GEOTAB

Geotab USA, Inc.
770 E. Pilot Rd,
Suite A
Las Vegas, Nevada
89119, USA

+1 (800) 397 7102

www.geotab.com

Geotab Inc. comments to NHTSA’s updated draft 2020 Cybersecurity Best Practices for the Safety of Modern Vehicles [Docket No. NHTSA-2020-0087]

Geotab Inc. respectfully submits these comments to the National Highway Traffic Safety Administration (NHTSA) in response to the Agency's invitation for public comment regarding the updated draft cybersecurity best practices document titled “2020 Cybersecurity Best Practices for the Safety of Modern Vehicles.”

Geotab Company Information

Geotab Inc. (“Geotab”) is a proven leader in IoT and connected transportation. Geotab securely connects commercial vehicles to the internet, providing advanced web-based analytics to help businesses better manage their fleets and make data-driven decisions. Geotab’s key industry differentiator is its open platform solution, which promotes a network of cooperation, enabling businesses to integrate data processed from Geotab connected vehicles into any system regardless of business size or operational needs.

Geotab has the largest single-source telematics contract to date by GSA Fleet, a division of GSA (General Services Administration),[1] which provides centralized procurement for U.S. federal agencies. This rare, single-source award from GSA Fleet reinforces Geotab’s ability to provide secure and highly specialized technology to the government sector. As a vertically integrated telematics provider, Geotab manages the entire technology stack, from the in-cab hardware and embedded firmware used to encrypt and transmit data, to the secure server-side hosting and software applications.

As the first telematics company to achieve FIPS 140-2 validation[2] for its cryptographic library, Geotab places security at the forefront of its innovations, ensuring rigorous security measures that meet industry-best cybersecurity practices. In addition, Geotab has achieved the International Organization for Standardization (ISO) 27001[3] certification, confirming the integrity of its Information Security Management System.

Geotab has achieved full Federal Risk and Authorization Management Program[4] (FedRAMP) authorization for its cloud-based telematics platform. Geotab’s FedRAMP status[5] validates the organization’s ability to meet stringent security requirements set forth by the U.S. federal government.

Geotab has a comprehensive privacy program to ensure all data processed by Geotab is secured and managed in accordance with applicable laws. Geotab’s End User Agreement forms the contract with end users, and the processing instructions from customers (data controllers) enable them to manage their vehicle fleet using the Geotab solution. Our personal information practices are set out in the Geotab Privacy Policy[6], and our security architecture is described in Geotab’s Technical and Organizational Measures Statement[7]. Geotab’s privacy and

[1] https://www.gsa.gov/buying-selling/products-services/transportation-logistics-services/fleet-management/vehicle-leasing/telematics
[2] https://csrc.nist.gov/Projects/cryptographic-module-validation-program/Certificate/3371
[3] https://www.iso.org/standard/54534.html
[4] https://www.geotab.com/press-release/fedramp-authorization/
[5] https://marketplace.fedramp.gov/#!/product/geotab-telematics-platform-government-gtp-gov?sort=productName
[6] https://docs.google.com/document/d/1sVygLN02w2xNovFY4q5vw-oAzfYxCd7WLhyToElgDbs/pub
[7] https://docs.google.com/document/d/1b8F7XB86Z0h8xyD4GF3wH3vzwtdzMhKb-SmhYkz8lGs/edit#heading=h.uk8r0k8xx328

security program has undergone review from legal, compliance, and security experts to ensure the solution complies with the law and our customers' fleet data is secure.

Geotab is a member of the World Wide Web Consortium (W3C)[8] and GENIVI[9], to standardize signal data, as well as the standard committees within the International Organization for Standardization (ISO) and Institute of Electrical and Electronics Engineers. Geotab adheres to industry published best practices such as the Volpe Primmer, NMFTA cyber matrix, and FMCSA guidance. Geotab does include each of the activities related to security and privacy policies in our public facing documents on the Geotab Security[10] page.

Executive Summary

We appreciate NHTSA's commitment to cybersecurity in the modern vehicle and believe these recommendations are aligned in good faith. With our following comments we intend to promote further clarity regarding definitions and technical best practices that, as currently drafted, could pose risks to innovation, fair business practices, consumer choice, and the rights of vehicle owners.

We believe the verbiage in some instances leads to ambiguous interpretations, as can be inferred from phrases such as "only authorized privileged users." While the best practices seek to address cybersecurity, we believe some statements may be wrongfully interpreted to justify harmful restrictions, leading ultimately to the complete prohibition of third-parties.

