Automotive Industry SBOM Project – Prologue (1/3)

- Disclaimer
- From NHTSA "Cybersecurity Best Practices for the Safety of Modern Vehicles," Draft 2020 Update – released for public comment January 2020:

  4.2.6 Inventory and Management of Software Assets on Vehicles

  - *[G.10] Manufacturers should maintain a database of operational software components[19,20] used in each automotive ECU, each assembled vehicle, and a history log of version updates applied over the vehicle's lifetime.*
  - *[G.11] Manufacturers should track sufficient details related to software components,[21] such that when a newly identified vulnerability is identified related to an open source or off-the- shelf software,[22] manufacturers can quickly identify what ECUs and specific vehicles would be affected by it.*

Automotive Industry SBOM Project - What? (2/3)

A supplier-led project to:

- Study and understand SBOM principles and operations
- Align and emulate - NTIA, FDA/Healthcare, other agencies/industries
- Make the case for SBOM in the auto industry
- Unified voice from suppliers
- Practical approach and solution with input from customers/partners
- Perform exercises in implementation
- Recommend and get agreement from industry
- Encourage/foster voluntary adoption by suppliers

Automotive – Tasks and Deliverables – How? (3/3)

- Learn: 3 x1 hour tutorials by NTIA Healthcare MSP leaders (complete)
- Cycle:
    - Planning: Timelines, resources, example components, logistics, metrics, formats, tools, other (Cycle 1 underway)
    - Execution: Build SBOMs and conduct exercises
    - Review: Post-mortem, lessons learned
    - Adjust: Improvements, streamlining
- Report: Supplier recommendations for industry standards to automakers (~12 months)