CANADA'S VEHICLE CYBER SECURITY GUIDANCE

Transport Canada Transports Canada

Canada

Cette publication est aussi disponible en français sous le titre Lignes Directrices sur la cybersécurité des véhicules au Canada.

TP 15440E

TC-1006428

PRINT

Cat. No. T46-61/2020E-PDF

ISBN 978-0-660-34036-4

PDF

Cat. No. T46-61/2020E-PDF

ISBN 978-0-660-34036-4

The information in this copy of this publication may not be updated to reflect amendments made to original content. For up-to-date information contact the Department of Transport Canada.

TABLE OF CONTENTS

Message from the Minister of Transport **4**

Executive Summary **5**

Introduction **7**

Purpose 7

Scope 8

Context 8

Cyber Security Roles and Responsibilities in Canada 10

Canada's Statutory Framework 11

International Vehicle Cyber Security Guidance and Standards 12

Vehicle Cyber Security Guidance: Key Principles **13**

1. Organizations should identify and manage cyber security risks 14

1.1 Cyber security governance 14

1.2 Risk management frameworks 14

1.3 Supply chain security 14

2. Organizations should protect the vehicle ecosystem 15

2.1 Layered cyber defences 15

2.2 Privacy protection 16

2.3 Information protection procedures 18

2.4 Training and awareness programs 18

3. Organizations should detect, monitor and respond to cyber security events 19

3.1 Event detection, monitoring and analysis 19

3.2 Security audits 19

3.3 Vulnerability management plan 19

3.4 Incident management and response 20

4. Organizations should recover from cyber security events safely and quickly 20

4.1 Incident recovery 20

4.2 Partnership building and information sharing 21

4.3 Cyber security as a process of continuous improvement 21

Considerations and Opportunities for Canada **22**

Conclusion **23**

Annex 1: Glossary **24**

Annex 2: Vehicle Cyber Security Best Practices - Reference Material **27**

MESSAGE FROM THE MINISTER OF TRANSPORT

I am pleased to introduce *Canada's Vehicle Cyber Security Guidance*, which provides technology neutral and non-prescriptive guiding principles to help ensure vehicles are cyber-safe for Canadians.

Canada's transportation system is highly interconnected and complex, with each mode – road, marine, air, and rail – undergoing a digital transformation that could improve the safe and efficient movement of goods and people. Promising technological advancements, including connected and automated vehicles (CAVs), have the potential to enhance safety on Canadian roads. At the same time, they pose new cyber security challenges that underscore the importance of building cyber resilience into our transportation system.

Cyber security is a shared responsibility amongst all levels of government, the private sector, and individuals. Vehicle cyber security is a particularly complex issue that involves many horizontal partners, such as the vehicle manufacturing and aftermarket sectors. It also carries important safety considerations for the future, as more and more vehicles are equipped with technologies that rely on the security of interconnected digital systems.

Transport Canada continues to lead a safety-focused approach to the introduction of CAVs, recognizing the need to foster innovation and remain technology neutral, while prioritizing road safety. Building on Canada's robust motor vehicle safety regime, Transport Canada continues to adapt its regulatory framework to include strategic policies, guidance, and tools that help support a flexible national approach to safe testing and development. *Canada's Vehicle Cyber Security Guidance* is a key addition to this suite of initiatives that can help industry and non-technical stakeholders develop a consistent approach to CAV cyber security.

I would like to extend my gratitude to the many national partners who have provided their feedback and support for *Canada's Vehicle Cyber Security Guidance*. I look forward to continuing these strong partnerships as we work together to ensure the safety and security of Canada's transportation system into the future.

Marc Garneau

The Honourable Marc Garneau, P.C., M.P.
Minister of Transport

EXECUTIVE SUMMARY

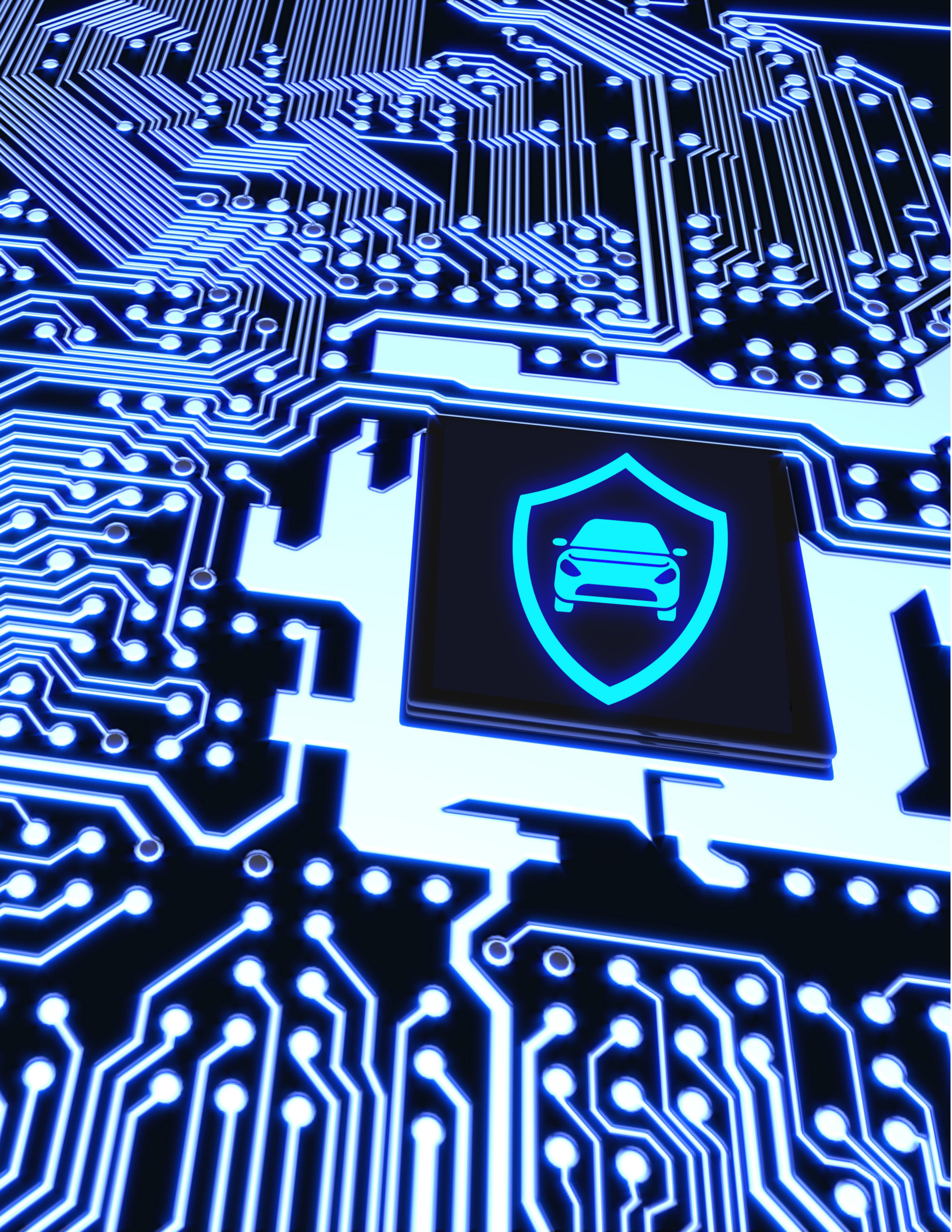
Modern vehicle technology could improve road safety for all Canadians and offer new forms of mobility, but with increasing levels of connected and automated features, the vehicle cyber security threat landscape grows in scale and complexity. *Canada's Vehicle Cyber Security Guidance* (Cyber Guidance) has been developed to advance the state of vehicle cyber security in Canada.

Cyber Guidance aims to support industry stakeholders by providing technology neutral and non-prescriptive guiding principles to strengthen cyber security throughout the vehicle lifecycle. Building on existing cyber security best practices, Cyber Guidance uses a risk-based approach to help automotive industry stakeholders mitigate and manage vehicle cyber security risks.

The principles within the Cyber Guidance encourage organizations to:

- identify how they will manage cyber security risks;
- protect the vehicle ecosystem with appropriate safeguards;
- detect, monitor, and respond to cyber security events; and,
- recover from cyber security events safely and quickly.

Safety and security are inextricably linked in modern vehicles. In order to harness the full safety benefits of vehicle technologies, government and industry know that strong cyber security practices must be incorporated into the transportation system. From security-by-design to responsible data management practices, and post-deployment considerations, it is essential that cyber security is prioritized throughout all stages of the vehicle lifecycle. Cyber Guidance underscores Transport Canada's (TC) commitment to work closely with stakeholders and cyber security experts to support the safe and secure testing and deployment of new vehicle technologies on Canada's roads.