Today, there are millions of internet-connected vehicles in operation in America's mega fleets, government service, car rental, and car leasing operations, medium and small business fleets and independent trucking. All these organizations rely on real-time, wireless access to operational data generated by their in-motion vehicles to run an efficient and responsible business. Without losing sight of safety and security, considering these cybersecurity best practices, we believe it is also important to keep the diverse economic perspectives in light of this issue. We welcome the opportunity to discuss these matters further with NHTSA.

Comments By Section

General Cybersecurity Best Practices

Leadership Priority on Product Cybersecurity

In section 4.1 Leadership Priority on Product Cybersecurity, Geotab agrees with the sentiment for companies developing or integrating vehicle electronic systems or software to be prioritizing commitment and accountability on vehicle cybersecurity. Furthermore, at Geotab, we use independent third-party experts to validate our platform from end to end. We believe all these companies must have an independent voice for cybersecurity-related considerations within the vehicle safety design process.

[8] https://www.w3.org/auto/events/data-ws-2019/report.html
[9] https://at.projects.genivi.org/wiki/download/attachments/63799455/Why%20CVII%20for%20suppliers%20-%20GENIVI-W3C-Geotab-AW%20Webinar%2019th%20November.pdf?version=1&modificationDate=1605892218000&api=v2
[10] https://www.geotab.com/security/

Penetration Testing and Documentation

Section 4.2.7 Penetration Testing and Documentation recognizes the importance for manufacturers to evaluate commercial off-the-shelf and open-source software components. However, these evaluation efforts would benefit from also being executed in collaboration with independent third-party security testing. Additionally, manufacturers should have internal processes in place to mitigate security findings and vulnerabilities. Geotab independent cybersecurity validation includes penetration testing by independent security consultants.

Information Sharing

Geotab is a proud member of the Auto-ISAC, and takes Auto-ISAC's mission for collaboration in driving security measures into every phase of the vehicle's life-cycle. As more organizations connect their vehicles, it is important for Auto-ISAC to continue to reach out to the mixed fleet owners for input on how they currently use telematics, and how the mixed fleet owners expect their data consumption to progress.

Aftermarket/User Owned Devices

Vehicle Manufacturers

Section 6.1 Vehicle Manufacturers sub point G.40 states that "any connection to a third-party device should be authenticated and provided with appropriate limited access." We are concerned with how this statement's interpretation could be operationalized. From our perspective, the statement as written could be interpreted by the manufacturers to limit access to zero access, without a fair and transparent process in place.

We believe that vehicle owners should be able to authenticate themselves to a manufacturer for access to their vehicle-generated data. Such an authentication process happens purely for security reasons, not commercial ones, and provides consideration for how these efforts are carried out as to be careful to avoid breaches of antitrust law.

Furthermore, we find sub point G.40 to be contrary to open source principles and the open vehicle concept. By suggesting third-party devices should be authenticated and provided with "appropriate limited access", it implies manufacturers are able to install restrictive cryptographic gateways, and presumes the manufacturer as the preferred accessor to vehicle-generated data. This lack of clarity on "appropriate limited access" will further imply physical or cryptographic gateways to vehicle-generated data reads, providing sole authentication to the manufacturer, and not the vehicle owners.

Standardization could be at the physical interface level, i.e. OBDII port, or USB connector, wireless and also software interface level. Data protocols should be standardized, where initial requirements may be managed dynamically over time through a system of dynamic governance. The possibility should exist shall independent operators choose not to use a manufacturer server-based solution, an example of this is in vehicle pre-processing without aggregation by the manufacturer required. This also applies to direct consent management and commercial contact with our own clients.

Aftermarket device manufacturers

Regarding section 6.2, Aftermarket Device Manufacturers. The manufacturers designing the vehicles should follow existing and, when available, the emerging security standards to prevent any lapses. One standard currently in process is ISO/SAE 21434,[11] where aftermarket connectivity cannot create cyber-physical safety issues with the vehicle. The standards' community is actively working on standards to address the issue of aftermarket connectivity that cannot create cybersecurity breaches. Such advancements need to be considered and adopted by the manufacturers.

Furthermore, regarding "varying levels of cybersecurity protections on the vehicle side of the interface," consideration for the upcoming regulation like the European UNECE WP29 Automotive Cybersecurity Regulation[12] to be a template to assist manufacturers to produce more secure vehicles.

Serviceability

Regarding Section 7, Serviceability. As a company who prioritizes cybersecurity and serviceability to our end-users, we agree and appreciate NHTSA's recognition for the balance between third-party serviceability and cybersecurity, and how cybersecurity should not be a reason to justify the limiting of serviceability. However, this section states to not unduly restrict access by third-party repair services as long as they are authorized. We are concerned that the term "unduly" is not well-defined, which can be interpreted by manufacturers to simply not authorize any third-party, which would be problematic.

