By Order of the Maritime Administrator.

Dated: October 18, 2016.

T. Mitchell Hudson, Jr.,

Secretary, Maritime Administration.

[FR Doc. 2016–26036 Filed 10–27–16; 8:45 am]

BILLING CODE 4910–81–P

DEPARTMENT OF TRANSPORTATION

Maritime Administration

[Docket No. MARAD–2016 0107]

Requested Administrative Waiver of the Coastwise Trade Laws: Vessel QUIET CHAOS; Invitation for Public Comments

AGENCY: Maritime Administration, Department of Transportation.

ACTION: Notice.

SUMMARY: As authorized by 46 U.S.C. 12121, the Secretary of Transportation, as represented by the Maritime Administration (MARAD), is authorized to grant waivers of the U.S.-build requirement of the coastwise laws under certain circumstances. A request for such a waiver has been received by MARAD. The vessel, and a brief description of the proposed service, is listed below.

DATES: Submit comments on or before November 28, 2016.

ADDRESSES: Comments should refer to docket number MARAD–2016–0107. Written comments may be submitted by hand or by mail to the Docket Clerk, U.S. Department of Transportation, Docket Operations, M–30, West Building Ground Floor, Room W12–140, 1200 New Jersey Avenue SE., Washington, DC 20590. You may also send comments electronically via the Internet at *http://www.regulations.gov.* All comments will become part of this docket and will be available for inspection and copying at the above address between 10 a.m. and 5 p.m., E.T., Monday through Friday, except federal holidays. An electronic version of this document and all documents entered into this docket is available on the World Wide Web at *http://www.regulations.gov.*

FOR FURTHER INFORMATION CONTACT: Bianca Carr, U.S. Department of Transportation, Maritime Administration, 1200 New Jersey Avenue SE., Room W23–453, Washington, DC 20590. Telephone 202–366–9309, Email *Bianca.carr@dot.gov.*

SUPPLEMENTARY INFORMATION: As described by the applicant the intended service of the vessel QUIET CHAOS is:

Intended Commercial Use of Vessel: Primarily overnight charter sighting seeing and sport fishing trips. Occasional day trips.

Geographic Region: ''Oregon, Washington State, California, and Alaska (excluding those waters in Southeast Alaska that are north of a line between Gore Point and Cape Suckling, including the North Gulf Coast and Prince William Sound).''

The complete application is given in DOT docket MARAD–2016–0107 at *http://www.regulations.gov.* Interested parties may comment on the effect this action may have on U.S. vessel builders or businesses in the U.S. that use U.S.-flag vessels. If MARAD determines, in accordance with 46 U.S.C. 12121 and MARAD's regulations at 46 CFR part 388, that the issuance of the waiver will have an unduly adverse effect on a U.S.-vessel builder or a business that uses U.S.-flag vessels in that business, a waiver will not be granted. Comments should refer to the docket number of this notice and the vessel name in order for MARAD to properly consider the comments. Comments should also state the commenter's interest in the waiver application, and address the waiver criteria given in § 388.4 of MARAD's regulations at 46 CFR part 388.

Privacy Act

Anyone is able to search the electronic form of all comments received into any of our dockets by the name of the individual submitting the comment (or signing the comment, if submitted on behalf of an association, business, labor union, etc.). You may review DOT's complete Privacy Act Statement in the **Federal Register** published on April 11, 2000 (Volume 65, Number 70; Pages 19477–78).

By Order of the Maritime Administrator.

Dated: October 18, 2016.

T. Mitchell Hudson, Jr.,

Secretary, Maritime Administration.

[FR Doc. 2016–26040 Filed 10–27–16; 8:45 am]

BILLING CODE 4910–81–P

DEPARTMENT OF TRANSPORTATION

National Highway Traffic Safety Administration

Petition for Exemption From the Federal Motor Vehicle Theft Prevention Standard; Fiat Chrysler Automobiles US LLC

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

ACTION: Grant of petition for exemption.

SUMMARY: This document grants in full the Fiat Chrysler Automobiles US LLC, (FCA) petition for exemption of the ''MP'' MPV line in accordance with 49 CFR part 543, *Exemption from Vehicle Theft Prevention Standard.* This petition is granted because the agency has determined that the antitheft device to be placed on the line as standard equipment is likely to be as effective in reducing and deterring motor vehicle theft as compliance with the parts-marking requirements of 49 CFR part 541, *Federal Motor Vehicle Theft Prevention Standard.* (Theft Prevention Standard). FCA also requested confidential treatment for specific information in its petition. While official notification granting or denying its request for confidential treatment will be addressed by separate letter, no confidential information provided for purposes of this notice has been disclosed.

