Request for Research Funding for FY 2019-2020			
Requesting Office	District 7	**Priority** High	6 of 8
Proposed Title	Identify Sources and Risks on Cyber Security for Connected Vehicle Infrastructure		
Justification	Cybersecurity has been intensively investigated in various systems. In the connected vehicles (CV) context, reliable implementation of CV applications relies heavily on cyber security measures. Although cyberattacks have been investigated on the vehicle side (Kleberger Petit and Shladover, 2015), sources and risk levels from possible cyberattacks on infrastructure are not yet well investigated. It is not clear what measures and precautions that state DOTs need to prepare in managing incoming connected vehicle infrastructure. To address this gap, this research aims to identify sources and risk levels for cyberattacks on CV infrastructure from the state DOT management point of view. It is important for FDOT to identify components in their infrastructures susceptible to cyberattacks, and types of cyberattacks may happen to each component. Then we will propose a risk evaluation system that categorizes the risks into different levels based on their impacts on safety, mobility, and energy consumption. Possible countermeasures and preparations against these attacks will be proposed. The outcomes of this research will help FDOT understand vulnerabilities and possible consequences of CV related infrastructure. This information is the foundation for FDOT to determine how to securely operate CV infrastructure and what types of information and data to share via the CV infrastructure.		
Impact	Cybersecurity on CV systems has been well discussed but there lacks implementable and measurable methods for state DOTs to apply in preparing and managing their systems. This research will allow FDOT to identify detailed sources of possible risks and evaluate their risk levels to better prepare future infrastructure investment and management. This study will support FDOT to reach a leading status among all states in making implementable measures and standards in enhancing CV infrastructure security and protecting DOTs from their liability exposure. Without conducting this research, future CV infrastructure investment may be subject to higher risks of cyberattacks and consequences**.**		
Affected Offices	Traffic Engineering and Operations and District Traffic Operations Office		
Existing Work	Kleberger, P., Olovsson, T., & Jonsson, E. (2011, June). Security aspects of the in-vehicle network in the connected car. In *Intelligent Vehicles Symposium (IV), 2011 IEEE* (pp. 528-533). IEEE. Petit, J., & Shladover, S. E. (2015). Potential cyberattacks on automated vehicles. *IEEE Trans. Intelligent Transportation Systems*, *16*(2), 546-556. Summary: There are a number of studies investigating cybersecurity issues on vehicles related issues, such as V2X communication and autonomous vehicle control. There is no study particularly focused on infrastructure side risks and their impact levels from the infrastructure point of view.		
Keywords Used In Existing Work Search **(Cannot leave blank)**	Connected vehicles, cybersecurity, infrastructure, cyberattacks		
Related Contracts (Give contract numbers)	N/A		
Funding Request	Estimated cost: 150,000	**Anticipated Duration**	18 months
Project Manager	Mr. Daniel Buidens co-PM: Dr. Raj Ponnaluri	**Contracting Method**	Direct contract with Dr. Pei-Sung Lin at the University of South Florida's Center for Urban Transportation Research (CUTR)

Urgency	2	Reliable implementation of connected vehicle applications relies heavily on cybersecurity measures. Although cyberattacks have been investigated on the vehicle side, sources and risk levels from possible cyberattacks on infrastructure are not yet well investigated. Before cyberattacks on infrastructure become a serious problem, FDOT and local transportation agencies need to understand what measures and precautions necessary to prepare in managing incoming connected vehicle infrastructures.
Implementability	2	This proposed research aims to identify sources and risk levels for cyberattacks on CV infrastructure from the state DOT management point of view. The findings and recommendations from this project can help FDOT and local agencies implement needed security measures, focus on the identified infrastructure components, and apply the proper methods to detect and prevent the cyberattacks on CV infrastructure.

Project Benefits (Succinct, complete explanation)

- Support FDOT to reach a leading status of CV infrastructure cyber risk measures and standards
- Help FDOT prepare for planning and operations of CV infrastructure
- Improve transportation system safety, mobility and environmental friendliness against malicious cyberattacks

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**
o **Materials Enhancement**		
o **Materials Savings**	Optimizing investment on CV infrastructure	Method: Provide a risk-consequence table. Based on risk and consequence levels of the CV infrastructure, FDOT can select to invest low-risk and low-consequence CV infrastructure components rather than high-risk, high-consequence components
o **Time Savings**	Travel time improvements due to reduced cyberattacks	Data: Utilize trajectory data on I-75 before the merging point of I-275 collected from Dr. Li's project "Trajectory Investigation for Enhanced Microsimulation Calibration Guidance" sponsored by FHWA. Method: We will construct scenarios with different cyberattack types with simulations and evaluate the mobility benefit.
o **Lives Saved/Injuries Prevented**	Reduction of safety hazards against malicious cyberattacks	Method: We will construct scenarios with different cyberattack types with the dynamic safety prediction model developed by Dr. Zhenyu Wang and Dr. Pei-Sung Lin under an ongoing FDOT research project to quantify the safety benefit.
o **Other (Explain)**		

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