

**Congress of the United States**  
**House of Representatives**  
Washington, DC 20515-1303

December 29, 2014

The Honorable Gene Dodaro  
Comptroller General of the United States  
441 G Street, NW  
Washington, DC 20548

Dear Mr. Dodaro:

There are over 250 million registered vehicles in the United States, and each year the cyber-physical systems in these vehicles become more complicated. Simultaneously, the consequences of a security breach in these systems have increased, especially with regards to safety and privacy. For example, safety critical functions, including brakes, are electronically controlled and personal information, such as location, are electronically communicated. Many people, including DARPA researchers, have shown that it is feasible to hack vehicles and take control of safety critical functions. These cyber-physical vulnerabilities pose a risk to individual vehicle operators, as well as the homeland in the case of a coordinated attack. In light of these concerns, we would like to request that GAO examine the following issues:

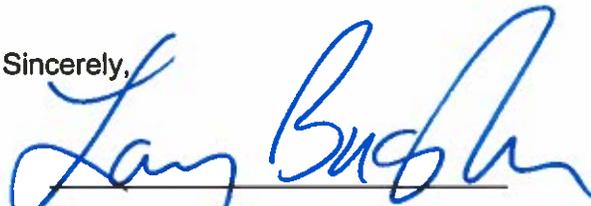
1. What are the current and foreseeable vehicular cyber-physical vulnerabilities and risks, especially concerning safety, privacy, and homeland security?
2. What research and development efforts is the Department of Transportation (DOT) undertaking to address and communicate current and foreseeable risks?
3. Are there technologies available to mitigate the risks associated with vehicle cyber-physical systems that are not being implemented?

Thank you for your timely attention to this request. If you have any additional questions, please contact Shawn Kimmel in Congressman Daniel Lipinski's office at shawn.kimmel@mail.house.gov or at (202) 225-5701.



Daniel Lipinski  
Committee on Science, Space, and  
Technology  
Ranking Member, Subcommittee on  
Research and Technology

Sincerely,



Larry Bucshon, M.D.  
Committee on Science, Space, and  
Technology  
Chairman, Subcommittee on  
Research and Technology