On-Road Transportation Cybersecurity

ITS Canada Technology Workshop - Calgary
May 9, 2017

Ken Moshi, Senior Analyst, ecoTECHNOLOGY for Vehicles, Transport Canada

Disclaimer

- Neither Transport Canada, nor its employees, makes any warranty, express or implied, or assumes any legal liability or responsibility for the accuracy or completeness of any information contained in this presentation, or process described herein, and assumes no responsibility for anyone's use of the information. Transport Canada is not responsible for errors or omissions in this presentation and makes no representations as to the accuracy or completeness of the information.

- Transport Canada does not endorse products or companies. Reference in this presentation to any specific commercial products, process, or service by trade name, trademark, manufacturer, or otherwise, does not constitute or imply its endorsement, recommendation, or favoring by Transport Canada.

- References and hyperlinks to external web sites do not constitute endorsement by Transport Canada of the linked web sites, or the information, products or services contained therein. Transport Canada does not exercise any editorial control over the information you may find at these locations.

Contents

- On-road transportation cybersecurity
  - Critical infrastructure
  - Cyber attacks & threats – general characteristics
  - Canadian Cyber Incident Response Centre (CCIRC)
- Connected Vehicle Security Credential Management System (SCMS)
- Open discussion

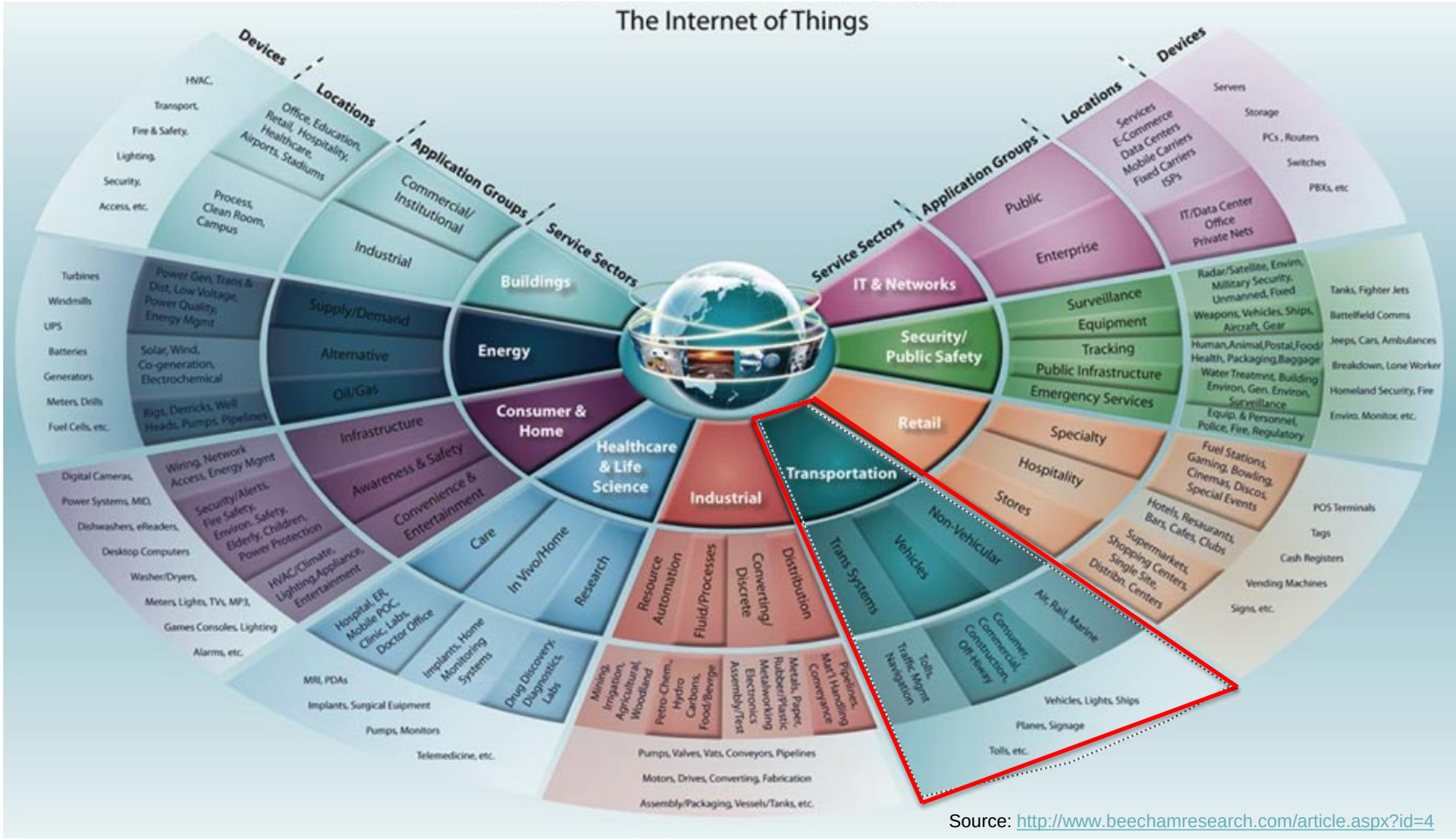
Critical Infrastructure

- Processes, systems, facilities, technologies, networks, assets and services **essential** to the health, safety, security or economic well-being of Canadians and the effective functioning of government.
- Stand-alone or interconnected and interdependent within and across provinces, territories and national borders.
- Disruptions of critical infrastructure could result in catastrophic loss of life, adverse economic effects and significant harm to public confidence.

Source: https://www.publicsafety.gc.ca/cnt/ntnl-scrt/crtcl-nfrstrctr/index-en.aspx

