U.S. Department of Transportation

National Highway Traffic Safety Administration

ODI RESUME

OFFICE OF DEFECTS INVESTIGATION

NHTSA

Authentic US Government Information
National Highway Traffic Safety Administration uses a *digital certificate* to ensure the content has remained unchanged

Investigation:	DP 21-005		
Prompted by:	Defect Petition		
Date Opened:	12/23/2021	**Date Closed:**	02/07/2022
Investigator:	Ryan Rahimpour	**Reviewer:**	Joshua Neff
Approver:	Stephen Ridella		
Subject:	SAE J1939 Data Bus Vulnerability		

MANUFACTURER & PRODUCT INFORMATION

Manufacturer:	Generic Manufacturer
Products:	2001 School Bus and 2006 Class-8 Semi-Tractor
Population:	1,000,000 (Estimated)
Problem Description:	A petitioner identified a University of Michigan report alleging that a vulnerability exists in the Society of Automotive Engineers (SAE) J1939 Data Bus standard with respect to 2001 school buses and 2006 Class-8 semi-tractors, enabling vehicle critical safety functions, such as the accelerator control system or braking system, to be susceptible to unauthorized access and control.

FAILURE REPORT SUMMARY

	ODI	Manufacturer	Total
Complaints:	1	0	0
Crashes/Fires:	0	0	0
Injury Incidents:	0	0	0
Fatality Incidents:	0	0	0

ACTION / SUMMARY INFORMATION

Action: Petition is denied, close DP.

Summary:

In a letter dated September 27, 2021, Mr. James Lamb, Executive Director of the Small Business in Transportation Coalition (SBTC), petitioned the National Highway Traffic Safety Administration (NHTSA), requesting the initiation of a defect investigation into the potential hacking susceptibility of the Society of Automotive Engineers (SAE) J1939 Data Bus standard. SAE J1939 is the vehicle bus recommended practice used for communication and diagnostics among vehicle components. In support of the petition, the petitioner cited a study from University of Michigan (Michigan) researchers alleging a SAE J1939 Data Bus vulnerability in a Model Year (MY) 2001 school bus and a MY 2006 Class-8 semi-tractor. The study alleges that, due to the vulnerability, vehicle critical safety functions such as the accelerator control or braking systems are susceptible to unauthorized access and control and increases risk to motor vehicle safety.

On December 23, 2021, the Office of Defects Investigation (ODI) opened DP21-005 to evaluate the petitioner's request. The petitioner did not specify the make and model of the vehicles with the alleged safety defect. The only categories of relevant vehicles specified were found in the study: MY 2001 school buses and MY 2006 Class-8 semi-tractors. ODI has not received any complaints of any type related to this alleged vulnerability (The single complaint identified above is the petition.). This evaluation included searches of complaints from vehicle owners, operators, and fleet supervisors. Further, based on the available information, ODI has not found any similar events/complaints/ allegations suggesting a real-life vulnerability.

The vehicle compromises reported in the Michigan study required physical access to the J1939 connector in order to affect vehicle critical safety functions such as the accelerator control or braking systems. Whether there is a potential for remote compromise is a factor that NHTSA has considered in evaluating the likelihood or frequency of a potential safety defect. The Michigan study did not demonstrate a remote compromise of these vehicles. In addition, based on

the age of the subject model year school buses and semi-tractors, they do not have over-the-air software update capabilities/internet connection to make remote compromise possible. Therefore, given a thorough analysis of the potential for finding a safety-related defect in the subject vehicles, and in view of NHTSA's enforcement priorities, a defects investigation is unlikely to result in a finding that a defect related to motor vehicle safety exists.

NHTSA is authorized to issue an order requiring notification and remedy of a defect if the Agency's investigation shows a defect in the design, construction, or performance of a motor vehicle that presents an unreasonable risk to safety (49 U.S.C. §§ 30102(a)(9), 30118). Given the absence of any similar events/incidents related to this matter and lack of demonstrated potential for remote compromise, it is unlikely that an order concerning the notification and remedy of a safety-related defect would be issued due to any investigation opened as a result of granting this petition.

Therefore, upon full consideration of the information presented in the petition, and the potential risks to safety, the petition is denied. The denial of this petition does not foreclose the Agency from taking further action if warranted, or the potential for a future finding that a safety-related defect exists based upon additional information the Agency may receive. A notice of denial of this petition will be published in the Federal Register.