ANSI/CAN/UL/ULC 338:2025

JOINT CANADA-UNITED STATES
NATIONAL STANDARD

STANDARD FOR SAFETY

Vehicle Theft Deterrent Equipment and Systems: Electronic Immobilization System and Aftermarket Installation Requirements

Approved American National Standard
ANSI

ANSI/UL 338-2025

SCC CCN

SCC FOREWORD

National Standard of Canada

A National Standard of Canada is a standard developed by a Standards Council of Canada (SCC) accredited Standards Development Organization, in compliance with requirements and guidance set out by SCC. More information on National Standards of Canada can be found at www.scc.ca.

SCC is a Crown corporation within the portfolio of Innovation, Science and Economic Development (ISED) Canada. With the goal of enhancing Canada's economic competitiveness and social well-being, SCC leads and facilitates the development and use of national and international standards. SCC also coordinates Canadian participation in standards development, and identifies strategies to advance Canadian standardization efforts.

Accreditation services are provided by SCC to various customers, including product certifiers, testing laboratories, and standards development organizations. A list of SCC programs and accredited bodies is publicly available at www.scc.ca.

UL Standard for Safety for Vehicle Theft Deterrent Equipment and Systems: Electronic Immobilization System and Aftermarket Installation Requirements, ANSI/CAN/UL/ULC 338

Third Edition, Dated June 24, 2025

Summary of Topics

This new Third edition of ANSI/CAN/UL/ULC 338, dated June 24, 2025, has been issued to reflect the latest ANSI and SCC approval dates and to incorporate the proposal dated March 28, 2025.

The new requirements are substantially in accordance with Proposal(s) on this subject dated March 28, 2025.

No Text on This Page

ANSI/UL 338-2025

JUNE 24, 2025

1

ANSI/CAN/UL/ULC 338:2025

Standard for Vehicle Theft Deterrent Equipment and Systems: Electronic Immobilization System and Aftermarket Installation Requirements

First Edition – May, 1998
Second Edition – July, 2023

Third Edition

June 24, 2025

This ANSI/CAN/UL/ULC Safety Standard consists of the Third Edition.

The most recent designation of ANSI/UL 338 as an American National Standard (ANSI) occurred on June 24, 2025. ANSI approval for a standard does not include the Cover Page, Transmittal Pages, Title Page, Preface or SCC Foreword.

This Standard has been designated as a National Standard of Canada (NSC) on June 24, 2025.

No Text on This Page

CONTENTS

No Text on This Page

Preface

This is the Third Edition of ANSI/CAN/UL/ULC 338, Standard for Vehicle Theft Deterrent Equipment and Systems: Electronic Immobilization System and Aftermarket Installation Requirements.

ULSE is accredited by the American National Standards Institute (ANSI) and the Standards Council of Canada (SCC) as a Standards Development Organization (SDO).

This Standard has been developed in compliance with the requirements of ANSI and SCC for accreditation of a Standards Development Organization.

This ANSI/CAN/UL/ULC 338 Standard is under continuous maintenance, whereby each revision is approved in compliance with the requirements of ANSI and SCC for accreditation of a Standards Development Organization. In the event that no revisions are issued for a period of four years from the date of publication, action to revise, reaffirm, or withdraw the standard shall be initiated.

In Canada, there are two official languages, English and French. All safety warnings must be in French and English. Attention is drawn to the possibility that some Canadian authorities may require additional markings and/or installation instructions to be in both official languages.

This Third Edition joint American National Standard and National Standard of Canada is based on, and now supersedes, the Second Edition of ULC 338.

Comments or proposals for revisions on any part of the Standard may be submitted at any time. Proposals should be submitted via a Proposal Request in the Collaborative Standards Development System (CSDS) at https://csds.ul.com.

This Edition of the Standard has been formally approved by the Technical Committee (TC) on Automobile Theft Deterrent Equipment and Systems, TC S300V.

This list represents the TC S300V membership when the final text in this Standard was balloted. Since that time, changes in the membership may have occurred.

TC S300V Membership

NAME	AFFILIATION	CATEGORY	REGION
R. Phillips (Chair)	Vehicle Road Safety Solutions (VRSS)	General Interest	Canada
G. Baker	General Motors	Producer	USA
A. Bonilla	NYPD	Authorities Having Jurisdiction / Regulator	USA
N. Bradley	Missouri State Highway Patrol	Authorities Having Jurisdiction / Regulator	USA
M. Briggs	VSST LTD	General Interest	United Kingdom

TC S300V Membership Continued on Next Page

TC S300V Membership Continued

NAME	AFFILIATION	CATEGORY	REGION
L. Chavez	UL Solutions	Testing and Standards Organization	USA
R. Force	Colorado State Patrol	Authorities Having Jurisdiction / Regulator	USA
B. Gast	Équité Association	Consumer	Canada
A. Gilders	UL Standards & Engagement	Non-Voting	Canada
J. Kerr	Canadian Automobile Association (CAA)	Consumer	Canada
G. Overwater	Global Automakers of Canada	Producer	Canada
R. Spallinger	National Insurance Crime Bureau	Consumer	USA
P. Steier	AAMVA	Authorities Having Jurisdiction / Regulator	USA
S. Whitfield	Mastergard Enterprises Inc./Mastergard Vehicle Security & Safety	Producer	Canada
P. Wooderson	Horiba Mira	General Interest	USA
N. Weeks (Project Manager)	UL Standards & Engagement	Non-Voting	USA

International Classification for Standards (ICS): 13.220.10, 13.220.20

For information on ULSE Standards, visit https://www.shopulstandards.com, call toll free 1-888-853-3503 or email us at ClientService@shopULStandards.com.

This Standard is intended to be used for conformity assessment.

The intended primary application of this Standard is stated in its scope. It is important to note that it remains the responsibility of the user of the standard to judge its suitability for this particular application.

CETTE NORME NATIONALE DU CANADA EST DISPONIBLE EN VERSIONS FRANÇAISE ET ANGLAISE

INTRODUCTION

1 Scope

1.1 The requirements of this Standard cover the following items regardless of the propulsion system used:

a) Passenger cars;

b) SUVs;

c) Light-duty trucks and vans [under 3,107 kg (6,850 pounds)];

d) Medium-duty vehicles [3,108 – 4,536 kg (6,851 – 10,000 pounds)];

e) Heavy-duty vehicles [over 4,536 kg (10,000 pounds)];

f) Heavy equipment; and

g) Motorcycles.

1.2 The requirements of this Standard do not cover the following items:

a) Aircraft;

b) Watercraft; and

c) Power sport (e.g., recreational or off-road vehicles).

1.3 Both original equipment manufacturer (OEM) systems and aftermarket systems shall meet the requirements of this Standard.

1.4 Electronic immobilization systems shall be passively armed, and once armed, they shall prevent the unauthorized movement of the vehicle under its own power.

1.5 As an optional protection mechanism, these requirements cover the addition of alarm warning functions, where permitted, to the core immobilization system in order to protect the vehicle's contents and to protect the electronic immobilization system.

