As other commenters have mentioned the newest form of this document is a marked improvement over previous iterations. I am especially fond of the title change in order to emphasize this document's focus on, "cybersecurity issues that impact the safety of motor vehicles throughout the lifecycle of design, operation, maintenance, and disposal." Too often regulatory documents can fall victim to scope creep, and become too unwieldy to be useful for their original intent. This comment is meant to show my support for the stated goal of this document as well as outline some concerns I, as well as other commenters, hold. These opinions are informed by my current research as a student as well as my previous experience as an IT generalist and cybersecurity analyst.

It is clear that some form of cybersecurity standards in the automotive industry, as well as most others, is critical for the safety of any involved individuals or groups. As stated this document will focus on security areas that threaten the safety of vehicles and their passengers which is a necessary level of focus in order to craft effective standards. Making the regulations non-binding ensures industry cooperation on the issue, and is praised by multiple non-partisan groups such as the Brookings Institute and Information Technology & Innovation Foundation (ITIF). Additionally, both aforementioned groups support the "industry-led" attitude towards developing these regulations. Working with these manufacturers is the best way to ensure compliance with the regulations as well as making sure resources are being used to safeguard vulnerabilities or attack surfaces that are most targeted by bad actors. In addition to the views of these groups, drivers cannot be expected to have a technical skill set in using these vehicles outside of standard vehicle operation. These regulations place the burden of these security vulnerabilities where they belong, on manufacturers. Consumers cannot be asked to shoulder the potential threat to their vehicles from cyber attack, and with the rise of automated driving systems, the systems which allow cars to operate will be inaccessible to the majority of all drivers. This document's stated goals are essential, and in all stated aspects is an improvement over its predecessors, which will lead to improved safety for motor vehicles and their operators.

The first concern I will raise is maintaining the ability for consumers to use after-market modifications and repairs. Additionally, consumers have a right to access information from their vehicle as long as that information does not inherently create an exploitable weakness. Other commenters have shared stories of farmers being unable to engage in simple repairs due to security measures on their farming equipment and it would be a shame to allow this problem to affect the even larger population of motorists that would be affected by these guidelines. The citizenry clearly values its ability to seek these after-market modifications or third party repairs, with "right to repair" laws being supported nationwide, including recently in my home state of Massachusetts with 75% approval. Protecting the rights of consumers to work on their own vehicles and preventing an effective monopolization of auto-repair should be factored into any regulations considered in this document.

The second concern is the risk of creating a security "monoculture." In other words, creating a standard practice that is so consistent, that security becomes predictable to would-be attackers. This is a difficult issue to navigate since it means that all vehicles will not be able to use the same security infrastructure. Companies will have to create their own secure countermeasures to threats to achieve the best standard practices set by this document, and securely share them with the NHTSA if applicable. It is good that the summary of this document explains that all aspects of the automotive cybersecurity lifecycle will be examined, and it should continue to be reiterated that effective cybersecurity is a sustained, ongoing process. Since updating software once vehicles have left the dealership is a logistical nightmare, it is important that special attention be paid to vulnerabilities before leaving the lot. A zero-day vulnerability across a particular vehicle being sold would have catastrophic safety implications, compounded further if the same exploit could be used between the cars of multiple manufacturers due to a security monoculture. It will be important that manufacturers achieve these best practices via different methods and that the NHTSA, if made aware of manufacturers' plans and redundancies, are able to advise as needed.

All these concerns aside, the *Cybersecurity Best Practices for the Safety of Modern Vehicles* is a necessary document in an era where too often technological advancements outpace regulation. The alternative of providing no guidance to manufacturers and letting them set their own standards, would be unwise and risk the safety of countless motor vehicles. A central document containing best practices met differently by each manufacturer, monitored by the NHTSA appears to be the best solution for the issue.