TRANSPORT CANADA'S VEHICLE CYBER SECURITY STRATEGY

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 15473E

PDF

Cat. No. T46-62/2021E-PDF

ISBN 978-0-660-38864-9

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

I'm pleased to introduce Transport Canada's Vehicle Cyber Security Strategy, which identifies overarching priorities with a view to strengthen the cyber security resilience of vehicles and the supporting road transportation infrastructure in Canada. These priorities align with Transport Canada's continued commitment to demonstrate leadership, and work collaboratively with partners, to promote a secure and resilient vehicle cyber security ecosystem in support of the safety of our national transportation system.

From coast to coast to coast, Canada's road transportation system is in a period of profound technological change. Connected and automated vehicles hold enormous potential for our country; they can dramatically improve road safety, offer new forms of mobility, spur economic growth, and reduce our collective impact on the environment. At the same time, it's important that we continue to monitor potential cyber security risks as a result of increased interconnectivity and automation in vehicles and their surroundings.

Transport Canada has been presented with a defining challenge: harness the potential of new vehicle technologies, which represent the next generation of road transportation, while ensuring that safety remains the top priority. This strategy is a foundational policy document that supports Transport Canada's commitment to maintain road safety and security, in close partnership with stakeholders - from industry, manufacturers, academia, public sector, standards setting bodies, and of course Canadians. This strategy will play a critical role in helping us to understand the complex vehicle cyber security threat landscape, and to define our role in the digital ecosystem.

I'm also pleased to note that the strategy helps fulfil Transport Canada's commitment under *Transportation 2030: A Strategic Plan for the Future of Transportation in Canada* to support the use of connected and automated vehicles on public roads to improve road safety and increase mobility. Our commitment to address current and emerging cyber security challenges in the road transportation sector also supports the department's *Transformation Strategy*.

Finally, I would like to extend my thanks to the many stakeholders – including all levels of government, industry, and academia - who have provided their feedback and support for the strategy. It is essential for organizations to work together to manage and mitigate cyber security risks in this rapidly evolving sector, and it is encouraging to see the collective progress we've made so far. I look forward to our continued collaboration, as we work together to deliver on the shared priorities that will help ensure the safety and security of Canada's transportation system into the future.

The Honourable Omar Alghabra, P.C., M.P.
Minister of Transport

Executive Summary

Vehicle technologies and the supporting infrastructure are evolving rapidly and have the potential to improve road safety, introduce new forms of mobility, and create economic opportunities. This digital transformation, combined with a constantly changing cyber security threat environment, also introduces new challenges that underscore the importance of building cyber resilience into Canada's transportation networks. Connected and automated vehicles (CAVs) and the infrastructure that supports them can be vulnerable to cyber security threats, meaning that road safety is increasingly dependent on the resiliency of interconnected and complex cyber-physical systems within systems.

Transport Canada's (TC) Vehicle Cyber Security Strategy (Cyber Strategy) sets out forward-looking vehicle cyber security goals and priorities with a view to strengthening road transportation cyber resilience in Canada. The strategy will help the department achieve its vision of continuing to be a leader in ensuring a secure and resilient automotive cyber security ecosystem.

In support of this vision, the strategy sets out 3 overarching cyber security goals for road transportation which, taken together, constitute a robust and forward looking approach to strengthen vehicle cyber security in Canada.

- **Goal 1: Incorporate vehicle cyber security considerations into policy and regulatory frameworks**
  TC will continue to provide technology-neutral policies and guidance related to vehicle cyber security, and ensure that policy and regulatory frameworks remain agile, to support ongoing industry and government developments.
- **Goal 2: Promote awareness and foster a modernized, innovative approach to vehicle cyber security**
  TC will continue to strengthen engagement with government and industry partners; explore opportunities to support consumer understanding and awareness of vehicle cyber security, and CAVs in general; and will continue advancing research and testing initiatives.
- **Goal 3: Address emerging and adjacent issues in the vehicle cyber security landscape**
  The complex and interconnected nature of automotive cyber security requires collaboration and cooperation among a broad range of stakeholders, and TC will continue to explore opportunities to address cyber security risk in the broader ecosystem of road transportation technology.

Cyber security is a responsibility shared by all levels of government, the private sector, and individual Canadians. TC will continue to build upon ongoing work with national and international stakeholders to lead a coordinated, forward-looking, and safety-focused approach to vehicle cyber security. The goals and priorities set out in this document provide a strategic roadmap identifying key areas in which to further develop policy guidance and tools, and undertake research and testing. At the same time, the Cyber Strategy builds upon the Government of Canada's broader suite of tools to support the use of secure vehicle technologies and smart roadway infrastructure, including *Canada's Vehicle Cyber Security Guidance*, and *Public Safety's National Cyber Strategy*. Taken together, these efforts will help inform the next steps on vehicle cyber security in Canada, and will complement the department's broader approach to ensure the safe introduction of CAVs.

