Request for Research Funding for FY 2023-2024			
Project Number (Research Center Use Only): TEO-24-01			
Requesting Office	State Traffic Engineering and Operations	**Priority** High	1 of 11
Proposed Title	Mitigation of Cybersecurity Vulnerabilities for Traffic Control Infrastructure		
Justification	***Current Situation*** The Florida Department of Transportation (FDOT) has performed assessments for elements of the connected vehicle infrastructure including traffic controllers and Roadside units (RSU) via its recently completed research project entitled, "Identify Sources and Risks on Cybersecurity for Connected Vehicle Infrastructures" (1). An assessment of additional controllers (from six vendors) was conducted to identify existing vulnerabilities with their latest firmware. This research was completed in November 2022 and provided FDOT with recommendations for mitigations of the identified risks, as well as recommendations for specification development for the State Traffic and Operations Office's Traffic Engineering Research Laboratory (TERL). In the recent NCHRP 03-127 report titled "Cybersecurity of Traffic Management Systems" (2), the Transportation Research Board (TRB) provided guidance for state and local transportation agencies on mitigating the risks from cyber-attacks on the field side of traffic management systems (TMS) (including traffic signal systems, intelligent transportation systems, vehicle-to-infrastructure systems (V2I), and closed-circuit television systems) and, secondarily, on informing the agency's response to an attack. The report also provided risk assessment of typical TMS design and a cybersecurity web guidance tool that aids an agency in making its TMS field network more resistant to cybersecurity attacks. A second phase was proposed but was ultimately rejected as the committee decided not to fund additional research on devices such as controllers or other hardware. This leaves state DOTs with the responsibility of establishing their own guidelines and principles in cybersecurity. To implement recommendations from the recently completed FDOT research project and the NCHRP 03-127 project, and assist state and local DOTs to identify sources and risks on cybersecurity for traffic infrastructure and improve the cybersecurity of those systems – in particular, those in conjunction with CV/AV technology – several efforts are proposed: (1) develop a set of specifications and testing procedures for identified cyber vulnerabilities of traffic controllers and associated infrastructure, (2) develop mitigation tools and problem resolution by working with manufacturers, and (3) perform assessment of additional hardware currently used in the field to increase operational security to improve and enhance cybersecurity for traffic infrastructure. ***Why the research is needed*** This proposed research is needed to address several potential vulnerabilities in traffic controllers that can impact FDOT's signal system. The research team will work with FDOT TERL to increase the cybersecurity of traffic devices used in the field and increase awareness of the cybersecurity threats to which devices used in traffic are vulnerable. During phase 1 of this recently completed FDOT research project, a comprehensive literature review was conducted on cybersecurity concerns, potential cyber vulnerabilities on CV technologies and associated CV infrastructure, liability issues for cyberattacks, protocols and network communications needs, and mitigation strategies. The team also identified and interviewed key researchers, experts, manufacturers, vendors, and TMC Operations and/or IT managers to assess the cyber vulnerabilities of CV technology and associated CV infrastructure. One issue that became prominent during the COVID-19 pandemic was the need to consider Supply Chain Risk Management (SCRM) with vendor-provided systems. SCRM is a new requirement in the new 1.1 version of NIST Cybersecurity Framework and items to consider with vendors include: • Where hardware/software is made or assembled • Lifecycle of a system (design, development, distribution, deployment, acquisition, maintenance, destruction) • Lack of proper stocked items if hit with disruption • Counterfeit products • Insertion of malicious software/hardware		

	This will eliminate large delays on the acquisition of new systems and provide a contingency plan in case another major disruption happens in the near future. ***Proposed Research Project Objectives*** Objectives and associated tasks of the proposed project are as follows: 1. Develop specifications for traffic controllers to mitigate the vulnerabilities found in Phase 1. The team will work with TERL on the development of specifications that will require traffic controller manufacturers to increase their protection and close any holes in the security. 2. Develop a testing procedure and guidelines for specification testing. The team will work with TERL to develop a procedure and steps for testing the vulnerabilities so that products can be tested against these threats. 3. Provide support in cybersecurity testing of traffic controllers and establish the procedure for testing. 4. Support FDOT in responsible disclosure with traffic controller manufacturers so that the vulnerabilities can be disclosed and a realistic timeline for mitigation can be implemented. This will include both short-term and long-term solutions as some vulnerabilities might require firmware/software updates that take longer to implement. 5. Assess other devices used in traffic management (e.g., conflict monitors, traffic cameras, vehicle detectors, network switches, etc.). ***Research Effects on FDOT Mission Critical Focus Areas*** FDOT's mission is to provide a safe transportation system that ensures the mobility of people and goods, enhances economic prosperity, and preserves the quality of Florida's environment and communities. The mission of the FDOT Traffic Engineering and Operations office is to improve safety and mobility through the efficient application of traffic engineering principles and practices. This proposed research fully supports these missions. The proposed research will contribute to improving safety and mobility, especially mitigating potential cybersecurity threats to the transportation network. This in turn will not allow delay or crashes to occur because of a cyberattack on the systems network or devices. The proposed research also fully supports FDOT's vital focus to Improve Safety, Enhance Mobility, and Inspire Innovation.
Impact	**How shall the results impact practice? Consequences of not doing the research?** The major results of this proposed research will include: (1) a set of specifications to be added in the traffic controller specifications for approval, (2) a testing procedure, protocol, and guidelines needed to test the identified vulnerabilities in traffic controllers, (3) resolution of issues and application of mitigations with vendors to close gaps in cybersecurity, and (4) results of assessment of additional devices agreed upon with TERL. The consequences of not conducting the research include: • FDOT will not have specifications added for traffic controllers against identified vulnerabilities • FDOT will not have a testing procedure to evaluate the current traffic controllers and additional hardware against cybersecurity vulnerabilities • FDOT will not have assessed the current vulnerabilities of additional hardware devices used in traffic management • FDOT will not increase its cybersecurity presence and awareness and close loops in the current systems used in the field.
Affected Offices	State Traffic Engineering and Operations Office
Existing Work	1. Identify Sources and Risks on Cybersecurity for Connected Vehicle Infrastructures. [Project]. Florida Department of Transportation. Start date: 21 May. 2020. https://rip.trb.org/view/1708031

