DEPARTMENT OF TRANSPORTATION

National Highway Traffic Safety Administration

Cybersecurity Best Practices for the Safety of Modern Vehicles

Request for Comments

Docket No. NHTSA-2020-0087

Comments of AT&T Services, Inc.

INTRODUCTION

AT&T Services, Inc., on behalf of itself and its affiliates (together, "AT&T"), respectfully submits these comments in response to the National Highway Traffic Safety Administration ("NHTSA," "the Agency") Request for Comments on the Agency's draft *Cybersecurity Best Practices for the Safety of Modern Vehicles*.

As the leading provider of cellular network connectivity to motor vehicles in the United States, AT&T had more than 43.5 million cars and almost 5.5 million fleet vehicles connected to its network at the end of 2020. More than 31 million of those vehicles have been added to AT&T's network since NHTSA last issued its cybersecurity best practices in October 2016.[1] AT&T also provides global connectivity solutions to automotive manufacturers around the world.

AT&T was among the first automotive supplier members to join the Auto-ISAC in 2016 and is the only mobile network operator (MNO) member. AT&T is also an active participant

[1] National Highway Traffic Safety Administration (2016), *Cybersecurity Best Practices for Modern Vehicles*, announced via Federal Register document, 81 FR 75190 (Oct. 28, 2016), available at https://www.nhtsa.gov/document/cybersecurity-best-practices-modern-vehicles.

through association memberships in the C2 Consensus on IoT Device Security Baseline Capabilities, and a founding member of the Coalition to Reduce Cyber Risk ("CR2"), a global organization "promoting best-in-class approaches to cybersecurity risk management" across industries and around the world.[2] AT&T's Chief Security Organization is actively engaged in a range of research efforts into Internet of Things cybersecurity, with a particular focus on connected vehicle security.

Given AT&T's extensive involvement in vehicle connectivity, cybersecurity, its expertise in securely connecting all manner of devices, AT&T is pleased to provide the following comments on NHTSA's *Cybersecurity Best Practices for the Safety of Modern Vehicles*.[3]

DISCUSSION

I. NHTSA'S APPROACH TO CYBERSECURITY

NHTSA's stated commitment to voluntary and non-binding guidance,[4] as well as its effort to collate the work of industry led efforts,[5] are both commendable elements of its approach to vehicle cybersecurity. Similarly, the Agency has appropriately chosen to focus this Draft Best Practices document on those aspects of vehicle cybersecurity that affect vehicle safety.[6] Sustaining this approach through the finalization of this iteration of the best practices and, more importantly, through NHTSA's ongoing approach to working with the automotive industry to continually mitigate safety-impacting vehicle cybersecurity risks will help the Agency achieve

[2] https://www.crx2.org/about

[3] National Highway Traffic Safety Administration, *Cybersecurity Best Practices for the Safety of Modern Vehicles*, Draft 2020 Update, Docket No. NHTSA-2020-0087, Attachment 1, ("Draft Best Practices"), available at https://downloads.regulations.gov/NHTSA-2020-0087-0001/attachment_1.pdf.

[4] National Highway Traffic Safety Administration, Request for Comments, Cybersecurity Best Practices for the Safety of Modern Vehicles, Docket No. NHTSA-2020-0087, 86 Fed. Reg. 2481 (Jan 12, 2021)("RFC").

[5] RFC, 2842.

[6] Ibid.

its aims.

II. BEST PRACTICES KEY AREAS

NHTSA's RFC states that the "updated draft document is structured around five key areas: (1) General Cybersecurity Best Practices, (2) Education, (3) Aftermarket/User Owned Devices, (4) Serviceability, and (5) Technical Vehicle Cybersecurity Best Practices,"[7] and AT&T agrees that these are five important and appropriate categories. Organizing the guidelines around these areas is a helpful way to encourage the automotive industry to attend to the specific challenges to safety-affecting vehicle cybersecurity that emanate from each area.

However, the best practices draft document itself does not explicitly discuss or address these areas as being distinct categories, beyond the document's section headers. The Background section of the best practices document should include a discussion of these five key areas and how and why NHTSA sees each area impacting vehicle cybersecurity and safety. Similarly, the enumeration convention within the best practices draft itself collapses the individual best practices from five into just two categories: [G.n_i] for General and [T.n_j] for Technical. The enumeration convention should instead be expanded to reflect each of these five areas by adding the conventions of [E.n_k] for Education, [A.n_l] for Aftermarket/User Owned Devices, and [S.n_m] for Serviceability. While in this iteration of the draft these three areas each contain few specific best practices (one for Education, three for Aftermarket, and two for Serviceability), a clearer delineation should help reinforce for readers the varied dimensions impacting automotive cybersecurity and leave room for future additions.

[7] RFC, 2485.

III. Comments on Specific Best Practices Recommendations

> *[G.7] Any unreasonable risk to safety-critical systems should be removed or mitigated to acceptable levels through design, and any functionality that presents an unavoidable and unnecessary risk should be eliminated where possible.*[8]

NHTSA's RFC identifies best practice [G.7] as a new addition to this updated document, intended "to align with the National Traffic and Motor Safety Act's prohibition of manufacturers selling motor vehicles and motor vehicle equipment that may contain unreasonable risks to safety."[9] Such alignment is indeed sensible and, as a voluntary best practice, [G.7] is unobjectionable. However, the potential for shifts in what NHTSA chooses to include within the scope of "motor vehicle equipment" in the context of vehicle cybersecurity combined with the range of external systems connected to modern vehicles presents concerns. NHTSA should refine its discussion of [G.7] to specify which entities it believes should be responsible for removal of unreasonable risks to safety-critical systems when those systems may reside outside the vehicle itself and are thus not within the currently generally accepted scope of "motor vehicle equipment."