Introduction

Road transportation technology is becoming increasingly sophisticated with the advent of connected and automated vehicles (CAVs)[1] and intelligent transportation infrastructure (ITS). These technologies are transforming the Canadian transportation system, and have the potential to improve road safety, along with potential economic and environmental benefits. At the same time, it's essential that the government and stakeholders keep pace with the complex and evolving cyber security landscape to mitigate potential threats and vulnerabilities, and realize the full potential of emerging vehicle technologies.

Transport Canada's (TC) Vehicle Cyber Security Strategy (Cyber Strategy) outlines goals and priorities to inform TC's leadership and ongoing commitment to support government, industry, and academic efforts to enhance the vehicle cyber security environment. The Cyber Strategy aligns with TC's broader approach to support the safe and secure introduction of CAVs, and it also complements the Government of Canada's overarching approach to cyber security.

Vision for the Strategy

New vehicle technologies hold the potential to enhance road safety. At the same time it is important that the appropriate processes and safeguards are in place to mitigate threats to their integrity. Recognizing that vehicle cyber security is a shared responsibility, and that security is inextricably linked with safety and privacy, a collaborative approach is essential to advance Canada's cyber security posture. As such, TC is committed to continue working with stakeholders including all levels of government, manufacturers, industry, and academia, to set out a coordinated approach to vehicle cyber security. To this end, the Cyber Strategy has been developed to meet the current and medium-term needs of the vehicle cyber security landscape, and ultimately set out a strategic direction to carry out the department's vision.

Vision: TC will continue to demonstrate leadership, and work collaboratively with partners, to promote a secure and resilient vehicle cyber security ecosystem in support of the safety of our national transportation system.

To accomplish this vision, the department has identified three overarching vehicle cyber security goals, which complement TC's overall approach to CAV safety and security:

- Incorporate vehicle cyber security considerations into policy and regulatory frameworks
- Promote awareness and foster a modernized, innovative approach to vehicle cyber security
- Address emerging and adjacent issues in the vehicle cyber security landscape

[1] Connected vehicles use different types of wireless technology to communicate with their surroundings. Although the technology can differ between vehicles, most new vehicles sold today have some version of connectivity. An automated vehicle uses a combination of sensors, controllers, onboard computers and software to help the vehicle control at least some driving functions instead of a human driver. Many of today's vehicles already have driver assistance technologies that use lower levels of automation ranging from level 0 to 2 according to the *Taxonomy and Definitions for Terms Related to On-Road Motor Vehicle Automated Driving Systems (J3016_202104)*, published by the international standards organization SAE International. This includes features like automatic emergency braking, lane keeping assistance and adaptive cruise control.

Scope of the Strategy

The Cyber Strategy applies to the entire vehicle lifecycle – from design and production, to deployment, repair and maintenance, and into the aftermarket sector. While it is primarily focused on light duty vehicles equipped with connected and automated features, there is also applicability for other vehicle types, such as government fleets, heavy duty trucks, and electric vehicles, among others.

Recognizing the inherent interconnectivity of vehicle cyber physical systems, the strategy reflects a holistic view of cyber security that extends beyond the physical boundaries of the vehicle. To this end, the strategy includes high-level considerations for the supporting physical and digital infrastructure that informs and facilitates the safe operations of vehicles, including those equipped with CAV technologies.

Roles and Responsibilities

In Canada, all levels of government, the private sector, and individual Canadians share responsibility for motor vehicle safety and cyber security. Increasingly complex and interconnected vehicle technologies underscore the necessity for national, multi-disciplinary stakeholders to continue collaborative efforts to address vehicle cyber security, and support the safe introduction of CAVs, which represent the next generation of road transportation.

Federal, Provincial/Territorial and Municipal Governments

Federal, provincial/territorial and municipal levels of government share responsibility for motor vehicle safety and security in Canada. Provincial and territorial governments oversee many of the laws and regulations governing the use of vehicles on public roads. These responsibilities include driver licensing; vehicle registration; motor vehicle insurance and liability; vehicle maintenance standards; and enacting traffic laws. Municipalities are responsible, to varying degrees, for managing passenger transportation, including public transit and taxis; parking; traffic control; and enacting and enforcing by-laws. Municipalities and provincial/territorial governments share responsibility for enforcing traffic laws, and for adapting infrastructure to support the deployment of connected and automated vehicles. Some responsibilities, such as those for public education and awareness are shared across all three levels of government. TC works closely with provinces and territories to ensure a coordinated national approach to road safety and security.

The Minister of Transport is responsible for the administration and enforcement of the *Motor Vehicle Safety Act* (MVSA). Under the 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. Manufacturers of vehicles or equipment are responsible for certifying that they comply with applicable standards and regulations and the Department conducts post-market surveillance, such as compliance inspections, testing and audits, to ensure compliance with federal requirements. Furthermore, manufacturers are required to notify TC when a defect is suspected in the design or construction of a vehicle or equipment that may endanger the safety of persons, or cause damage to property or the environment, including safety defects caused by the vehicle's cyber-physical system.