Transportation is 1 of 10 Critical Infrastructure Sectors

Everything talking to everything…



Source: http://www.beechamresearch.com/article.aspx?id=4

Cyber Attacks & Threats – General Characteristics

- Many cyber-attacks share these characteristics:

Low Cost; Low Risk; Effective

- The threat actors responsible for the majority of cyber based incidents in today's digital economy normally fall into the following categories:
  - **Industrial Espionage** – Seeking classified and proprietary information e.g. market and pricing strategies, client information, product designs or formulas.
  - **State-Sponsored Cyber Espionage** – Well-funded, supported by national programs, sophisticated capabilities to compromise and exploit vulnerable systems.
  - **Hacktivism/Recreational Hacking** – Attacking systems for personal gain, reputation, or political motivations.
  - **Criminals** – Persons who seek any data that can be sold or used for a profit or for other harm

Adapted from: Public Safety Canada. *Fundamentals of Cyber Security for Canada's CI Community*. 1st ed, 2016.

Transportation IS vulnerable…

Researchers find it's terrifyingly easy to hack traffic lights

Open wireless and default passwords make controlling a city's intersections trivial.

LEE HUTCHINSON - 8/20/2014, 2:39 PM

ars TECHNICA

B.C. Transit detects threat to its computer systems

ANDREW DUFFY / TIMES COLONIST
DECEMBER 10, 2015 08:46 PM

CNN Money

Cyber-Safe

Cars can be hacked by their tiny, plug-in insurance discount trackers

Car Hackers Remotely Steal Keyless BMW within Seconds

Keyless convenience could lose you your car.

AVIATION

WATCH A HACKER TAKE OVER A DRONE REMOTELY

ROBOT TOYS ARE VULNERABLE TO SKILLED ATTACKS

By Kelsey D. Atherton Posted August 18, 2015

Cultural shift needed…

"The real problem...[is] a lack of security consciousness in the field...**[The traffic controller vendor] stated that the company, 'has followed the accepted industry standard and it is that standard which does not include security.'"**

Source: http://www.eecs.umich.edu/eecs/about/articles/2014/traffic-woot14.pdf

Who is responsible for cybersecurity?
Operations? Procurement? IT?