INTRODUCTION

Vehicle technologies are emerging at a rapid pace and modern vehicles have become highly complex cyber physical systems. The global shift to connected and automated vehicles (CAVs) is well underway in Canada, bringing enormous potential safety benefits for Canadians. At the same time, this digital transformation introduces new cyber security challenges that underscore the importance of prioritizing cyber resilience in Canada's transportation system.

The automotive sector, with the support of government, industry, and standards-setting bodies, has already made important strides in strengthening vehicle cyber security, such as participating in information sharing forums, investing in research and testing, and contributing to the development of standards, guidance, and tools. However, as vehicle ecosystems become increasingly sophisticated and interconnected, the cyber-attack surface grows. It is incumbent on all stakeholders (e.g., governments, industry associations, manufacturers, etc.) to develop an approach to CAVs that prioritizes safety, security, and privacy.

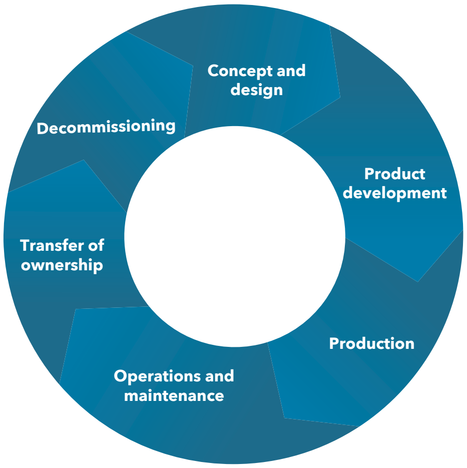
In order to harness the full safety potential of modern vehicles, governments must encourage the responsible development and deployment of new technologies. TC's approach leverages flexible policy frameworks, non-regulatory guidance and tools, as well as modernized legislation and regulations to support the testing and deployment of CAVs, while ensuring that safety is paramount. Cyber Guidance is a key feature of TC's forward-looking regulatory framework and offers strategic principles that should be considered throughout the vehicle lifecycle.

PURPOSE

Cyber Guidance addresses a key TC commitment to develop cyber security guidance for the transportation sector, as set out in the January 2018 report of the Standing Senate Committee on Transportation and Communications, entitled *Driving Change: Technology and the Future of the Automated Vehicle*.[1]The principles within Cyber Guidance align with international best practices and represent a foundational framework for strengthening vehicle cyber security in Canada.

Cyber Guidance provides technology neutral and non-prescriptive guiding principles to strengthen cyber security throughout the vehicle lifecycle. It is intended to support stakeholders in developing, deploying, and maintaining cyber resilient vehicle technologies and reduce the likelihood of cyber attacks against vehicle systems. Stakeholders are encouraged to read this document in conjunction with existing best practices and technical standards (see Annex 2: Reference Material).

Vehicle Lifecycle



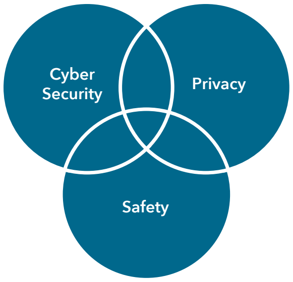
[1] Source: Senate of Canada, Driving Change: Technology and the future of the automated vehicle. January 2018. https://sencanada.ca/content/sen/committee/421/TRCM/Reports/COM_RPT_TRCM_AutomatedVehicles_e.pdf (accessed June 4, 2019).

SCOPE

This document provides strategic cyber security guidance for all phases of the vehicle lifecycle and, where appropriate, in the supporting vehicle infrastructure, including external, but related, information systems, services, and data. Specifically, Cyber Guidance is focused on the vehicle and/or product security, which includes components and infrastructure that are on or directly connected to the vehicle/product.[2] It was designed primarily for light passenger vehicles with varying degrees of connectivity and automated features, including legacy vehicles, but will have applicability for other vehicle types, such as heavy duty vehicles.[3] It will also have applicability for the post-production sector including dealers, aftermarket suppliers, and service providers. Cyber Guidance is intended for individuals and organizations designing, manufacturing, supplying, and maintaining systems, software, and services for motor vehicles and motor vehicle equipment.

CONTEXT

New vehicle technologies are transforming the road transportation sector. From passenger cars to commercial motor carriers, vehicles are becoming sophisticated cyber physical systems. Often described as computers on wheels, they are equipped with embedded Electronic Control Units (ECU) running millions of lines of code that control mechanical and/or electronic vehicle systems, including safety critical functions such as the powertrain, braking, stability control, and supplemental restraint systems. At the same time, vehicles are increasingly connected to external devices and infrastructure through a variety of communications technologies, such as cellular, Wi-Fi, Bluetooth, Dedicated Short Range Communications (DSRC), and others.



This combination of connectivity and computerization in modern vehicles means that cyber security is inextricably linked with safety and privacy. Vehicles depend on a wide range of essential information and operational technology to function as intended. The increased complexity of vehicle system architecture has resulted in a large and diverse attack surface with multiple physical access points, such as network communication interfaces, an array of sensors including LIDAR, RADAR, cameras, GPS, in-vehicle hardware, firmware, and software.[4] A cyber security breach – either deliberate or accidental – could have adverse consequences, such as compromising vehicle safety, unauthorized access of confidential information, and vehicle theft, among others. Organizational understanding of the vehicle threat landscape is critical to effectively managing and mitigating cyber security risks.

While the most dramatic examples of cyber-attacks have been demonstrated by "white-hat" cyber security researchers, malicious cyber-attacks targeting the vehicle sector are on the rise, and the data rich environment generated by the connected vehicle ecosystem is an attractive target.[5] Vehicles can collect and process significant amounts of personal information (e.g. communications, location data, driver behaviour) through a variety of onboard sensors, functionalities, and services. Data is intrinsic to ongoing vehicle development, testing, deployment, safe operations, and maintenance. The responsible collection, use, and disclosure of personal information is a critical component to the development and deployment of new vehicle technologies.

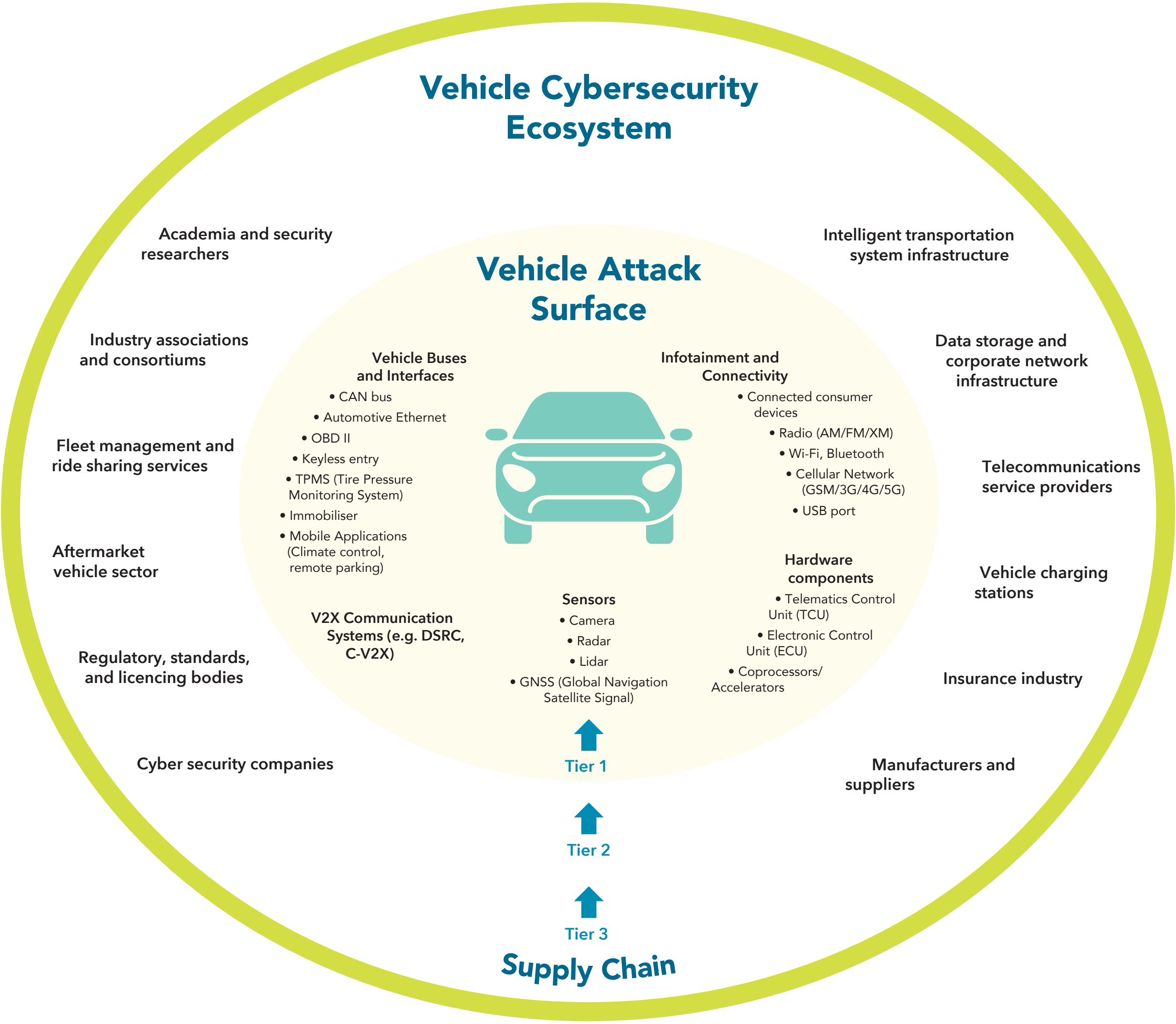
[2] Broader road transportation infrastructure is an important component of the connected vehicle ecosystem, but is not the core focus of this guidance. Please see "Section 5.0: Considerations and opportunities for Canada" for additional cyber security projects related to the connected vehicle ecosystem.

