TABLE OF CONTENTS

RELATED SBD REPORTS

528 – Connected Car Legislation Guide

The Connected Car Legislation Guide provides an in-depth analysis of how and where legislation is impacting on automotive connected services.

It identifies the threats and opportunities generated by government mandates, licensing requirements, restrictions, policies, and guidelines within Europe, USA, China, Russia and Brazil.

CYB

Cyber Security

#539

Automotive Cyber Security Legislation Guide

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Guide has been designed to be a usable reference tool, highlighting the important requirements whilst noting legacy and outdated publications so that you can confidently focus your attention on the issues that matter.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.

COVERAGE	FREQUENCY	PUBLICATION FORMAT	PAGES
GLOBAL, NA, CHINA, EUROPE	ANNUALLY, QUARTERLY, ONE-OFF	PDF, POWERPOINT, EXCEL, ONLINE	50+

Request price

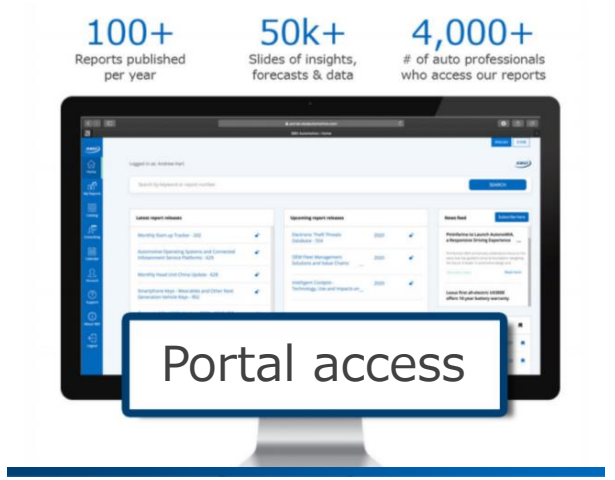
Key questions answered

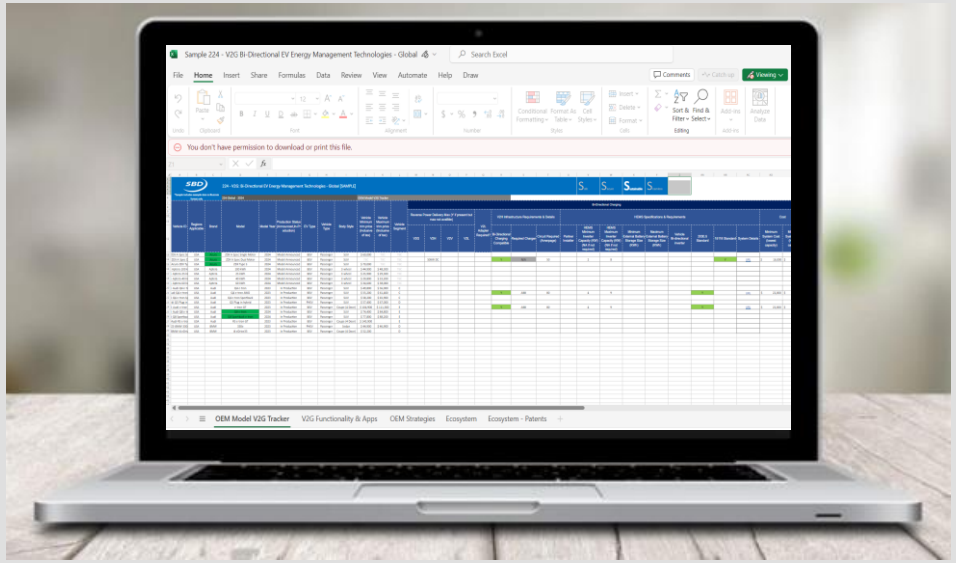
- What threats and opportunities are generated by government mandates, guidelines and standards?
- What are the key relevant legislation points from other countries on new policies?
- What exactly the best practices & standards for complying with all cyber security legislation?
- How should we be looking at our business to evaluate our cyber security compliance?