1.6 An electronic immobilization system, as covered by these requirements, consists of one or more assemblies of electrical components designed to prevent the unauthorized movement of the vehicle under its own power.

1.7 A component of an electronic immobilization system or alarm warning system, where permitted, such as attachment plug, siren, horn, switch, transponder, remote transmitter, wire, etc., shall comply with the requirements for that component, except that such requirements be modified if appropriate for the particular application.

1.8 Installation of the electronic aftermarket immobilization system shall be in accordance with the system manufacturer's instructions, and any accessory parts shall be per the specifications outlined by the aftermarket manufacturer using their licensed installers that are in good standing, having met requirements of this Standard.

1.9 All aftermarket manufacturers shall demonstrate their systems meet all applicable requirements in this Standard with on-vehicle testing to verify they function as designed in accordance with this document.

1.10 The requirements also provide a set of clear best practices and installation processes for licensed installers and installation facilities handling the installation of aftermarket immobilizers, licensed installers, and installation processes.

2 Units of Measurement

2.1 Values stated without parentheses are the requirements. Values in parentheses are explanatory or approximate information.

3 Referenced Publications

3.1 The documents shown below are referenced in the text of this Standard. Unless otherwise stated elsewhere in this Standard, such reference shall be considered to indicate the edition and/or revisions of the document available at the date on which the Committee approved this Standard.

3.2 The following publications are referenced in this Standard:

BSI PAS 1885, *The Fundamental Principles of Automotive Cyber Security. Specification (British Standard)*

ASTM B117, *Standard Practice for Operating Salt Spray (Fog) Apparatus*

ECE/TRANS/WP.29/2020/79, *UN Regulation on uniform provisions concerning the approval of vehicles with regard to cyber security and of their cybersecurity management systems*

FIPS 140-2, *Security Requirements for Cryptographic Modules*

NIST Special Publication 800-53, *Initial Public Draft, Security, and Privacy Controls for Information Systems and Organizations for secure database management*

IEC 60068-2-27, *Environmental Testing - Part 2-27: Tests – Test Ea and guidance Shock*

ISO 7637-1, *Road vehicles – Electrical disturbances from conduction and coupling – Part 1: Definitions and general considerations*

ISO 7637-3, *Road vehicles – Electrical disturbances from conduction and coupling – Part 3: Electrical transient transmission by capacitive and inductive coupling via lines other than supply lines*

ISO 10605, *Road vehicles – Test methods for electrical disturbances from electrostatic discharge*

ISO 11451-1, *Road vehicles – Vehicle test methods for electrical disturbances from narrowband radiated electromagnetic energy – Part 1: General principles and terminology*

ISO 11451-2, *Road vehicles – Vehicle test methods for electrical disturbances from narrowband radiated electromagnetic energy – Part 2: Off-vehicle radiation sources*

ISO 11451-3, *Road vehicles – Vehicle test methods for electrical disturbances from narrowband radiated electromagnetic energy – Part 3: On-board transmitter simulation*

ISO 11451-4, *Road vehicles – Vehicle test methods for electrical disturbances from narrowband radiated electromagnetic energy – Part 4: Harness excitation methods*

ISO 11452-1, *Road vehicles – Component test methods for electrical disturbances from narrowband radiated electromagnetic energy – Part 1: General principles and terminology*

ISO 11452-2, *Road vehicles – Component test methods for electrical disturbances from narrowband radiated electromagnetic energy – Part 2: Absorber-lined shielded enclosure*

ISO 11452-3, *Road vehicles – Component test methods for electrical disturbances from narrowband radiated electromagnetic energy – Part 3: Transverse electromagnetic (TEM) cell*

ISO 11452-4, *Road vehicles – Component test methods for electrical disturbances from narrowband radiated electromagnetic energy – Part 4: Harness excitation methods*

ISO 11452-5, *Road vehicles – Component test methods for electrical disturbances from narrowband radiated electromagnetic energy – Part 5: Stripline*

ISO 11452-7, *Road vehicles – Component test methods for electrical disturbances from narrowband radiated electromagnetic energy – Part 7: Direct radio frequency (RF) power injection*

ISO/IEC 17020, *Conformity assessment – Requirements for the operation of various types of bodies performing inspection*

ISO/IEC 17065, Conformity assessment – Requirements for bodies certifying products, processes and services

ISO/SAE 21434, *Road vehicles – Cybersecurity engineering*

UN Regulation No. 155, *Uniform provisions concerning the approval of vehicles with regards to cyber security and cyber security management system*

SAE J3061, *Cybersecurity Guidebook for Cyber-Physical Vehicle Systems*

UL 2900-1, *Software Cybersecurity for Network- Connectable Products, Part 1: General Requirements*

UL 5500, *Remote Software Updates*

4 Glossary

4.1 For the purpose of this Standard, the following definitions apply:

4.2 ACTIVE ARMING – The intentional arming of the electronic immobilization system with direct operator intervention.

4.3 AFTERMARKET VEHICLE THEFT DETERRENT DEVICE – A vehicle theft deterrent device available for installation that was not fitted at OEM vehicle assembly.

4.4 ARM – To engage or activate the electronic immobilization system.

4.5 CAN bus – A controller area network (CAN bus) is a vehicle electrical architecture designed to allow microcontrollers and devices to communicate with each other's applications without a host computer.

4.6 CODE GRABBING – The unauthorized interception via a receiver of a secure disarming combination transmitted remotely by an authorized user.

4.7 CODED DISARMING DEVICE – A unique authorized electronic or physical device or secured physical/electronic disarming combination that is required to disarm the electronic immobilization system.

4.8 COMMON DISARMING DEVICE – A unique authorized electronic or physical device or secured physical/electronic disarming combination that is required to disarm the electronic immobilization system for fleets.

4.9 COMPUTER SAFE – Tools and equipment suitable for use on computer circuitry without damaging the circuitry or vehicle.

4.10 DISARM – To deactivate the electronic immobilization system, allowing normal propulsion operation.

4.11 ELECTRONIC IMMOBILIZATION SYSTEM – An electrical or electronic system which prevents the unauthorized movement of a vehicle under its own power.

4.12 FREE FIELD – An environment in which a sound wave may propagate in all directions without obstructions or reflections within the frequency range of interest.

4.13 KEYPAD – A device or set of devices intended to be actuated in a pre-determined sequence.

4.14 IGNITION KEY – The key code-carrying device or a technical solution that allows for the immobilizer to be disarmed.

4.15 LICENSED INSTALLER – Individual (worker) trained and licensed by a Certification Organization and engaged in the application of aftermarket vehicle theft deterrent devices. The Licensed Installer is responsible for the actual installation and site requirements.

4.16 OEM SYSTEM – A system that is provided by the manufacturer of the vehicle and installed at the time of vehicle assembly.

4.17 ON BOARD DIAGNOSTICS II (OBD II) PORT – An automotive term referring to the access point for a vehicle's self-diagnostic and reporting capability that gives the vehicle owner or repair technician access to the status of the various vehicle sub-systems.