[3] There are unique cyber security considerations for other vehicle types such as commercial motor carriers (**Class 6-8 Commercial Trucks**) which use the SAE 1939 "open" standard for networking and communications.

[4] For detailed vehicle threat and vulnerability taxonomies please see: U.N. Task Force on Cyber Security and Over-the-Air Issues. Draft Recommendation on Cyber Security of the Task Force on Cyber Security and Over-the-air issues of UNECE WP.29 GRVA. September 9, 2018. https://www.unece.org/fileadmin/DAM/trans/doc/2018/wp29grva/GRVA-01-17.pdf; European Union Agency for Cybersecurity. ENISA Good Practices for Security of Smart Cars. November 2019. https://www.enisa.europa.eu/publications/enisa-good-practices-for-security-of-smart-cars; forthcoming ISO/SAE 21434 cyber security engineering standard.

[5] Upstream Security. Upstream Security Global Automotive Cybersecurity Report 2019: Research into Smart Mobility Cyber Attack Trends. 2018. https://www.upstream.auto/upstream-security-global-automotive-cybersecurity-report-2019/.

The vehicle cyber security environment is complex. Vehicles have a long lifecycle during which time software, firmware, and hardware should be supported to remain cyber resilient in a constantly changing threat environment. Manufacturing and maintaining cyber resilient vehicles is further complicated by a heavily-tiered and increasingly non-traditional supply chain in which all vendors and service providers have a responsibility to prioritize cyber security in their product lifecycle, as well as in their operations, in order to contribute to the overall security and safety of the ecosystem. The supply chain extends into the aftermarket sector, where automotive device manufacturers, diagnostic and repair services, and vehicle modifiers access, and may alter, vehicle systems and data. Organizations will need to work collaboratively to ensure vehicle systems and services continue to interact safely and securely.


Vehicle Cybersecurity Ecosystem
Academia and security researchers
Industry associations and consortiums
Fleet management and ride sharing services
Aftermarket vehicle sector
Regulatory, standards, and licencing bodies
Cyber security companies
Intelligent transportation system infrastructure
Data storage and corporate network infrastructure
Telecommunications service providers
Vehicle charging stations
Insurance industry
Manufacturers and suppliers
Vehicle Attack Surface
Vehicle Buses and Interfaces
• CAN bus
• Automotive Ethernet
• OBD II
• Keyless entry
• TPMS (Tire Pressure Monitoring System)
• Immobiliser
• Mobile Applications (Climate control, remote parking)
Infotainment and Connectivity
• Connected consumer devices
• Radio (AM/FM/XM)
• Wi-Fi, Bluetooth
• Cellular Network (GSM/3G/4G/5G)
• USB port
Hardware components
• Telematics Control Unit (TCU)
• Electronic Control Unit (ECU)
• Coprocessors/ Accelerators
Sensors
• Camera
• Radar
• Lidar
• GNSS (Global Navigation Satellite Signal)
V2X Communication Systems (e.g. DSRC, C-V2X)
Tier 1
Tier 2
Tier 3
Supply Chain

This graphic is intended for illustrative purposes and should not be considered an exhaustive list of the vehicle attack surface and vehicle cyber security ecosystem.

CYBER SECURITY ROLES AND RESPONSIBILITIES IN CANADA

In Canada, cyber security is a responsibility shared by all levels of government, the private sector, and individual Canadians. Federally, Public Safety Canada (PS) provides national leadership on cyber security policy through *Canada's National Cyber Security Strategy* (Cyber Security Strategy), which is based on three pillars: security and resilience; cyber innovation; and leadership and collaboration.[6] Federal departments support PS and the Cyber Security Strategy by overseeing the cyber security of their sector's critical infrastructure.

TC has developed a multi-pronged, safety-focused approach to supporting the safe and secure testing and deployment of new vehicle technologies, including CAVs. TC is working collaboratively with stakeholders to modernize Canada's legislative and regulatory frameworks to support emerging vehicle technologies. In parallel, TC continues to expand upon its suite of national non-regulatory policies and guidance that set clear expectations for the safe testing and deployment of CAVs in Canada. Cyber Guidance is an important component of this approach.

The Communication Security Establishment (CSE)'s Canadian Centre for Cyber Security (the Cyber Centre) supports TC and other federal departments in addressing cyber security in their respective sectors. The Cyber Centre is the central trusted federal government source of operational cyber security information and advice for government, industry, critical infrastructure owners and operators, as well as the Canadian public. The Cyber Centre is complemented by the Royal Canadian Mounted Police's (RCMP) National Cybercrime Coordination Unit (NC3). The NC3 is a new initiative and, as such, implementation activities are underway. Once established, the unit will coordinate Canadian law enforcement cybercrime operations and collaborate with international partners; provide digital investigative advice and guidance to Canadian police; produce actionable cybercrime intelligence; and establish a new national public reporting mechanism for Canadians and businesses to report cybercrime and fraud incidents to law enforcement.

Innovation, Science and Economic Development Canada (ISED) also has a pivotal role in supporting the safe and secure introduction of CAVs to Canada's roads. ISED is responsible for setting and enforcing compliance with technical standards and licensing requirements related to wireless technologies integrated in vehicles and roadside infrastructure. The Department is also responsible for addressing related data, intellectual property, and privacy considerations, as well as investing in and fostering innovation and skills in the Canadian automotive, transportation digital technology and cyber security sectors. With respect to privacy, ISED oversees federal private sector privacy laws. The Minister of ISED administers the *Personal Information Protection and Electronic Documents Act* (PIPEDA) and ensures that the Act both protects consumers and supports economic growth and innovation. The Office of the Privacy Commission (OPC) for Canada, an Agent of Parliament, is responsible for enforcing PIPEDA.

All levels of government and industry have a responsibility to advance a coordinated national approach to cyber security in the transportation sector. Provincial and territorial governments oversee many of the laws and regulations governing the use of vehicles on public roads. Municipalities are responsible, to varying degrees, for managing passenger transportation, and together these levels of government share responsibility for enforcing traffic laws, and for adapting physical and digital infrastructure to support the testing and deployment of CAVs.

Public sector leadership is necessary to foster global alignment on the development of international standards, cyber security best practices, and evidence-based regulations. Governments develop the appropriate legislative and regulatory frameworks that establish basic safety and security expectations, and foster continued technological advancement.

[6] Public Safety Canada. National Cyber Security Strategy. 2018. https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/ntnl-cbr-scrt-strtg/index-en.aspx (Accessed June 4, 2019).

CANADA'S STATUTORY FRAMEWORK

In Canada, motor vehicle transportation is a shared responsibility between federal, provincial and territorial governments. Under the *Motor Vehicle Safety Act* (MVSA), TC establishes safety regulations that apply to the importation of motor vehicles and prescribed motor vehicle equipment, and the shipment of newly manufactured motor vehicles and designated equipment across provincial/territorial boundaries. The objective of these regulations is to reduce the risk of death, injury, and damage to property and the environment.

