BALOUGH LAW OFFICES, LLC

Feds Seek Comments on Proposed Guidance on Vehicle Cyberattacks

For the first time, under a proposed Enforcement Guidance Bulletin, automobile makers will need to take into account cybersecurity vulnerabilities for their vehicles.

The National Highway Traffic Safety Administration (NHTSA) published a request for public comments (RPC) in which it outlined the factors it would take into account to determine if cybersecurity risks pose an "unreasonable risk to safety."

The RPC noted that vehicle software "presents its own unique safety risks." For example, "[w]here an autonomous vehicle or other emerging automotive technology causes crashes or injuries, or has a manifested safety-related failure or defect, and a manufacturer fails to act, NHTSA will exercise its enforcement authority to the fullest extent." To avoid NHTSA action, "manufacturers of emerging technology and the motor vehicles on which such technology is installed are strongly encouraged to take steps to proactively identify and resolve safety concerns before their products are available for uses on public roadways."

In the RPC, the NHTSA said it would consider the following factors to determine whether a vulnerability imposes an unreasonable risk to safety:

- The amount of time elapsed since the vulnerability was discovered (e.g., less than one day, three months, or more than six months);
- The level of expertise needed to exploit the vulnerability (e.g., whether a layman can exploit the vulnerability or whether it takes experts to do so);
- The accessibility of knowledge of the underlying system (e.g., whether how the system works is public knowledge or whether it is sensitive and restricted);
- The necessary window of opportunity to exploit the vulnerability (e.g., an unlimited window or a very narrow window); and
- The level of equipment needed to exploit the vulnerability (e.g., standard or highly specialized).

The NHTSA said it is not necessary that actual hacking has occurred for it to initiate a recall, but a recall may be required if it is foreseeable that hackers will try to exploit the vulnerability.

"For instance, if a cybersecurity vulnerability in any of a motor vehicle's entry points (e.g., Wi-Fi, infotainment systems, the OBD-II port) allows remote access to a motor vehicle's critical safety systems (i.e., systems encompassing critical control functions such as breaking, steering, or acceleration), the NHTSA may consider such a vulnerability to be a safety-related defect compelling a recall."

Comments are due by May 2, 2016.

Balough Law Offices has made several presentations and written articles regarding the cybersecurity risks caused by the vulnerability of cars to hacking.

Balough Law Offices, LLC, is a Chicago-based law firm that focuses on cyberspace, intellectual property, and business law. Our homepage is balough.com.