4.18 PASSIVE ARMING – The arming of the electronic immobilization system without direct operator intervention.

4.19 ROLLING CODES – The transmission via radio frequency, by an authorized user, of a different secure disarming combination on each successive disarming attempt.

4.20 SECURE DISARMING COMBINATION – A mathematical sequence in the form of a series of electrical signals which is unique to the specific electronic immobilization system installed in a given vehicle and which is required to disarm that system.

4.21 VALET MODE – The temporary locking-out of the passive arming function of the electronic immobilization system.

CONSTRUCTION

5 Wiring

5.1 All system wiring shall be uniform in colour for aftermarket systems.

5.2 The gauge of wire used in the system shall be equivalent to or greater than the wiring circuit to which it is connected.

5.3 Each wire used in the system shall have a maximum of two connections.

5.4 This section does not apply to CAN Bus software immobilizations.

6 Enclosure

6.1 The requirements of this section shall apply to aftermarket systems only.

6.2 The system shall not have any permanent identifying marks on the outside of any enclosure which may serve to identify wires and other inputs or outputs to any component of the electronic immobilization system.

6.3 For the life of the vehicle, all enclosures shall withstand wear and fatigue resulting from the vehicle environment (e.g., abrasion, fraying, water intrusion, noise vibration harshness (NVH), etc.) to which they are likely to be subjected during normal operation without affecting their performance and continue to meet the requirements of Section 16, Performance Testing.

6.4 All external relays installed with the electronic immobilization system shall be enclosed to protect against malfunction due to dust or other material which may impair their intended operation and shall be rated for the intended application under all environmental conditions to which they may be exposed.

6.5 The manufacturer shall supply, with the electronic immobilization system, all external relays required for the installation of an electronic immobilization system on a given application. External relays or components required for optional accessories shall be specified by the manufacturer.

7 Arming of Electronic Immobilization System

7.1 General

7.1.1 Arming of the aftermarket immobilization function of the electronic immobilization system shall be passive arming when the ignition is off and initiated no earlier than immediately upon turning the vehicle off with the built-in delay provision of restarting the stalled vehicle and no sooner than 30 seconds and no later than 60 seconds after ignition is turned off.

7.1.2 Arming of the OEM electronic immobilization system shall be performed passively when the ignition is turned off and occurs within 60 seconds of the ignition being turned off.

7.1.3 There shall be no feature in the electronic immobilization system, intentional or otherwise, that interferes with the safe operation of the vehicle, which may potentially damage the vehicle or compromises the safety of the occupants of the vehicle. This includes any event which causes unburned fuel to enter the exhaust catalyst.

7.2 Passive arming

7.2.1 In vehicles where the vehicle manufacturer requires an ignition key for normal propulsion system operation, an electronic immobilization system is considered passive arming when no further action on the part of the vehicle user is required to arm the electronic immobilization system after the vehicle user turns off the ignition and removes the ignition key.

7.2.2 In order for an electronic immobilization system to be passive arming under 7.2.1, the key code carrying device shall include the function of the ignition key. When the vehicle operator powers down the vehicle and removes the key code carrying device, the system shall be armed in accordance with 7.1.1.

7.2.3 In vehicles where the vehicle manufacturer does not require an ignition key for propulsion system operation, an electronic immobilization system is considered passive arming when no further action is required to arm the electronic immobilization system after the vehicle user turns off the ignition.

7.3 Coded device

7.3.1 With the exception of systems where the coded disarming device or secure disarming combination is integral with the ignition key, removal of the coded disarming device with the engine running shall not turn off the vehicle's ignition, cause the engine to stall or otherwise interfere with the safe operation of the vehicle.

7.3.2 In electronic immobilization systems where the coded disarming device or secure disarming combination is not integral with the ignition key, applying the coded disarming device or entering the secure disarming combination with the engine running/propulsion system active shall not interfere with the safe operation of the vehicle.

7.4 Status change

7.4.1 If an audible change-of-status indicator is in use, it shall be a duration of 3 seconds or less and shall comply with local noise regulations.

7.5 Voltage interruption

7.5.1 For aftermarket applications, the interruption of the supply voltage to a disarmed electronic immobilization system and subsequent reapplication of voltage shall not create a change of status to the electronic immobilization system.

7.5.2 All aftermarket systems for immobilization must not have an external fuse for main power that can be removed and disrupt system rearming.

DISARMING OF ELECTRONIC IMMOBILIZATION SYSTEM

8 General

8.1 The electronic immobilization system shall be disarmed by the use of a coded disarming device or secure disarming combination.

8.2 The means by which the coded disarming device or secure disarming combination may communicate its code to the electronic immobilization system include, but are not limited to, the displacement of mechanical elements through electrical contact or through radio frequencies (RF).

8.3 All disarming methods for the electronic immobilization system shall meet the requirements in this Standard.

9 Coded Key/Secure Combination

9.1 Once an electronic immobilization system is armed, it shall not be possible to disarm the system without the correct coded disarming device or secure disarming combination.

9.2 Each individual electronic immobilization system shall disarm only in response to a specific coded key device or secure disarming combination. All other coded devices or secure disarming combinations shall have no effect. There shall be no universal master coded disarming device or master secure disarming combination which will disarm all vehicles equipped with the same system or all electronic immobilization systems of the same model number.

9.3 Reference Sections 25 through 26 for requirements pertaining to coded device and secure combinations of fleets.

9.4 There shall be no permanent visible indication of any coded disarming key device or secure disarming combination in the vehicle.

9.5 The production run of each electronic immobilization system model shall be such that the range of deactivating secure disarming combinations or coded disarming devices is randomly distributed.

9.6 In the event that the original coded disarming device or secure disarming combination was lost and has been replaced by a new device or secure disarming combination, and the electronic immobilization system has not been replaced, a function shall be provided in the electronic immobilization system to prevent the use of the original key device or secure disarming combination. If the electronic immobilization system has been replaced, it shall meet the requirements of this Standard.

9.7 Any reprogramming procedure or emergency disarming procedure of the electronic immobilization system shall incorporate a delay after the introduction of an incorrect code such that attempting half of the possible codes will require no less than 24 hours.

9.8 If the coded disarming device or secure disarming combination is separate from the ignition key and mechanically latches into a socket, receptacle, or lock, it shall not be possible to start the vehicle's engine until this device or secure disarming combination is physically removed from the socket, receptacle, or lock.

9.9 If the coded disarming device or secure disarming combination is not an integral part of the ignition key of the vehicle, once disarmed, the electronic immobilization system shall return back to the armed condition unless the vehicle ignition is applied within 2 minutes.

10 Voltage Interruption

10.1 Interruption of the supply voltage to the electronic immobilization system shall not disarm the electronic immobilization system.

10.2 All aftermarket systems for immobilization that are not equipped with a main power supply internal circuit breaker shall be able to rearm upon main power disruption.

11 Disarming by Remote Means

11.1 Transponders and remote controls shall be in sealed enclosures meeting the requirements of the following subsections:

a) 16.1, General;

b) 16.2, Normal Operation;

c) 16.10, Bump;

d) 16.11, Drop;

e) 16.12, Electromagnetic Compatibility;

f) 16.13, Durability Test for Electronic Immobilization Systems Equipped with Alarm Warning; and

g) 16.15, Sealing Against Dust and Water.

