

# WHY AN AUTO-ISAC?

## WITH CONNECTIVITY COMES CYBER RISK

	Yesterday			Today			Tomorrow	
Vehicle Features	Sensors	Automated Assist	Apps	Cellular Modem	Partial Automation	In-Vehicle Commerce	V2V, V2I, V2X	Full Automation
Gov't Interest	IT Standards	Privacy Legislation	Markey Report		Regulation / Legislation			
Attack Scenario	Single Vehicle Spoofing and Manipulation		Remote Control	Wide-Scale PII Theft	Fleet-Wide DDOS	Fleet-Wide Vehicle Control or Disablement		
Threat Actors	White Hat: Academic Research		White Hat: Popular Media		Criminal, Hacktivist, Terrorist and Nation State			
Attack Vector	Physical	Software and Apps		Supply Chain	Vehicle Comms Networks	Third-Party Systems	Network Infrastructure	
Business Impact	Minor Disruption				Major Business Disruption			

**Risk is increasing and will continue to grow...**

**Automakers recognized the growing vehicle cyber risk & proactively joined together to form the Auto-ISAC in 2015**

## MISSION

Serve as an unbiased information broker to provide a **central point of coordination and communication** for the global automotive industry through the analysis and sharing of trusted and timely cyber threat information.

## SCOPE

Light- and heavy-duty vehicles, commercial vehicle fleets and carriers. Currently, we are focused on product cyber security, and anticipate expanding into manufacturing and IT cyber related to the vehicle.

## WHAT WE DO