Under the MVSA, prescribed classes of vehicles imported and sold in Canada are required to comply with Canada's *Motor Vehicle Safety Regulations* and its associated *Canadian Motor Vehicle Safety Standards* (CMVSS), which sets out an extensive range of safety requirements that apply to vehicles, including those with CAV technologies. Companies must certify that all new vehicles and equipment manufactured, shipped inter-provincially or imported into Canada comply with the applicable safety standards set out in the CMVSS. Canada's motor vehicle safety regime can use its investigative, as well as its compliance and enforcement authorities in instances where a defect in the vehicle's cyber-physical systems could lead to safety issues. For instance, when a safety defect in a vehicle is suspected, including any safety defect caused by CAV technology, TC investigates and, if a defect is found, orders the manufacturer to take corrective action.[7]

[7] For more details on Canada's motor vehicle safety regime please refer to Canada's Safety Framework for Automated and Connected Vehicles https://www.tc.gc.ca/en/services/road/documents/tc_safety_framework_for_acv-s.pdf.

INTERNATIONAL VEHICLE CYBER SECURITY GUIDANCE AND STANDARDS

Cyber Guidance builds on existing vehicle cyber security best practices published by governments, industry associations, and standards-setting bodies. This guidance is informed by the Automotive Information Sharing and Analysis Centre's (Auto-ISAC)[8] best practice guidelines for securing the vehicle ecosystem, as well as vehicle cyber security best practices published by trusted international regulators.[9] This guidance document also relies on the U.S. National Institute of Standards and Technology's Cybersecurity Framework (NIST CSF).[10] The NIST CSF is a voluntary framework designed for owners and operators of critical infrastructure and is structured around five pillars: identify, protect, detect, respond, and recover. The framework is supported by a large body of detailed guidance and standards on cyber security best practices for effective planning and operation of critical information and cyber physical systems.

Canada is exercising global leadership on standards development for CAV technologies and is active on a number of working groups under the United Nations (U.N.) World Forum for Harmonization of Vehicle Regulations' Working Party on Automated/Autonomous and Connected Vehicles (WP.29/GRVA). Notably, TC co-chairs the Validation Methods for Automated Driving (VMAD) under the GRVA, with a mandate to establish international safety testing requirements for automated vehicles, and is active on a number of other GRVA sub-groups.[11]

TC is closely monitoring ongoing international efforts to develop global cyber security standards for vehicles, including draft regulations developed by the Task Force on Cyber Security / Over-the-Air (OTA) Updates under the GRVA,[12] and the forthcoming ISO/SAE 21434 standard on "Road vehicles- Cybersecurity engineering," which will define common terminology and set out criteria for cyber security engineering practices throughout the vehicle lifecycle.

[8] Auto-ISAC was established in 2015, operates as a central hub for sharing, tracking and analyzing intelligence about cyber threats, vulnerabilities and incidents related to the connected vehicle. Auto-ISAC has global representation and represents 99 percent of all light-duty vehicles on the road in North America.

[9] NHTSA released "Cybersecurity Best Practices for Modern Vehicles" the U.K.'s "The Key Principles of Vehicle Cyber Security for Connected and Automated Vehicles," the European Automobile Manufacturers Association's "Principles of Automobile Cyber Security", and Auto-ISACs Best Practices Guides, among others. In the absence of well-developed legislative and regulatory frameworks, international counterparts and industry experts have issued guidance and key principles that address cyber security of vehicles and road transportation infrastructure. For example, the SAE's "Cybersecurity Guidebook for Cyber-Physical Vehicle Systems" (SAE J3061) published in 2016, provides high-level guidance on vehicle cyber security for a complete vehicle lifecycle and lays the foundation for further standards development activities. And, in 2019, the Task Force on Cyber Security and OTA Updates, under the U.N.'s World Forum for Harmonization of Vehicle Regulations, concluded the test phase for draft regulations on cyber security and software updates. Technical guidance material produced by multilateral working groups, and by internationally recognized experts, is an important resource for stakeholders as they update their own vehicle policy framework. TC also encourages stakeholders to follow ongoing standards development work, the International Organization for Standardization (ISO) and the Society of Automotive Engineers (SAE) International established a working group to develop a new standard for vehicle cyber security that better addresses the needs and risks of the automotive sector. The proposed standard, ISO/SAE 21434, reflects cyber security engineering practices and will enable automakers to show due diligence by ensuring vehicles are reasonably secure for their lifecycle, and demonstrate that they have adopted a risk-based approach to cyber security. Furthermore, the standard ISO 26262 addresses the functional safety of electronic and electrical systems of vehicles, including the possible malfunction of these systems. Given the connected nature of safety and security, this standard can also be broadly applied to vehicle cyber security.

[10] National Institute of Standards and Technology's Cyber Security Framework V.1., April 2018. https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf.

[11] TC is also active on the Functional Requirements for Automated Vehicles (FRAV), Automatically Commanded Steering Functions (ACSF), and the Automatic Emergency Braking System (AEBS) working groups under the GRVA.

[12] TC is also following the work of the Informal Working Group on Data Storage System for Automated Vehicle / Event Data Recorder (DSSAD/EDR), which was established under the GRVA in July 2019.

VEHICLE CYBER SECURITY GUIDANCE: KEY PRINCIPLES

The Cyber Guidance uses a risk-based approach allowing any size organization, at varying levels of cyber maturity, to apply the principles in a manner that is consistent with their risk management strategy. A risk-based approach acknowledges that eliminating cyber security risk entirely is unrealistic, and instead focuses on the identification, prioritization, and management of risk to inform effective risk-reduction measures. Risk management activities underscore each of the principles and should be applied throughout the vehicle lifecycle: concept and design; production, operation, and maintenance; transfer of ownership, and end-of-life activities. A risk-based approach should also be followed in the broader vehicle ecosystem, including the supply chain, the aftermarket vehicle sector, and in the supporting infrastructure.

The following principles are intended to be accessible to a non-technical audience and offer strategic cyber security guidance for the vehicle sector and interested stakeholders. They should not be construed as a technical standard or considered an exhaustive solution for vehicle cyber security. TC encourages stakeholders to consider Cyber Guidance in conjunction with best practices, guidance and standards developed by PS, CSE, and other federal government departments with cyber expertise, trusted international regulators, industry associations, relevant cyber security resources for other sectors, and standards setting bodies (See Annex 2: Vehicle Cyber Security Best Practices - Reference Material).

1. Organizations should identify and manage cyber security risks

1.1 Cyber security governance

1.2 Risk management frameworks

1.3 Supply chain security

2. Organizations should protect the vehicle ecosystem

2.1 Layered cyber defences

2.2 Privacy protection

2.3 Information protection procedures

2.4 Training and awareness programs

3. Organizations should detect, monitor and respond to cyber security events

3.1 Event detection, monitoring and analysis

3.2 Security audits

3.3 Vulnerability management plan

3.4 Incident management and response

4. Organizations should recover from cyber security events safely and quickly

4.1 Incident recovery

4.2 Partnership building and information sharing

4.3 Cyber security as a process of continuous improvement

1. ORGANIZATIONS SHOULD IDENTIFY AND MANAGE CYBER SECURITY RISKS

1.1 CYBER SECURITY GOVERNANCE

Cyber security must be prioritized and implemented alongside system safety. It should be championed at the senior executive-level and consistently communicated to all personnel. Organizations should encourage open communication on product and organizational cyber security risk management across teams and between working-level and leadership.

Organizations should develop formal governance frameworks to clearly identify roles and responsibilities for managing and addressing cyber security risk throughout the vehicle/product lifecycle and within the organization. Accountability at every level of the organization, including senior executives, will reinforce cyber security as a corporate priority and help ensure that the necessary financial, organizational, and human resources are available to support effective cyber security risk management, including risk avoidance and risk mitigation activities.

A strong governance framework will promote a robust and resilient organizational cyber security culture. Cyber security governance frameworks should be regularly reviewed, assessed, and strengthened according to a predetermined schedule.

1.2 RISK MANAGEMENT FRAMEWORKS

Organizations should implement a layered, risk-based approach to cyber security. Risk management frameworks, and underlying methodologies, should be tailored to each organization's specific needs and security objectives. Risk management is the continual process of identifying, assessing, and responding to risk. An organizational risk management strategy should be formally documented with objectives, roles, and responsibilities clearly identified and, at a minimum, should address cyber security risks to safety critical systems and personally identifiable information (PII).

Original equipment manufacturers (OEMs), equipment suppliers, and service providers should integrate risk management processes into the system development lifecycle. Appropriate testing should be performed at regular milestones, according to a predetermined schedule. (See *Principle 3 Organizations should detect, monitor, and respond to cyber security events*).

OEMs and suppliers should conduct regular cyber security threat and risk assessments throughout the product lifecycle to systematically identify, assess and prioritize risks, including risks potentially introduced by the supply chain (see *Principle 1.3 Supply chain security*). Threats should be identified, assessed as to their severity, and prioritized for remediation.