11.2 The effective operating range for remote disarming devices for the immobilizer shall have a maximum distance of 0.25 m (0.82 feet) for transponders and 2.00 m (6.56 feet) for remote controls unless they are equipped to use rolling code protection or are resistant to code grabbing. The effective operating range shall be from the transponder or remote control to the electronic immobilization system receiver.

11.3 There shall be a minimum of 50,000 code combinations for each remote disarming device in order for the device to be considered resistant to code scanning.

11.4 For a remote disarming device to be resistant to code scanning, a minimum time of 24 hours shall be required to successfully scan 5,000 codes. All codes shall be repeated a maximum of once every 5,000 disarming attempts.

11.5 For a remote disarming device to use rolling code protection or encrypted code protection, the mathematical probability of obtaining the correct code within 24 hours shall be less than 0.04. It shall not be possible to disarm the system by re-transmitting in any sequence the previous 5 codes generated by a legitimate disarming device or secure disarming combination. The data describing the algorithm used to generate rolling codes shall be provided by the manufacturer for testing purposes. The actual algorithm shall not be required.

DISARMING BY NON-REMOTE MEANS

12 General

12.1 The disarming device shall be mounted inconspicuously in the passenger compartment of the vehicle.

12.2 There shall be no visible identification on the disarming device in order to prevent the unauthorized identification of the current disarming device or secure disarming combination.

12.3 The disarming device shall meet either one of the following conditions:

a) If the disarming device has 10,000 or more effective disarming codes, it shall require a minimum of 24 hours to scan 5,000 codes; or

b) If the disarming device has less than 10,000 effective disarming codes, the device shall incorporate a delay after the input of at least three incorrect codes such that the minimum duration to attempt disarming with half of the possible disarming codes is at least 24 hours.

12.4 Any future technologies like biometrics or other similar, unique device code to disarm a system shall demonstrate equivalent resistance against theft.

13 Keypads

13.1 If the disarming device is a keypad, there shall be no wear patterns developed over repeated use. To determine compliance, 10,000 entries shall be applied to the keypad surface as employed in the intended application. The keypad shall not demonstrate any wear or defacement following this test.

13.2 If the disarming device is a keypad, the disarming code shall consist of a minimum of four keystrokes, positions, or other individual inputs and shall be capable of being reset by the user only when the electronic immobilization system is disarmed.

13.3 This section does not apply to CAN Bus software immobilizations.

14 Means of Immobilization

14.1 Aftermarket systems

14.1.1 An aftermarket system shall perform one of the following that inhibits:

a) For internal combustion:

1) Starter; and

2) Any two of the following:

i) Fuel;

ii) Ignition;

iii) Power supply; or

iv) One or more additional circuit(s) which inhibit(s) propulsion activation or mobility.

b) For all other propulsion systems, any three circuits which inhibit propulsion activation or mobility.

14.1.2 The electronic immobilization system referred to in 14.1.1 shall not include safety-related systems such as lighting, braking, restraints, or windshield wipers.

14.2 OEM systems

14.2.1 An OEM system shall isolate at least one of the control units, affecting multiple circuits, required to achieve vehicle self-mobility.

14.2.2 In order to resume normal vehicle operation, the isolated control unit(s) (i.e., engine control unit, fuel control unit, ignition control unit, electric propulsion control units, transmission control unit) shall require a specific coded or encrypted signal.

14.2.3 Replacement of the isolated control unit(s) to a functional, non-immobilized state shall require a minimum of 5 minutes.

15 Optional Features

15.1 Immobilizer warning functions

15.1.1 The electronic immobilization system may include a visible or audible indicator to alert the user that a change of the status of the system (i.e., from armed to disarmed or vice versa) has occurred.

15.2 Alarm warning functions

15.2.1 General

15.2.1.1 If used, the objective of the addition of the alarm warning function to the basic electronic immobilization system is to deter theft from vehicle or vandalism as a supplement to the drive-away protection of the electronic immobilization system.

15.2.1.2 If a manufacturer of an electronic immobilization system also makes available an alarm warning function, the combined system (electronic immobilization system with alarm warning) shall comply with this Standard.

15.2.1.3 The alarm warning function shall have a minimum of one input to detect unauthorized entry into the vehicle.

15.2.1.4 The alarm warning function shall not false alarm when subjected to the tests outlined in Section 16, Performance Testing.

15.2.1.5 The alarm warning shall be actively and/or passively armed. Passive arming shall be owner/operator selectable and consistent with locked vehicle doors.

15.2.1.6 An external audible or visual signal may be used to indicate a change in system status (from armed to disarmed or vice versa). The duration of the signal shall be a maximum of 150 ms for an audible signal.

15.2.1.7 The alarm warning device shall be installed in accordance with the manufacturer's instructions.

15.2.2 Audible deterrent

15.2.2.1 The output of the alarm warning shall be an audible device such as a siren or the OEM system horn (i.e., the vehicle signaling horn) and may also include visible warning devices.

15.2.2.2 All applicable local noise abatement regulations shall take precedence, including nuisance alarms.

15.2.2.3 The audible device, except the OEM system horn, shall have a minimum sound pressure level of 105 dB and a maximum sound pressure level of 130 dB at a distance of 1 m (3.25 feet) and shall be tested in an environment where there are no reflective surfaces within the frequency region of interest, such as a free field or anechoic chamber.

15.2.2.4 The duration time of the audible deterrent shall not exceed 1 minute. The system shall reactivate once a new manipulations or alarm event from the same or different trigger zone is detected.

15.2.2.5 The audible device, if it is not the OEM system horn, shall continue operation as designed if any or all wires to this device are cut.

15.2.2.6 The OEM audible device shall be kept active for security measures for 5 minutes in 25 to 30 second cycles for back-up batteries.

15.2.3 Valet/Temporary bypass mode feature

15.2.3.1 The manufacturer of the electronic immobilization system may provide a valet mode feature.

15.2.3.2 Valet mode shall be activated using the coded disarming device or secure disarming combination in possession of the user.

15.2.3.3 Bypass switches or un-coded valet mode options shall meet the requirements of 15.2.3.2.

15.2.3.4 Valet mode shall automatically disengage (i.e., electronic immobilization system returns to passive arming) after a maximum of 15 engine starts while under valet mode.

15.2.3.5 Automatic re-engagement by OEM systems of passive arming shall not be required if audible and visible indications are suitably disruptive and are provided on each ignition cycle.

16 Performance Testing

16.1 General

16.1.1 The tests outlined in 16.2 – 16.16, inclusive, shall be conducted on every component related to the electronic immobilization affected by this Standard.

16.1.2 OEMs may perform self-tests to ensure conformity assessment.

16.1.3 When an aftermarket remote starter is used, it shall not disarm the immobilizer and shall be deactivated by a key carrying device/secure disarming combination before the vehicle is allowed to be moved under its own power.