DATES: The exemption granted by this notice is effective beginning with 2017 model year (MY).

FOR FURTHER INFORMATION CONTACT: Ms. Carlita Ballard, International Policy, Fuel Economy and Consumer Programs, NHTSA, West Building, W43–439, 1200 New Jersey Avenue SE., Washington, DC 20590. Ms. Ballard's phone number is (202) 366–5222. Her fax number is (202) 493–2990.

SUPPLEMENTARY INFORMATION: In a petition dated June 1, 2016, FCA requested an exemption from the parts-marking requirements of the Theft Prevention Standard for its ''MP'' MPV line beginning with MY 2017. The petition requested an exemption from parts-marking pursuant to 49 CFR part 543, *Exemption from Vehicle Theft Prevention Standard,* based on the installation of an antitheft device as standard equipment for the entire vehicle line.

Under 49 CFR part 543.5(a), a manufacturer may petition NHTSA to grant an exemption for one vehicle line per model year. In its petition, FCA provided a detailed description and diagram of the identity, design, and location of the components of the antitheft device for its ''MP'' MPV line. FCA stated that its MY 2017 ''MP'' MPV line will be installed with the Sentry Key Immobilizer System (SKIS)/MiniCrypt antitheft device as standard equipment on the entire vehicle line. The SKIS will provide passive vehicle protection by preventing the engine from operating unless a valid electronically encoded key is detected in the ignition system of the vehicle. Key components of the antitheft device will include an immobilizer, Radio Frequency Hub Module (RFHM), Engine Control Module (ECM), Body Controller

Module (BCM), the transponder key which performs the immobilizer function and an Instrument Panel Cluster (IPC) which contains the telltale function only. According to FCA, all of these components work collectively to perform the immobilizer function. FCA stated that the SKIS does not provide an audible alert, however, the vehicle will be equipped with a security indicator in the instrument panel cluster that will flash if an invalid transponder key is detected.

FCA's submission is considered a complete petition as required by 49 CFR 543.7 in that it meets the general requirements contained in 543.5 and the specific content requirements of 543.6.

In addressing the specific content requirements of 49 CFR part 543.6, FCA provided information on the reliability and durability of the device. FCA conducted tests based on its own specified standards (*i.e.,* voltage range and temperature range) and stated its belief that the device meets the stringent performance standards prescribed. Specifically, FCA stated that its device must demonstrate a minimum of 95 percent reliability with 90 percent confidence. In addition to the design and validation test criteria, FCA stated that 100% of its systems undergo a series of three functional tests prior to being shipped from the supplier to the vehicle assembly plant for installation in the vehicles.

FCA stated that the SKIS will be placed on its keyless entry and keyed vehicles. According to FCA, in its keyed vehicles, the SKIS immobilizer feature is activated when the key is removed from the ignition system (whether the doors are open or not). Specifically, the RFHM is paired with the IGNM that contains either a rotary ignition switch (keyed vehicles) or a START/STOP push button (keyless vehicles). FCA stated that the functions and features of the SKIS are all integral to the BCM in this vehicle. The RFHM contains a Radio Frequency (RF) transceiver and a microprocessor and it initiates the ignition process by communicating with the BCM through SKIS. The microprocessor-based SKIS hardware and software also uses electronic messages to communicate with other electronic modules in the vehicle.

FCA also stated that, in its keyed vehicles, the SKIS uses RF communication to obtain confirmation that the transponder key is a valid key to operate the vehicle. The RFHM receives Low Frequency (LF) and/or RF signals from the Sentry Key transponder. For its keyed vehicles, the IGNM transmits an LF signal to excite the transponder in the key when the ignition switch is turned to the ON position. The IGNM waits for a signal response from the transponder and transmits the response to the RFHM. If the response identifies that the transponder key is invalid or if no response is received from the transponder key, the RFHM will send an invalid key message to the Engine Control Module, which will disable engine operation and immobilize the vehicle after two seconds of running.

Only a valid key inserted into the ignition system will allow the vehicle to start and continue to run. FCA stated that, in its keyless vehicles, the RFHM is connected to a Keyless Ignition Node (KIN) with a START/STOP push button as an ignition switch. FCA stated that when the keyless START/STOP button is pressed, the RFHM transmits a signal to the transponder key through LF antennas to the RFHM. The RFHM then waits for a signal from the key FOB transponder. If the response from the transponder identifies the transponder key as invalid or the transponder key is not within the car's interior, the engine will be disabled and the vehicle will be immobilized after two seconds of running.