Canadian Cyber Incident Response Centre (CCIRC)

Suite of Technical and Operational Products

BUILDING A **SAFE** AND **RESILIENT CANADA**

- Technical advisories, alerts, and flashes
- Malware analysis
- C-suite & policy

24/7

Remaining Cyber Safe While Travelling: Security Recommendations

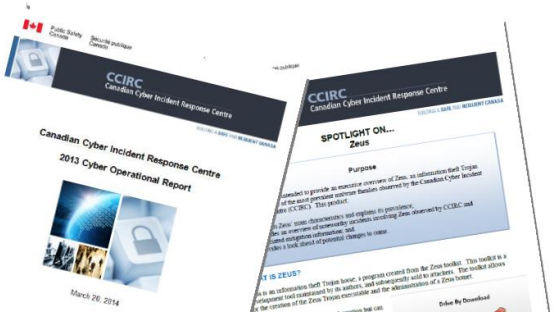
Number: IN13-002
Date: 15 February 2013

Purpose

Top 4 Strategies to Mitigate Targeted Cyber Intrusions

The Canadian Cyber Incident Response Centre (CCIRC) recommends that network administrators implement the following four mitigation strategies, which can prevent as much as 85% of targeted cyber attacks:

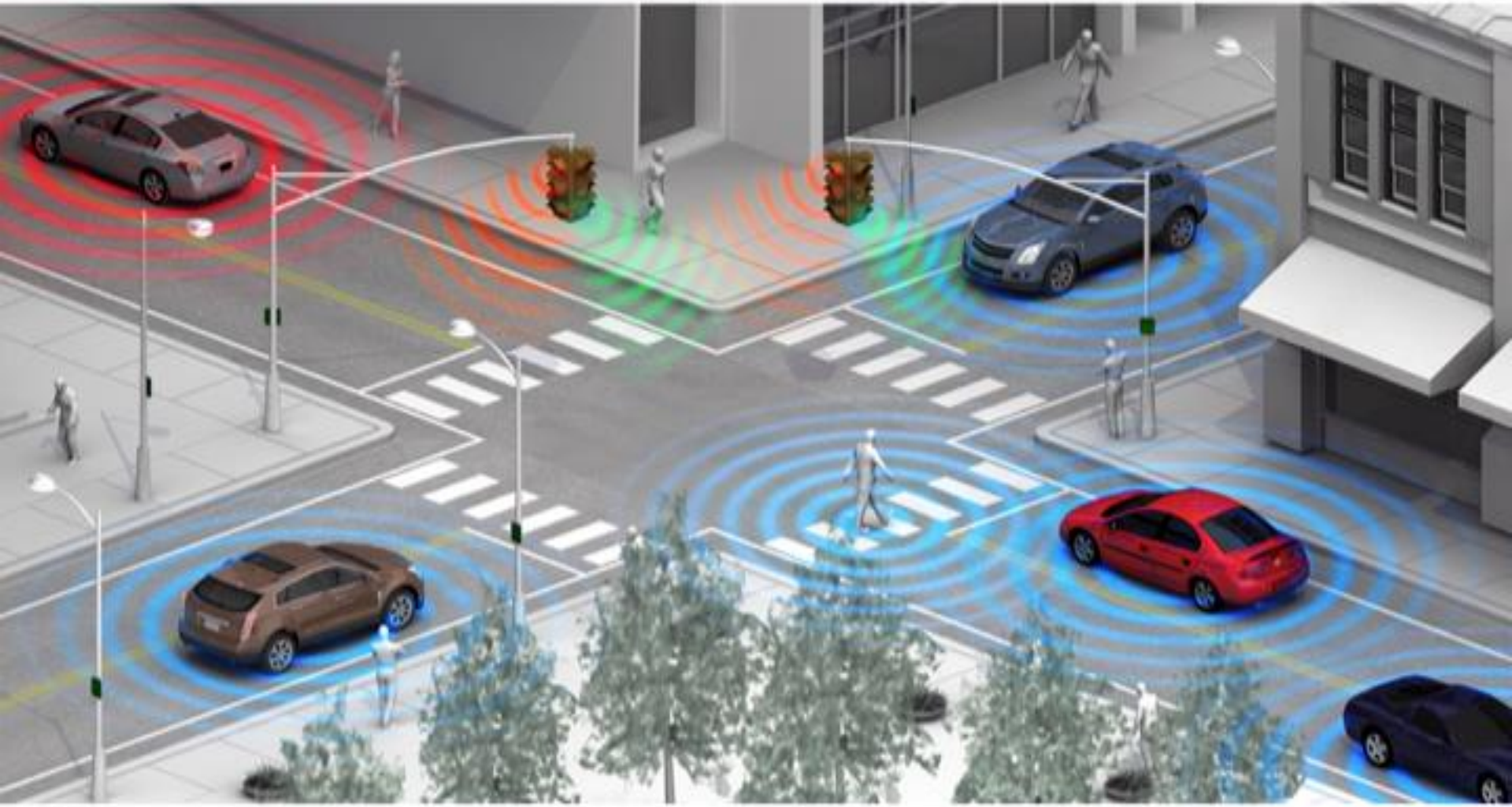
Ranking	Mitigation Strategy	Rationale
1	Use **application whitelisting** to help prevent malicious software and unapproved programs from running.	Application whitelisting is one of the best security strategies as it allows only specified programs to run while blocking all others, including malicious softwa
2	**Patch applications** such as Java, PDF viewers, Flash, web browsers	Vulnerable applications and operating systems target of most attacks. Ensuring these are pa with the latest updates greatly reduces the r exploitable entry points available to an attac



