Cybersecurity
Southwest Research Institute® (SwRI®) applies proven cybersecurity best practices and standards to the challenge of improving the cyber resilience of global networks and cyber-physical systems. Through active research and development, SwRI is expanding the state of the art in:

- Future-proof security solutions
- Application security
- Network traffic monitoring
- Embedded systems security

SwRI has developed a uniquely tailored cybersecurity process for identifying and evaluating the complex security issues associated with emerging automotive technology. SwRI works with commercial and heavy-duty original equipment manufacturers (OEMs) and suppliers, performing security consulting, including whole vehicle and component security penetration testing.

- Electronic control unit (ECU) penetration assessments
- Connected and autonomous vehicle (CAV) sensor vulnerability assessments
- Secure firmware/software over-the-air (SOTA) updates

Experience

- Threat analysis and risk assessments
- Vehicle-to-vehicle (V2V)
- Connected and autonomous vehicles
- Electric vehicles
- Requirements analysis, design, prototyping, integration and testing
- Independent evaluations

Resources

- 2M+ square feet of labs and facilities
- Custom security assessment tools
- Advanced penetration testing labs

We welcome your inquiries.
For more information, please contact:

Victor Murray
210.522.6589
cyberdefense@swri.org