16.2 Normal operation

16.2.1 The basic test cycle shall consist of the following steps:

a) Check that the electronic immobilization system becomes active within a proper time interval of turning off the ignition (and removing the ignition key, if applicable);

b) Check that the vehicle will not start and that all electronic immobilization system circuits are active in disabling the vehicle;

c) Disarm the electronic immobilization system, turn on the ignition, start (or simulate starting) the engine and check that all electronic immobilization system circuits allow the vehicle to move under its own power; and

d) All features shall operate as intended.

16.2.2 The test fails if at any time during the tests in 16.2.1 (a) – (d) the electronic immobilization system changes state inadvertently from armed to disarmed or from disarmed to armed.

16.3 Reverse polarity

16.3.1 Subject supply lines of the system to 13.0 ±0.2 V for 1 minute with reverse polarity.

16.3.2 Following the test outlined in 16.3.1, the electronic immobilization system shall comply with the tests outlined in 16.2, Normal Operation.

16.4 Excess voltage

16.4.1 Subject supply lines of the system unit to 18 ±0.2 V for 1 hour and to 24 ±0.2 V for 1 minute.

16.4.2 Following the test outlined in 16.4.1, the electronic immobilization system shall comply with the tests outlined in 16.2, Normal Operation.

16.5 Short Circuit and open circuit

16.5.1 Apply a short circuit to each individual electrical connection of the electronic immobilization system in turn, with respect to each polarity of the power supply. The short circuit shall be held for 5 seconds.

16.5.2 Replace all fuses following the test in 16.5.1.

16.5.3 Following the test outlined in 16.5.1, the electronic immobilization system shall comply with the tests outlined in 16.2, Normal Operation.

16.5.4 Following the tests in 16.5.1 – 16.5.3, with the electronic immobilization system armed, each wire to the electronic immobilization system shall in turn be an open circuit in sequence and reconnected. The vehicle shall not start during each open circuit. Following reconnection, the electronic immobilization system shall return to its original state prior to the open circuit.

16.5.5 Following the test in 16.5.4, open circuit all connections to the electronic immobilization system. The vehicle shall not start during the open circuit.

16.5.6 Following the test in 16.5.5, reconnect all open circuits. The electronic immobilization system shall return to its original state prior to the open circuit.

16.6 Voltage reduction or removal

16.6.1 The voltage reduction/removal test shall be conducted as outlined in 16.6.2 – 16.6.7. The electronic immobilization system shall operate as intended following each of the tests outlined in 16.6.2 – 16.6.7.

16.6.2 Armed state:

a) Arm the electronic immobilization system; and

b) Disconnect power supply.

16.6.3 Armed with intermittent power:

a) Arm the electronic immobilization system; and

b) Disconnect and reconnect power supply at 15 cpm for 2 minutes.

16.6.4 Disarmed state (per 7.5.2):

a) Disarm the electronic immobilization system; and

b) Disconnect power supply.

16.6.5 Disarmed with intermittent power:

a) Disarm the electronic immobilization system; and

b) Disconnect and reconnect power supply at 15 cpm for 2 minutes.

16.6.6 Voltage reduction (armed):

a) Arm the electronic immobilization system; and

b) Decrease voltage to electronic immobilization system from 13.7 to 7.5 V rate of 1 V/min.

16.6.7 Voltage reduction (disarmed):

a) Disarm the electronic immobilization system; and

b) Decrease voltage to electronic immobilization system from 13.7 to 7.5 V rate of 1 V/min.

16.7 Temperature and supply voltage

16.7.1 Prior to testing, the samples shall be conditioned for 4 hours at each test point specified in 16.7.2 and 16.7.3.

16.7.2 The electronic immobilization system shall operate as intended for components intended for placement in the passenger compartment of the vehicle when subjected to:

a) 85 ±2 °C (185 ±3.6 °F) at 95 ±3 % relative humidity (RH) and 15 ±0.2 V; and

b) -40 ±2 °C (-40 ±3.6 °F) at 50 ±2 % RH and 9 ±0.2 V.

16.7.3 The electronic immobilization system shall operate as intended for components intended for placement in the underhood area of the vehicle when subjected to:

a) 125 ±2 °C (257 ±3.6 °F) at 95 ±3 % RH and 15 ±0.2 V; and

b) -40 ±2 °C (-40 ±3.6 °F) at 50 ±2 % RH and 9 ±0.2 V.

16.8 Temperature/Humidity accelerated aging

16.8.1 The electronic immobilization system shall meet the requirements specified in 16.2, Normal Operation, while subjected to the conditions outlined in 16.8.2 and 16.8.3.

16.8.2 The components of the electronic immobilization system, except the batteries, designed for an environmental temperature of:

a) -40 to ±85 °C (-40 ± 185 °F): Shall be tested at the upper temperature of 85 ±2 °C (185 ±3.6 °F) and at an RH of 95 ±3 %; and

b) -40 to ±125 °C (-40 ± 257 °F): Shall be tested at the upper temperature of 125 ±2 °C (257 ±3.6 °F) and at an RH of 95 ±3 %.

16.8.3 The test consists of 10 cycles of 24 hours of the following test sequence. (The electronic immobilization system shall then meet the requirements of 16.2, Normal Operation):

a) Items which have to operate 125 °C (257 °F) shall be tested from (f) to (i). They shall then be assembled into a complete electronic immobilization system and submitted to all of the tests from (b) to (i) with the test temperature of 85 °C (185 °F);

b) The temperature shall be held at 23 ±5 °C (73 ±9 °F) for a minimum of 4 hours at 45 % to 75 % RH;

c) The temperature shall be raised to 55 ±2 °C (131 ±9 °F) at 95 ±3 % RH within 0.5 hours;

d) The temperature shall be held at 55 ±2 °C (131 ±9 °F) at 95 ±3 % RH for 10 hours;

e) The temperature shall be lowered to -40 ±2 °C (-40 ±3.6 °F) within 2.5 hours;

f) The temperature shall be held at -40 ±2 °C (-40 ±3.6 °F) for 2 hours;

g) The temperature shall be raised to the applicable requirements in accordance with 16.8.2 within 1.5 hours;

h) The temperature shall be held to the applicable requirements in accordance with 16.8.2 for 2 hours; and

i) The temperature shall be lowered to 23 ±2 °C (73 ±9 °F) within 1.5 hours.

NOTE 1: During periods (e) and (f), the RH is uncontrolled.

NOTE 2: At the end of a cycle, the test may be interrupted. During the interruption, the test samples shall remain at the ambient conditions as defined in (b). Interruption time shall be noted in the test report.

NOTE 3: The temperatures quoted are not the highest temperatures which may be experienced by components mounted within the engine compartment. When components are intended to be installed within 100 mm of any components of the engine exhaust or cooling systems or of the engine block, the temperature at 125 °C (257 °F) shall be increased by 15 °C (59 °F) .

16.9 Vibration

16.9.1 For this test, the components are subdivided into two types:

a) Type A: Components normally mounted on the vehicle; and

b) Type B: Components intended for attachment to the engine.