Risk management strategies should include sound asset management practices. Vehicle and equipment components should be inventoried and kept current including applicable software, firmware, hardware, network configurations, and interfaces, as well as the type of data collected. Data assets should be documented, and data owners advised of their responsibilities and rights, with respect to that data. Identified assets, including data, should be assessed as to their value and criticality, so that appropriate, risk-based security controls can be implemented.

1.3 SUPPLY CHAIN SECURITY

Security is only as strong as its weakest link. Integrated supply chain risk management is critical to the safe functioning of modern vehicles. Responsibility for securing the vehicle ecosystem's supply chain extends beyond OEMs and must include all levels of suppliers, sub-contractors, and third party vendors. Threat and risk assessments should consider the entire supply chain of operations, including the aftermarket vehicle sector.

In all procurement arrangements – whether from manufacturer to supplier, or supplier to supplier – the contracting organization's security requirements and expectations should be formally detailed in a contractual arrangement. This is also an important consideration in the context of passenger (e.g. rentals) and commercial (e.g. trucking industry) fleets.

Suppliers should be able to provide assurances that they have a cyber security policy or program in place; and, whenever possible, independent validation of suppliers' security products and processes should be required. The contractual arrangements should also stipulate that audits and regular reporting will be performed according to a predetermined schedule.

Systems integrators should consider establishing roots of trust to authenticate every component of the system, and should validate the authenticity and origin of supplies. All organizations must work together to enhance the security of the vehicle ecosystem, including establishing responsible data management policies. To support a culture of cyber security and information sharing, OEMs and suppliers should consider implementing vulnerability disclosure programs and actively engaging in cyber security information sharing forums (see *Principle 3.3 Vulnerability management plan* and *Principle 4.2 Partnership building and information sharing*).

2. ORGANIZATIONS SHOULD PROTECT THE VEHICLE ECOSYSTEM

2.1 LAYERED CYBER DEFENCES

Cyber Guidance does not propose specific technical solutions, but rather suggests that organizations adopt a defence-in-depth model that layers cyber security defences to avoid a single point of failure. Manufacturers and suppliers should address cyber security challenges using a risk-based, lifecycle management approach that is based on systems-engineering practices. They should implement processes and testing to assure data confidentiality, integrity, and availability throughout all stages of the vehicle lifecycle. A defence-in-depth model, in which multiple layers of security controls are implemented, will help foster security redundancy, fault tolerance, and reduce the likelihood of a cyber security breach.

At a minimum, the following security goals should be considered throughout the vehicle lifecycle:

- **Implement appropriate security controls**
  Organizations should implement appropriate security controls that will help mitigate risks and support an effective response to cyber security incidents throughout the vehicle lifecycle. At minimum, controls should consider the following core principles: isolation and segregation techniques in system architecture; design vehicles to fail securely and safely; establish trust boundaries and appropriate access controls; authenticate persons, sub-systems, services, messages, and external parties, as appropriate; record and audit event and system logs; and support device/firmware authentication throughout product lifecycle.
- **Data security**
  The confidentiality and integrity of data, both at rest and in transit, and communications should be secured using cryptographic applications that are adequate for the assessed degree of assurance in keeping with a risk-based approach. Data management policies should differ between in-vehicle versus external communications and data. The sensitivity of data stored both on and off-board the vehicle should be protected using appropriate cryptographic techniques commensurate with the assessed degree of risk. Data security should also include assured deletion of personal or sensitive information from both vehicular and backend systems during transfer of ownership, vehicle decommissioning, and in-between user sessions in ride-sharing services.
- **Secure internal communication**
  In-vehicle communications should be trustworthy and secure, such that the integrity, availability, and confidentiality of data, including in-vehicle critical safety messages are protected. The internal transfer of critical safety messages between subsystems should follow the principles of isolation and segregation in vehicle systems architecture to avoid common data buses, where possible. Communications, and data at rest, should be secured and authenticated using appropriate cryptographic techniques commensurate with the assessed degree of risk.

- **Secure external vehicle communications**
  OEMs and suppliers should adopt a policy to validate that all external communication interfaces from the vehicle/product to supporting infrastructure, such as Bluetooth, Wi-Fi, 3G/4G/5G, are secured before entering the production and deployment phases. External devices that may interface with vehicle systems should be isolated from the internal vehicle network and only granted limited access to required systems. Any debugging or testing interfaces should be access-restricted to authenticated and certified diagnostic or repair devices.
- **Identity management and access control**
  Persons, systems, and services requiring access to and potentially use of vehicle and supporting systems, services or data, should be identified, authenticated, and authorized using a pre-defined, repeatable process. The concept of least privilege should always be applied when granting access to sensitive information or technical assets, and the duration of sessions, as well as the number of authentication attempts, should be limited.
- **Secure software development**
  Secure coding practices should be followed to minimize the number of potential software vulnerabilities. Organizations should have documented processes to manage, review, and test custom and third-party integration. Software should be operated in a test environment prior to deployment, and alongside a staged rollout with roll back options implemented allowing for return to a stable, operational state in the event of unforeseen circumstances. Typically, firmware updates should not allow for rollbacks to prevent an attacker from using this mechanism to revert to a more vulnerable version. Organizations should be able to identify the version of all software and firmware on the vehicle.
- **Secure updates**
  Software, firmware, and hardware security should be managed throughout the vehicle's lifecycle. Organizations should implement a security update process that supports secure OTA, as well as on-board, updates. A firmware authentication check should be performed at device start up, as well as during updates. Mechanisms should be put in place to validate signed updates prior to installation. The process should ensure updates are performed safely and securely, and that a process is in place to inform users that an update is ready and/or scheduled for installation. Users should also be notified when an update has occurred and whether there are any changes in system functionality.
- **Secure the extended vehicle environment**
  Securing the vehicle ecosystem, includes consideration for supporting services, infrastructure, and external data. Cyber security should be implemented in the broader vehicle ecosystem, including supporting road transportation infrastructure, traffic management systems, telecommunications carriers, cloud-based service providers, and fleet management platforms. Cyber security should also be integrated into the aftermarket services and supplies sector, including maintenance and repair shops, aftermarket vehicle products, and connected devices.

2.2 PRIVACY PROTECTION

Privacy risk management should be considered in combination with cyber security at each stage of the vehicle lifecycle. The federal PIPEDA, sets out rules for collection, use, and disclosure of personal information in the course of commercial activities. PIPEDA is a principles-based, technologically-neutral law of general application that governs all sectors of the economy. In British Columbia, Alberta, and Quebec, substantially similar provincial legislation applies to private organizations in the context of activities that take place solely within those provinces. Organizations are responsible for ensuring that their information handling practices comply with applicable laws. The OPC enforces compliance with PIPEDA, while the OPC's provincial counterparts enforce the laws of the substantially similar provinces. ISED is responsible for the administration of PIPEDA, including policy development related to the Act.

In November 2018, a new mandatory data breach reporting regime came into effect under PIPEDA. Organizations are now responsible for notifying affected individuals, and the OPC, of any breach of security safeguards that, 1) results in the loss, theft, or unauthorized access of personal information,[13]and 2) creates a real risk of significant harm to the affected

[13] PIPEDA defines "personal information" as "information about an identifiable individual"; information **does not need to be confidential or secret** to be considered "personal" under the law. This very broad definition encapsulates a significant amount of data in the vehicle context.

individuals. Organizations must also keep records of all data breaches, regardless of risk, and provide such records to the OPC on request.

Stakeholders, including the OPC and its counterparts, are increasingly exploring the need for mechanisms to assist in translating the technology-neutral requirements of privacy laws such as PIPEDA into the context of specific technologies and business models. This is particularly the case for emerging technologies that present novel privacy issues, including CAVs. In response to a recommendation set out in the Senate Standing Committee on Transportation's 2018 report, *Driving Change: Technology and the Automated Vehicle*, the Government committed to working with the OPC and other stakeholders to develop an industry-specific code of best practices for privacy protection. The Government began implementing this commitment through a multi-stakeholder process over the course of 2018 and 2019, which identified key elements for success that a code of practice would need to incorporate. In addition, in 2019, ISED released a discussion paper on PIPEDA reform that contemplated the creation of a formal role for codes, standards, and certification under the Act. Future efforts with stakeholders will build upon this work to strengthen privacy protection in CAVs.

