Published on *The National Law Review* https://natlawreview.com

2016 Outlook: NHTSA, Automotive Safety, and Cybersecurity

Article By:

Christopher H. Grigorian

2016 will likely be an active year for the ***National Highway Traffic Safety Administration (NHTSA)*** and increased enforcement actions and new technology and privacy measures are expected. Below are four things to keep in mind for the coming year.

Continued Aggressive Enforcement

The automotive industry was hit with more than $470 million in civil penalties during 2015. These penalties were imposed against manufacturers of all types of vehicles and equipment — passenger cars; trucks, emergency vehicles, and chassis; recreational vehicles; air bags and other equipment; and child restraints. Never has the message to the industry been clearer: Get compliant or get fined!

To reduce compliance risks, all vehicle and component manufacturers should take the following actions *now*:

- Implement (or review existing) safety compliance policies that provide internal guidance to company personnel for identifying and investigating potential safety defects and noncompliance.
- Implement (or review existing) procedures for complying with all associated NHTSA reporting requirements (e.g., defect reporting, early warning reporting, and reporting certain non-safety bulletins and customer communications).
- Revisit early warning reporting procedures to ensure they capture all relevant information (for suppliers, this means fatality claims and notices) and that early warning reports are filed with NHTSA on a timely basis.
- Conduct thorough training of key personnel across the organization — domestically and globally — on these policies and procedures, and on the importance of bringing potential safety concerns to the attention of appropriate personnel or safety committees.

The FAST Act

Recently, President Obama signed the bipartisan Fixing America's Surface Transportation Act or FAST Act, a five-year transportation bill that contains numerous motor vehicle safety provisions, which will significantly impact manufacturers. First and foremost, the legislation increases the civil maximum to $105 million from $35 million. Apart from the increase in civil penalty authority, there are many other provisions of which manufacturers should be aware, including but not limited to:

- whistleblower rewards
- improvements in availability of recall information
- provisions concerning ownership and use of data from electronic data records
- establishing a tire recall database
- tire fuel efficiency standards
- limits on rental of vehicles with open recalls
- dealers' obligation to check for open recalls

Notably absent from the legislation are provisions that would expressly impose criminal liability on manufacturers or individuals, despite prior legislative proposals that would have done so.

Driverless/Autonomous Vehicles and Crash Avoidance Technologies

NHTSA has been carefully studying the safety benefits of various advanced crash avoidance technologies for several years, with a particular focus on warning technologies.

The agency has also been studying vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2I) communications as a way to improve the effectiveness and availability of these safety systems. According to NHTSA, "by mandating V2V technology in all new vehicles, but not requiring specific safety applications, it is NHTSA's belief that such capability will in turn facilitate market-driven development and introduction of a variety of safety applications, as well as mobility and environment-related applications that can potentially save drivers both time and fuel." It recently announced that it is currently targeting to have a notice of proposed rulemaking (NPRM) on a V2V standard by May 2016.

Cybersecurity

Vehicle cybersecurity is not a new topic, but the issue gained more prominence after Fiat Chrysler Automobiles decided to recall 1.4 million vehicles to address software vulnerabilities identified by "white hat" cybersecurity researchers.

Meanwhile, several bills have been introduced in the U.S. Congress to address vehicle cybersecurity. In July, the Security and Privacy in Your Car Act, or SPY Car Act was introduced in the Senate. That bill would require NHTSA, in consultation with the Federal Trade Commission (FTC), to develop standards that prevent hacking into vehicle control systems.

In November, a separate bill was introduced in the U.S. House of Representatives. The SPY Car Study Act, would require NHTSA, in consultation with the FTC and other agencies, organizations, and manufacturers to conduct a study to determine appropriate standards for the federal regulation of vehicular cybersecurity.

Other developments include the announcement by the Alliance of Automobile Manufacturers and the Association of Global Automakers that they are establishing an Information Sharing and Analysis Center (ISAC) to facilitate industry-wide analysis and sharing of information on cyber threats and vulnerabilities.

National Law Review, Volume VI, Number 20