SUBCOMMITTEE ON CYBERSECURITY AND LONG-TERM POLICY

Scope of Considerations for Cybersecurity

Objective: To assess potential cybersecurity risks and examine State versus Federal roles in cybersecurity regulation, as well as data collection and consumer privacy.

Values
- Build on existing structure and system (i.e. “don’t reinvent the wheel”)
- Maintain adaptability and be able to adjust as industry changes

Goals
- Protection of consumer privacy
- Protection of intellectual property
- Sharing information needed for public sector responsibilities

Topics
Roles and responsibilities
- Determine federal and state roles in establishing cybersecurity requirements and enforcement
- Determine responsibilities of governments, manufacturers, and the public in preventing cyberattacks
- Determine responsibility for ensuring software and security are up to date

Responding to cyberattacks
- Ensure transparency and accountability in the event of a breach of security

Preventing cyberattacks
- Leverage existing cybersecurity systems, e.g. ISAC
- Assess potential security risks
- Address cybersecurity concerns regarding all AV technology
  - Vehicles, including heavy equipment vehicles such as tractors
  - Infrastructure
  - OEM equipment
  - Third party devices
  - Apps
- Ensure data integrity after a crash or incident, i.e. prevent evidence tampering
• Require manufacturers to provide reasonable security updates for the useful life of an automated vehicle

Protection of consumer privacy
• Prevent the misuse or dissemination of consumer information and vehicle data
• During testing, require testers to disclose what type of data they are collecting and with whom they are sharing that data

Data management
• Protection of intellectual property
• Sharing of anonymized data for policy, planning, and development
• Require data accuracy and ability to audit
• Transparency of guidance algorithms and prioritization of choices
• Transparency of reporting algorithms

Questions
Roles and Responsibilities
• What is the federal role in regulating cybersecurity for automated vehicles?
  ○ What cybersecurity regulations need to be consistent across jurisdictions during testing of automation vehicles?
  ○ What cybersecurity regulations need to be consistent across jurisdictions during deployment of automated vehicles?
• Is there a state role in regulating cybersecurity during testing of automated vehicles? If so, what responsibilities are assigned to the state?
• Is there a state role in regulating cybersecurity during deployment of automated vehicles? If so, what responsibilities are assigned to the state?
• Do local governments have a role in preventing cyberattacks on automated vehicles and related technology?
• What steps should manufacturers of automated vehicles take to prevent cyberattacks?
• What steps should owners of automated vehicles take to prevent cyberattacks?
• Who is responsible for ensuring that an automated vehicle’s software and security are up to date? If the state has a role, what processes are required to validate the software and security?

Preventing cyberattacks
• What are potential cybersecurity risks regarding automated vehicles?
• What types of automated vehicle technology are vulnerable to cyberattacks? E.g., passenger vehicles, freight vehicles, heavy equipment vehicles such as tractors, infrastructure, OEM equipment, third party devices, apps, etc.
• How can we leverage existing cybersecurity systems, e.g. ISAC?
• How can we ensure data integrity after a crash/incident and prevent evidence tampering?
Responding to cyberattacks
- In the event of a security breach, how can we ensure transparency and accountability?

Protection of consumer data
- Should testers be required to report what data they collect during testing and with whom they share that data?
- What are the potential short term and long term effects on consumer privacy? What are the potential consumer harms in this area?
- How much control should consumers have over their data? Who owns the data?
- Should anything be done to protect the privacy of pedestrians, other cars, etc. whose information will be collected by AVs?
- Should, and if so, how should, manufacturers explain their data usage to consumers?
- How can we ensure that data is not de-anonymized if used or shared for other purposes?

Data management
- What anonymized data do state and local governments need for policy, planning, and development purposes during the testing phase? What format would the data need to take to be usable for state and local governments?
- What anonymized data do state and local governments need for policy, planning, and development purposes during the deployment phase? What format would the data need to take to be usable for state and local governments?
- How can manufacturers ensure data is accurate and can be audited?
- What information is protected as intellectual property?

Scope of Considerations for Long-Term Policy

Objective: To determine which topics should be assessed in the 2019 legislative report.

Values
- Focus on long-term considerations
- Support and be consistent with Oregon's long-term policies, goals, and plans
- Meet goals for safety and for the transportation of goods and people
- Mitigate negative consequences of AVs and embrace opportunities created by AVs, e.g. improving safety, relieving congestion, expanding transportation options, addressing climate changes
- Meet sustainability goals
- Promote equity

Topics
Roles and responsibilities
- Maintain regulatory consistency across jurisdictions for ease of travel
• Avoid preempting local governments’ ability to advance local goals
• Align with other west coast/I-5 collaboration efforts

Sustainability
• To meet state’s climate pollution reduction goals, create AV policies that incentivize electric and low-emission vehicles

Land use and urban design
• Curbside management
• Transitional and long-term design

Road and infrastructure design
• Study cost of rebuilding infrastructure to accommodate AVs
• Determine ownership of smart tech and responsibility for ensuring cybersecurity
• Install AV-compatible infrastructure when roads are built or repaired

Road use management
• Participation of AVs in a road usage charge program
• Prioritize FAVES (Fully Autonomous Vehicles that are Electric)
• Support public transit and multimodal transportation
• Prioritize high capacity transit, then commerce, then single occupancy vehicles
• Research prioritizing off-peak freight movement
• Consider public interest and maintain public investment in public transportation and services

Pricing
• Gas tax and road usage charge programs
• Registration fees
• Impacts to local and state budgets

Equity
• ADA considerations
• Non-discriminatory programming, services, and data collection
• Ensure access to all Oregonians, e.g. providing good internet access in rural areas

Workforce changes
• Study impacts to workforce and rural communities
• Facilitate transitions through worker assistance and retraining
• Ensure new jobs created by AV industry meet High Roads standards
• Work with unions up front early in the process

Cybersecurity and data management
• State responsibilities regarding cybersecurity and privacy
• Data collection for planning purposes
- Licensing and resale data

Questions

- Should all these topics be addressed in the 2019 report? Should any of them be excluded?
- Do these topics fall within the jurisdiction of federal, state or local governments? How do we balance the need for (and benefits of) national consistency while considering local goals?
- Are there additional topics that could be examined in the 2019 report?
- Are there additional questions or considerations that should be addressed within each topic?
- What resources would be helpful for the Task Force on Autonomous Vehicles to review in relation to these topics?
- Do we have sufficient information to consider these topics? Are there topics that will require further study?