IoTAB Smart Traffic and Transit Technologies Subgroup

Draft Outline

- **Technology Overview**
  - Infrastructure – hardware, software, connectivity, edge computing
    - Hardware –
      - Traffic signals and controller assemblies,
      - Roadside units,
      - Traffic signal cameras and sensors that can detect near collisions to impact signal timing (ATSPM – Advanced Traffic Signal Performance Measure)
      - EV charging equipment (i.e., Level 1, Level 2, DC Fast Charging);
      - LIDAR/Camera sensors
      - Solar panels mounted on poles.
      - Parking sensors
      - Road maintenance sensors
      - Vehicle mounted sensors that also measure road conditions.
      - Off road equipment that interacts with these various sensors
      - Drones
      - (Planes/Airports?)
    - Systems - security, intelligence, monitoring, management, maintenance
    - Software – route planning – cars and buses
    - Connectivity- Cellular Vehicle to Everything (C-V2X), 5G, autonomous navigation (both edge and cloud)
    - Edge computing- self-driving vehicles-last mile delivery
    - Tied into the infrastructure (linkage to the IoT AB Smart and Critical Infrastructure)
    - Artificial intelligence

- **Opportunities and benefits (for personas)**
  - Safety applications/use cases- technology can save lives
    - emergency vehicle traffic pre-emption,
    - entering school or work zone,
    - pedestrian crossing ahead;
    - improving road safety;
    - protecting Vulnerable Road Users
    - Vision zero;
  - Support Function
    - Package and Food Delivery
  - Congestion mitigation/environmental benefits
    - orderly flow of traffic.
    - limit traffic to reduce congestion (congestion/smart toll pricing)
    - increase productivity (less time spent in traffic)
  - Commerce/trade –
    - want organizations to thrive when developing these devices.
    - incentivize companies to develop systems for common good and use;

        - ability to develop systems for companies outside the US; increase harmonization with other countries

- **Barriers (faced by personas for IoT implementation)**
    - Policy/regulation/practices –
        - need clarity with respect to privacy
            - Notice when PII captured;
            - transparency for the individual;
            - lack of clarity on what is collected can violate expectations;
            - important to minimize PII to limit risk to individuals;
            - organizations need to be clear on retention, not over-retain, delete data when no longer needed;
            - need transparency on what is collected, use of collected data, and retention of data
            - Linkage back to privacy subgroup
        - Policy on use of traffic camera data for accident investigation, assignment of insurance claim
        - Policies and regulations for self-driving automobiles/drones
            - Liability concerns when self-driving automobiles are hacked.
            - Liability concerns if drone delivers the wrong medicine
    - Accessibility and inclusion –
        - Benefits not necessarily available to everybody;
        - smarter the technology requires more presentation of information to users/general public and can't make assumptions about what is available;
        - EV charging not available in all areas
    - Education/Training and resources –
        - For the highway engineers, learning curve for communication/smart transportation technologies; not traditionally part of highway engineers background;
        - operation of smart traffic technology will require more support and training; need to design so that someone with a fourth-grade education can operate it
        - education and awareness for users needed especially if a traffic system runs through multiple jurisdictions
        - some state DOTs have very few staff
        - Workforce development issues that are unique to this area
    - Interoperability versus IP
        - developed technology needs to be protected and not stolen; don't want to lose control when manufactured by others;
        - important for IP for research and manufacturing to be linked together.
        - interoperability challenge when dealing with different jurisdictions
    - Cybersecurity Risk–
        - Connected devices used as gateway devices for other things.
        - Physical security- traffic cabinets can be opened with a single key
        - Organizations that don't have a robust cybersecurity approach
        - Need linkage back to Security Sub-team.
    - Funding -

        - public, public/private partnerships, private –
        - states have to submit plans to receive EV infrastructure funding;

- **Potential industry experts we have to speak with (Specific speakers TBD)**-
    - Select State DOTs;
    - representative from the Vision Zero network;
    - representative from the Highway engineering exchange program;
    - Australia smart cities expert,
    - Representative from a research firm that can talk about grid impacts with increased EVs (NREL, McKinsey, World Resources Institute).
    - Someone that can speak to security risks specific to transportation (future looking-especially with the increase in autonomous vehicles).

- **Potential industry references we should consider** - industry papers, case studies, other countries, etc.-
    - Federal Agencies - National Highway Transportation Safety Board; US DOT (work related to intelligent transportation systems- pilots in NYC, Tampa, and Wyoming:https://www.its.dot.gov/pilots/)
    - State and local jurisdictions: Georgia (Fulton Country School District), Utah, California
    - Smart City examples: Columbus, NYC, Singapore
    - Studies on the growth of the EV market and how it impacts the grid (possibly NREL, McKinsey, World Resources Institute).

- **Standards Organizations in this space**- NEMA, SAE, IEEE