Paperwork Reduction Act of 1995. The proposed collection OMB 2133–0025 Automated Mutual Assistance Vessel Rescue (AMVER) System is used to maintain a current plot of U.S.-Flag and U.S.-owned vessels. Since the last renewal, there was an increase in the total respondents to this collection, which has resulted in more responses and higher burden hours. There are no other changes to this collection. We are required to publish this notice in the **Federal Register** to obtain comments from the public and affected agencies.

ADDRESSES: Written comments and recommendations for the proposed information collections should be sent within 30 days of publication of this notice to *www.reginfo.gov/public/do/PRAMain.* Find this particular information collection by selecting ''Currently under 30-day Review—Open for Public Comments'' or by using the search function.

FOR FURTHER INFORMATION CONTACT: Alex Sedlacek, 202–366–1031, Division of Sealift Operations and Emergency Response, Maritime Administration, U.S. Department of Transportation, 1200 New Jersey Ave. SE, Washington, DC 20590, Email: *alexander.sedlacek@dot.gov.*

SUPPLEMENTARY INFORMATION:

Title: Automated Mutual-Assistance Vessel Rescue (AMVER) System.

OMB Control Number: 2133–0025.

Type of Request: Extension with Change of a Previously Approved Collection.

Abstract: The collection of information will be used to gather information regarding the location of U.S.-flag vessels and certain other U.S. citizen-owned vessels for the purpose of search and rescue in the saving of lives at sea and for the marshalling of ships for national defense and safety purposes.

Respondents: U.S.-flag and U.S. citizen-owned vessels.

Affected Public: Business or other for profit.

Estimated Number of Respondents: 185.

Estimated Number of Responses: 33,855.

Estimated Hours per Response: .07.

Annual Estimated Total Annual Burden Hours: 2,370.

Frequency of Response: Annually.

A 60-day **Federal Register** Notice soliciting comments on this information collection was published on September 12, 2024 at 89 FR 74371 (**Federal Register** (FR) 2024–20679).

(Authority: The Paperwork Reduction Act of 1995; 44 U.S.C. chapter 35, as amended; and 49 CFR 1.49.)

By Order of the Maritime Administrator.

T. Mitchell Hudson, Jr.,

Secretary, Maritime Administration.

[FR Doc. 2024–27344 Filed 11–21–24; 8:45 am]

BILLING CODE 4910–81–P

DEPARTMENT OF TRANSPORTATION

National Highway Traffic Safety Administration

[Docket No. NHTSA–2024–0086]

Denial of Motor Vehicle Defect Petition

AGENCY: National Highway Traffic Safety Administration (NHTSA), Department of Transportation.

ACTION: Denial of petition for a defect investigation.

SUMMARY: This notice sets forth the reasons for the denial of a petition submitted on June 7, 2023, by Kimberlyn Hearns (the petitioner) to NHTSA's Office of Defects Investigation (ODI). The petition requests that the Agency initiate an investigation into alleged remote attacks to the vehicle electrical control system associated with a variety of reported electrical malfunctions that render the petitioner's Model Year 2019 Toyota Yaris vehicle (subject vehicle) allegedly unusable. On August 30, 2023, NHTSA opened Defect Petition DP23–004 to evaluate the petitioner's request. After conducting a technical review of the petitioner's submissions, seeing no other complaints for 2019 Toyota Yaris vehicles related to the types of ''remote attacks'' described by the petitioner, and reviewing information provided by Toyota in response to an Agency request for information regarding the 2019 Yaris CAN bus, NHTSA has concluded that there is insufficient evidence to pursue further investigation. Accordingly, the Agency has denied the petition.

