



SEC #539

# Automotive Cyber Security Legislation Guide

Cyber Security

A comprehensive guide to the cyber security legislation, best practice guidelines and technical standards that impact on in-car and off-board systems.

The Automotive Cyber Security Legislation Guide identifies the threats and opportunities generated by government mandates, guidelines and standards within Europe, USA, China and Japan. Information is also provided on relevant legislation from other countries around the world on an ad-hoc basis when an important development emerges.

The Automotive Cyber Security Legislation Guide has been designed to be a usable reference tool, highlighting the important requirements whilst noting legacy and out-dated publications so that you can confidently focus your attention on the issues that matter.

The Guide provides the background and timeline of each piece of legislation, best practice and standards, and SBD's Cyber Security team has gone further, showing the **implications** and where you need to be looking, allowing the Legislation Guide to become a vital part of a robust cyber security strategy.

## TABLE OF CONTENTS



INTRODUCTION

LATEST UPDATES

LEGISLATION

A summary of the latest automotive cyber security legislation

BEST PRACTICES

A summary of industry and government guides for automotive cyber security

STANDARDS

A summary of national, international and industry standards for automotive cyber security

## RELATED SBD REPORTS



### SEC #905 Cyber Security Intelligence Guide

SBD Automotive recommends automotive OEMs and suppliers to stay updated with the latest cyber threats and develop a culture of understanding that the addition of new technology in vehicles can increase the risk of car hacking.

To support OEMs and suppliers, SBD has created the Cyber Security Threat Intelligence Guide, with information on public hacks, countermeasure products, and the effect of these latest developments for automotive companies' strategy.

### COVERAGE



NA



CHINA



EUROPE



GLOBAL

### FREQUENCY



ANNUALLY



QUARTERLY



ONE TIME

### PUBLICATION FORMAT



PDF



POWERPOINT



EXCEL



ONLINE

### PAGES

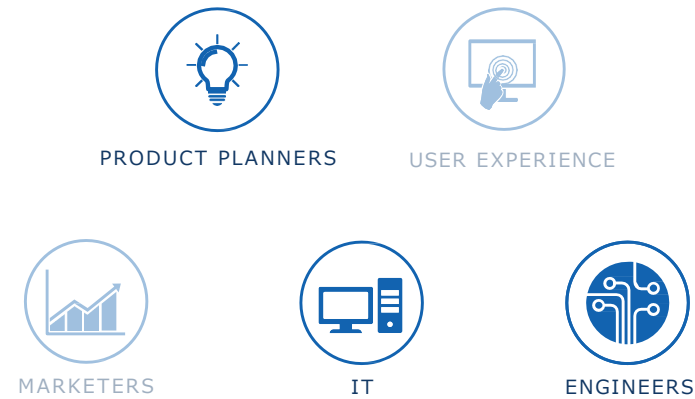


100+

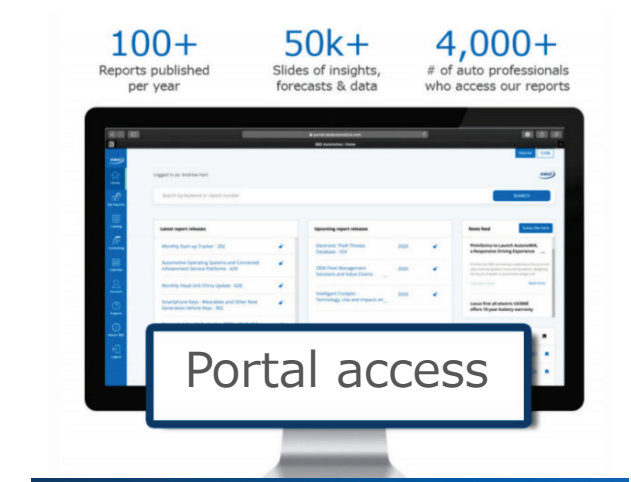
## Key features and benefits

- > Identifies the threats and opportunities generated by government mandates, guidelines and standards within Europe, USA, China and Japan
- > Strong focus on **implications**, allowing the Legislation Guide to become a vital part of a robust cyber security strategy
- > Government regulations and policies concerning cyber security for all vehicles
- > Particular focus on the cyber security requirements for autonomous vehicles (AVs)
- > Technical standards for vehicles published by national, international and industry bodies
- > Covering -
  - > UNECE
  - > ISO
  - > NHTSA
  - > UK DfT
  - > China GB/T
  - and much more

