CENTRE D'INNOVATION CENTRE

RDIMS – 18400039

ACATS – ITS Cybersecurity for Road Authorities - March 2022

PROGRAM TO ADVANCE CONNECTIVITY AND AUTOMATION IN THE TRANSPORTATION SYSTEM (ACATS) CYBERSECURITY INITIATIVES

Chris Nowak, Research Development Officer, Transport Canada

Transport Canada Transports Canada

Canada

AGENDA

- Why is infrastructure cybersecurity important?
- Road infrastructure cybersecurity convergence
- Cybersecurity considerations
- Infrastructure cybersecurity project
  - overview
  - status
- Security Credential Management System (SCMS)

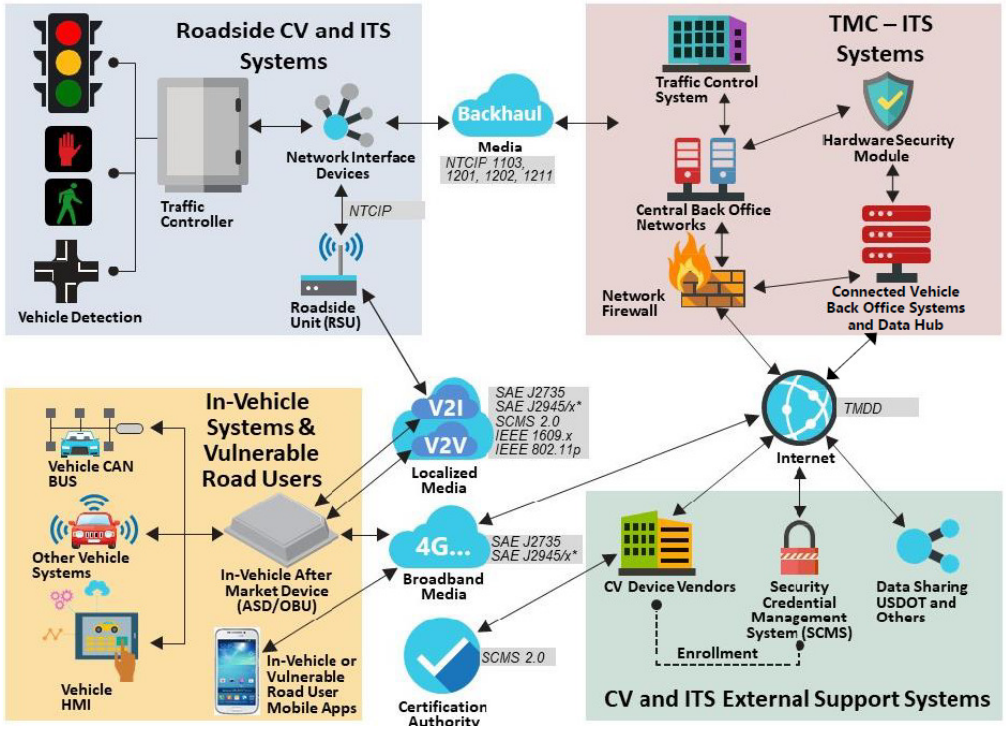
BACKGROUND - WHY IS INFRASTRUCTURE CYBERSECURITY IMPORTANT

The Traffic Management Systems (TMS) landscape of increased integration of road transportation infrastructure, vehicles, and communications is known as Intelligent Transport Systems (ITS)

Traditional TMS are comprised of multiple components, including :

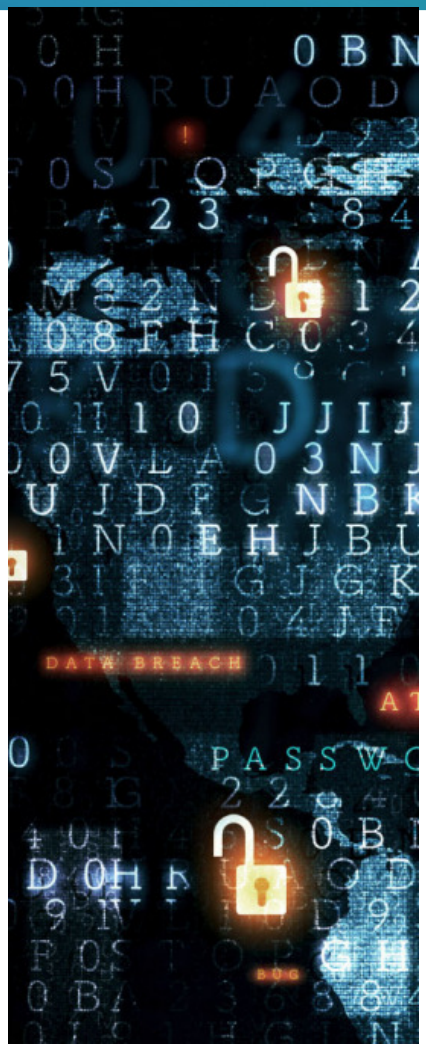
- **Signal controllers** – coordinating traffic signals
- **Traffic Sensors** – monitor traffic volumes
- **CCTV monitoring** – Traffic monitoring systems
- **Digital Signage** – displayed warnings and messages to road users

While the integration has enabled new opportunities for optimization and performance, it has also **created new opportunities for threat actors** to connect to and exploit the TMS.



