Request for Research Funding for FY 2021-2022			
Requesting Office	State Traffic Engineering and Operations Office	**Priority**	2 of 15
Proposed Title	Connected Vehicle Security Metrics and Threat Intelligence		
Justification	The emergence of connected and autonomous vehicles at an unprecedented pace ushered several local government-sponsored initiatives to start planning and building a transportation information network that utilizes intelligent sensors and sophisticated communication systems. Peripheral sensors that are used to assist the human operator in lane changing, obstacle avoidance, and parking are slowly being integrated in modern automotive vehicles. Although this newly found convenience is a boon to society, both socially and economically, it presents security challenges that are endemic to connected technologies. These challenges underscore the need to examine the state of connected vehicle security and design an effective threat intelligence portal. The objectives of the proposed project are as follow: 1. Design and develop a comprehensive set of security metrics for connected vehicles 2. Implement a prototype Machine Learning (ML) system that will process sensor data for intelligent security analytics and 3. Create a web-based threat intelligence portal for connected vehicles.		
Impact	It is a generally accepted principle that security is a process and not an end goal. Because processes need continuous improvement, it is imperative that metrics, both quantitative and qualitative, be developed and implemented. After all, as an old adage would state, what cannot be measured cannot be improved. The impact of these metrics on the security of connected vehicles should not be underestimated. When human lives and well-being coupled with socio-economic implications are all in the balance, we cannot help but pay serious attention to these issues. In addition, an effective and realistic threat modeling and intelligence platform would enhance users' abilities to perceive the current state of security in connected vehicles and would assist connected vehicle system planners, administrators and manufacturers with adequate knowledge of existing and perceived threats that can be acted upon in real-time.		
Affected Offices	State Traffic Engineering and Operations Office, District Traffic Operations Offices		
Existing Work	Vehicle Network Security Metrics; Vehicle Security Learning Tools and Scenarios; Connected Vehicle Security		
Keywords Used In Existing Work Search **(Cannot leave blank)**	Common Vulnerability Scoring System (CVSS), Security Metrics, Threat Intelligence, Vehicle Network Protocol, Vehicle Security Attacks, Machine Learning, Sensor Data		
Related Contracts (Give contract numbers)	Florida Center for Cybersecurity, under grant number 3901-1009-00-A (2019 Collaborative SEED Program) National Security Agency under grant number H98230-19-1-0333 Office of Naval Research (ONR) under grant number N00014-21-1-2025		
Funding Request	$257,590	**Anticipated Duration**	24 Months
Project Manager	Raj Ponnaluri, PhD, PE, PTOE, PMP	**Contracting Method**	Direct contract with University of West Florida (Dr. Guillermo A. Francia, III, Dr. Tirthankar Ghosh, Dr. Gregory Hall)
Urgency	1	Connected and automated vehicles offer communication and exchange of information with surrounding environment including other connected vehicles and infrastructure. Connected vehicles can be considered as computers on wheels: from navigation systems to infotainment to HMI (human-machine interface). Security of these technologies remains at the centerpiece of public concern when it comes to mass market penetration. But are security protocols being properly considered in implementing such technologies? Are these systems built to last in today's high-threat cyber environments? This research project will take a deep dive into these concerns and explore what FDOT can do more in terms infrastructure deployment and building partnerships with car manufacturers to address these issues head-on.	

Implementability	1	This project is solely implementation focused. The project will develop matrices cataloging the security threats for connected and automated vehicle technologies, implement an ML system that will process sensor data for intelligent security analytics, and create a web-based threat intelligence portal.

Project Benefits (Succinct, complete explanation)

Benefits Derived

The project enables the realization of the following benefits toward enhanced Connected Autonomous Vehicle (CAV) security:

- Development of connected vehicle security metrics with which continuous improvement could be measured;
- Implementation of an ML system capable of sensor and system/network log data analytics for intrusion detection and anomalous behavior monitoring; and
- Enhanced threat modeling and sharing risk framework through real-time threat intelligence analysis and vulnerability assessment.

Methodology and Deliverables

Vehicle Security Metrics

The metrics will be developed based on published literature and standards. Relevant data will include, but not be limited to, the Common Vulnerability Scoring System (CVSS), the Common Criteria for Information Technology Security Evaluation, security threat intelligence, and vehicle communication attack surfaces. The pertinent standards will include the ISO/SAE 21434 (Cybersecurity Engineering), IEEE 1609-12 (WAVE), IEEE 802.11 (WiFi), SAE J3101, IATF 16949:2016, and IEEE 29119-1:2013 (Software and Systems Engineering).

Deliverables include a set of vehicle security metrics, project documentation, and a prototype of an interactive system for calculating security metrics and visualizing the metrics and the major security parameters.

Machine Learning (ML) System

The ML system will be designed for both prediction and classification. It will utilize data gathered during the prevailing condition of the transport system at a macro level for infrastructure planning purposes, for predicting impending precarious states and for detecting anomalous behavior.

Deliverables include a prototype of the ML system and the datasets used for training and testing. These datasets will become the baseline data that can be used for future enhancement of the ML system.

Threat Intelligence

We propose to develop a threat modeling and threat intelligence platform for connected vehicles. The platform will consist of two components: a threat modeling engine, and a threat intelligence portal. The threat modeling engine will list all vulnerabilities and evaluate all feasible threats against each of the sub-systems of the connected vehicle, namely V2V, V2I and V2X, and will come up with a CVSS score for each threat. A threat database will be built with all feasible threats against each subsystem and their corresponding CVSS score. The threat database, along with other external threat feeds and initial Indicators of Compromise (IoC), will be fed to the threat intelligence portal, which will generate a list of final IoCs and package them in standard Structured Threat Information Expression (STIX) format. The portal will provide a threat sharing functionality and connectivity to a Malware Information Sharing Platform (MISP) server. It will also provide a search functionality for searching IoCs. The threats will be mapped to the MITRE ATT&CK Framework to provide better visibility and acceptance.

Project Benefits (Select all that apply and explain)	**Quantifiable Benefits (units, dollars, etc…if applicable)**	**Methodology or Data Sources Used to Determine Quantifiable Benefits. If not applicable, please give justification of project benefits**
○ Materials Enhancement	Enhanced preparedness against cybersecurity threats	Security metrics and threat intelligence will significantly improve the CAV system evaluation, security monitoring and continuous improvement processes
○ Materials Savings	Proactive measures will save resource investment after security breach	Project outcomes will provide pertinent data and system insights that can be used to guide critical decision making such as those in material and service procurement
○ Time Savings	Reduced operational downtime of connected and automated vehicle systems operation due to any potential security threat	Time savings could be realized through reduced downtime and development efforts with improvements in security
○ Lives Saved/Injuries Prevented	Reduce cybersecurity threats may avoid any unintended consequence	Excellent potential contributions towards saving lives and preventing injuries due to enhanced security of CAV infrastructure
○ Other (Explain)	Less cybersecurity threats and proactive measures	Project outcomes will provide additional information necessary for system and infrastructure maintenance and the prevention of productivity loss due to security issues

*Comments should explain and support urgency, financial benefit, and implementability scores