Purpose of Advisory

The purpose of this advisory is two-fold: 1) To make DOTs aware of a recent article published by the University of Michigan on “a number of security flaws that exist due to systemic failures by the designers” and 2) reinforce and build upon known solutions to hardening the center to field network.

Summary of University of Michigan Paper

The University of Michigan paper is titled, “Green Lights Forever: Analyzing the Security of Traffic Infrastructure” where a number of vulnerabilities in a wirelessly networked traffic signal system were identified, explained, and demonstrated. This was done with cooperation of a local transportation agency (see paper attached). The impacts are significant and push the envelope of safe operation to the MMU and Conflict Monitor in guaranteeing safety. We also feel this research paper provides sufficient information for other attackers to replicate these attacks.

Short term solutions To Hardening Center to Field Wireless Network

The vulnerabilities revealed by University of Michigan and the DMS SUN_HACKER incident both exploit in significant fashion known weakness of improperly configured wireless communication network. Wireless network are still an important component of transportation operations, but they must be operated in a safe and resilient manner. AASHTO, along with members of the Transportation Systems Management and Operations Subcommittee and the Federal Highway Administration, have made recommendations for immediate action in the past. The following steps build upon those recommendations:

1. **Devices shall never deploy in the field with factory default passwords**
    1.1. This will include all equipment on the communication path, inclusive of edge devices, routers, modems, and traffic management center.
    1.2. Use a strong password based on recommended best practices
    1.3. Tips on stronger password can be found here - https://www.us-cert.gov/sites/default/files/publications/PasswordMgmt2012.pdf
2. **Use a VPN to encrypt traffic when using commercial wireless services**
3. **Immediately enable logging of traffic on the center to field network.** Log files are critical for forensic analysis if there is an incident. It is also needed for more advanced protection systems at a later date.
4. **Immediately enable any encryption services built into your wireless equipment.** Order of preference shall be WPA2-Personal, WPA2-Enterprise, WPA, and finally WEP only if no alternative is available. Please note that WEP security is completely compromised, but the legal repercussion of circumventing encryption could be a deterrent.
5. **Disable SSID broadcast from wireless equipment.**
6. **If possible, randomize the MAC address of the field devices and utilize MAC address filtering where possible.**
7. **Turn off or disable all unused ports and unnecessary services** (telnet, ping, ftp, etc) in all field devices.

These are recommended steps for immediate action that should be taken if wireless communication is utilized in your transportation system. There will be operation and maintenance labor cost to plan and implement these recommendation. There should not be any additional cost to adopt these recommendations, but it could not be ruled out due to the number of different equipment currently in use. There are other steps that can be taken to further harden the transportation network against attack. These steps are not a replacement for a comprehensive cyber security plan.

Where To Report Suspicious Activity

In the near term, the following are the recommended reporting procedures.

1. In cases with **no injuries, property or facility damage**. Suspicious Activities should be reported to ICS-CERT (ics-cert@hq.dhs.gov) and your State's FHWA Division Office.
2. In cases where **there are injuries, property or facility damage**. Report the incident to Law Enforcement, followed by ICS-CERT (ics-cert@hq.dhs.gov), and your state's FHWA Division Office.