This research supports

- PRODUCT PLANNERS
- ENGINEERS
- MARKETING
- C-SUITE

Do I have access?



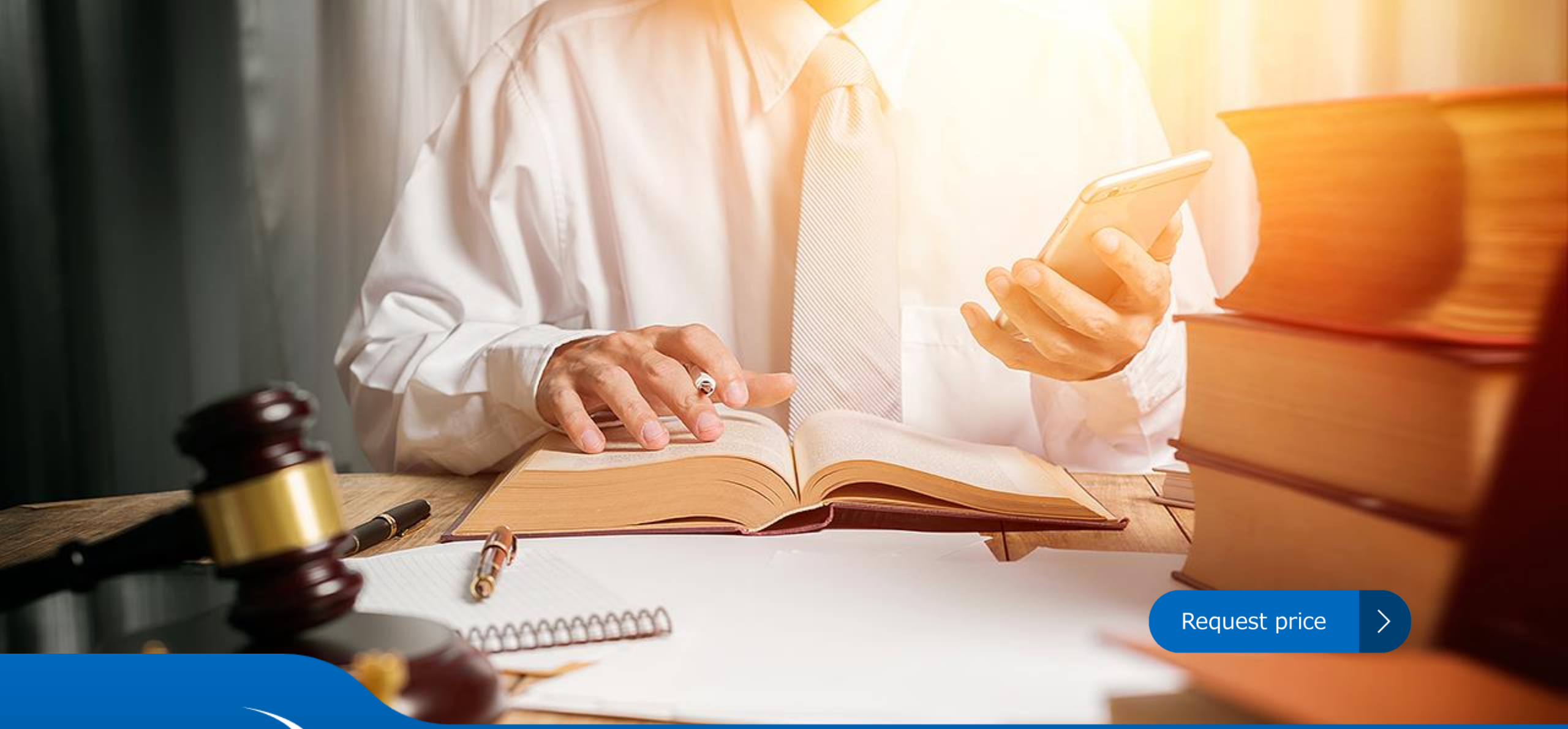


View Excel Data Sheet Sample

Automotive Cyber Security Legislation Guide

For a deep dive into the background and timeline of each piece of legislation, best practice and standards