FOR FURTHER INFORMATION CONTACT: Mr. Tariq Bond, Vehicle Defects Division—D, Office of Defects Investigation, NHTSA 1200 New Jersey Ave. SE, Washington, DC 20590. Telephone (202) 366–5472. Email: *Tariq.Bond@dot.gov.*

SUPPLEMENTARY INFORMATION:

Introduction

Interested persons may petition NHTSA requesting that the Agency initiate an investigation to determine whether a motor vehicle or an item of replacement equipment does not comply with an applicable motor vehicle safety standard or contains a defect that relates to motor vehicle safety. 49 U.S.C. 30162; 49 CFR 552.1. Upon receipt of a properly filed petition, the Agency conducts a technical review of the petition, material submitted with the petition, and any additional information. 49 U.S.C. 30162(c); 49 CFR 552.6. The technical review may consist solely of a review of information already in the possession of the Agency or it may include the collection of information from the motor vehicle manufacturer or other sources. After conducting the technical review and considering appropriate factors, which may include, but are not limited to, allocation of Agency resources, Agency priorities, and the likelihood of success in litigation that might arise from a determination of noncompliance or a defect related to motor vehicle safety, the Agency will grant or deny the petition. *See* 49 U.S.C. 30162(d); 49 CFR 552.8.

Background Information

In a letter dated June 7, 2023, Kimberlyn Hearns (the petitioner) submitted a petition attributing electrical malfunctions of his 2019 Toyota Yaris (subject vehicle) to remote attacks by unknown parties targeted on the subject vehicle's Controller Area Network (CAN bus).[1] The petitioner requested an Agency investigation of the susceptibility of the subject vehicle to the alleged attacks and for assistance securing a full refund of the vehicle price. Over four total submissions from the June 7, 2023 petition to August 2, 2023, the petitioner supported his request with a chronology of events detailing the vehicle fault, service history, and a listing of published cybersecurity articles. In addition, before filing the petition, the petitioner sent three pieces of related correspondence to the Agency from late December 2022 to February 2023.

NHTSA has based its decision on a review of the material cited by the petitioner in his petition, information submitted by Toyota in response to the Agency's request, and other pertinent information in NHTSA's databases. Staff from NHTSA's Vehicle Research and Test Center (VRTC) supported the review at all stages.

Subject Vehicle History

The subject vehicle is a Model Year (MY) 2019 Toyota Yaris LE equipped with a 1.5L I4 gasoline engine. According to a vehicle history report, the subject vehicle has only been owned by one person (the petitioner), started receiving service in August of 2019, and has not experienced any reported

[1] Modern automobiles (including the subject vehicle) contain multitudes of microcontrollers that communicate over a self-contained computer network known as a Controller Area Network.

collisions or damage. The vehicle history report indicated regular servicing of the subject vehicle by the Toyota dealership that sold it to the petitioner, with no atypical problems evident through June of 2022 and after approximately 40,000 miles of service. During this time, the subject vehicle received remedies related to two Toyota field campaigns: Service Campaign 20TC03 [2] (performed September 2020) and Safety Recall 21V617 [3] (performed January 2022).

In mid-November of 2022, with 46,136 miles of service,[4] the petitioner reported hearing three beeps while driving at low speed, accompanied by engine shut down. After a delay, the petitioner was able to restart the vehicle, but a Check Engine Light (CEL) remained illuminated. The petitioner's dealer diagnosed the problem as a bad battery and installed a replacement battery.

Over the ensuing two weeks, and approximately 700 miles, the petitioner reported several instances of engine power loss, malfunctioning indicator lights, and a head unit delayed start malfunction, leading to service at a different Toyota dealer in early December 2022. That dealer's invoice reported that no problem had been identified after several service checks, inspection of the ECU wiring, and after approximately 30 miles of test driving over a two-day period. At the time of its release from this dealership, the invoice reported that the subject vehicle had an odometer reading of 47,009 miles. Toyota reported that the dealership had also contacted its Technical Assistance Center for further guidance.

The vehicle history report indicates that the subject vehicle traveled only 44 miles over the following three months, returning to its regular servicing dealership in late March 2023, about a week after another report from the petitioner of flashing warning lights and repeated horn activation while the petitioner was inside his house. The petitioner reported that this mid-March incident coincided with a suspicious vehicle driving by his house. The petitioner also stated that in late March, a service visit to his regular servicing dealership included the removal of an aftermarket vehicle security system manufactured by Rockledge Securities.[5]

No further service records from Toyota or the vehicle history report appear after March 27, 2023. The petitioner reported eleven instances of continued malfunctions from March 30 through June 3, 2023 related to horn activation, inoperative key-fob, no-start condition, and fuel gauge inaccuracies. The petitioner also reported that two of these malfunctions coincided with suspicious vehicles driving by his house. The petitioner then began documenting various additional events, including a no-start condition followed by a jump-start, inaccurate/slowly responding fuel gauge, intermittent CEL, ''nearly unreadable'' instrument cluster, an inability to turn off the engine, and inoperative fan, wipers, and signals. Petitioner also cited attempts to maintain the battery state of charge by idling the subject vehicle in his driveway. At the time of the petitioner's last contact with NHTSA in August 2023, the petitioner reported that his subject vehicle was unusable, despite efforts to maintain the charge of its battery.

