Subcommittee on Cybersecurity and Long-Term Policy Meeting 1

May 30, 2018
Salem, OR

Task Force Members in Attendance**:** Cheryl Hiemstra (lead), Carrie MacLaren, David McMorries, Graham Trainor, Jared Franz, Becky Steckler, Lt. Tim Tannenbaum (non-voting), Jeremiah Ross (non-voting)

Task Force Members Not in Attendance: Jim Pfarrer

ODOT Staff: Eryca Dinsdale, Amy Joyce, Jenna Adams-Kalloch, Andrew Dick, Ali Lohman, Melanie Ware, Paul Duncan

Public attendance: Paul Cosgrove, Lori-Anne Sayles, Evan Manvel, Nicole Stoenner (Chief of Staff to Task Force Member Representative McLain), Laura Tocheny

---

Welcome and Introductions (Cheryl Hiemstra, Lt. Timothy Tannenbaum)

Chery Hiemstra and Lt. Tannenbaum welcomed the subcommittee members and reiterated the goals and scope of work assigned to the task force by the Legislature.

Cybersecurity Considerations

Values

The subcommittee discussed the values identified during the workshop. They committed to avoid reinventing the wheel and to create regulations that can adapt to the needs of a rapidly changing industry. The subcommittee also discussed the need to be aware of work on AV policy going on at the federal and international levels.

Goals

The subcommittee evaluated the goals identified during the workshop, including 1) protection of consumer privacy, 2) protection of intellectual property, and 3) sharing information needed for public sector responsibilities. The group considered whether it was more appropriate to address consumer privacy in the 2018 or the 2019 report. They also noted a need to balance data sharing with privacy concerns.

Jared Franz observed that the data collected from AVs could be useful for analyzing equity issues.

Roles and Responsibilities

Cheryl Hiemstra noted that federal level guidelines are sparse on cybersecurity as of yet, and Oregon lawmakers may want to consider filling that regulatory gap.

The subcommittee spoke about data protection and cybersecurity requirements for testing automated vehicles. Jeremiah Ross cautioned against expecting testing and deployment to be discrete periods. He suggested getting out in front of the issue and avoiding a two-phase approach. Carrie MacLaren suggested building and testing the deployment framework during testing phase.

Preventing Cyberattacks

The subcommittee noted that state and local governments might not have the resources to effectively combat all kinds of cyberattacks, but felt the state could have some impact. Securing patching requirements, enforcement of National Institute of Standards and Technology (NIST) standards, and Independent Verification and Validation processes were mentioned.

The subcommittee discussed the possibility of unauthorized or aftermarket modifications to AV software.

Carrie MacLaren raised the idea of assigning liability to bad outcomes of tampering or other irresponsible conduct instead of specifically legislating to restrict conduct.

The subcommittee spoke about ways to ensure compliance, including revoking registration, regular testing, automatic patches, or even disabling non-compliant vehicles.

The subcommittee discussed patching requirements and obligations on the parts of owners and manufacturers.

Protection of Consumer Privacy and Data Management

The subcommittee spoke about the possibility of differing privacy and reporting standards for private and commercial vehicles. Several noted the usefulness of AV data for planning purposes. Becky Steckler said that data can be anonymized or aggregated and be both private and useful.

In the interest of time, the subcommittee tabled further discussion of cybersecurity issues and moved on to long-term policy considerations.

Long-Term Policy Considerations

The subcommittee discussed what should be in the 2019 report.

Carrie MacLaren questioned if “long-term” was an appropriate way to frame these issues. She asked if they might be better thought of as “deployment issues.”

Becky Steckler noted that transportation network companies are already causing some new trends in transportation use that are expected to be magnified with AVs.

The subcommittee recognized the possible consequences for revenue streams of local governments.

The subcommittee discussed exploring an employment impact study.

Graham Trainor voiced his concerns that workforce issues are being shortchanged by being paired with cybersecurity. He noted that work to prepare for workforce changes might need to start soon.

Public Comment

Nicole Stoenner, representing task force member Rep. Susan McClain, urged the subcommittee to view issues through a lens of equity issues and to consider transit in their discussions.

The subcommittee agreed with these points. Lt. Tannenbaum suggested the formation of a social justice subcommittee for the 2019 report.

Graham Trainor spoke about his concern that the task force is showing a lack of urgency in thinking about these long-term and workforce issues. He mentioned that there should be a way for local government to maintain a role in ensuring the safety of their constituents.

Areas of Consensus and Areas for Further Discussion

<u>Cybersecurity Issues</u>

The subcommittee agreed that the task force should keep federal policy close in mind for cybersecurity issues.

Areas for further discussion

- How the state, manufacturers, and others must respond to a cyberattack or data breach

<u>Consumer Privacy</u>

The subcommittee agreed on the need to balance the use of data with privacy of users.

Areas for further discussion

- Creation of specific data sharing standards for personal vehicles, heavy-duty commercial vehicles, and commercial fleets

<u>Testing and Deployment</u>

The subcommittee agreed that testing should be a top priority, but that policies should be created for both testing and deployment as soon as possible.

Areas for further discussion

- Specific differences between testing and deployment standards
- How much and what data should be required from testers balanced with the need to protect intellectual property

<u>The Role of AV Owners in Cybersecurity</u>

The subcommittee agreed that aftermarket AVs and AV modifications will need to be addressed at some point. The subcommittee agreed that Original Equipment Manufacturers (OEMs) will need to have a level of cybersecurity responsibility during testing.

Areas for further discussion

- Anti-tampering methods and requirements

<u>Long-Term Policy Considerations</u>

The subcommittee generally agreed that so-called "long-term" issues may need to be addressed sooner than their title suggests, and might be better thought of as "deployment issues." The subcommittee felt that looking at the issues before them through a "lens of equity" was important.

Areas for further discussion

- Employment impact studies
- Offsetting the fiscal impact on state and local revenues
- Finalizing which issues need to be addressed for the coming deadlines

Action Items

David McMorries to research cybersecurity methods.

Subcommittee members to send Carrie MacLaren information to create "data wishlist."

ODOT staff to provide information on other states' requirements around cybersecurity during testing.

Becky Steckler to provide list of state land use and transportation goals relevant to this effort.