Jeanna Neefe Matthews
Associate Professor of Computer Science, Clarkson University
Statement on AV START Act
July 23 2018

My name is Jeanna Matthews. I am a computer science professor and computer security researcher. I have experience identifying vulnerabilities in complex systems from the virtualization software underpinning cloud computing to software used in the criminal justice system to compare DNA in evidence samples to a suspect's DNA. For over 10 years, I have been part of the Association for Computing Machinery (ACM) technology policy effort.

Modern automobiles are extremely complex, Internet-connected, software-controlled systems. Just like it is difficult to keep bugs and malicious actors out of our laptops, it is difficult to keep them out of modern cars. However, unlike a laptop, the computer system in a car is attached to 4000 pounds of metal that can travel at 75 miles per hour or more.

Security vulnerabilities in autonomous vehicles represent a huge risk to human safety. Successful attacks on automobiles have already been demonstrated including gaining control of steering and braking over the Internet. The AV START Act would only require manufacturers to have a written plan for identifying and reducing cybersecurity risks. That is simply not enough. More substantive cybersecurity standards are only common sense before we the public - drivers, passengers, bicyclists, pedestrians- are asked to share the road with autonomous vehicles.

As a computer security researcher, I know well that security through obscurity is not enough. We need requirements for transparency and iterative improvement. We should be requiring that manufacturers conduct and document thorough threat analysis and risk assessments. There should be requirements for sharing of information and data on cybersecurity vulnerabilities, attacks and patches. Manufacturers should also be required to separate critical safety systems from other systems (e.g. infotainment) whether through a firewall or a completely separate architecture in the vehicle to reduce the exposure of critical safety systems to additional attack surfaces.

Attaching the AV START Act to a must-pass FAA bill is an egregious maneuver to avoid common sense investments in public safety, government oversight and industry accountability. It would be a blank check to an industry that is not prepared to police itself. Computer security researchers, like me, know how easy it is to overestimate your company's engineering abilities and underestimate both software flaws and the ability of attackers in a rush to market.

Simply put, rushed legislation plus 4000 pound vehicles plus no human driver plus software vulnerabilities equals a recipe for disaster and human tragedy.