PIPEDA defines "personal information" as "information about an identifiable individual"; information does not need to be confidential or secret to be considered "personal" under the law. This very broad definition encapsulates a significant amount of data in the CAV context. The Act contains general requirements for the handling of personal data that stem from ten fair information principles:

1. **Accountability:** Organizations are responsible for personal information under their control, and remain accountable for that information should they transfer the data to a third-party processor.
2. **Purpose:** The collection, use, and disclosure of personal information must be limited to reasonable purposes, which organizations must identify to individuals at the time of collection.
3. **Consent:** Organizations must obtain individuals' consent to collect, use, and disclose personal information (subject to limited exceptions).
4. **Limiting collection:** Organizations must limit their collection of personal information to that which is necessary for the purpose identified to the individual.
5. **Limiting use, disclosure, and retention:** Organizations may not use or disclose personal information for purposes other than those it identified to the individual at the time of collection (subject to limited exceptions).
6. **Accuracy:** Personal information must be accurate, complete, and up-to-date.
7. **Safeguards:** Organizations must protect personal information with security safeguards that are proportionate to the sensitivity of the information.
8. **Openness:** Organizations shall be open and transparent about their information management policies and practices.
9. **Individual access:** Organizations must inform individuals of the existence, use, and disclosure of their personal information on request.
10. **Challenging compliance:** Individuals shall be able to challenge compliance with these requirements directly with the organization.

2.3 INFORMATION PROTECTION PROCEDURES

Security policies should be in place to protect information systems and assets. Data, source code, virtual machines, configuration files, credentials, and other critical digital assets should be regularly and securely backed-up. Data back-ups, including back-up restoration and procedures, should be periodically tested and verified to assure the confidentiality, integrity, and availability of data, as well as the resiliency of backups, in the event of a security incident.

The physical operating environment and personnel management practices should also be addressed in information protections processes. Procedures and plans supporting information protection should be documented, including:

- an Incident Management Plan;
- a Vulnerability Management Plan;
- a Disaster Recovery Plan; and
- a Business Continuity Plan.

2.4 TRAINING AND AWARENESS PROGRAMS

An effective cyber security defense requires a knowledgeable workforce. Product cyber security is more effective if the originating organization is itself protected. Organizations should develop a corporate security awareness and training program for employees. Cyber security training should be mandatory for all employees, including executives and senior management. The cyber-safe culture should be championed at the highest executive-level.

In addition to corporate cyber security programs, organizations should also develop dedicated training programs for product developers and engineers. Programs should include information on possible product vulnerabilities, mitigations strategies, current cyber-security standards and best practices, as well as exercise incident response, remediation, and recovery activities during a cyber security event.

Manufacturers should develop, market, and deliver education and awareness material to promote cyber literacy of users, owners, and operators. From a safety and security perspective, it is important that users are aware of a vehicle or product's functionality and the type of data being collected during ownership, operation, and maintenance of the vehicle, including data implications during transfer of ownership or decommissioning of a vehicle.

3. ORGANIZATIONS SHOULD DETECT, MONITOR AND RESPOND TO CYBER SECURITY EVENTS

3.1 EVENT DETECTION, MONITORING AND ANALYSIS

Organizations should implement the capability to detect, monitor, and analyze threats to the vehicle systems, sub-systems, and supporting infrastructure. Organizations should conduct threat detection, monitoring, and analysis with appropriately skilled and trained technical staff. Threat intelligence should be shared internally, and with appropriate external stakeholders to maximize its impact.

In general, the rapid detection of security incidents is related to an organization's ability to identify and analyse anomalous activity in both product (in-vehicle and backend systems) and corporate environments. Organizations should establish baseline activity levels and behaviours of vehicle systems, networks, software, data flows, and other processes. Vehicle systems, networks and interfaces with external systems and services should be monitored to identify unauthorized users, connections, and other anomalous activity. System and application logs should be regularly reviewed to identify anomalous events or suspect patterns of activity. Organizations should also consider establishing a Security Operations Center, to centralize information and activities related to potential cyber security incidents.

3.2 SECURITY AUDITS

Vehicle cyber security best practices, and the implementation of appropriate security controls, should be assured and verifiable through regular, objective, independent assessments, and periodic audits. Organizations should regularly review, document, and test their cyber security processes to ensure they remain effective in a constantly changing threat environment. Self-reviews should be supplemented by penetration testing of systems, networks, and applications to identify vulnerabilities that could potentially be exploited. Independent security audits should be performed regularly. Documentation should be meticulous, version controlled, and maintained for the duration of the vehicle lifecycle.

3.3 VULNERABILITY MANAGEMENT PLAN

Manufacturers should develop vulnerability management plans to identify, analyze, and manage vulnerabilities in their operating environment. Plans should include steps on how an organization will triage and remediate identified security vulnerabilities. Organizations should also actively monitor open resources for security alerts and advisories.

Vulnerability disclosure programs are an effective means of sharing potential vulnerabilities in the motor vehicle ecosystem. It provides a mechanism for organizations, including suppliers and manufacturers, to receive vulnerability reports from cyber security researchers. The vendor should maintain a responsible disclosure program that allows for vulnerabilities discovered in the system (device, mobile app, or backend) by researchers, and other external entities to be reported, tracked, and mitigated. Vulnerability programs should include sufficient legal provisions to protect researchers.

3.4 INCIDENT MANAGEMENT AND RESPONSE

Organizations should maintain an incident management plan (IMP) and conduct regular exercises to prepare for and respond to cyber security incidents. The IMP should clearly define: processes, roles and responsibilities, and resources to investigate and respond to an incident; processes to identify, triage, and escalate an incident; mechanisms for coordinating the technical and business activities to contain, remediate and recover from an incident; and processes to close out response activities.[14]

When an incident is detected and verified, the IMP should be executed. Notifications from security event detection systems should be assessed, prioritized, and investigated. Incidents, exploits, and vulnerabilities should be reported to the appropriate internal and external stakeholders. Cyber incidents may be reported to the Cyber Centre via its Contact Centre (contact@cyber.gc.ca). In addition, stakeholders are encouraged to share intelligence with the Auto-ISAC, with whom incident information may be shared for the benefit of the community. Organizations should report incidents to their local law enforcement agency or the RCMP if a cyber incident is suspected to be criminal in nature. Organizations should also report to the Canadian Anti-Fraud Centre (CAFC) at 1-888-495-8501 or www.antifraudcentre.ca if the cyber incident involves fraudulent activity.

Any cyber security incident affecting a vehicle should be contained to limit its impact. This could include temporarily blocking external network interfaces or services, limiting systems capabilities, or safely shutting down vehicle systems. Once an incident is contained to limit its severity, timely and appropriate actions should be taken to remediate the incident, such as bringing the vehicle in for maintenance or deploying an OTA update. After an incident has been remediated, organizations should have a process to restore system functionality and normal business operations (see *Principle 4.1 Incident Recovery*).

4. ORGANIZATIONS SHOULD RECOVER FROM CYBER SECURITY EVENTS SAFELY AND QUICKLY

4.1 INCIDENT RECOVERY

After an incident, it is expected that a post-incident analysis will be completed in order to identify associated vulnerabilities, establish remedies, and to document lessons learned. Careful system diagnostics should be conducted to identify any altered data, modified or inserted code, and any malicious applications that may have been installed. If necessary, back-ups should be used to restore systems, data and services to their pre-incident state and the appropriate authorities should be notified. Where criminal action is suspected, forensic procedures should be invoked to collect evidence. In the event of broader impacts and outages which may impact business processes or operations, the organization's Business Continuity Plan or, if appropriate, the Disaster Recovery Plan should be invoked and followed.

Restoration and recovery activities, timelines, status updates, and outcomes should be communicated to executive and management teams. Affected parties should be advised and appropriate communications issued to partners, suppliers, end-users, public authorities, and in some cases the media, to provide valid information on the event and its remediation.

[14] Auto-ISAC. Incident Response: Best Practice Guide Version 1.2. 18. https://www.automotiveisac.com/best-practices/download-best-practice-guides/. (Accessed June 6, 2019).

4.2 PARTNERSHIP BUILDING AND INFORMATION SHARING

The cyber threat environment is complex. An effective cyber security defence requires collaboration between multiple stakeholders including OEMs, suppliers at each tier of the supply chain, aftermarket product and service providers, the security community, government bodies, and industry associations. Organizations are encouraged to share automotive threat intelligence with peers, intelligence bodies, consumers, and government.

Organizations are encouraged to work closely with the Government of Canada including TC, the Cyber Centre, ISED, RCMP, other federal departments; and provincial, territorial, and municipal governments. Partnership building and information sharing within the private sector is also strongly encouraged through organizations such as Auto-ISAC, which facilitates information sharing between OEMs and industry suppliers on cyber security issues.

4.3 CYBER SECURITY AS A PROCESS OF CONTINUOUS IMPROVEMENT

Cyber security is not an end state, but a process of continuous improvement. Organizations should maintain a database to log threats, incidents, and lessons learned in order to prepare for and prevent a similar incident from re-occurring. Organizations should continuously improve and adapt their cyber security mechanisms and processes to meet the changing threat landscape. Through rigorous evaluations, security reviews, and testing of cyber security processes and controls, organizations should continuously strive to strengthen their cyber resilience.