Building on the strengths of Canada's robust motor vehicle safety regime, the Department supports the testing and deployment of CAVs through the development of guidance and tools that set out clear safety and security expectations for manufacturers to follow. These efforts are informed by research and testing, as well as continued collaboration and information sharing with Canadian and international partners.

Recognizing that a number of federal departments have shared commitments to advance cyber security in Canada, TC works with federal government program partners to promote a cohesive and consistent approach to cyber security in Canada. In support of a robust vehicle cyber security program, TC regularly engages with the following federal departments, to share information, identify areas of collaboration, and leverage expertise.

> **Public Safety Canada (PS)** provides national leadership on cyber security policy through *Canada's National Cyber Security Strategy* and associated *Action Plan*, working with a range of stakeholders to advance cyber security domestically and internationally. The National Cyber Security Strategy is centered around three foundational pillars: security and resilience; cyber innovation; and leadership and collaboration, which taken together, guide the Government of Canada in helping to protect citizens and businesses from cyber threats.

> **The Communications Security Establishment (CSE)** is the national lead for cyber security operations, which is coordinated through the Canadian Centre for Cyber Security (CCCS, the Cyber Centre). The CCCS provides operational cyber security information and advice for government, industry, critical infrastructure owners and operators, and the Canadian public.

> **The Royal Canadian Mounted Police (RCMP)** coordinates Canadian law enforcement cybercrime operations and collaborates with international cybercrime enforcement partners, which is facilitated through the National Cybercrime Coordination Unit (NC3) and its Canadian Anti-Fraud Center (CAFC).

> **The Department of National Defence (DND)** develops military related innovative technology. Defence Research and Development Canada (DRDC) and its Centre for Security Science (CSS) provide military organizations with tools and technology to handle cyber threats.

> **The National Research Council Canada's (NRC)** Automotive and Surface Transportation Research Centre operates facilities in Ontario and Quebec where all levels of the automotive and manufacturing supply chain can collaborate with NRC specialists and national researchers on shared transportation issues.

> **Innovation, Science and Economic Development Canada (ISED)** sets and enforces technical standards and licensing requirements for wireless technologies integrated in vehicles and roadside infrastructure. ISED also administers the *Personal Information Protection and Electronic Documents Act* (PIPEDA), which sets the rules for the collection, use, and disclosure of personal information in the course of commercial activities (including with respect to security safeguarding) and is enforced by the Office of the Privacy Commissioner.

Stakeholders

TC works with a broad range of stakeholders, including manufacturers, industry and academia, to support cyber security research, testing, and the development of vehicle cyber security guidance and tools. As these stakeholders are responsible for the design and production of the electronic systems that underpin a vehicle’s hardware and software components, they are well positioned to support the assessment and mitigation of cyber security risk. Notably, TC meets regularly with automotive industry associations, as well as other stakeholder groups, to share information and best practices, and stay abreast of current developments with respect to vehicle safety and security. This engagement is essential to maintain the dialogue on key issues related to vehicle cyber security, which in turn will help set out a coordinated approach that prioritizes safety, security, and privacy.

Continued dialogue with academia is also an important element to establishing a coordinated approach to cyber security in Canada. Colleges and universities contribute to the development of technological research and innovation, and academic findings can generate unique insight into processes established to identify and address cyber security challenges. At the same time, academia also plays a critical role in talent recruitment and skills development, which is essential to meet the cyber security demands of an increasingly digital sector.

In addition, TC is actively working with the international community to develop global guidance and standards for the safety and security of vehicle technologies. Notably, this includes participation in international working groups within the United Nations (UN) Global Forum for Road Traffic Safety (Working Party 1), the UN World Forum for the Harmonization of Vehicle Regulations (Working Party 29), and other standard setting organizations such as SAE International and the International Standards Organization. The risks that accompany new road transportation technologies do not recognize national borders, and will necessitate a coordinated and collaborative international approach. Given the integrated nature of the North American market, and the importance of cross-border movement of people and goods, TC engages regularly with the United States Department of Transportation, including the National Highway Traffic Safety Administration, to set out a cohesive and coordinated cross-border approach. Ultimately, sustained engagement with international partners provides an opportunity to share information and best practices, align regulatory requirements as appropriate, and contribute to international consensus building for vehicle cyber security.

Importance of Vehicle Cyber Security

Emerging technological advancements are transforming the road transportation sector, and have the potential to enhance the safety of Canadian roadways. At the same time, rapid technological development, including connected and automated features, can increase the vehicle’s “attack surface”. A cyber security breach in the road transportation sector could lead to potential safety and operational consequences, such as the compromise of vehicle safety, personal information, and vehicle theft, among others. Given the complexity and ongoing technological developments in road transportation, it is essential for stakeholders to keep pace with the evolving nature of the vehicle cyber landscape to effectively manage and mitigate cyber security risks and associated vulnerabilities.