CENTRE D'INNOVATION CENTRE

ROAD INFRASTRUCTURE CYBERSECURITY CONVERGENCE



- Cybersecurity of transportation infrastructure is an emerging critical system that requires active risk management
- The convergence of Information Technology (IT, e.g. ITS technologies) and Operational Technology (OT - e.g. traffic lights, message signs) is creating new attack vectors in TMS
- TMS will play in important role in enabling higher levels of vehicle automation through infrastructure-to-vehicle connectivity providing safety warnings, map data, and traffic signal timing information etc.
- The CAV ecosystem can only be as secure as the most vulnerable component
- Support road infrastructure authorities to enhance cyber resilience to *identify, protect, detect, respond and recover* from cyber threats

CYBERSECURITY CONSIDERATIONS

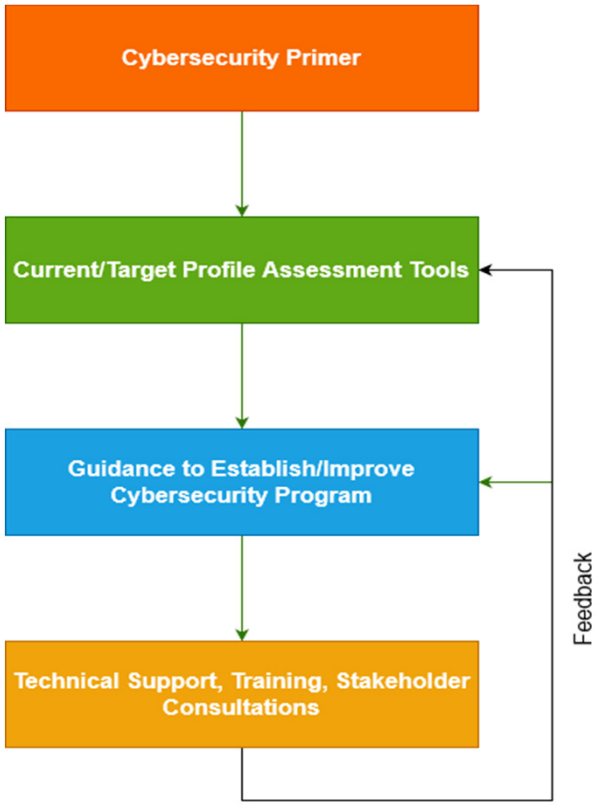
- Build cybersecurity community and capacity
  - High demand and low supply of cybersecurity experts, particularly in transportation sector
  - Collaborate with industry, academia and government

- Enhance cybersecurity state of the ITS ecosystem through:
  - Building cybersecurity capacity and raising awareness
  - Supporting the development of cybersecurity tools, frameworks and guidance

INFRASTRUCTURE CYBERSECURITY PROJECT - DELOITTE

Enhancing the Cybersecurity Readiness of Canada's Road Infrastructure Owner/Operators for Higher Levels of Connectivity and Automation

1. Develop road infrastructure **cybersecurity primer** and **briefing documents** for staff and managers in various roles (operations, finance, HR, policy etc.).
2. Develop **cybersecurity self-assessment tools** for road infrastructure authorities to evaluate their current and target cybersecurity readiness.
3. Develop **guidance on using the tools** and creating/improving a cybersecurity program tailored for TMS operations and associated infrastructure.
4. Provide **training and hands-on technical support** to road infrastructure authorities in performing cybersecurity assessments and developing cybersecurity programs.
5. Provide **cybersecurity analysis and strategic advice** on an as needed basis relating to emerging cybersecurity issues in transportation infrastructure.
6. Perform **infrastructure vulnerability analysis** on transportation sector on an as needed basis to inform the management of emerging cybersecurity risks.