> *[G.9] Clear cybersecurity standards should be specified and communicated to the suppliers that support the intended protections.*[10]

Recommended best practice [G.9] appears to pertain to cybersecurity expectations across the automotive supply chain. NHTSA should clarify that this recommendation encourages *customers* in the automotive supply chain to stipulate clear cybersecurity requirements for their suppliers' products and services. The current language of [G.9] uses the phrase "clear cybersecurity *standards*…"[11] (*emphasis* added). While NHTSA notes in footnote 18 the

[8] Draft Best Practices, 5.
[9] RFC, 2483.
[10] Draft Best Practices, 6.
[11] Draft Best Practices, 6.

discussion of customer-supplier relationships in ISO/SAE 21434, NHTSA should either explicitly endorse and incorporate ISO/SAE 21434's treatment of the customer-supplier issue into [G.9] or rephrase the recommendation to read: "Clear cybersecurity requirements that support the intended protections should be specified [by the customer] and communicated to the suppliers." Such rephrasing will clarify that NHTSA is not specifying an actual standard for use in customer-supplier relationships but rather encouraging cybersecurity protections to be incorporated into those relationships.

> *[G.10] Manufacturers should maintain a database of operational software components used in each automotive ECU, each assembled vehicle, and a history log of version updates applied over the vehicle's lifetime.*[12]

The best practice [G.10] calls for "manufacturers" to "maintain a database of operational software components[.]"[13] As with other recommendations, NHTSA should clarify which entities the Agency intends to include as "manufacturers" for the purpose of this best practice. As the OEM ultimately determines what software should be operational on its vehicles, it stands to reason that OEMs are who NHTSA is referring to here. The Agency should specify this in [G.10].

> *[G.30] Commensurate to assessed risks, organizations should have a plan for addressing newly identified vulnerabilities on consumer-owned vehicles in the field, inventories of vehicles built but not yet distributed to dealers, vehicles delivered to dealerships but not yet sold to consumers, as well as future products and vehicles.*[14]

NHTSA's recommendation in best practice [G.30] to "have a plan for addressing newly identified vulnerabilities"[15] in various categories of existing vehicles is prudent. NHTSA should consider whether to strengthen this recommendation by encouraging such incident response plans to, when practical for those sets of vehicles with the capability, include remote remediation

[12] Draft Best Practices, 6.
[13] RFC, 6.
[14] Draft Best Practices, 10.
[15] Draft Best Practices, 10.

of the vulnerability via an Over-the-Air (OTA) software or firmware update. As stated in NHTSA's October 2020 report "Cybersecurity of Firmware Updates," "the benefit of reliable, prompt software updates for in-field electronics is significant."[16] This is certainly the case during certain categories of incidents that may require software or firmware updates to resolve.

> *[T.13] Manufacturers should treat all networks and systems external to a vehicle's wireless interfaces as untrusted and use appropriate techniques to mitigate potential threats.*[17]
>
> *[T.22] Maintain the integrity of OTA updates, update servers, the transmission mechanism and the updating process in general.*[18]
>
> *[T.23] Take into account, when designing security measures, the risks associated with compromised servers, insider threats, men-in-the-middle attacks, and protocol vulnerabilities.*[19]

The premise of best practice [T.13] is sound but the wording is awkward and unclear. NHTSA should refine this best practice to read: "Manufacturers should recognize that wireless connections to vehicles pose the potential for remote exploitation of vehicles and use appropriate techniques to mitigate potential threats." This change would also reconcile [T.13] with [T.22] and [T.23], pertaining to Over-the-Air (OTA) Software Updates.[20] As NHTSA's own report on firmware updates notes, OTA updates "are widely considered essential for networked devices."[21] The change to [T.13] proposed here aligns it with and reinforces the calls in [T.22] to maintain "the integrity of… the transmission mechanism"[22] and in [T.23] to account for "men-in-the-middle attacks, and protocol vulnerabilities."[23]

[16] Bielawski, R., Gaynier, R., Ma, D., Lauzon, S., & Weimerskirch, A. (2020, October). *Cybersecurity of Firmware Updates* (Report No. DOT HS 812 807). National Highway Traffic Safety Administration, iii.
[17] Draft Best Practices, 15.
[18] Draft Best Practices, 17.
[19] Draft Best Practices, 17.
[20] Draft Best practices, 17.
[21] Bielawski, R., et. al., *Cybersecurity of Firmware Updates,* ii.
[22] Draft Best Practices, 17.
[23] Draft Best practices, 17.

CONCLUSION

AT&T welcomes NHTSA’s update and revision to its cybersecurity best practices and commends the Agency for the thoughtfulness and diligence with which it has developed this resource. We hope our comments here can help NHTSA further refine its final iteration of this version of the best practices and we look forward to continuing to work with our industry partners and NHTSA to advance the cybersecurity of modern vehicles.

Respectfully submitted,

/s/

Sarah Geffroy
David Chorzempa
David Lawson

AT&T Services, Inc.
1120 20th Street NW
Suite 800
Washington, D.C. 20036
(202) 457-2121 (phone)

March 15, 2021