We do agree on the language of "authorized by the vehicle owner." We hold the perspective that the vehicle owner has the right to authorize and determine who has access to the vehicle-generated data to solve their unique needs.

Technical Vehicle Cybersecurity Best Practices

Cryptographic Credentials

In section 8.2 Cryptographic Credentials, sub point T.3, we are concerned about the term "authorized" as it is unclear who is being authorized to whom, as well as how such an authorization process would work. In the same sentence we are concerned about "elevated level of access" as it is unclearly defined. Further clarity regarding "elevated level access" is needed to better recommend if vehicle-generated data is read broadcast data, a request using SAE/ISO protocol's, a set vehicle parameters, or an update to the vehicle ECU's. Each of these is elevated access relative to the next.

To Geotab, the term "elevated level of access" implies a hierarchy to vehicle-generated data. We are interested in clarification on how such credentials would work in the field, considerations for achieving these various levels for non-manufacturing companies.

[11] https://www.sae.org/standards/content/iso/sae21434.d1/
[12] https://argus-sec.com/unece-wp29-automotive-cybersecurity-regulation/

Vehicle Diagnostic Functionality

We believe section 8.3 Vehicle Diagnostic Functionality sub point T.5 regarding diagnostic features needs further clarity, as this could have an indefinite number of interpretations. In addition, we believe it is the owner of the vehicle who should control how and when diagnostic features should be activated. The current definition limits diagnostics to a specific mode of operation, which is undefined, and could lead to inconsistent adoption.

One example from our perspective regards the prevention of the bleeding of brakes via the OBD port command, in which the vehicle should be in a service mode - engine off, or a similar stationary mode. Our concern is that this recommendation is not explicit enough. For instance, if the “specific mode” allows a less cyber-physical diagnostic service, such as a clear Diagnostic Trouble Code, it should not be more restrictive that it has to maintain a reasonable level of safety. This is not the same as when bleeding the vehicle brakes via OBD port command.

Regarding sub point T.7, we request further clarification on what is meant by “global symmetric keys and ad-hoc cryptographic techniques for diagnostic access should be minimized.” As we understand, “global symmetric keys” is one key for everyone, and thus would require a certificate-based authentication with a chain of trust. We appreciate NHTSA’s further clarification as to how NHTSA’s recommendation related to cryptographic credentials.

Diagnostic Tools

Section 8.4, Diagnostic Tools: to our knowledge, “authentication keys” are to be kept secure, though there is nothing secure about the keys themselves. As such, the emphasis on the security controls placed on those keys is what is necessary to keep those keys secure. These keys require sufficient cryptographic protection to prevent abuse, so that they are not practically visible and/or able to be reverse engineered.

Regarding sub point T.8, we are interested in further clarification on how vehicle and diagnostic tool manufacturers would control the tool’s access to the vehicle systems.

Vehicle Internal Communications

Regarding section 8.5 Vehicle Internal Communications sub point T.9, we are concerned with the statement “inaccessible through external vehicle interface,” as critical safety codes should be “read only.” This critical data needs to be able to be read and used, as a “read only” intervention in the critical safety message is prevented.

Section 8.5 Vehicle Internal Communications makes mention of dedicated transport mechanisms for safety critical signals that will be inaccessible through external vehicle interfaces. However, many signals can be safety critical or used by safety critical components. This recommendation as stated could excuse a restrictive gateway on many signals that we are currently used to reading off the CAN bus/OBDII port.

Network Ports, Protocols, and Services

8.7.3 Network Ports, Protocols, and Services, sub point T.16 mentions “Eliminating unnecessary internal protocol services.” Geotab requests further clarification regarding who and what defines which protocols are “unnecessary.” Likewise, regarding sub points T.17 and T.18, further clarification is needed to determine limitations, essential functionality and authorized parties. As vehicle-generated data is dynamic, our customers require such functionality as diagnostic trouble codes and sensor outputs which include vehicle accelerations, engine rpm, steering input.

Software Updates / Modifications

Regarding section 8.8, Software Updates / Modifications, sub point T.21, we are concerned about how automotive manufacturers would “employ state-of-the-art technologies for limiting the ability to modify firmware to authorized and appropriately authenticated parties.”

Over-the-Air Software Updates

Section 8.9 Over-the-Air (OTA) Software Updates, states that “Manufacturers that design-in and offer OTA software update capability on their vehicle.” The aftermarket should have the possibility to provide vehicle ECU updates OTA. As vehicles are long-term durable assets, their needs for long-term patch maintenance requires emphasis. Technically, Geotab can provide vehicle ECU firmware updates for vehicles that do not have built-in capabilities for vehicle ECU OTA updates. Thus, we believe aftermarket solutions should be allowed to provide ECU updates, given OEM engagement. It is also important to have a process that ensures authenticity of ECU updates.