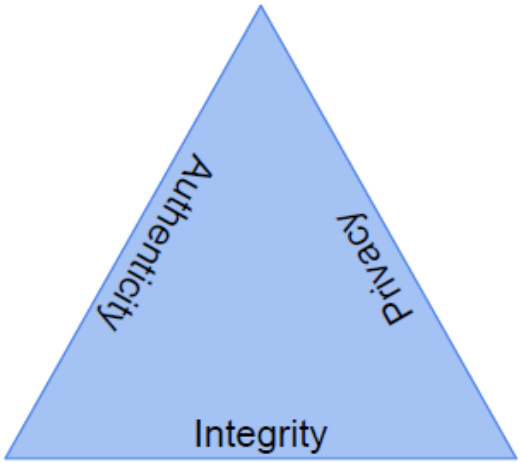
cyber-incident@canada.ca

www.publicsafety.gc.ca/ccirc

This will only become more challenging…



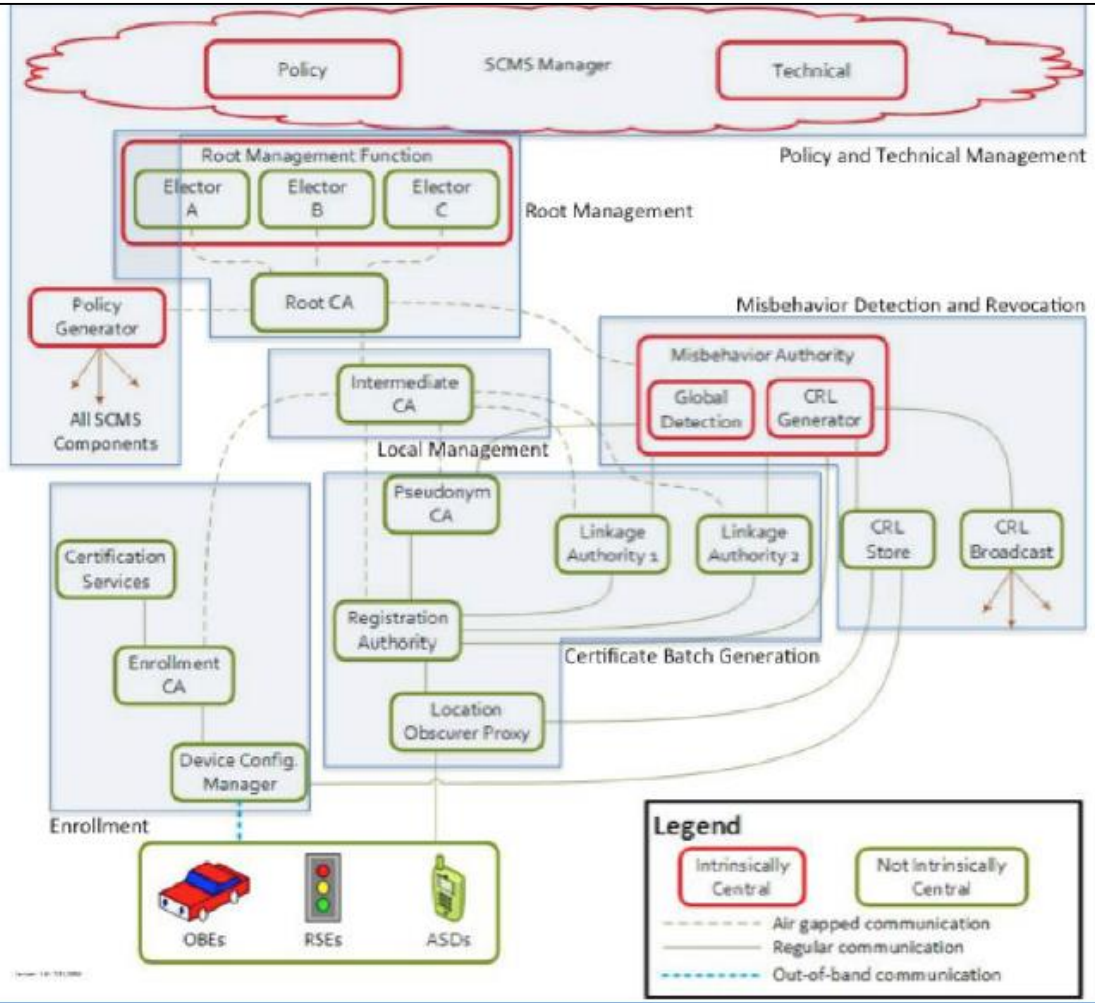
Security Credential Management System (SCMS)