To avoid any perceived delay when starting the vehicle with a valid transponder key and also to prevent unburned fuel from entering the exhaust, FCA stated that the engine is permitted to run for no more than two seconds if an invalid transponder key is used. Additionally, FCA stated that only six consecutive invalid vehicle start attempts will be permitted and that all other attempts will be locked out by preventing the fuel injectors from firing and the starter will be disabled.

FCA stated that its vehicles are also equipped with a security indicator that acts as a diagnostic indicator. FCA stated that if the RFHM detects an invalid transponder key or if a transponder key related fault occurs, the security indicator will flash. If the RFHM detects a system malfunction or the SKIS becomes ineffective, the security indicator will stay on. The SKIS also performs a self-test each time the ignition system is turned to the RUN position and will store fault information in the form of a diagnostic trouble code in RFHM memory if a system malfunction is detected. FCA also stated that the vehicle is equipped with a Customer Learn transponder programming feature that when in use will cause the security indicator to flash.

FCA stated that each ignition key used in the SKIS has an integral transponder chip included on the circuit board. Each transponder key has a unique transponder identification code that is permanently programmed into it by the manufacturer and must be programmed into the RFHM to be recognized by the SKIS as a valid key. FCA stated that once a Sentry Key has been programmed to a particular vehicle, it cannot be used on any other vehicle.

FCA further stated that it expects the 'MP' MPV vehicle line to mirror the lower theft rate results achieved by the Jeep Grand Cherokee vehicle line when ignition immobilizer systems were installed as standard equipment on the line. FCA stated that it has offered the SKIS immobilizer device as standard equipment on all Jeep Grand Cherokee vehicles since the 1999 model year. According to FCA, the average theft rate, based on NHTSA's theft rate data, for Jeep Grand Cherokee vehicles for the four model years prior to 1999 (1995–1998), when a vehicle immobilizer device was not installed as standard equipment, was 5.3574 per one thousand vehicles produced and significantly higher than the 1990/1991 median theft rate of 3.5826. However, FCA also indicated that the average theft rate for the Jeep Grand Cherokee for the nine model years (1999–2009, excluding MY 2007 and 2009) after installation of the standard immobilizer device was 2.5704, which is significantly lower than the median. The Jeep Grand Cherokee vehicle line was granted an exemption from the parts-marking requirements beginning with MY 2004 (67 FR 79687, December 30, 2002). FCA further exerts that NHTSA's theft data for the Jeep Grand Cherokee indicates that the inclusion of a standard immobilizer device resulted in a 52 percent net average reduction in vehicle thefts.

Based on the evidence submitted by FCA, the agency believes that the antitheft device for the 'MP' MPV line is likely to be as effective in reducing and deterring motor vehicle theft as compliance with the parts-marking requirements of the Theft Prevention Standard (49 CFR 41). The agency concludes that the device will provide four of the five types of performance listed in 49 CFR part 543.6(a)(3): promoting activation; preventing defeat or circumvention of the device by unauthorized persons; preventing operation of the vehicle by unauthorized entrants; and ensuring the reliability and durability of the device.

Pursuant to 49 U.S.C. 33106 and 49 CFR part 543.7(b), the agency grants a petition for exemption from the parts-marking requirements of part 541, either in whole or in part, if it determines that, based upon substantial evidence, the

standard equipment antitheft device is likely to be as effective in reducing and deterring motor vehicle theft as compliance with the parts-marking requirements of part 541. The agency finds that FCA has provided adequate reasons for its belief that the antitheft device for the vehicle line is likely to be as effective in reducing and deterring motor vehicle theft as compliance with the parts-marking requirements of the Theft Prevention Standard (49 CFR part 541). This conclusion is based on the information FCA provided about its device.

For the foregoing reasons, the agency hereby grants in full CFCA's petition for exemption for its 'MP' MPV line from the parts-marking requirements of 49 CFR part 541, beginning with its 'MP' MPV model year vehicles. The agency notes that 49 CFR part 541, Appendix A–1, identifies those lines that are exempted from the Theft Prevention Standard for a given model year. 49 CFR part 543.7(f) contains publication requirements incident to the disposition of all part 543 petitions. Advanced listing, including the release of future product nameplates, the beginning model year for which the petition is granted and a general description of the antitheft device is necessary in order to notify law enforcement agencies of new vehicle lines exempted from the parts marking requirements of the Theft Prevention Standard. FCA stated that an official nameplate for the vehicle has not yet been determined. However, as a condition to the formal granting of FCA's petition for exemption from the parts-marking requirements of 49 CFR part 541 for the MY 2017 'MP' MPV line, the agency fully expects FCA to notify the agency of the nameplate for the vehicle line prior to its introduction into the United States commerce for sale.