16.9.2 The components of the electronic immobilization system shall be submitted to a sinusoidal vibration mode whose characteristics are as follows. The test shall be performed along each of the three axes:

a) Type A: The electronic immobilization system shall be vibrated at an amplitude of 2 mm (0.08 inches) at a frequency of 20 Hz to 300 Hz in increments of 10 Hz per min until a resonant frequency is obtained. Once the resonant frequency is obtained, it shall be maintained for 15 minutes. If no resonant frequency is obtained, the electronic immobilization system shall be vibrated at 300 Hz for 4 hours; and

b) Type B: The electronic immobilization system shall be vibrated at an amplitude of 0.5 mm (0.02 inches) at a frequency of 10 Hz to 500 Hz in increments of 10 Hz per min until a resonant frequency is obtained. Once the resonant frequency is obtained, it shall be maintained for 15 minutes. If no resonant frequency is obtained, the electronic immobilization system shall be vibrated at 500 Hz for 4 hours.

16.9.3 Following the tests specified in 16.9.2, the electronic immobilization system shall comply with the requirements of 16.2, Normal Operation.

16.10 Bump

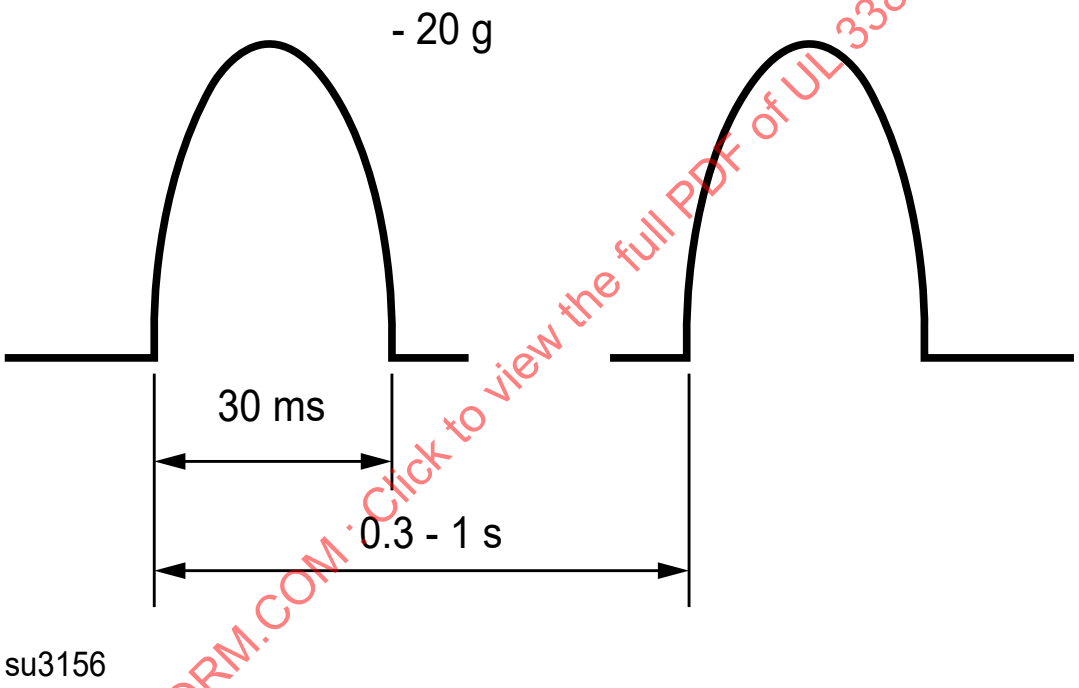
16.10.1 This test shall use test equipment described in IEC 60068-2-27.

16.10.2 The electronic immobilization system and any handheld devices shall be mounted on a test rig and shall be subjected to the conditions specified in Table 16.1 and the waveform in Figure 16.1.

Table 16.1
Severity of Conditioning

Parameter	Severity
Acceleration	196.2 m/s^2 or 20 g (643.70 ft/s or 0.04 pounds)
Duration	30 ms
Directions	3 mutually perpendicular
Number of bumps per direction	1

Figure 16.1
Waveform



16.10.3 After bumping in all three directions, subject the electronic immobilization system to 16.2, Normal Operation. It shall exhibit no mechanical damage other than superficial scratches.

16.11 Drop

16.11.1 All hand-held devices (e.g. remote control devices), shall be submitted to a free fall test of 1 ±0.01 m (39 ±0.39 inches) onto a concrete surface five times.

16.11.2 After this test, the device shall function in accordance with this Standard, and the enclosure shall show no damage other than superficial scratches.

16.12 Electromagnetic compatibility

16.12.1 Supply line immunity

16.12.1.1 Tests for immunity against supply line disturbances shall be conducted as outlined in 16.12.1.2 – 16.12.1.4.

16.12.1.2 Apply the test pulse 1 – 5 (Refer to Table 16.2) according to ISO 7637-1 to the supply lines as well as to other connections of the electronic immobilization system, which may be operationally connected to supply lines.

Table 16.2
Severity/Functional Status (Supply Lines)

Test pulse	Degree of severity	Functional status
1	III	C
2	III	A
3a	III	C
3b	III	A
4a	III	B
4b	I	A
5	III	A

16.12.1.3 With the electronic immobilization system in disarmed state, the test pulses 1 – 5 shall be applied with degree of severity III. The required functional status for all applied test pulses shall be A. Refer to Table 16.2.

16.12.1.4 With the electronic immobilization system in the armed state, the test pulses 1 – 5 shall be applied. The required functional status for all applied test pulses is given in Table 16.2.

16.12.2 Sensor line immunity

16.12.2.1 Tests for immunity against disturbance coupled on sensor lines shall be conducted as outlined in 16.12.2.2.

16.12.2.2 Leads which are not connected to supply lines (e.g. special sensor lines), shall be tested in accordance with ISO 7637-3. The required functional status for all applied test pulses is given in Table 16.3.

Table 16.3
Severity/Functional Status (Sensor Lines)

Test pulse	Degree of severity	Functional status
a	III	C
b	III	A

16.12.3 High frequency immunity

16.12.3.1 Tests for immunity against radiated high frequency disturbances shall be conducted as outlined in 16.12.3.2 and 16.12.3.3.

16.12.3.2 Testing of the immunity of an electronic immobilization system in a vehicle may be performed according to one of the methods described in one of the following standards:

a) ISO 11451-1;

b) ISO 11451-2;

c) ISO 11451-3; or

d) ISO 11451-4.

16.12.3.3 Laboratory testing may be performed according to one of the methods described in one of the following standards:

a) ISO 11452-1

b) ISO 11452-2

c) ISO 11452-3

d) ISO 11452-4

e) ISO 11452-5

f) ISO 11452-7

16.12.3.4 Test severity level II shall be applied and the functional status “A” shall be maintained during and after the test.

16.12.3.5 For values of severity levels see the relevant part of ISO 11451 and ISO 11452.

NOTE: A description of the functional status is given in Part 1 of both of these standards.