## This research is useful for



## Do I have access?



## Request a quote for

### Automotive Cyber Security Legislation Guide

Request price





Request price



Q1 2021

# AUTOMOTIVE CYBER SECURITY LEGISLATION GUIDE

CYB539-211

The Automotive Cyber Security Legislation Guide provides an in-depth analysis of how and where legislation is impacting on in-car and off-board automotive systems. It identifies the threats and opportunities generated by government mandates, guidelines and standards within **Europe, USA, China** and **Japan**. Information is also provided on relevant legislation from other countries around the world on an ad-hoc basis when an important development emerges.

Legislation	Best practice	Standards
This section includes updates on enacted and draft legislation that directly or indirectly impacts on vehicle cyber security, including UNECE, US senators etc.	This section includes updates on best practice guidelines that directly or indirectly impact on vehicle cyber security, including NHTSA, ENISA, Auto-ISAC etc.	This section includes updates on national, international and industry standards that directly or indirectly impact on vehicle cyber security, including ISO, SAE, China GB/t etc.
Page 9 - 19	Page 20 - 55	Page 56 - 102

***Note:** The Automotive Cyber Security Legislation Guide is a live resource that is updated with new information each quarter. Research for this edition concluded on the **26<sup>th</sup> March 2021**. Please contact SBD if you would like additional information relating to other legislation or markets to be included within future editions.*



# Example slides from the report

The image shows the cover of a report. The top half features a photograph of a person in a white lab coat or uniform, possibly a lawyer or a professional, sitting at a desk. They are looking at a smartphone in their right hand while their left hand rests on an open book. A gavel is visible on the desk to the left. The bottom half of the cover is a dark blue banner with the SBD logo on the left, the text 'Q1 2021' in the center, and 'CY8539-211' on the right. Below this banner, the title 'AUTOMOTIVE CYBER SECURITY LEGISLATION GUIDE' is written in white, all-caps, sans-serif font.

**SBD** Q1 2021 CY8539-211  
**AUTOMOTIVE CYBER SECURITY LEGISLATION GUIDE**

Request price >

## Legislation

## Best Practice

## Standards

### Automotive

### All Cars – Enacted

### Index for All Cars – Enacted

UNECE WP.29 R155 Cyber

UNECE WP.29 R156 SW Update

### Background

WP.29 is the World Forum for Harmonization of Vehicle Regulations within the institutional framework of the UN Economic Commission for Europe (UNECE). Part of WP.29 is the GRVA, a sub working group on automated/autonomous and connected vehicles, which also includes a task force for cybersecurity and OTA software updates.

WP.29 develops regulations on measures to ensure cybersecurity and data protection of connected vehicles and vehicles with automated driving technologies (ADT).

UN Regulation 155 proposes minimum cybersecurity engineering processes and type approval procedures for market access and it outlines requirements for an automotive Cybersecurity Management System (CSMS).

### Implications

UNECE R155 is the world's first regulation regarding automotive cybersecurity, and it will have an immediate impact on the market. Under the WP.29 regulations, OEMs selling in UNECE member countries must provide evidence of adequate cyber risk management practices along the entire value chain and throughout the product lifecycle.

Failure to comply will mean that new models are not Type Approved and so can't be sold in UNECE member countries, with the same requirements applied to all models sold a short time later.

### Latest news

March 2021

Latest Revised Version - E/ECE/TRANS/505/Rev.3/Add.154 - UN Regulation No. 155 - Cyber security and cyber security management system published. More [here](#)

February 2021

UN Regulation No. 155 on Cyber Security and Cyber Security Management Systems entered into force in January 2021. More [here](#).