If FCA decides not to use the exemption for this vehicle line, it must formally notify the agency. If such a decision is made, the vehicle line must be fully marked as required by 49 CFR parts 541.5 and 541.6 (marking of major component parts and replacement parts).

NHTSA notes that if FCA wishes in the future to modify the device on which this exemption is based, the company may have to submit a petition to modify the exemption. 49 CFR part 543.7(d) states that a part 543 exemption applies only to vehicles that belong to a line exempted under this part and equipped with the anti-theft device on which the line's exemption is based. Further, 49 CFR part 543.9(c)(2) provides for the submission of petitions ''to modify an exemption to permit the use of an antitheft device similar to but differing from the one specified in that exemption.''

The agency wishes to minimize the administrative burden that 49 CFR part 543.9(c)(2) could place on exempted vehicle manufacturers and itself. The agency did not intend in drafting part 543 to require the submission of a modification petition for every change to the components or design of an antitheft device. The significance of many such changes could be *de minimis*. Therefore, NHTSA suggests that if the manufacturer contemplates making any changes, the effects of which might be characterized as *de minimis,* it should consult the agency before preparing and submitting a petition to modify.

Issued in Washington, DC under authority delegated in 49 CFR part 1.95.

Raymond R. Posten,

Associate Administrator for Rulemaking.

[FR Doc. 2016–26072 Filed 10–27–16; 8:45 am]

BILLING CODE 4910–59–P

DEPARTMENT OF TRANSPORTATION

National Highway Traffic Safety Administration

[Docket No. NHTSA–2016–0104]

Request for Comment on Cybersecurity Best Practices for Modern Vehicles

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

ACTION: Request for public comment.

SUMMARY: NHTSA invites public comment on its *Cybersecurity Best Practices for Modern Vehicles*. The document is available for a 30 day comment period at *http://www.nhtsa.gov/staticfiles/nvs/pdf/812333_CybersecurityForModernVehicles.pdf*.

DATES: You should submit your comments early enough to ensure that Docket Management receives them no later than November 28, 2016.

ADDRESSES: Comments should refer to the docket number above and be submitted by one of the following methods:

- *Federal Rulemaking Portal: http://www.regulations.gov*. Follow the online instructions for submitting comments.
- *Mail:* Docket Management Facility, U.S. Department of Transportation, 1200 New Jersey Avenue SE., West Building Ground Floor, Room W12–140, Washington, DC 20590–0001.
- *Hand Delivery:* 1200 New Jersey Avenue SE., West Building Ground Floor, Room W12–140, Washington, DC, between 9 a.m. and 5 p.m. ET, Monday through Friday, except Federal Holidays.
- *Instructions:* For detailed instructions on submitting comments and additional information on the rulemaking process, see the Public Participation heading of the **SUPPLEMENTARY INFORMATION** section of this document. Note that all comments received will be posted without change to *http://www.regulations.gov,* including any personal information provided.
- *Privacy Act:* Anyone is able to search the electronic form of all comments received into any of our dockets by the name of the individual submitting the comment (or signing the comment, if submitted on behalf of an association, business, labor union, etc.). You may review DOT's complete Privacy Act Statement in the **Federal Register** published on April 11, 2000 (65 FR 19477–78). For access to the docket to read background documents or comments received, go to *http://www.regulations.gov* or the street address listed above. Follow the online instructions for accessing the dockets.

FOR FURTHER INFORMATION CONTACT: For technical issues: Mr. Arthur Carter of NHTSA's Office of Vehicle Crash Avoidance & Electronic Controls Research at (202) 366–5669 or by email at *arthur.carter@dot.gov*. For legal issues: Mr. Steve Wood of NHTSA's Office of Chief Counsel at (202) 366–5240 or by email at *steve.wood@dot.gov*.

SUPPLEMENTARY INFORMATION: A top NHTSA priority is enhancing vehicle cybersecurity to mitigate cyber threats that could present unreasonable safety risks to the public or compromise sensitive data such as personally identifiable information. And, the agency is actively engaged in approaches to improve the cybersecurity of modern vehicles. The agency has been conducting research and actively engaging stakeholders to identify effective methods to address the vehicle cybersecurity challenges. For example, in January 2016, NHTSA convened a public vehicle cybersecurity roundtable meeting in Washington, DC to facilitate diverse stakeholder discussion on key vehicle cybersecurity topics. Over 300 individuals attended this meeting. These attendees represented over 200 unique organizations that included 17 Original Equipment Manufacturers (OEMs), 25 government entities, and 13 industry associations. During the roundtable meeting, the stakeholder groups identified actionable steps for