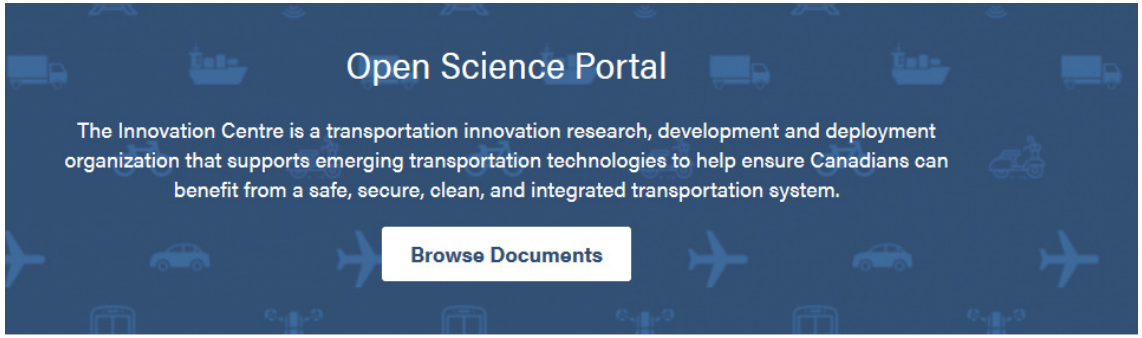


CYBERSECURITY PROJECT - STATUS

- Contract started in September 2021
- Project duration - 18 months
- Steering and Advisory Committee work ongoing
- Development of Cybersecurity Primer, Cybersecurity briefing materials and self-assessment tools in progress
- Future training sessions and webinars – chance to provide feedback and input

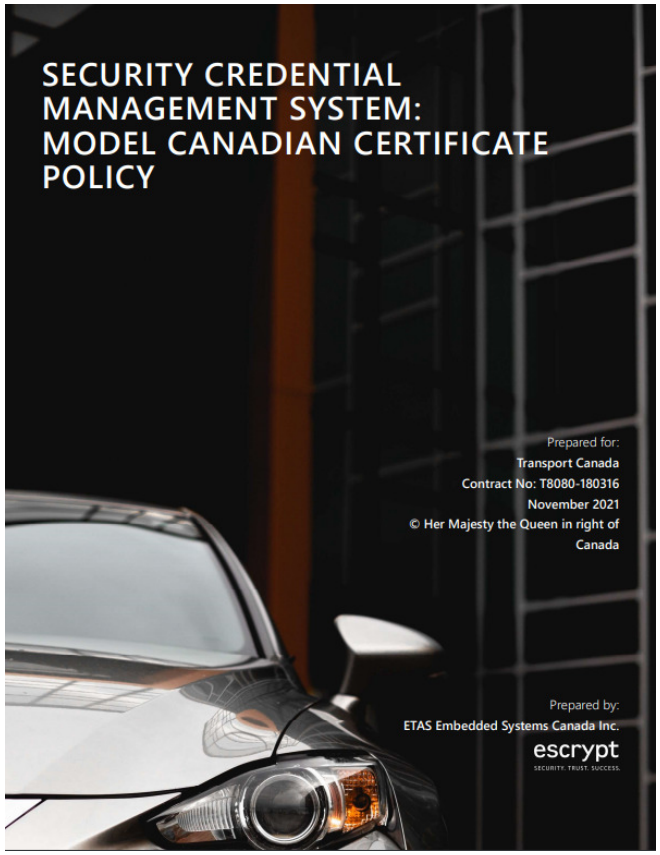
SECURITY CREDENTIAL MANAGEMENT SYSTEM (SCMS)

Security Credential Management Systems – Model Canadian Certificate Policy - (Nov 30, 2021): https://tcdocs.ingeniumcanada.org/



Security Credential Management System (SCMS) - Model Canadia...
Cybersecurity | Nov 30, 2021

- Report: SCMS CP link/



SECURITY CREDENTIAL MANAGEMENT SYSTEM (SCMS)

Document	Objective
Requirement Analysis Report Link	Review of technical literature, Canadian privacy legislation, assessment of Canadian stakeholder needs/considerations.
Option Analysis Report Link	Identify options to operate and govern a nationally coordinated SCMS, gather stakeholder feedback.
Recommended Operating and Governance Model Development Report Link	Develop recommended technical operating model (including high-level architecture) for both pilot and production SCMS operations in Canada, develop governance model.
Model Certificate Policy Report Link	In accordance with operating model, develop detailed operating procedures and policies to ensure consistency and interoperability between SCMS providers.
Spectrum Misbehaviour Analysis Report Link	Research on using SCMS architecture to detect and report spectrum misuse instances.

CENTRE D'INNOVATION CENTRE

Thank you!

For more information, please contact:

Chris Nowak, P. Eng.
Research Development Officer
Innovation Centre – ACATS
Transport Canada

Tel: (343) 571-4961
chris.nowak@tc.gc.ca