Potential Cyber Threats and Impacts

Consistent with the cyber security landscape across critical infrastructure sectors, there is a diverse array of cyber threat actors[2] in the transportation ecosystem, ranging from an individual, to a

[2] Cyber threat actors are states, groups, or individuals who, with malicious intent, aim to take advantage of vulnerabilities, low cyber security awareness, or technological developments to gain unauthorized access to information systems in order to access or otherwise affect victims’ data, devices, systems, and networks. The

sophisticated adversary operating as part of a larger entity. The scale of an attack will vary according to the individual or group's technical capabilities, motivation and resources, and whether they have direct or remote access to their target.

The complexity of the transportation ecosystem is accentuated by the transformation of vehicles into cyber-physical systems that are not only equipped with internal electronic systems but are now also connected to external devices and network communication interfaces. While this combination can provide for enhanced automation, safety and convenience features, this also increases access points for potential cyber-attacks. Robust cyber security measures can mitigate the risk of vehicle component manipulation through access points, such as:

- physical network interfaces which allow external sources to connect to the vehicle networks, including CD/DVD media, infotainment systems, On-Board Diagnostic (OBD) ports and Universal Serial Bus (USB) ports
- wireless interfaces and connectivity features which allow the vehicle to send and receive data through an array of wireless interfaces that provide short range and/or long range connectivity, such as dedicated short range communications (DSRC), cellular, Bluetooth, Wi-Fi, and radio frequency which can support diverse features like remote tire pressure monitoring systems (TPMS) and remote "smart key" keyless entry and keyless ignition systems
- interfaces with the telematics system, which integrate telecommunications and informatics for intelligent applications in vehicles, and stores personal information

It's crucial that all stakeholders – from government, to industry, manufacturers, and service providers - understand the vehicle threat landscape and prioritize robust cyber security concepts and best practices (like risk management, protecting the entire vehicle ecosystem, vulnerability management, incident monitoring and response, and continuous improvement) to effectively maintain the overall safety, security and privacy of the road transportation ecosystem.[3]

Goals and Priorities for Vehicle Cyber Security

TC and the broader stakeholder community have already set out a strong foundation for vehicle cyber security. The department will continue to build on this work by focusing on the following goals and corresponding priorities over the coming years, while pursuing ongoing collaboration with stakeholders. Taken together, these efforts will help inform the next steps in support of vehicle cyber security resilience.

globalized nature of the Internet allows these threat actors to be physically located anywhere in the world and still affect the security of information systems in Canada. Canadian Centre for Cyber Security. *Threat and Threat Actors*. https://www.cyber.gc.ca/sites/default/files/publications/itsg33-ann2-eng.pdf. Accessed 8 April 2021.

[3] For additional information on cyber security concepts and best practices refer to *Transport Canada's Vehicle Cyber Security Guidance, Transport Canada's Vehicle Cyber Security Assessment Framework and Tool*, and other international standards such as *SAE/ISO Draft International Standard 21434: Road vehicles cybersecurity engineering*.

Goal 1

Incorporate vehicle cyber security considerations into policy and regulatory frameworks

CAVs and the supporting infrastructure technologies are developing rapidly. As such, in March 2018, the *Motor Vehicle Safety Act* was amended to strengthen the Minister of Transport's enforcement and compliance authorities in the area of road safety and afford greater flexibility to keep pace with emerging technologies in the automotive industry. To complement these key legislative amendments, TC will continue to provide technology-neutral policies and guidance related to vehicle cyber security, and ensure that policy and regulatory frameworks remain agile, to support ongoing industry and government developments.

- Priority 1.1: Non-regulatory Guidance, Tools and Policies
- Priority 1.2: Modernizing Policy and Regulatory Frameworks
- Priority 1.3: Alignment with International Standards and Requirements

Priority 1.1: Non-regulatory Guidance, Tools and Policies

To support industry efforts and inform the way forward on CAVs, TC has focused on the development of non-regulatory guidance and tools. Of note, TC published *Canada's Vehicle Cyber Security Guidance* in May 2020, which provides a set of technology-neutral guiding principles to support industry in strengthening vehicle cyber resilience. The guidance offers best practices on managing cyber security risks and protecting the entire vehicle ecosystem with safeguards, as well as how to detect, monitor, respond to, and recover from vehicle cyber security events.

Building on the release of this guidance, TC is continuing to explore new opportunities to undertake research and develop policies and other tools to support cyber security throughout the vehicle supply chain. For example, TC has developed a *Vehicle Cyber Security Assessment Framework and Tool* that will provide a method for manufacturers and suppliers to assess and better understand their cyber security posture. In addition, TC has contracted the development of tools, guidance, and training to help road authorities (e.g. infrastructure owner/operators) improve cyber security of road transportation infrastructure systems (e.g. Traffic Management Systems).

Priority 1.2: Modernizing Policy and Regulatory Frameworks

The *Motor Vehicle Safety Act* is the basis for an agile and responsive regulatory environment for road safety that promotes CAV innovation and fosters greater flexibility. In addition to developing complementary guidance and tools to accompany the regulatory framework, the Department will continue to review existing regulatory and policy frameworks to ensure they remain flexible and agile to keep pace with new technologies. This flexibility will ensure TC is prepared for new developments that may emerge in vehicle cyber security, their evaluation and adoption by industry, and their integration into government policies, requirements, and regulatory frameworks.

