WASHINGTON STATE AUTONOMOUS VEHICLE WORK GROUP

Washington State Autonomous Vehicle Work Group Subcommittee Discussion Form

Subcommittee	System Technology and Data Security
Date of Meeting	May 21, 2020

1) NOTEWORTHY TOPICS OF DISCUSSION, SUMMARY OF DISCUSSION, AND OUTCOME OF DISCUSSION

- **Review of Current Technologies** - How connected vehicle (CV) technology is/can be applied to autonomous vehicles (AV) and the work force
- Today vehicles are communicating in the 5.9 GHz safety band when talking to roadside units with dedicated short-range communications (DSRC)
    - Connecting to vehicles and infrastructure provides benefits – Safety, congestion reduction, ability to minimize things like left hand turn crashes at intersections, etc.
    - 5.9GHz is an important band, it is unique – Dedicated for ITS, albeit FCC might make changes to the band and availability to different technologies
    - V2X (cellular vehicle-to-everything) may be appearing in the upper portion of the 5.9GHz band

- **Operational Networks and Ownership-**It is not a given that the public sector retains ownership of the network and data – how vehicles are actually connecting to and using the network is shifting
        - Example: “OLLI”, a low-speed AV shuttle, is not connected to anything
            - Uses cameras, sensors, etc. to operate
            - Public sector may not be able to access or get data from a vehicle like this
- **Enclave Protection** - Enclave security leverages the concept of the CIA triad – Confidentiality, integrity, and availability
        - Enclave security helps provide confidentiality, availability, and integrity to each enclave or ‘zone’ within the same network, independently
            - Example: Ethernet or a fiber rim to provide secure, discrete, and available information to multiple entities
                - DOT traffic controller data, connectivity for CCTV public access, 4.9 radios for police and fire
                - Able to do so over software-defined network with a lighter implementation
- **Security and Standards -**
- Operational and field networks – Need to understand assets, vulnerabilities, threats
    - Involves IT infrastructure, field operational technology infrastructure, third parties
    - Need to agree on common standards; looking to feds for guidance
- Start with a plan, and implement policies and procedures, without recreating the wheel
    - Develop a strategy and conduct a self-assessment
    - Deploy and migrate
    - Operate
    - Optimize

2) NEXT STEPS AND PLANS FOR SUBCOMMITTEE

Continue meeting to discuss recommendations for cybersecurity considerations based on subject matter expertise provided. Identify near-term steps to address exiting gaps for transportation systems and services regarding cybersecurity. Next meeting to be determined.