- Crucial requirements that must be met are:
  - Ensure authenticity and integrity of messages
  - Minimize opportunity for tracking personal vehicles
- System also mandates:
  - Privacy for users: No PII can be collected
  - Prevent tracking by insiders & outsiders
  - Assume errors will happen and hackers will attack the system
  - Detect and remove misbehaving systems
  - Minimize over the air messaging bandwidth
- Tricky Result:
  - Create a high volume of anonymous short lived identities
  - … and still be able to revoke these identities when needed

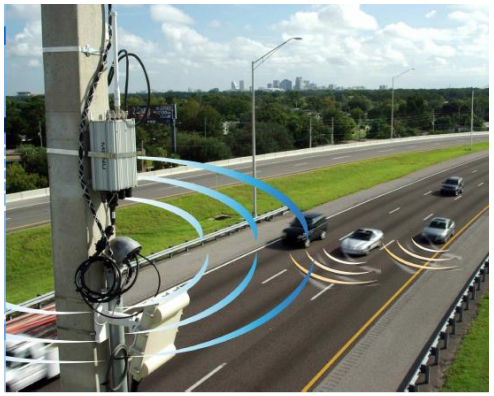
SCMS Architecture

- **Policy & Technical Management**
  Manages overall system
- **Root Management**
  Establishes the system-wide"root of trust"
- **Local Management**
  Issues local certificates
- **Enrollment**
  Activates new devices in the system
- **Certificate Batch Management**
  Delivers batches of pseudonym certificates
- **Misbehavior Detection**
  Identifies bad actors, creates and distributes a Certificate Revocation List



What does this mean for you?

- V2I enabled traffic control devices will require security credentials
  - Like a vehicle, each roadside unit must be enrolled and it must periodically download new certificates
  - This will require full-time or periodic network access
- Large ITS operators may run their own Intermediate Certificate Authority (ICA)
  - Allows them to locally issue credentials for new equipment, perform repairs, modify some local policies
  - Alternative is to share a system with other regional operators
- Credentials needed for special vehicles (e.g. public safety, maintenance) and applications (e.g. road closure, signal preemption)



Adapted from TrustPoint Technologies. 2016

Discussion

- How is your organization approaching cybersecurity?
- Vendors/suppliers: are clients asking about cybersecurity?
- How do we address the “cultural shift”?

Thank You

ecoTECHNOLOGY for Vehicles écoTECHNOLOGIE pour véhicules

For more information, please contact:

Ken Moshi

Senior Analyst, ecoTECHNOLOGY for Vehicles Program

Transport Canada,
Place de Ville, Tower C
Ottawa, Ont. K1A 0N5

Tel: (613) 462-1096
ken.moshi@tc.gc.ca

RDIMS: 12943382