



MEETING SUMMARY

Meeting: System Technology & Data Security Subcommittee

Location: WSP USA Offices, Seattle

Date: February 27, 2019

Attendees:

Name	Organization	Executive Committee Member? (Y/N)
Alex Alben	Washington Office of the Chief Information Officer (OCIO)	Y
Will Saunders	OCIO	N
Michael Schutlzer	Washington Technology Industry Association (WTIA)	N
Paul Parker	Washington State Transportation Commission	N
Larry Gruginski	WSDOT	N
Thomas Smailus	Washington Society of Professional Engineers	N
Azmeena Hasham	Verizon - Smart Communities	N
Ian Griswold	WTIA	N
Jessica Nadelman	City of Seattle	N
Kelly Rula	Seattle DOT	N
Danny Malarkey	Sightline Institute	N
Markell Moffett	WSP USA	N

Introductions and Updates

Will Saunders

- Will Saunders will be leading this meeting, filling in for Alex Alben (attending by phone).
- Meeting attendees captured.
- Walked through agenda topics.
- Goal of this meeting is to get consensus on Principles Document to provide to Executive Committee as subcommittee's first recommendation

Topic Closed.



MEETING SUMMARY

Review Recommendations / Principle Document and Work Plan for 2019

Will Saunders

(See AV Data Privacy and Security Subcommittee Principles and Recommendations document)

- Primary driver for this document is to define rational scope for this subcommittee
 - What are the objectives the subcommittee is trying to accomplish?
 - What is in vs. out of scope?
 - Easy for conversations about data privacy and security to become wide-ranging
- Principles and ongoing subcommittee work will be iterative
 - Continue to ask “how does this link to our framework?”
 - Ongoing review of scope boundaries
 - Not standalone – other subcommittees with similar goals and overlapping efforts
- Objective to get final Principles Document to Executive Committee in the near future
 - Executive Committee not meeting until May/June
 - Annual AV Workgroup Report indicated very few subcommittees has submitted recommendations
 - Letter from Executive Committee forthcoming, requesting work products from subcommittees
 - This subcommittee is well-positioned to submit a first work product
 - Recommendations Form to be used as cover sheet for Principles Document
- **DECISION: Process to finalize Principles Document:**
 - Use Google Docs to share and provide input
 - Set Google Docs to “comments only” to restrict group editing
 - Will Saunders to publish to Google Docs by end of day 2/27/19
 - Invitation to provide comments will be sent to all Subcommittee Members, regardless of attendance at subcommittee meeting
 - Members will have 10 days to provide comments
- **ACTION ITEM (All Subcommittee Members) Review and comment on the Principles Document 2/28/19 thru 3/9/19.**

The edited document will be circulated for a final vote by all subcommittee members, most likely a web form. The overall vote tally (assuming we get a quorum) will determine whether the principles are forwarded to the Executive Committee as a recommendation.

The following link points to a Google Docs version of the Principles Document attached to the meeting invitation.

<https://docs.google.com/document/d/1k0MPWEyUMX5Vm6FJThlVFppQt0Wi6ARJivqkCY7eZ4k/edit?usp=sharing>

If Google Docs is not a good fit for a reviewer, alternatively comment on the BoxNote linked below with a Box.com account – please send the Box.com account’s email address to Will Saunders, and he will add the email address as an approved collaborator.



MEETING SUMMARY

<https://app.box.com/s/9oaso8s44khpqlccxz5591vzr168ohh8>

- Group discussion on Principles Document:
 - Document mentions two phases, testing and deployment, then addresses broader principles. Do the principles apply to both testing and deployment phases?
 - Yes – Will clarify.
 - **ACTION ITEM (Will Saunders)** – Update document to reference that principles apply to both testing and deployment.
 - Would there be additional principles or content to add to address actual deployments – more stringent/granular?
 - Agreed, don't need to be specific now.
 - **ACTION ITEM (Will Saunders)** – Call out that additional content will be added at a later date to address actual deployments.
 - Security section – Need to add more information about nature of encryption (*no specific action item or owner identified*)
 - Is this document sufficiently robust to meet Executive Committee expectations for a recommendation?
 - Yes. Important part is to be transparent.
 - Other committees have provided more extensive reports.
 - This document is robust enough to address subcommittee's recommendation
 - Group decided not to be over-regulatory, but rather focus on core principles
 - Don't regulate too soon – A lot of things still need to be worked out
 - Potential next step for subcommittee to engage with Safety subcommittee to identify aligning or opposing objectives
 - Example: Law Enforcement trying to identify when they can get access to data from AVs
 - May not be issue for testing, will be for ultimate deployments
 - Issue has come up in legislative session ([HB1325](#) and [SB5378](#))
 - **ACTION ITEM (Paul Parker / Will Saunders)** – Connect with chair(s) of Safety subcommittee, setup meeting soon to explore what this subcommittee is looking at vs. what Safety is – what is aligning, what is opposing.
 - There is a lot happening in AV technology space, not just deployments of Robot Taxis and Waymo. AV delivery vehicles, low speed shuttles, other activity that is more likely to be commercial deployments.
 - Good lens to put on as reviewing/commenting on Principles Document
 - May be good to add additional AV technology activities to scope (robot walkers, personal delivery devices (PDD))
 - How parsed out should in/out of scope lists be?
 - *For Parsing:* Different delivery methods may affect how we look at principles and standards. AV train deployments will be very different from heavy trucks – may be good to list separately.