Click for Sample



Request price

SBD

AUTOMOTIVE CYBER SECURITY LEGISLATION GUIDE

Contents

539 Cyber Security Legislation Guide

Data Deep Dive
View and analyze deep data in your own way

Total number of pages - 53

Introduction

Introduction

The digitization of modern cars continues to progress rapidly with an ever-rising penetration of connected and automated functionalities. However, this influx of new features has also exposed the cars to external vulnerabilities from a cyber security point of view. The security researchers have found out various 'gateways' through which malicious hackers can get access to the mission-critical elements in the car.

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

The **Cyber Security Legislation Guide** has been designed to be a usable reference tool, listing the important and the most recent announcements whilst also highlighting the learnings from legacy/outdated publications so that the readers can confidently focus their attention on the issues that matter. The Guide provides the status and timeline of each piece of legislation, best practice and standards, and SBD's team has gone further, discussing some of the most relevant topics in detail allowing the Legislation Guide to become a vital part of a robust cyber security strategy.

Section	Content
Bird's Eye View	Overview of trends and insights relevant to the legislation guides series
Executive Summary	This section highlights some of the recently enforced and introduced regulations/legislations/guidelines
The Basics	A brief overview of the different type of legal aspects (regulation, legislation, standards etc.) covered in this report along with the regions in focus.
Analysis	Key regulatory activities that are impacting the automotive cyber security development and best practices published by the authorities
Summary Tables	Summarizing the legislative activities identified in the associated Excel spreadsheet in terms of their recency and status.
Next Steps	Can SBD help you with any unanswered questions?

Note: *This guide only highlights the actual regulatory activities and does not give any recommendations. This guide's analytical and forward-looking statements shouldn't be construed as legal advice.*

Example slides from the report

Request price

What? Snapshot of key regulatory activities

	Introduced* Legislation/Regulations recently introduced	Enforced/Published** Legislation/Regulations recently enforced
Global	**Information Privacy and Other Legislation Amendment Bill 2023** This bill proposes legislative amendments to Queensland's information privacy framework to better protect personal information and provide appropriate responses and remedies for data breaches and misuse of personal information by agencies.	*No new legislation/regulations were enforced recently*
China	*No new legislation/regulations were introduced recently in China*	**Chongqing Economics and Telematics Regulation [2023] No.18** The publication was introduced and passed on 2023/12/23 and was enforced on 2024/1/22
Europe	*No new legislation/regulations were introduced recently in Europe*	**(EU, Euratom) 2023/2841** This proposal establishes a framework for ensuring common cybersecurity rules and measures among the EU institutions, bodies and agencies (signed by the President on 13th Dec. 2023)
USA	**Satellite Cybersecurity Act (Bill 1425)** Aims to provide commercial satellite system with federal support towards their cybersecurity **Department of Homeland Security Civillian Cybersecurity Reserve Act** It aims to establish a Civilian Cybersecurity Reserve in the Department of Homeland Security as a pilot project to address the cybersecurity needs of the United States with respect to national security, and for other purposes.	**NTIA Policy and Cybersecurity Coordination Act** It amends the National Telecommunications and Information Administration Organization Act to establish the Office of Policy Development and Cybersecurity, and for other purposes. **Executive Order on Improving the Nation's Cybersecurity** Update to Memorandum M-22-18, Enhancing the Security of the Software Supply Chain through Secure Software Development Practices, requires agencies to comply with the NIST Guidance.

