. Action: Adam to put together a list of things he wants the committee to review prior to the meeting next week.
- Paul Knight update – Strategic Plan has section on key deliverables for the organization with ownership assigned. Adam recommended that he and Paul get together to create a list of deliverables. Example: SC created the functional model which needs to be updated in 2016. The SC shows us as the owner. We should talk through all the deliverables, the assessment guide, the evaluation methodology and a few other things. Action: Adam to set up meeting with Paul Knight to discuss deliverables.
 - Important to start making decisions about what we put in the strategic plan and tracker. There is also going to be a scoping statement that should be approved on October 15. Important to look at the scoping statement to help us to define what our work looks like.
 - Scoping statement is flexible. We may or may not need some of the current deliverables given where we are as an organization. The deliverables are things which came from a strategic plan that was written some time ago and may not represent what we need to do going forward. The strategy plan will not be completed until the end of the year. Example – the security evaluation is in some respects the security requirements, which we might want remove.

New business:

- Please register for the virtual Plenary taking place October 15, 2015.

Wrap up and actions for next week:

- We need to postpone the Healthcare discussion with Dr. Tom and Jim Kragh that was originally scheduled for October 15. Instead, Adam Madlin will discuss the Strategic Plan.

Action: Linda to sent email to Jim Kragh about the schedule.

- Next meeting: October 15, 2015

- Meeting was adjourned at 2:10 p.m. EDT.

Action Items:

See above.