MEETING SUMMARY

- *Against Parsing:* Data privacy and security should apply regardless of the AV application.
 - If too prescriptive, may preclude things unintentionally (e.g. If “passenger in vehicle” is terminology being focused on, may miss “robot walkers”)
- *Additional comments:* Important to always ask the question “whose data is being protected and under what circumstances?”
- Cybersecurity standards – Is the AV industry coming up with anything in this area?
 - Self-interest of private industry is to collect any/all data from any source they can to understand how the AV and related data are being utilized
 - With no “rules of the road” in this space, industry is deciding company-by-company what data they want to protect.
 - Up to lawmakers to put restrictions on.
 - Are other states/jurisdictions coming up with anything in this area?
 - GDPR is a good place to start
 - NASCIO Future Privacy Forum presented on conversations with OEMs – cybersecurity best practices are widely agreed upon within industry
 - Data Protection and Privacy has less consensus among industry than cybersecurity
- Software Update expectations – If an issue/accident occurs because a software update did not occur, or a software update caused the issue:
 - What is in the purview of this subcommittee?
 - Principle – Within purview. Companies need to update software. If update causes a data breach, that is a problem.
 - Outcome – Outside of purview. The actual outcome of an issue (e.g. brakes don’t work and vehicle crashes) outside scope of this subcommittee (goes to Safety, Liability, etc.)
 - Guidance on quality assurance/controls required for testing and deployment of updates?
 - Part of a larger conversation at a Federal level.
 - Classic legislative argument that needs to be resolved:
 - 1 – Are we legislating outcomes or processes? If process, why? More difficult than outcomes.
 - 2 – Who ‘gets’ the legislative outcomes or process? Tension between state and city – preemptive or not.
 - Not much movement at Federal level. We have an opportunity to lead.
 - Other states are watching and learning from WA.
 - Other states are carbon copying WA AV legislation.
 - Decisions from this subcommittee and the overarching AV Workgroup can help shape the standards at the Federal level.



MEETING SUMMARY

- **DECISION:**
 - Focus now on finalizing principles.
 - Next steps are to figure out what else this subcommittee wants to explore in 2019 (Work Plan).

Topic Closed.

Status and Plans for Other Subcommittees

Will Saunders

- Safety subcommittee submitted two recommendations
 - Health Impact Assessment – no further discussion in this meeting.
 - Educate the Public – Question from this subcommittee: What does the communications plan/budget entail?
 - Who is being communicated to?
 - What is being communicated?
 - Are they speaking on our behalf, and have the right information?
 - Need to find out more details on this effort.
- Other subcommittee status/plans not discussed in detail.

Topic Closed.

Wrap Up

Will Saunders

All topics below were decisions agreed upon by attendees.

- Meeting Frequency/Structure:
 - Short, focused meetings moving forward
 - 30-45 minutes per meeting
 - Bi-weekly cadence
 - One topic per meeting
 - Provide call-in capabilities
- Testing Regime Proposal:
 - No current testing regime/requirements
 - Priority of Subcommittee Work Plan to develop Testing Regime Proposal (for recommendation at May/June Executive Committee meeting)
 - ACTION ITEM (Will Saunders) – Follow up with Ted Bailey on Testing/Deployment Company outreach, request to push up timeline (currently set for June 2019).
- Subcommittee Priorities:
 - 1 – Find out more about testing in WA – Who, where, when
 - 2 – Develop proposal for Testing Regime
 - 3 – Draft Work Plan for 2019 exploration topics and next steps

Meeting Adjourned.

NEXT MEETING: The next meeting date is tentatively scheduled for April 2019.