16.12.4 Electrostatic discharge immunity

16.12.4.1 Immunity against electrical disturbances shall be tested in accordance with ISO/TR 10605.

16.12.5 Radio frequency interference immunity

16.12.5.1 An electronic immobilization system that radiates or utilizes radio frequency energy shall comply with the appropriate regulations before it is submitted for test.

NOTE: The appropriate regulations are administered by the government agencies Innovation, Science and Economic Development Canada and the Federal Communications Commission. A letter of confirmation or the equivalent from Innovation, Science and Economic Development Canada and the Federal Communications Commission may be required as evidence of compliance.

16.13 Durability test for electronic immobilization systems equipped with alarm – Warning

16.13.1 The standard test cycle shall be arm, trigger alarm system, disarm.

16.13.2 For cycling purposes, the disarming shall be 2 ±1 seconds after the audible warning has started to sound.

16.13.3 The test cycle shall be repeated 5,000 times, except that every 20th test cycle shall be disarmed only after the audible warning has stopped sounding automatically.

16.13.4 The alarm shall be triggered by all the sensors/detectors in rotation. That is, if there are 10 sensors, inducing non-perimeter types as options, then each sensor shall operate 500 times.

16.14 Current consumption (Power rating)

16.14.1 The combined maximum current draw in standby mode of the electronic immobilization system, while armed, and all optional accessories, shall not exceed 25 mA at 12 ±0.1 V, and at -40 ±2 °C (-40 ±3.6 °F) and 85 ±2 °C (185 ±3.62 °F).

16.15 Sealing against dust and water

16.15.1 Dust

16.15.1.1 All components of the electronic immobilization system and options shall be subjected to the dust test outlined in 16.15.1.2 – 16.15.1.5.

16.15.1.2 The operation of the electronic immobilization system shall not be impaired by an accumulation of dust.

16.15.1.3 To determine compliance with 16.15.1.2, a de-energized sample in its intended mounting position is to be placed in an airtight chamber having an internal volume of at least 0.085 m^3 (0.28 $feet^3$).

16.15.1.4 Approximately 60 g (0.13 pounds) of cement dust, maintained at 20 to 50 % RH and capable of passing through a 200 mesh screen, is to be circulated for 1 hour by means of compressed air or a blower so as to completely envelop the sample in the chamber. The airflow is to be maintained at an air velocity of approximately 0.25 m/s (0.82 ft/s).

16.15.1.5 Following the exposure to dust, the unit is to be removed carefully, mounted in its intended position, energized from a rated source of supply and shall comply with the requirements of 16.2, Normal Operation.

16.15.2 Water immersion

16.15.2.1 All hand-held devices shall operate as intended after being subjected to immersion in distilled water for a period of 15 minutes at a depth of 100 mm (3.94 inches).

16.15.3 Salt spray (Fog)

16.15.3.1 All components of the electronic immobilization system and all options intended for mounting outside the passenger compartment shall be subjected to the tests outlined in 16.15.3.2 – 16.15.3.5.

16.15.3.2 The apparatus for salt spray (fog) testing is to consist of a fog chamber having inside dimensions of 1200 mm by 900 mm by 800 mm (47.24 inches by 35.43 inches by 31.50 inches), a salt-solution reservoir, a supply of conditioned compressed air, and a dispersion tower that produces a salt fog. The apparatus shall be constructed in accordance with ASTM B117, sample supports provision for heating the chamber, and necessary means of control.

16.15.3.3 The dispersion tower is to be located in the centre of the chamber and is to be supplied with humidified air at a pressure of 117 to 131 kPa (17 to 19 psi) (gauge) so that the salt solution is aspirated as a fine mist or fog into the interior of the chamber.

16.15.3.4 The salt solution is to consist of 5 % by mass of common salt [sodium chloride (NaCl)] and distilled water. The pH value of the collected solution is to be between 6.7 and 7.2, at a relative density of

1.0255 to 1.0400 at 25 °C (77 °F). The temperature of the chamber is to be maintained at 35 °C (95 °F) with a tolerance of ±1 °C (1.8 °F) throughout the test.

16.15.3.5 Drops of solution that accumulate on the ceiling or cover of the chamber are to be diverted from dropping onto the samples. Drops of solution that fall from samples are not to be recirculated but are to be removed by a drain located at the bottom of the chamber.

16.16 Attack test

16.16.1 The electronic immobilization system shall not be disarmed within 5 minutes when tested in the vehicle via manipulation or component replacement.

16.16.2 The list of tools below may be used in 16.16.1:

a) Electrical manipulation;

b) Basic Torque;

c) Advanced Torque;

d) Impact;

e) Basic Cut;

f) Pick Manipulation;

g) Component substitution;

h) Battery Powered Attack Tools; and

i) Electronic Attack Tools.

NOTE: This list cannot be entirely exhaustive, other tools and equipment may be specified as theft methods evolve and adapt with advances in technology.

16.16.3 Reference Annex B for specific tools identified in 16.16.2.

CAN BUS

17 General

17.1 An aftermarket system that uses CAN bus software immobilization to disable vehicle operation shall be in accordance with this section.

17.2 Requirements in 14.1, Means of Immobilization of Aftermarket Systems, shall not apply to CAN bus software immobilization.

18 Performance

18.1 The CAN bus software immobilizer shall prevent the vehicle from moving under its own power.

18.2 If a CAN bus software immobilizer uses a key carrying device, this device shall comply with requirements in Section 24, Cybersecurity.

18.3 The CAN bus software immobilizer shall have passive arming upon vehicle electronics going to sleep or after 60 s following key off.

18.4 Any installation of a CAN bus software immobilizer shall include a label applied near the VIN label on the B-pillar (inside door frame) and shall be registered in a centralized database for technical support for authorized callers without identifying the manufacturer or licensed installer of the device.

19 CAN Bus Remote Starters

19.1 If a CAN bus immobilizer allows for remote start operation, the CAN bus immobilizer shall prevent the vehicle from moving while in remote start mode.

20 CAN Bus Performance Testing

20.1 Requirements pertaining to performance testing for CAN Bus immobilizers shall be in accordance with Section 16, Performance Testing, with the exception of 16.16, Attack Test.

20.2 In lieu of passing the attack test, the licensed installer shall ensure that the CAN Bus immobilizer be hidden in such a way that it cannot be located and defeated within a 5 minute time period.

21 CAN Bus Software Immobilizer Disarming

21.1 Disarming a CAN bus immobilizer may be done with a correct code sequential key depression using the OEM control functions.

21.2 Other devices may be used such as key fobs and radio-frequency (RF) interfaces and shall comply with Section 24, Cybersecurity.

21.3 It shall not be possible to use the OBD II or CAN Bus system through an unauthorized access to deactivate the aftermarket CAN bus immobilizer.

22 Centralized Database

22.1 The centralized database shall be made available at all times for all aftermarket product installations (the purpose of the central registry is to provide transparency and auditability system that is centrally located. This provides the industry stakeholders the ability to know they are getting what they are expecting with the standard.

22.2 The centralized database shall be in accordance with national/regional regulations on personal information and data privacy.