In 2019, the Government of Canada published the *Transportation Sector Regulatory Review Roadmap*, which sets out TC's plan to address regulatory barriers to innovation and investment in the transportation sector, including CAVs. Building on this work, TC published the *Regulatory Roadmap on International Standards*, which identifies opportunities for Canada to take an enhanced leadership role in the development of international standards, including for CAVs and other emerging vehicle technologies. Moving forward, TC will continue to actively participate in the Government-wide Regulatory Review process, including identifying opportunities to incorporate considerations for vehicle cyber security.

TC will also continue working with other lead federal departments to advance complementary vehicle cyber security initiatives. For example, as part of Canada's national approach to cyber security, the Department will continue to monitor PS led initiatives, such as the *National Cyber Security Strategy* and corresponding *Action Plan*, to identify opportunities to incorporate vehicle cyber security. In addition, TC will continue to work with PS on the Critical Cyber Systems initiative[4], to ensure vital cyber systems within the road transportation sector remain safe and reliable and are protected from cyber security threats and vulnerabilities.

Priority 1.3: Alignment with International Standards and Requirements

TC is actively engaged in broader international efforts to support the development of global safety

[4] To strengthen and protect the cyber security of Canada's critical infrastructure, the Government intends to propose new legislation and make necessary amendments to existing federal legislation in order to introduce a new critical cyber systems framework. For more information, please see: Canada. *Investing* in the *Middle Class Budget 2019*. https://www.budget.gc.ca/2019/docs/plan/budget-2019-en.pdf. Accessed 12 April 2021.

standards for new vehicle features with proven safety benefits. As part of this work, TC participates in meetings, and monitors the work of the international Task Force on Cyber Security and Over-the-Air updates, which was established under the United Nations Economic Commission for Europe's (UNECE) World Forum for the Harmonization of Vehicle Regulations (WP.29) Working Party on Automated/autonomous and Connected Vehicles.

In January 2021, new cyber security regulations developed by the task force on cyber security and over-the-air updates came into force. The UN regulation on cyber security is intended to provide a framework for countries with a vehicle-type approval regulatory system[5] to ensure that cyber security risks are identified and managed in vehicle design, as well as monitored and assessed regularly. Currently, the task force is developing guidance on technical requirements for contracting parties to the 1998 agreement, to which Canada is a signatory. The guidance will provide advice on cyber security and software update processes for the vehicle, including governance and lifecycle aspects.

At the same time, TC follows the efforts of other standard-setting organizations working to develop requirements for vehicle cyber security. For instance, the International Standards Organization and SAE International (ISO/SAE) have developed a *Draft International Standard 21434: Road vehicles cybersecurity engineering*. The standard can serve as a baseline for vehicle manufacturers and suppliers to ensure that cyber security risks are managed efficiently and effectively, and is closely related to ISO *5112 Road vehicles - Guidelines for auditing cybersecurity engineering*[6].

Moving forward, TC will continue to track the outcomes of the Task Force on Cyber Security and Over-the-Air updates, as well as the development of the ISO/SAE 21434 standard, and will consider the proposed guidance in the context of ongoing work to strengthen Canada's vehicle cyber security posture. In addition, TC will continue to engage with counterparts in the United States. Given our common self-certification regulatory regime, which is unique in the international community, it's important that Canada and the U.S. work together to bring forward a shared perspective and ensure alignment in our approaches, to the extent possible.

[5] It's important to note that the regulation was developed in the context of a type-approval system, which differs from the Canadian self-certification framework, under which manufacturers must follow the robust safety standards set out in the regulations

[6] ISO/PAS 5112 Road vehicles — Guidelines for auditing cybersecurity engineering" is a vehicle cyber security auditing guideline currently under development. For more information please see: https://www.iso.org/standard/80840.html. Accessed 12 April 2021.

Goal 2

Promote awareness and foster a modernized, innovative approach to vehicle cyber security

TC works closely with national road transportation stakeholders to collaborate on initiatives, share information and updates, and work towards common goals. To complement this work, the Department will strengthen engagement with government and industry partners; explore opportunities to support consumer understanding and awareness of vehicle cyber security, and CAVs in general; and continue advancing research and testing initiatives.

- Priority 2.1: Active Participation in Federal/Provincial/Territorial and Industry Fora
- Priority 2.2: Research, Testing and Validation
- Priority 2.3: Public awareness and education on vehicle cyber security
- Priority 2.4: Planning and Preparedness

Priority 2.1: Active Participation in Federal/Provincial/Territorial and Industry Fora

Unprecedented collaboration across the cyber security sector, the automotive industry, and governments is necessary to adequately address and govern the shared responsibilities and challenges associated with automotive cyber security.

