United States Senate

June 11, 2020

Acting Administrator James Owens
National Highway Traffic Safety Administration
1200 New Jersey Avenue, SE
Washington, DC 20590

Dear Acting Administrator Owens:

We appreciate your December 5, 2019, response regarding how the National Highway Traffic Safety Administration (NHTSA) approaches cybersecurity issues with internet-connected cars. However, after reviewing your response, we remain concerned that NHTSA has taken a hands-off approach to the growing threats to public safety from vulnerabilities in internet-connected cars. We also believe that NHTSA is neglecting to oversee and keep the public informed about over-the-air (OTA) software updates designed to fix safety defects in cars without a physical recall. We write today to detail these concerns, as well as to urge NHTSA to take more robust action to protect all drivers, passengers, and pedestrians put at risk.

We are deeply troubled by NHTSA's deafening silence in response to the repeated reports of vulnerabilities and risks of hacking of internet-connected cars. In your reply to our initial letter, you stated that "NHTSA is not aware of any malicious hacking attempts that have created safety concerns for the motoring public."[1] However, this statement sets aside the many examples of demonstrated vulnerabilities in cars on the road that have been publicly reported in recent years, and relies on the goodwill of those who have reported these risks.

For instance, after Chinese researchers posted a video in 2016 showing that they could remotely activate the brakes in a Tesla, NHTSA appeared to take no action.[2] Less than a year later, Chinese researchers demonstrated another remote hack on a Tesla,[3] and followed it up with a similar hack on a BMW in 2018, again resulting in no public response by NHTSA.[4] In February of this year, U.S. researchers demonstrated that road-monitoring camera systems can be hacked into misreading speed limit signs, causing a car to autonomously speed up 50 miles per hour.[5] As

[1] Adam J. Sullivan (Assistant Secretary for Governmental Affairs), *Letter to Senator Markey* (December 5, 2019). https://www.markey.senate.gov/download/dot-nhtsa-response-to-cybersecurity-of-internet-connected-cars-letter.
[2] Andy Greenberg, Tesla Responds to Chinese Hack With a Major Security Upgrade, WIRED (Sept. 27, 2016), https://www.wired.com/2016/09/tesla-responds-chinese-hack-major-security-upgrade/.
[3] Eduard Kovacs, *Tesla Model X Hacked by Chinese Experts*, SECURITY WEEK (July 28, 2017). https://www.securityweek.com/tesla-model-x-hacked-chinese-experts.
[4] BMW Press Club, *First-ever BMW Digitalization and IT Research Award goes to Tencent Keen Security Lab for their connectivity and cybersecurity research*, BMW (May 22, 2018). https://www.press.bmwgroup.com/global/article/detail/T0281245EN/first-ever-bmw-group-digitalization-and-it-research-award-goes-to-tencent-keen-security-lab-for-their-connectivity-and-cybersecurity-research-the-two-companies-plan-to-expand-their-cooperation-and-joint-research-work.
[5] Isobel Asher Hamilton, *Hackers stuck a 2-inch strip of tape on a 35-mph speed sign and successfully tricked 2 Teslas into accelerating to 85 mph*, BUSINESS INSIDER (Feb. 19, 2019), https://www.businessinsider.com/hackers-trick-tesla-accelerating-85mph-using-tape-2020-2.

we also flagged in our initial letter, automakers themselves have reported potential cyber vulnerabilities in their investor filings.[6]

These reports are all public information that NHTSA should be proactively monitoring and using to evaluate threats to cybersecurity. We are fortunate that these researchers acted responsibly and professionally, but we should not assume that only good-faith actors are investigating such threats. We believe NHTSA must end its dangerously reactive approach to cybersecurity and do more to protect consumers before a malicious attack leading to a fatality occurs.

These repeated examples of vulnerabilities demonstrate another urgent issue that NHTSA has not adequately addressed: the rise of OTA software updates to fix safety-related defects without a physical recall. With a growing number of internet-connected cars on the road, automakers are increasingly using OTA updates to fix both cybersecurity vulnerabilities and physical safety issues. For example, Tesla has used OTA updates to address braking distance and battery fire problems.[7] In light of this trend, we believe that NHTSA should not limit its involvement to physical recalls and needs to have a process in place to systematically monitor, handle, and inform the public about digital fixes. As NHTSA itself has previously recognized, software defects are still defects, and automakers have a responsibility to "follow the recall process before issuing a remote fix."[8]

NHTSA has failed to put into place a reliable and active mechanism to investigate OTA software updates and facilitate public awareness of such safety concerns. While NHTSA did investigate some OTA updates in 2019, these actions appear to have been driven by defect petitions filed by consumers rather than any proactive NHTSA process.[9] There is no indication that NHTSA is conducting robust oversight or guaranteeing public disclosure of OTA software updates, even if they are addressing a safety-related defect that would have previously resulted in a physical recall. We therefore urge NHTSA to develop processes that will ensure automakers are publicly accountable for all safety-related defects no matter how they are fixed.

In light of our concerns around proactively protecting the public from cyber security vulnerabilities and overseeing OTA updates by automakers, we respectfully request that NHTSA answer the following questions by July 2, 2020.

1) How is NHTSA proactively protecting the public from cybersecurity threats to internet-connected cars?

---

[6] *E.g.*, Ford Motor Company, 2018 Annual Report (Form 10-K) Page 18 (Feb. 21, 2019) ("We have been the target of these types of attacks in the past and such attacks are likely to occur in the future."). https://www.sec.gov/Archives/edgar/data/37996/000003799618000015/f1231201710-k.htm.

[7] Patrick Olsen, *Tesla Model 3 Gets CR Recommendation After Braking Update*, CONSUMER REPORTS (May 30, 2018), https://www.consumerreports.org/car-safety/tesla-model-3-gets-cr-recommendation-after-braking-update/. Sean O'Kane, *Tesla is being investigated for a software update meant to limit fire risk*, THE VERGE (Oct. 4, 2019), https://www.theverge.com/2019/10/4/20898741/tesla-cars-nhtsa-software-ota-safety-update-battery-fires-range.

[8] Katie Burke, *Over-the-air updates may alter NHTSA recall policy*, AUTOMOTIVE NEWS (Jan. 23, 2017), https://www.autonews.com/article/20170123/OEM11/301239815/over-the-air-updates-may-alter-nhtsa-recall-policy.

[9] *Id.*

a. Is NHTSA monitoring, and does it act, when researchers demonstrate successful hacks on connected cars?

b. If NHTSA is not monitoring these research reports, who is responsible for monitoring cybersecurity threats to connected cars?

c. Is there a process in place for automakers to notify NHTSA about cybersecurity vulnerabilities, and if so, what does NHTSA do with this information?

d. Is NHTSA monitoring, and does it act, when automakers publicly report, even if not directly to NHTSA, potential cybersecurity threats to their vehicles?

2) How does NHTSA monitor and respond to OTA software updates for internet-connected cars?

a. Do automakers voluntarily notify NHTSA about their OTA updates? If so, does every automaker notify NHTSA, or just some? If not, how does NHTSA track other public notices of OTA updates?

b. What processes does NHTSA use to evaluate OTA updates, and when do such updates trigger a NHTSA investigation?

3) Does NHTSA have the legal authority to change its regulations to require public disclosure of OTA software updates designed to correct safety-related defects?

a. If so, will it use that power to make these changes?

b. If not, what legislation does NHTSA require to give it this authority?

Thank you for your continued attention to this important matter.

Sincerely,

Edward J. Markey
United States Senator

Richard Blumenthal
United States Senator