**In some regions the word 'issued', 'proposed' for the legislation that are used*
***Standards and Guidelines/Best Practices are often not enforceable by law. They are introduced and reviewed by the subject experts before being published.*

EU policymakers have reached a consensus on cybersecurity laws

Regulation Overview

Status		Introduced	✓	Draft		Enforced

The European Union (EU) Cybersecurity Act establishes a pan-European cybersecurity certification framework and a new mandate for ENISA, the apex agency for cybersecurity in Europe. This regulation aims to strengthen the EU's cybersecurity structures and offer a comprehensive set of measures to develop its member states' capabilities in responding to cyber threats. The first area is to strengthen the powers of ENISA by making it a permanent agency of the EU and the second is to establish a European cybersecurity certification framework to ensure the application of **a common certification for ICT goods.**

Details

EU Cybersecurity Act (What all it includes)

The EU Cybersecurity Act introduces for the first time EU-wide rules for cybersecurity certification. Companies in the EU will be able to certify their products, processes and services. Under the framework, multiple schemes will be created for different categories of ICT products, processes and services.

The schemes will specify the security standards met by certified products and indicate the period of validity for the certificates issued.

However, the automotive industry is in discussion with the EU to review if vehicles will be excluded from the certification requirements given that cyber security will be assessed as part of the Type Approval process.

What's New?

Proposed Regulation on 'managed security services' amendment (2023)

On 18 April 2023, the European Commission proposed a targeted **amendment** to the EU Cybersecurity Act. The amendment aims to enable the adoption of European cybersecurity certification schemes for 'managed security services', in addition to **information and technology (ICT) products, ICT services and ICT processes**, which are already covered under the Cybersecurity Act. Managed security services play an increasingly important role in the prevention and mitigation of cybersecurity incidents.

This covers various aspects like **incident response, penetration testing, security audits and consultancy**. The proposed amendments also adapt the scope of the European cybersecurity certification framework and introduce a definition of 'managed' services in line with the NIS 2 Directive.

Additionally, the new amendment also mandates ENISA to prepare the technical ground for specific certification schemes. It will oversee informing the **public on the certification schemes and the issued certificates through a dedicated website.** ENISA is mandated to increase operational cooperation at EU level, helping EU Member States who wish to request it to handle their cybersecurity incidents, and supporting the coordination of the EU **in case of large-scale cross-border cyberattacks and crises.** ENISA will also compile and publish guidelines and develop good practices, concerning the cybersecurity requirements for ICT products in cooperation with national cybersecurity certification authorities.

Latest update: European Council and the Parliament the Council presidency and European Parliament's negotiators reached a provisional agreement on the 'cyber solidarity act', as well as on a targeted amendment to the cybersecurity act (CSA). The next step is for the co-legislators to review and formally adopt. More here

Key Takeaways

The new amendment does not affect the Cybersecurity Act's consistency with Regulation (EU) 2016/679 ("the GDPR") and its provisions on establishing certification mechanisms. The Cybersecurity Act remains without prejudice to the certification of data processing operations, including when such operations are embedded in products and services, under the GDPR.

China is developing its own automotive cyber standards

Standard Overview

Status		Introduced		Draft	✓	Published

Whilst the rest of the world has focused on global ISO/SAE 21434 to embedded cyber into the development process, China is developing its own standards that recommend specific technologies and/or security controls for critical in-car and off-board systems.

The National Information Security Standardisation Technical Committee (TC260) in China recently announced the release of 12 national cybersecurity standards. These standards cover various areas including entity authentication, information system security assurance, public key infrastructure, VPN access, and data security. The standards will come into effect on October 1, 2023.

Details

Legislation: GB Cyber Requirements

The Chinese Ministry of Industry and Information Technology (MIIT) has plans to introduce over 100 optional standards relating to automotive cyber security by 2025. However, in 2021 the MIIT announced that the following two of the standards would be upgraded to mandatory GB, meaning that all OEMs must comply with the requirements:

- **Cybersecurity technical requirements and test methods for whole vehicle**
- **General technical requirement of vehicles software update.**

For OEMs that have already started implementing UNECE R155 and are looking into implementing R156 there is minimal rework expected, as it is understood the two new standards will be similar to and that they align with UNECE R155 and R156 respectively. The implementation timing is expected to be for new models type approved from mid-2023.