November 2020

UNECE publishes a draft Interpretation Document on R155 to help OEMs and the automotive industry gain a better understanding of the requirements and how they will be assessed.

May 2020

ISO publishes draft standard (ISO/PAS 5112) that provides guidance for auditors evaluating OEMs to ISO/SAE 21434.

September 2020

Cyber-resilience of intelligent transport systems is discussed in the annual roundtable meeting comprising UNECE and OSCE members. More [here](#)

June 2020

UNECE's working party on autonomous and connected vehicles publishes draft UN regulations on cybersecurity and cybersecurity management system (CSMS). More [here](#)

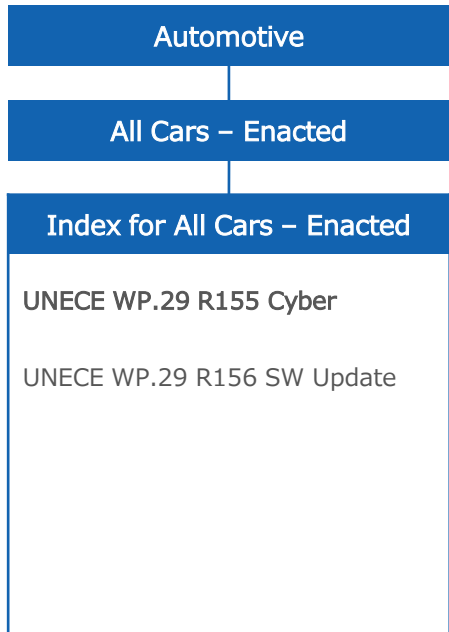
November 2019

A draft version of this regulation is published on the CS/OTA wiki. More [here](#).

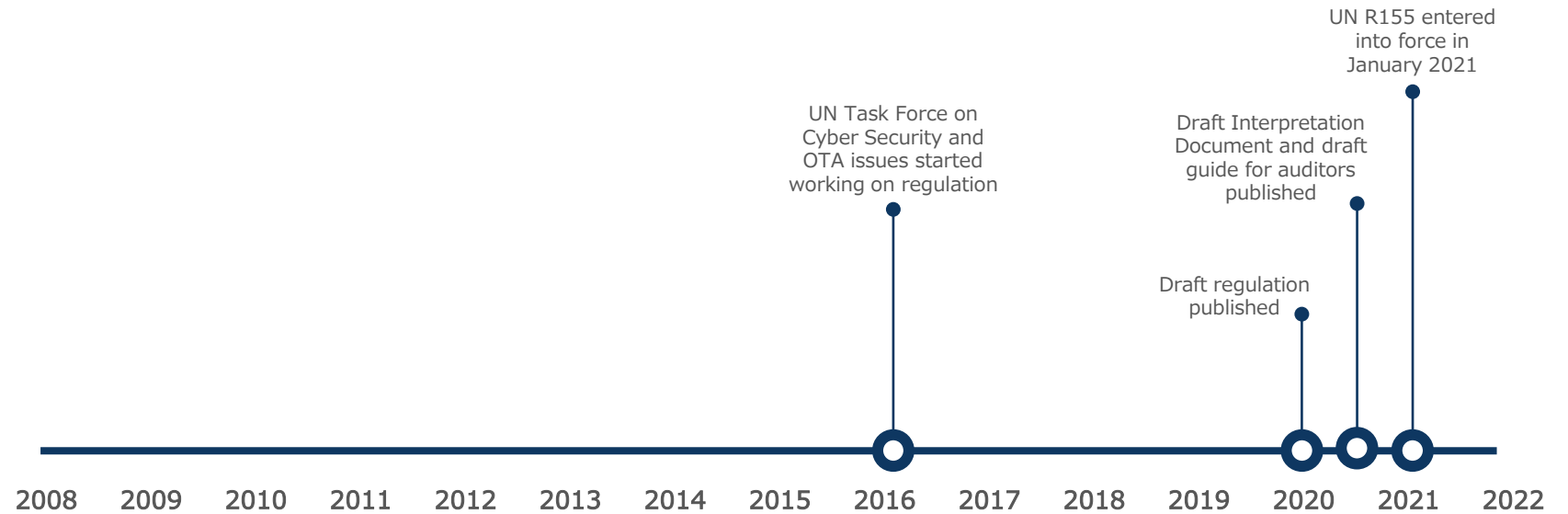
November 2016

UN Task Force on Cyber Security and OTA issues started working on regulation.