TC works closely with other federal departments through a number of interdepartmental working groups, and with provincial and territorial governments through the Canadian Council of Motor Transport Administrators (CCMTA). The CCMTA coordinates all matters dealing with the administration, regulation and control of motor vehicle transportation and highway safety, with membership comprised of representatives from all provincial and territorial governments, and the federal government, where TC plays a key leadership role. Moreover, TC actively participates in the CCMTA working group on CAVs, and has leveraged this forum to contribute to and consult on multiple policy initiatives, including vehicle cyber security.

In addition, TC engages regularly with industry partners, which provides an opportunity to share information, stay abreast of emerging issues and consult on vehicle cyber security initiatives. For example, TC participates in industry information-sharing fora, such as the Automotive Information Sharing and Analysis Center (Auto-ISAC) whose members include light- and heavy-duty vehicle original equipment manufacturers (OEMs), suppliers and commercial vehicle companies. Auto-ISAC supports a robust risk-based global approach to road transportation cyber security and shares cyber security intelligence, including vulnerabilities and threat feeds to facilitate the prevention, mitigation and response to cyber incidents. TC also participates in a regular program of meetings with auto industry associations and other stakeholder groups in Canada to consult on vehicle safety and security developments, including issues related to vehicle cyber security.

TC will continue to forge strong partnerships with all levels of government and national industry stakeholders, including OEMs, suppliers, academics, and cyber security experts, to develop and share information on emerging vulnerabilities, risk analyses, and cyber mitigation and remediation strategies.

Priority 2.2: Research, Testing and Validation

Across Canada, all levels of government, the private sector, and academia, are leveraging Canada's unique geography, variable weather conditions, and diverse road surfaces to undertake research on emerging vehicle technologies, including the rigorous testing and validation required to fully understand the capabilities and vulnerabilities of these technologies prior to their integration into the road transportation system. Given the connected and interdependent nature of emerging vehicle technologies, cyber security is a fundamental issue that must be addressed.

Within the federal government, TC and other departments conduct their own testing activities to identify safety and security risks, and best practices. For instance, TC's Motor Vehicle Test Centre (MVTC) in Blainville, Quebec, is a world-class facility for testing vehicles and equipment. With a focus on mandate-related safety testing and evaluation, the MVTC is examining and evaluating CAV technologies, such as advanced driver assistance systems (ADAS), connected vehicle applications, and cooperative truck platooning systems, in support of future standards and regulatory development.

The Department will also monitor the work of the National Research Council Canada's Automotive and Surface Transportation Centre, which engages in research and testing related to advanced vehicle technologies (e.g., examining cyber security vulnerabilities in connected features, mapping and connectivity for automated driving). Going forward, TC will continue to explore opportunities to collaborate with program partners to advance research and testing efforts.

In addition, TC has established funding programs to support the safe integration of CAVs, including projects to advance vehicle cyber security. For example, TC has launched the Enhanced Road Safety Transfer Payment Program (ERSTPP), which invests in projects that promote road safety, including the innovative design, testing, and integration of CAVs and other safety enhancing technologies. These programming activities allow Canada to be better prepared for the wider use of CAVs on our roads and for the development of supporting digital infrastructure. TC has also launched the Program to Advance Connectivity and Automation in the Transportation Systems (ACATS) to help Canadian jurisdictions prepare for the array of technical, regulatory and policy issues that will emerge as a result of the introduction of CAVs, including infrastructure readiness and cyber-resiliency. The program supports research and testing, and the development of codes, standards and guidance materials. ACATS also supports capacity-building and knowledge-sharing activities, including increasing the cyber security capacity and posture of Canada's transportation infrastructure owners and operators. The program has provided grant and contribution funding towards several CAV testing and evaluation projects.

As part of forward-looking efforts, TC will look for opportunities to bolster existing vehicle cyber security research and testing, and identify new approaches and areas to test and evaluate the cyber security of road transportation technologies (e.g., intrusion, prevention, and detection of incidents; software and hardware developments; product update and maintenance; supply chain, etc.), with a view to supporting the safe introduction of new and emerging technologies in Canada.

Priority 2.3: Public awareness and education on vehicle cyber security

TC-led public opinion research indicates that consumer awareness of CAV functionality is critical to its successful acceptance and safe adoption. Today's vehicle consumers report that the capabilities of ADAS features, such as lane-keeping assist and adaptive cruise control, are not universally understood. To raise awareness and provide factual information on CAVs, TC has launched a dedicated CAV web presence, which includes vehicle cyber security considerations.

TC recognizes that educating consumers on safe cyber security practices is essential to ensuring the safety and security of all road users, and the integrity of a vehicle's digital systems and functionality. This is particularly important as motor vehicles are equipped with low levels of automation, and will eventually be equipped with more highly automated features that rely on the exchange of digital information to operate, and require installing software updates as part of normal vehicle maintenance.

Building on the release of TC's *Vehicle Cyber Security Guidance*, which provides best practices for industry, the department will work on expanding its current CAV web presence to include additional information on vehicle cyber security for consumers, to maintain safety and privacy, and to prevent theft. Taking further action, TC will continue to explore new and innovative opportunities to engage the public on vehicle cyber security issues, which could include: public opinion research, targeted engagement, and demystifying the functionality of vehicle systems.