Standard: China GB/T- Automotive Standard

The GB/T cyber standards are being developed in batches.

- In March 2022, the first batch of GB/T automotive cyber standards have been published and status updates provided on the second batch. In September 2022, minor updates on availability of draft GB/T standards

The majority of China's automotive cyber standards will be published as GB/T recommended national standards (although 2 will be GB mandated national standards), but it is expected that most domestic OEMs will formally adopt the requirements for their future models. It is unclear if the recommended standards will be mandated, or if OEMs will suffer any indirect penalty for not adopting the standards, but as a first step all domestic and foreign OEMs should at least audit their systems against the requirements to establish their current baseline position.

The new standards released by TC260 includes GB/T 15843.3-2023, GB/T 17902.1-2023, GB/T 20274.1-2023, and others, are updated versions that replace previous GB/T standards in their respective domains.

Key Takeaways

China is creating unique standards for automotive cybersecurity, in contrast to the global approach of integrating it into the development process through ISO/SAE 21434. These standards by China suggest particular technologies and security measures for crucial in-car and off-board systems. This legislation is known as GB Cyber Requirements, while the corresponding standard is referred to as China GB/T- Automotive Standard.

What's New?

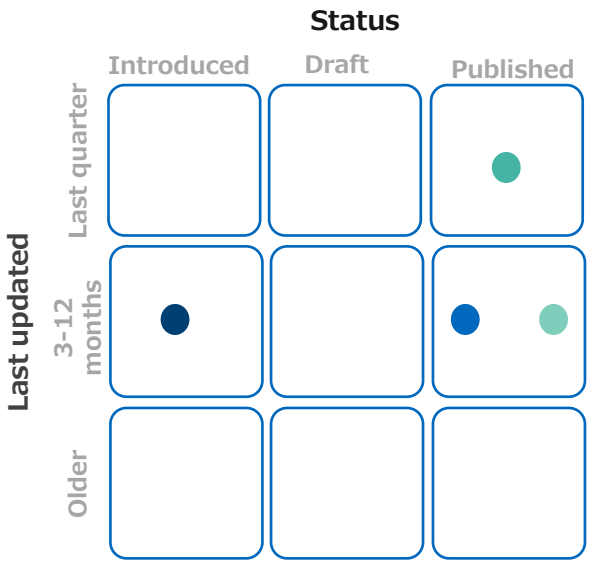
GB/T 43557-2023 : The standard describes the types of information and elements of cybersecurity information reporting, as well as the key elements of cybersecurity information reporting activities. and elements of cybersecurity information reporting activities. This standard is effective since July 1st, 2024**.** Link

GB/T 34942-xxxx: This document mainly provides guidance for third-party assessment organizations to carry out security capability assessment of cloud computing services. It is a replacement of GB/T 34942-2017. (Link)

USA – Guidelines & Best Practices

Latest activity vs status

About the policy activity placement in the grid



Name of the law	Recent development(s)	Next activity/milestone
The NIST Cybersecurity Framework 2.0 Draft (Federal)	NIST has expanded the CSF's core guidance and developed related resources to help users get the most out of the framework.	Version 2.0 released in February 2024
Guide to Securing Remote Access Software (Federal)	The joint guide (CISA, FBI, NSA) provides an overview of risks to smart cities, including expanded and interconnected attack surfaces; information and communications technologies (ICT) supply chain risks; and increasing automation of infrastructure operations.	No significant change since the last development
Cybersecurity Framework Profile for EV Fast Infrastructure (Federal)	NIST IR 8473 provides users with a national-level, risk-based approach for managing cybersecurity activities for EV XFC systems.	The guidance has been finalized
State Cybersecurity Strategy (NY)	New York Governor announced the states' first cybersecurity strategy aimed at protecting the State's digital infrastructure from the cyber threats.	$90 million investment for cybersecurity included in the Fiscal Year 2024 Budget