22.3 The database shall be managed in accordance with NIST Special Publication 800-53.

22.4 Data shall be maintained at a centralized or in-house service (not shared or cloud resources).

22.5 The only PII data recorded shall be names and contact details for owners of items marked with service provider products.

22.6 The data shall not be shared with third parties other than for the purposes of crime prevention and detection and to provide certified repair providers with system identification and contact information for the original product manufacturer. Data shall not be used for commercial purposes.

22.7 Access to this database and any product/warranty information beyond the basic manufacturer of the immobilizer shall be restricted to:

a) Licensed Installers (access to enter and review records for this approved installation location).

b) Law Enforcement and Official Public Agencies (access for the purpose of crime prevention and detection)

22.8 The aftermarket product manufacturer shall keep a record of the following:

a) The information provided in the Immobilizer Installation Registration Form in Annex E.

b) Any override or system reset codes.

23 Data Access

23.1 At a minimum, the database shall contain fields that record the following information or enable the listed functionality:

a) Allow for a validation check to match the vehicle ID sticker (placed as described in 23.1 of this Standard) to the VIN number on the registered vehicle.

b) The type of immobilizer system installed shall be identified.

c) The manufacturer of the immobilizer system shall be identified.

d) The contact information of the immobilization system manufacturer shall be provided.

e) The model and version of the immobilization system shall be identified.

f) The original licensed installer of the immobilization system shall be identified.

g) The contact information of the original licensed installer shall be provided.

h) The date of installation of the immobilization system shall be provided.

CYBERSECURITY

24 General

24.1 Cybersecurity requirements for vehicle theft deterrent devices shall be in accordance with one of the following standards:

a) UNECE Regulation 155;

b) ECE/TRANS/WP.29/GRVA/2020/79; or

c) ISO/SAE 21434.

NOTE: Additional guidance on cybersecurity requirements for vehicle theft deterrent devices is located in Annex C.

FLEETS

25 General

25.1 The requirements of 6.2 shall apply to Fleets, with the following exceptions:

a) Fleets shall be allowed to request and use a common disarming device; and

b) Upon disposal of the vehicle, the common disarming device shall be disabled.

26 Performance

26.1 A function shall exist to disable any common disarming device for an immobilizer.

26.2 The fleet management shall determine fleet disablement. The OEM or the aftermarket device manufacturer shall provide a method of universal disablement for fleet managers but shall not be required to administer the disarming function.

PERFORMANCE

27 System Overview

27.1 The primary focus of the electrical or electronic immobilization system is for theft-of-vehicle, driveaway protection, accomplished through disabling multiple power train operating circuits.

27.2 The electronic immobilization system shall not degrade the safe operation of the vehicle in which the electronic immobilization system is installed.

27.3 Any optional equipment available with the electronic immobilization system shall not conflict with the theft deterrent function of the electronic immobilization system or the safe operation of the vehicle.

27.4 Subject to 27.5 and 27.9, the arming of the electronic immobilization system shall be passive arming.

27.5 The arming protocol of the electronic immobilization system shall include provisions for the immediate restart of the vehicle in case of an unintentional stall without compromising the passive arming operation of the electronic immobilization system.

27.6 Disarming of the electronic immobilization system shall be accomplished by means of a coded disarming device or secure disarming combination allowing the engine to start by normal means.

27.7 A minimum of two coded disarming devices or one secure disarming combination shall be supplied with the system.

27.8 The manufacturer of the electronic immobilization system shall have the option to supply to the end user additional coded disarming devices and secure disarming combinations through a secure distribution method.

27.9 The electronic immobilization system and all optional accessories shall be powered by the main vehicle battery when in armed mode. Optional accessories and disarming devices may incorporate secondary power sources.

MARKINGS

28 Instructions and Drawings

28.1 The manufacturer of the electronic immobilization system shall provide written operating instructions intended for the end-user. These instructions shall include details on maintenance (e.g., low battery indication, battery replacement procedure, battery specifications, malfunction instructions, etc.)

and a warning against leaving a duplicate coded disarming device or a copy of the secure disarming combination anywhere in the vehicle.

28.2 The electronic immobilization system manufacturer shall make available installation instructions and application guidelines to the licensed installer for aftermarket systems. Such guidelines shall include, but are not limited to, a listing of vehicle models which have been approved by the electronic immobilization system manufacturer as compatible with the device, along with wiring diagrams specific to the applicable vehicle and electrical ratings.

28.3 There shall be no visible markings on the vehicle to indicate the manufacturer, model number, licensed installer, or any other attribute of the electronic immobilization system.

ANNEX A (Informative) – THIRD PARTY CERTIFICATION

A1 Third-Party Certification

A1.1 It is intended that aftermarket devices encompassed in this Standard may be certified by an independent third-party certification organization accredited by the Standards Council of Canada and/or in accordance with ISO/IEC Guide 65 or ISO/IEC 17065 when implemented, in conformance to the requirements detailed in this Standard.

A1.2 A certification organization is an impartial body possessing the necessary competence and reliability to operate a certification system in which the interests of all parties concerned with the functioning of the system are represented.

A1.3 It is intended that all licensed aftermarket device installers should have successfully completed a training program endorsed by the system manufacturer. They should also successfully meet the expectations within this Standard, which should be checked every 24 months.

A1.4 As an alternate to third-party certification, aftermarket devices encompassed in this Standard can be inspected and tested by Type A inspection bodies accredited by the Standards Council of Canada and/or in accordance with ISO/IEC 17020 in conformance to the requirements detailed in this Standard.

NOTE: Type A inspection bodies provide third party inspections. Type A inspection bodies are defined in ISO/IEC 17020, Section A.1, Requirements for Inspection bodies (Type A).

ANNEX B (Informative) – ATTACK TOOLS

B1 Attack Tools

B1.1 Examples of attack tools includes, but is not limited to, the items listed in Table B1.1, Attack Tools.

Table B1.1
Attack Tools

Electrical Manipulation	Wire Wire cutters Wire strippers Insulation displacement connectors Crocodile clips 0-36 V power supply Piezoelectric spark generator Code scanners
	Code grabbers with analysis, (processing and re-transmission capability) Multimeter Basic mechanical manipulation Pen knife Swiss army executive Paper clip metal Magnet two small strong permanent magnet (BM 35 Neodymium Iron Boron) 25 mm (0.98 inches) (diameter) x 16 mm (0.63 inches) Pipe wrench 20 mm (0.79 inches) Stiff wire length
	Welding wire length Flexible steel wire length “Slim-jims” set Nylon packaging tape 10 mm (0.39 inches) width String 1 m (5,280 feet) Steel rule 300 mm (11.81 inches) Wedges with tapered profiles Wind Bag Files set Mirror small
	Lamp 12 V Compressed air bottle Pliers set Screwdrivers set Spanners/wrench set Lock puller hand-held Aerosol foam quick setting foam or gel, can 0.5 L (0.13 gallons) Freezing agent can, 0.5 L (0.13 gallons)

Table B1.1 Continued on Next Page