Moreover, according to market research, the Global Automotive Cyber Security Market was valued at USD 1.9 billion in 2020 and is expected to reach USD 4.0 billion by 2025[7]. This growth represents an exceptional opportunity for the Canadian economy, because there is substantial industry demand for new highly qualified personnel capable of performing the many disciplines which make up vehicle cyber security, including engineers, security analysts, auditors, and more. TC

[7] Markets and Markets. *Automotive Cybersecurity Market by Form (In-Vehicle, External Cloud Services), Security (Endpoint, Application, Wireless Network), Application (Infotainment, Powertrain, ADAS & Safety), Vehicle Type, EV Type, and Region - Global Forecast to 2025*. October 2020. "https://www.marketsandmarkets.com/Market-Reports/cyber-security-automotive-industry-market-170885898.html. Accessed 12 April 2021.

funded a study on “Developing Cyber Talent for Canadian Road Authorities,”[8] which provided insight into a comprehensive approach to address challenges regarding cyber security talent and skill development in the road transportation sector. The Department continues to monitor efforts underway across federal government departments to build the cyber security workforce of the future and address the cyber security talent gap.

Priority 2.4: Planning and Preparedness

The road transportation sector must be adequately prepared to manage vehicle cyber security incidents that affect road users and the road transportation network. In support of this work, TC will continue to expand its engagement with other lead federal departments, as well as the road transportation and cyber security communities, to ensure a coordinated approach to incident readiness and response activities.

This includes working with other lead federal departments, such as the Communications Security Establishment and its Canadian Centre for Cyber Security. The Cyber Centre leads the government’s response to cyber security events, and works hand-in-hand with the private and public sector to provide support for complex cyber issues. TC will remain engaged with the Communications Security Establishment to provide considerations for road transportation stakeholders, and will also maintain participation in the Auto-ISAC, to gain insight on real-life incidents and management best practices from industry experts.

TC will continue to participate in national and international cyber security tabletop exercises, bringing forward vehicle cyber security considerations as appropriate, and leveraging best practices and lessons learned to inform future vehicle cyber security activities.

[8] Ye, Z., Donaldson, K., Davidson, R. *Developing Cyber Talent for Canadian Road Authorities. Information and Communications Technology Council (ICTC).* 2017. *https://www.ictc-ctic.ca/wp-content/uploads/2019/05/ICTC_Cyber-Talent-Transport_May28-2019.pdf*. Accessed 12 April 2021.

Goal 3

Addressing Emerging and Adjacent Issues in the Vehicle Cyber Security Landscape

The following priorities represent the range of activities TC may explore to carry out a modernized, innovative and adaptable approach to vehicle cyber security. Each priority addresses cyber security needs for various types of road transportation technology, as well as the recommended approach necessary to meet those needs. The complex and interconnected nature of vehicle cyber security requires collaboration and cooperation among a broad range of stakeholders. The following is a non-exhaustive list of priorities that could be considered under this goal.

- Priority 3.1: Privacy protection and personal information management
- Priority 3.2: Digital Infrastructure Security
- Priority 3.3: Supply Chain Security
- Priority 3.4: Aftermarket considerations
- Priority 3.5: Special purpose vehicles and electric vehicles

Priority 3.1: Privacy protection and personal information management

Privacy protection is inextricably linked to vehicle cyber security and road safety. As motor vehicles are equipped with more interconnected systems that communicate within a vehicle, among vehicles, and with road users and road infrastructure, a significant amount of personal information is generated on vehicle performance and vehicle occupants that can be used for research and commercial purposes. As such, privacy risk management and responsible personal information management policies should be considered in conjunction with cyber security throughout a vehicle's lifecycle.

The collection and storage of personal information must comply with relevant policy laws, including the federal privacy law for the private sector, the *Personal Information Protection and Electronic Documents Act* (PIPEDA). PIPEDA sets out rules for collection, use, and disclosure of personal information in the course of commercial activities. It 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 Office of the Privacy Commissioner (OPC) enforces compliance with PIPEDA, while the OPC's provincial counterparts enforce the laws of the substantially similar provinces. Innovation, Science and Economic Development Canada (ISED) is responsible for the administration of PIPEDA, including policy development related to the Act. Notably, ISED is leading the development and implementation of the proposed *Consumer Privacy Protection Act* which, if approved, would represent Canada's approach to modernize PIPEDA, and the current federal privacy regime for governing the collection, use, and disclosure of personal information for commercial activity in Canada.

TC will continue working with ISED to provide important context relative to the road transportation sector, as appropriate. Specifically, TC will continue to examine the interconnected relationship between vehicle cyber security, privacy protection, and road safety, to support ISED and the OPC.

Priority 3.2: Digital Infrastructure Security

Connected vehicles present an opportunity to improve the safety and efficiency of road transportation by enabling communication between vehicles and smart infrastructure (e.g. traffic signals, rail crossings, traffic signs, etc.) and other road users (e.g. pedestrians, motorcyclists and cyclists). The secure communication between vehicles and connected road infrastructure is paramount to ensuring a safe and secure road transportation system.