CONSIDERATIONS AND OPPORTUNITIES FOR CANADA

Vehicle cyber security is a global challenge that requires international collaboration. Working with partners, Canada is well positioned to be a leader in developing safe and secure vehicle technologies. Canada has a well-established automotive manufacturing sector and leading capabilities in information and communications technology, artificial intelligence, and cyber security. Moving forward, all stakeholders will need to continue to invest in attracting cyber security talent and fostering innovation in the vehicle sector.

Although cyber security is in many respects borderless, the legislative and regulatory landscape in Canada is unique, and jurisdictions will need to work together to build a cohesive national approach. Motor vehicle safety is a shared responsibility between the federal government, provinces and territories, and municipalities, with each jurisdiction having a critical role to play in promoting vehicle cyber security. Canada's unique privacy legislation, which includes PIPEDA, the *Privacy Act*, and provincial/municipal privacy laws will also present some distinctly Canadian considerations for stakeholders as they design and develop CAV technologies (see *Principle 2.2 Privacy protection*). ISED's collaboration with the OPC, including TC and other key stakeholders, is an important step towards the development of an industry-specific code of best practices for privacy protection in the CAV ecosystem.

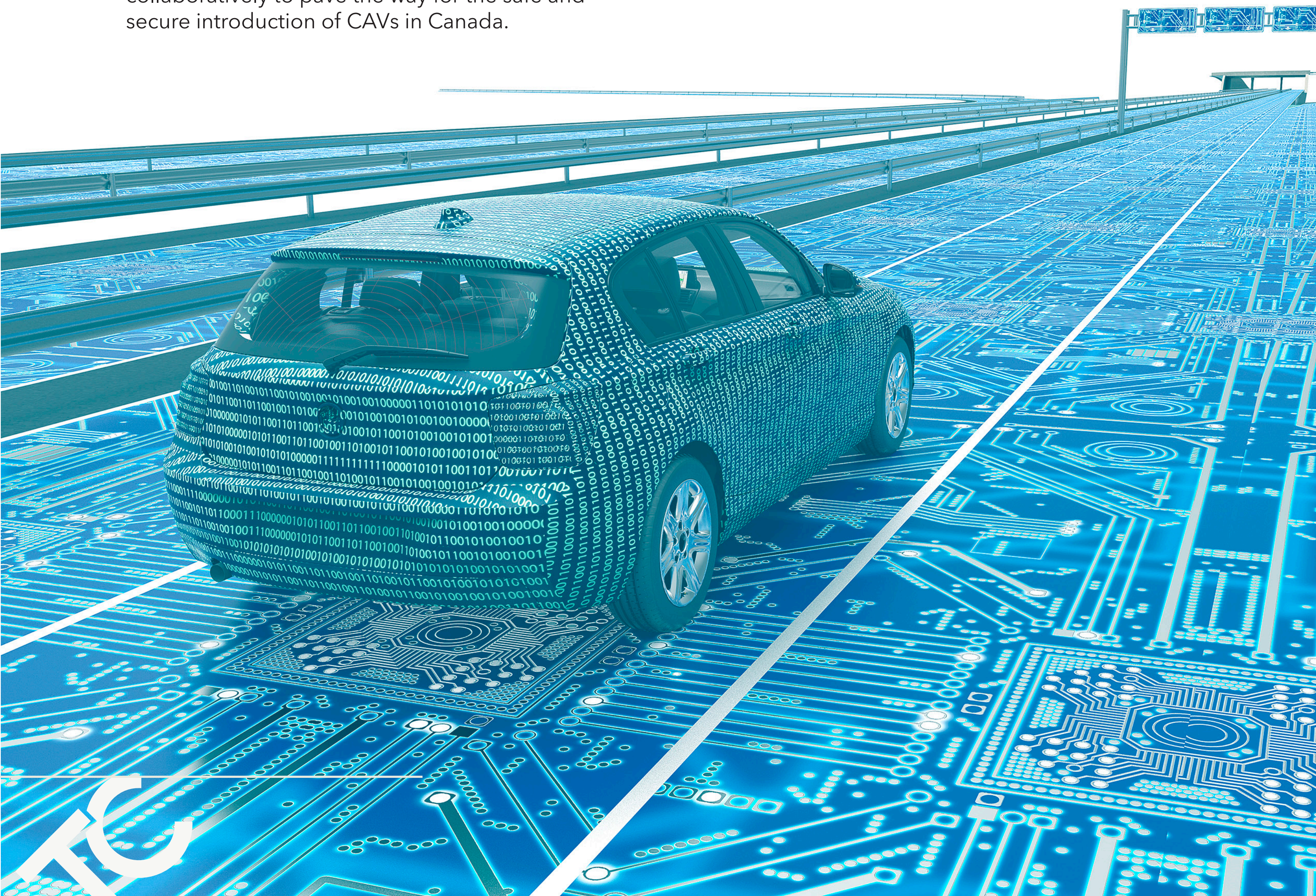
While there has been significant progress, the vehicle cyber security environment remains complex and there are opportunities to address existing and emerging challenges. For instance, vehicle cyber security will likely have implications for the insurance industry that will warrant closer inspection in close consultation with stakeholders. There are also opportunities to work with stakeholders to better understand and mitigate cyber security risks in specific areas of the vehicle ecosystem such as: road transportation infrastructure; the aftermarket sector, including maintenance and repair shops, and telematics service providers; and artificial intelligence in highly automated driving systems, to name a few.

TC is actively working to address emerging challenges. In the context of road safety, TC works with a broad range of stakeholders across all levels of government, industry, and academia to support cyber security research and testing. Funding programs, such as TC's Enhanced Road Safety Transfer Payment Program, and the Program to Advance Connectivity and Automation in Transportation Systems (ACATS), can be leveraged to support Canadian research, testing and trials on CAVs, including cyber security related projects. In support of enhancing security and privacy in connected vehicle communications, TC is advancing a framework for a nationally coordinated Security Credential Management System; which in turn will promote safer vehicle communications and foster interoperability across North America. Canada has also assigned and aligned spectrum across borders, enabling early cross-border tests and pilots, with recent investments in 5G test beds opening the door to innovation.

TC is committed to continue working with trusted international partners to support the development of harmonized vehicle cyber security frameworks and standards. In parallel, Canada will continue to align efforts with the U.S. to identify joint initiatives for advancing cross-border collaboration on CAV cyber security. Given the integrated nature of the North American automotive marketplace and transportation networks, including cross-border traffic and trade, these efforts will promote interoperability of CAV technologies across borders. TC will continue to contribute to the development of international standards for CAV safety and security and demonstrate global leadership in this rapidly evolving sector.

CONCLUSION

Canada's Vehicle Cyber Security Guidance is an important step toward advancing the state of vehicle cyber security in Canada, and sets out a strong foundation for future collaborative opportunities. TC is steadfast in its commitment to continue working with stakeholders to monitor trends and advancements in vehicle security, and to build upon the existing suite of guidance and tools to support forward-looking vehicle cyber security priorities. This includes ongoing work with international partners, including the U.S., to support alignment of vehicle cyber security activities, where appropriate. Taken together, these efforts will foster a strengthened vehicle cyber security posture as we work collaboratively to pave the way for the safe and secure introduction of CAVs in Canada.



ANNEX 1: GLOSSARY[15]

Alterers: Companies that alter vehicles between the time they are certified as complete or final manufacture has been completed and certified, and the first retail sale per Motor Vehicle Safety Regulations (MVSR), Section 9: "Altered Vehicle".

Artificial Intelligence: A subfield of computer science that develops intelligent computer programs to behave in a way that would be considered intelligent if observed in a human (e.g. solve problems, learn from experience, understand language, and interpret visual scenes).

Attack: An attempt to gain unauthorized access to business or personal information, computer systems or networks for (normally) criminal purposes. A successful attack may result in a security breach or it may be generically classified as an "incident."

Attack surface: The set of ways in which an adversary can enter a system and potentially cause damage.

Automated Vehicle: Uses a combination of sensors, controllers and onboard computers, along with sophisticated software. It allows the vehicle to control at least some driving functions, instead of a human driver (for example, steering, braking and acceleration, and checking and monitoring the driving environment).

Availability: The property of being accessible and usable upon demand.

Bluetooth: A wireless protocol that allows two Bluetooth enabled devices to communicate with each other within a short distance (e.g., 30 ft.).

Confidentiality: A property that information is not disclosed to users, processes, or devices unless they have been authorized to access the information.