	2. Cybersecurity of Traffic Management Systems. [Project]. National Cooperative Highway Research Program, American Association of State Highway and Transportation Officials (AASHTO), Federal Highway Administration. Start date: 16 Aug. 2017. https://rip.trb.org/view/1440198 3. Guidelines for State Transportation Agency Chief Executive Officers on Cybersecurity Issues and Protection Strategies. [Project]. National Cooperative Highway Research Program, Federal Highway Administration, American Association of State Highway and Transportation Officials (AASHTO). Start date: 1 Jun. 2020. https://rip.trb.org/view/1628635 4. Cybersecurity for the Advanced Transportation Controller Standards Family. [Project]. Intelligent Transportation Systems - Joint Program Office. Start date: 1 Mar. 2021. https://rip.trb.org/view/2067961 5. Cybersecurity for ITS Best Practices Development. [Project]. Intelligent Transportation Systems - Joint Program Office. Start date: 1 Feb. 2021. https://rip.trb.org/view/2067959 6. Road-side based cybersecurity in connected and automated vehicle systems. [Project]. Office of the Assistant Secretary for Research and Technology, Center for Connected and Automated Transportation. Start date: 1 Jan. 2021. https://rip.trb.org/view/1843623 7. Development of a NIST Cybersecurity Profile for the ITS Ecosystem. [Project]. Intelligent Transportation Systems - Joint Program Office. Start date: 15 Jan. 2020. https://rip.trb.org/view/2067960		
Keywords Used In Existing Work Search **(Cannot leave blank)**	cybersecurity, cyberattacks, ITS, traffic management systems, computer security; highway safety, risk assessment, traffic signal control systems		
Related Contracts (Give contract numbers)	BDV25-977-70		
Funding Request	$250,000	**Anticipated Duration**	18 months
Project Manager	Derek Vollmer, PE Co-PM: Kenny Shiver	**Contracting Method**	Direct contract with Center for Urban Transportation Research (CUTR) at the University of South Florida – Dr. Achilleas Kourtellis
Equipment	N/A	The team will work with either existing equipment purchased on other projects or equipment currently at the TERL.	
Urgency	Score = 1	The urgency for this project is high as cyber-attacks are becoming more mainstream and easier to implement. In addition, the threat to traffic systems has been traditionally low, but as new uses of idle computer systems become present and gain awareness (e.g., mining for bitcoin), traffic systems can become targets quickly on a large scale. Threats like ransomware that lock users out of their systems for ransom, are becoming increasingly common and agencies that are unprepared to respond can face huge consequences.	
Implementability	Score = 1	This is a project that continues work conducted in the previous years. The current and future threat to traffic systems is increasing and the results of this project will directly impact the ability of FDOT to protect its systems.	

Project Benefits (Succinct, complete explanation)

The significant benefits for conducting this proposed research project include the following:

1. Development of specifications for testing traffic controllers on cybersecurity vulnerabilities. This will increase cyber safety and secure the systems.
2. Develop procedures and testing protocols to be able to conduct the testing of controllers currently in use. Without this, the specifications can remain not implementable for the foreseeable future.
3. Close loops and identified issues on current controllers used in the field by working with their manufacturers to provide mitigations both long-term and short-term.
4. Identify additional vulnerabilities on hardware used in traffic management and assess mitigation strategies.

Project Benefits	**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**

(Select all that apply and explain)		
○ Materials Enhancement		
○ Materials Savings		
○ Time Savings	Reduction of time needed for the Traffic Engineering Research Lab to develop specifications and testing procedures	The application of this project will lead to remediation of existing vulnerabilities on traffic controllers and other traffic devices, implementation of cybersecurity testing and protocols and development of specifications for future testing. The results of this project will lead to remediation of existing vulnerabilities on traffic controllers and other traffic devices. They can reduce serious traffic congestion caused by cyberattacks of traffic control devices.
○ Lives Saved/Injuries Prevented		The results of this project will lead to remediation of existing vulnerabilities on traffic controllers and other traffic devices. They can prevent injuries and save lives from crashes caused by cyberattacks of traffic control devices.
○ Other (Explain)		The results of this project can benefit the department in ways that cannot be quantified, as the threat to cybersecurity is elusive and cannot be measured until an attack is made. Preparing for cyberthreats is like acquiring insurance for the system. Simply doing nothing is guaranteed to have negative impacts in the future.