To support provinces, territories, and municipalities in understanding and improving the cyber security posture of their road infrastructure and intelligent transportation systems, TC will be developing a suite of cyber security risk assessment tools, guidance materials, training, and technical support that are highly tailored to their business needs through the ACATS program.

TC is also helping to advance the development of a framework for a national Security Credential Management System (SCMS). The SCMS will help ensure that connected vehicle communications are secure and can be trusted by incorporating privacy-by-design principles, and enabling communication without revealing personal information about the vehicle or the driver. TC is an observing member of the SCMS Manager LLC and participates in their cross-border interoperability working group with the aim of promoting multi-jurisdictional and multi-provider interoperability across North America.

TC is also leading work to better understand positioning, navigation and timing (PNT) infrastructure requirements for next-generation transportation systems to help vehicles safely navigate Canadian roadways. Results will support a whole of government strategy for Canadian PNT/Global Navigation Satellite System (GNSS) infrastructure investment through the Positioning, Navigation and Timing Board, a multi-lateral group hosted by ISED to coordinate cross-cutting efforts on PNT related topics in a whole of government approach. This group is also examining the security of GNSS systems, particularly in the context of safety critical applications, like transportation.

Priority 3.3: Supply Chain Security

Maintaining a comprehensive cyber security posture across the vehicle lifecycle is predicated on the security measures implemented within the supply chain. The vehicle supply chain is long and complex, and further complicated by the emergence of connected and automated features in vehicles. In addition to traditional automotive equipment suppliers, the supply chain now includes new technology vendors that provide software, firmware and hardware components. 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. Given that motor vehicles can remain in use for decades, stakeholders need to ensure electronic components are cyber-secure before they are integrated into a system, and that they remain supported to respond to continuously evolving threats and vulnerabilities. TC will continue to monitor potential safety and security concerns related to the vehicle supply chain, and provide guidance and support, as appropriate.

Priority 3.4: Aftermarket considerations

Recognizing that the average vehicle remains in use for over a decade, a life-cycle approach to security must extend into the aftermarket sector. Vehicles are increasingly connected to external devices and digital infrastructure, whether for convenience features, operational requirements or fleet management systems, and they will require regular servicing and repair to operate safely. Further, over-the-air updates are likely to become increasingly standard for ensuring that software remains up to date.

Vendors, suppliers and service technicians in the aftermarket sectors (e.g. automotive device manufacturers, diagnostic and repair services, third party service providers etc.) should continually ensure that their operations and products keep pace with emerging threats and vulnerabilities in the vehicle ecosystem. Although provincial and territorial governments are responsible for regulations and enforcement strategies as they apply to maintenance, and the operation of motor vehicle equipment and installation of aftermarket equipment, TC will provide support, as appropriate, with a view to better understanding the risks and identifying possible opportunities to strengthen overall vehicle cyber security in Canada.

Priority 3.5: Special purpose vehicles and electric vehicles

The vehicle ecosystem is comprised of many vehicle types, ranging from light duty vehicles to government fleets, first responder vehicles, passenger (e.g. rentals) and commercial (e.g. heavy-duty trucks) fleets as well as electric vehicles and their associated infrastructure. Recognizing that special purpose vehicles may have distinctive safety and security components and may be used to transport different types of cargo, including dangerous goods, different vehicle types will require individual risk assessments that consider the likelihood and impact of a cyber security incident.

For example, many commercial motor vehicle operators are making use of fleet management systems which connect with a vehicle's electronic control module and can record, store and transmit data such as but not limited to vehicle status, position, speed, fuel economy, cargo identification and driver working hours. While these systems can be used to optimise fleet movements, reduce environmental impact, reduce driver fatigue and increase road safety, this connectivity could present cyber security vulnerabilities. TC is monitoring and engaging with stakeholders to assess and address emerging cyber security risks in this space, in order to support the safe and secure use of these systems.

Moving forward, TC will continue to monitor advances in the technology supporting special vehicles, including potential implications for cyber security vulnerabilities, and will work with stakeholders as appropriate to better understand mitigate emerging threats.

Conclusion

The increasing complexity and interconnectedness of vehicles and their supporting infrastructure highlight the importance of prioritizing cyber security risk management in every aspect of the vehicle ecosystem. To ensure that Canadians can remain confident in the security, safety and privacy of their vehicles, it's incumbent on all stakeholders – including government, industry, manufacturers and suppliers — to promote information sharing, research and testing, and guidance in support of vehicle cyber resilience.

The Cyber Strategy builds on Transport Canada's increasingly flexible motor vehicle safety regime and its suite of complementary guidance and tools to support the use of secure vehicle technologies by considering foundational cyber security concepts in the context of its vision, goals, and priorities. TC is committed to continue working with stakeholders to monitor trends and advancements in vehicle security, and leverage the Cyber Strategy's forward-looking roadmap as a springboard to further strengthen Canada's vehicle cyber security posture.