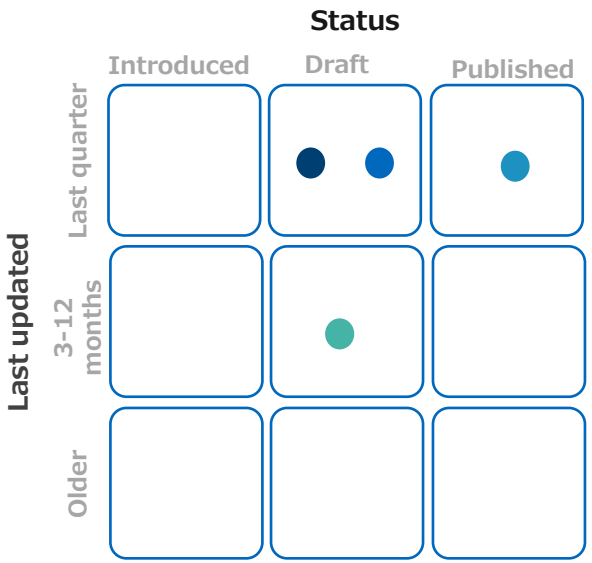
Key highlights

- **The NIST CSF (version 2.0) provides high-level guidance, including a common language and a systematic methodology for managing cybersecurity risk** across sectors and aiding communication between technical and nontechnical staff. It includes activities that can be incorporated into cybersecurity programs and tailored to meet an organization's particular needs.
- **NY Governor Hochul also signed legislation to expand New York's technology talent pool** and provide funding to help ensure that New York-based employers are able to hire and retain necessary cybersecurity personnel.

Global – Standards

Latest activity vs status

About the policy activity placement in the grid



Title of the standard	Recent development(s)	Next activity/milestone
ISO 15118-2: Road vehicles — Vehicle to grid communication interface	ISO 15118-2:2014 standard will be replaced by ISO/DIS 15118-2	In drafting stage
ISO/CD 15118-3 Road vehicles - Vehicle to grid communication interface Part 3: Physical and data link layer requirements	ISO 15118-3:2015 standard will be replaced by ISO/CD 15118-3	In drafting stage
ISO/IEC 24392:2023 Cybersecurity - Security reference model for industrial internet platform (SRM- IIP)	Document presents specific characteristics of industrial internet platforms (IIPs), including related security threats, context-specific security control objectives and security controls.	Published recently in the last quarter
IEEE 1609.4-2016/Cor 1-2019 IEEE Standard for Wireless Access in Vehicular Environments (WAVE) -- Multi-Channel Operation	Effective mechanisms that control the operation of upper-layer data transfers across multiple channels, without requiring knowledge of physical layer (PHY) parameters and describe the multi-channel operation channel routing and switching for different scenarios.	First published in 2019 and revised recently

Key highlights

- ISO 15118-3:2015 specifies the requirements of the physical and data link layer for a high-level communication, directly between battery electric vehicles (BEV) or plug-in hybrid electric vehicles (PHEV). It covers the **overall information exchange between all actors involved in the electrical energy exchange**. ISO 15118 (all parts) is applicable for manually connected conductive charging.

Request the price

Request price

Contact SBD Automotive

Do you have any questions?

If you have any questions or feedback about this research report or SBD Automotive's consulting services, you can email us at info@sbdautomotive.com or discuss with your local account manager below.

info@sbdautomotive.com

Book a meeting

USA | UK | Germany | India | China | Japan

Garren Carr
North America
garrencarr@sbdautomotive.com
+1 734 619 7969

Luigi Bisbiglia
UK, South & West Europe
luigibisbiglia@sbdautomotive.com
+44 1908 305102

SBD China Sales Team
China
salesChina@sbdautomotive.com
+86 18516653761

Andrea Sroczynski
Germany, North & East Europe
andreasroczynski@sbdautomotive.com
+49 211 9753153-1

SBD Japan Sales Team
Japan, South Korea & Australia
postbox@sbdautomotive.com
+81 52 253 6201