# UNECE WP.29 R155 Cybersecurity– Timeline



**Implementation timing**  
South Korea – 2020 guideline  
Japan – 2021 for AVs  
EU – 2022 for new models  
EU – 2024 for all models



## Relevant links

- [UN Regulation No. 155 - Cyber security and cyber security management system](#)
- [Draft Interpretation Document for UNECE R155](#)
- [ISO/WD PAS 5112 Road vehicles – Guidelines for auditing cybersecurity engineering](#)

Legislation

Best Practice

Standards

Automotive

All Cars – Enacted

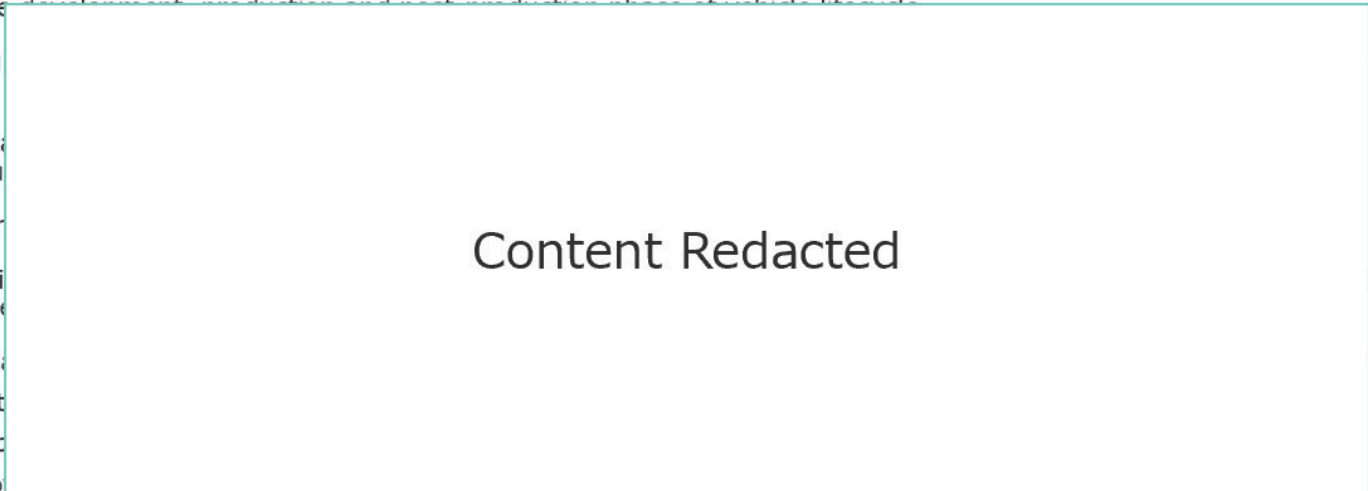
Index for All Cars – Enacted

UNECE WP.29 R155 Cyber

UNECE WP.29 R156 SW Update

The main highlights from the [UN Regulation No. 155 on Vehicle Cyber Security](#) are the following:

- Vehicle OEMs shall have a Cyber Security Management System (CSMS) in place, in compliance with this Regulation. CSMS shall consider the development, production and maintenance of vehicles throughout their lifecycle.
- Contracting for CSMS.
- The Certificate of Conformity shall include the CSMS certificate number.
- Within the next 18 months, OEMs shall submit a CSMS report to the competent authority.
- New reporting requirements for Technical Service Providers (TSPs).
- OEMs will have to take specific measures to:
  - Detect and report vulnerabilities.
  - Support the competent authority in its investigations.
  - Provide information on the security of the vehicle.



Compliance  
the  
ity or  
measures to:



Request price >