Connected Vehicle: Connected vehicles communicate with their surroundings using a number of wireless technologies such as dedicated short-range communication (DRSC), cellular, Wi-Fi, Bluetooth or satellite. Depending on the features it has installed, a connected vehicle may be able to communicate with: its occupants, such as through their mobile devices; with other vehicles and road users (Vehicle-to-Vehicle – V2V); with the surrounding transportation infrastructure, such as roadways and traffic lights (Vehicle-to-Infrastructure – V2I; Internet based applications and other entities (Vehicle-to-Everything – V2X).

Controller Area Network Bus (CANbus): The dominant serial communication network protocol used for intra-vehicle communication.

[15] All definitions used in this glossary were accessed in December 2019 and referenced the following sources: Transport Canada, Innovation Science and Economic Development Canada, the Canadian Center for Cyber Security Glossary https://cyber.gc.ca/en/glossary, as well as its page on cyber threat and cyber threat actors https://cyber.gc.ca/en/guidance/cyber-threat-and-cyber-threat-actors; Public Safety Canada's Funda¬mentals of Cyber security for Canada's CI Community https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/2016-fndmntls-cybr-scrty-cmmnty/index-en.aspx#a16; the National Initiative For Cybersecurity Careers And Studies Glossary of Common Cybersecurity Terminology https://niccs.us-cert.gov/about-niccs/glossary; the National Institute of Standards and Technology Glossary https://csrc.nist.gov/glossary/term/cyber_physical-system; the Senate of Canada Driving Change Technology and the future of the automated vehicle Report https://sencanada.ca/content/sen/committee/421/TRCM/Reports/COM_RPT_TRCM_AutomatedVehicles_e.pdf; Sunpower Electronics Ltd's page on Original Equipment Manufacturers https://www.sunpower-uk.com/glossary/what-is-an-original-equipment-manufacturer-oem/; Intel's Autonomous Driving Glossary https://newsroom.intel.com/wp-content/uploads/sites/11/2017/05/Autono¬mous-Driving-Glossary.pdf; NHTSA's Best Practices for Modern Vehicles https://www.nhtsa.gov/sites/nhtsa.dot.gov/files/documents/sae2017chatipoglu_0.pdf; National Institute of Standards and Technology Glossary https://csrc.nist.gov/glossary/term/cyber_physical-system; UNECE's Draft Recommendation on Cyber Security of the Task Force on Cyber Security and Over-the-air issues of UNECE WP.29 GRVA https://www.unece.org/fileadmin/DAM/trans/doc/2018/ wp29grva/GRVA-01-17.pdf.

Cyber physical systems: A system that includes engineered, interacting networks of physical and computational components.

Cyber resilience: The ability to adapt to changing conditions and prepare for, withstand, and rapidly recover from disruption.

Dedicated Short Range Communications (DSRC): DSRC systems consist of short-range, wireless links to transfer data between vehicles and roadside units, other vehicles, and portable units.

Defence-in-depth: An IT security concept (also known as the Castle Approach) in which multiple layers of security are used to protect the integrity of information. These layers can include antivirus and antispyware software, firewalls, hierarchical passwords, intrusion detection, and biometric identification.

Electronic Control Unit (ECU): An embedded unit in the vehicle that controls one or more electrical systems, such as the engine control unit or the human-machine interface.

Firmware: Computer programs and data stored in hardware such that the programs and data cannot be dynamically written or modified during execution of the programs.

Information Technology: Any equipment or interconnected system or subsystem of equipment that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information by the executive agency.

Integrity: The ability to protect information from being modified or deleted unintentionally or when it's not supposed to be. Integrity helps determine that information is what it claims to be. Integrity also applies to business processes, software application logic, hardware, and personnel.

In-vehicle infotainment (IVI): A collection of hardware and software that provide entertainment in the vehicle; for example, navigation systems, radio, video players, and Wi-Fi.

Least privilege: The principle of giving an individual only the set of privileges that are essential to performing authorized tasks. This principle limits the damage that can result from the accidental, incorrect, or unauthorized use of an information system.

LIDAR (or light detection and ranging): A pulsed laser that measures variable distances. In AVs, the LIDAR bounces these lasers off of objects in its surroundings (such as pedestrians and other vehicles) to map them in 3D so that the AV knows where it is positioned relative to those objects.

Operational Technology: Hardware and software that detects or causes a change through the direct monitoring and/or control of physical devices, processes and events in the enterprise.

Original Equipment Manufacturer (OEM): OEM refers to a product that is acquired by the company to be reused or incorporated into another product using the reseller's brand name.

Over-the-air updates: Any method of making data transfers wirelessly instead of using a cable or other local connection.

Remote exploitation: Exploitation of a victim machine (sic. Vehicle or vehicle system) by sending specially crafted commands from a remote network to a service running on that machine to manipulate it for the purpose of gaining access or information.

Risk: Exposure to a negative outcome if a threat is realized.

Security controls: A safeguard or countermeasure prescribed for a system or an organization designed to protect the confidentiality, integrity, and availability of its information and to meet a set of defined security requirements.

Telematics: The integration of telecommunications and informatics for intelligent applications in vehicles, such as fleet management.

Threat: A circumstance or event that has or indicates the potential to exploit vulnerabilities and to adversely impact (create adverse consequences for) organizational operations, organizational assets (including information and information systems), individuals, other organizations, or society.

Threat actor: A threat actor is a state, group, or individual who, with malicious intent, aim to take advantage of vulnerabilities, low cyber security awareness, and technological developments to gain unauthorized access to information systems in order to access or otherwise affect victims' data, devices, systems, and networks.

Threat and risk assessment: A process of identifying system assets and how these assets can be compromised, assessing the level of risk that threats pose to assets, and recommending security measures to mitigate threats.

Vulnerability: A flaw or weakness in the design or implementation of an information system or its environment that could be exploited to adversely affect an organization's assets or operations.

WiFi: A generic term that refers to a wireless local area network that observes the IEEE 802.11 protocol.

ANNEX 2: VEHICLE CYBER SECURITY BEST PRACTICES - REFERENCE MATERIAL

- Automotive Information Sharing and Analysis Centre (Auto-ISAC) Automotive Cybersecurity Best Practices – Key Cybersecurity Functions (2019)
- Chennakeshu, Sandeep. Blackberry. Cybersecurity for Automobiles: BlackBerry's 7-Pillar Recommendation (December 2017)
- European Automobile Manufacturers Association's (ACEA) Principles of Automobile Cyber Security (2017)
- European Union Agency for Cybersecurity (ENISA) Good Practices for Security of Smart Cars (November 2019)
- ISO 27001; Information technology - Security techniques - Information security management systems
- ISO 27035 – Information security incident management
- ISO/SAE 21434 – Road 993vehicles – Cybersecurity engineering (forthcoming)
- ISO/IEC 29147: 2018 - Information technology -- Security techniques -- Vulnerability disclosure: https://www.iso.org/standard/72311.html
- ISO/IEC 30111: 2019 - Information technology-Security techniques—Vulnerability handling processes: https://www.iso.org/standard/69725.html
- National Motor Freight Traffic Association RFP templates: Appendix II Cyber Security Requirements: https://github.com/nmfta-repo/nmfta-rfp_templates
- NIST Special Publication 800-53; Security and Privacy Controls for Federal Information Systems and Organizations
- National Institute of Standards and Technology's Framework for Improving Critical Infrastructure Cybersecurity V1.1. (April 16, 2018).
- PAS 1885:2018 – The fundamental principles of automotive cyber security. Specification
- PAS 11281:2018 – Connected automotive ecosystems. Impact of security on safety. Code of practice
- SAE J3061 – Cybersecurity Guidebook for Cyber-Physical Systems (January 2016)
- SAE J3101 – Requirements for Hardware Protected Security for Ground Vehicle Applications (Under development)
- SAE J3138 – Diagnostic Link Connector Security (June 2018)
- Transport Canada Testing Highly Automated Vehicles in Canada: Guidelines for Trial Organisations (June 2018)
- Transport Canada Canada's Safety Framework for Automated and Connected Vehicles (February 2019)
- Transport Canada Safety Assessment for Automated Driving Systems in Canada (February 2019)
- UNECE GRVA Task Force on Cyber Security and OTA Updates "Proposal for Recommendation on Cyber Security": https://www.unece.org/fileadmin/DAM/trans/doc/2019/wp29grva/ECE-TRANS-WP29-GRVA-2019-02e.pdf
- United Kingdom's Department for Transport (DfT) and the Centre for the Protection of National Infrastructure (CPNI) The Key Principles of Vehicle Cyber Security for Connected and Automated Vehicles (October 2016)
- U.S. National Highway Traffic Safety Administration (NHTSA) Cybersecurity Best Practices for Modern Vehicles (2016)