Subject Vehicle Connectivity

Although the petitioner asserts that his vehicle is under remote electronic attack, and stipulates that the subject vehicle is not defective; the Agency is still treating the submitted document as a part of a defect petition as initially requested.[6] The Agency requested that Toyota describe the subject vehicle's CAN bus and connectivity to outside wireless data sources. In response to the Agency's request, Toyota stated:

- This vehicle is not equipped with a cellular communication module; therefore, it is not capable of communicating with a cellular network.
- This vehicle's multimedia system is capable of connecting a cellular phone to support hands-free features, such as hands-free calling and streaming audio from the phone.
- This vehicle does not have advanced connectivity features, such as Apple CarPlay or Android Auto.
- The multimedia system, which includes Bluetooth connectivity, operates on a local CAN bus network dedicated communication for the vehicle's multimedia system.

ODI Analysis

ODI reviewed complaint data and information in NHTSA's databases concerning all 2019 Toyota Yaris vehicles and identified no other cyberattack allegations similar to those reported by the petitioner. This body of information also did not show any potential trend of similar electrical or power loss symptoms regardless of reported cause.

The symptoms reported by the petitioner could not be duplicated by the Toyota dealer in three separate service visits and may have originated from any number of sources. Beyond these service visits, the effects of other influences such as the Rockledge aftermarket security system (including its installation and removal), and battery maintenance via external charger or driveway idling cannot be assessed at this time. Toyota has reported that difficulty communicating with the petitioner [7] inhibits further efforts to inspect the vehicle. After assessing the material submitted by the petitioner, information submitted by Toyota in response to an Agency request regarding the petitioner's allegation, and other information in NHTSA's possession, NHTSA concludes that:

- Notwithstanding the conditions cited by the petitioner, the 2019 Toyota Yaris vehicle lacks the external cellular connectivity needed to make it vulnerable to remote cyberattacks.
- The subject vehicle's Bluetooth connectivity ability is limited to multimedia and hands-free communication.
- The Agency has uncovered no other evidence of related cyberattacks or similar symptoms in 2019 Toyota Yaris vehicles.

Accordingly, the Agency is denying the petition. As with all potential motor vehicle safety risks, NHTSA will continue to review any new information or incidents as they are submitted to the Agency.

Authority: 49 U.S.C. 30162(d) and 49 CFR part 552; delegation of authority at 49 CFR 1.95(a).[8]

Eileen Sullivan,

Associate Administrator, Enforcement.

[FR Doc. 2024–27431 Filed 11–21–24; 8:45 am]

BILLING CODE P

[2] 20TC03 was a quality campaign meant to reprogram the Engine Control Module (ECM) software due to the software installed being intended for vehicles with a different engine configuration.

[3] 21V617 is a fuel pump recall meant to remedy a defective fuel pump by replacement.

[4] Based on a contemporaneous service invoice.

[5] The model, capabilities, and installer of this device are unknown. However, the Rockledge Securities website advertises several vehicle security devices that may be wired into the vehicle and identifies the subject vehicle sales servicing dealership as one of several affiliated dealerships.

[6] Petitioner's letter to ODI dated February 28, 2023 states: ''my opinion and belief is that my 2019 Toyota Yaris is not defective. It was remotely hacked.''

[7] The petitioner has insisted to the Agency and Toyota that only written communications are accepted and that he will refuse phone calls, emails, and in person visits.

[8] The authority to determine whether to approve or deny defect petitions under 49 U.S.C. 30162(d) and 49 CFR part 552 has been further delegated to the Associate Administrator for Enforcement.