SECURING TRANSPORTATION INFRASTRUCTURE

How CyberLock Provides the Best Security Solutions for the Traffic Industry

CyberLock®

CyberLock, Inc. 1105 N.E. Circle Blvd., Corvallis, OR 97330
541-738-5500 • Fax 541-738-5501 • www.cyberlock.com • sales@cyberlock.com • support@cyberlock.com

SECURING TRANSPORTATION INFRASTRUCTURE

How CyberLock Provides the Best Security Solutions for the Traffic Industry | by CyberLock

Transportation Systems are one of sixteen Critical Infrastructure Sectors established by the US government. Within the Transportation Sector are seven modes, one of which is the Highway and Motor Carrier mode, which includes roadways, bridges, tunnels, vehicles, operational management systems, and more. In 2018, several agencies specific to the Transportation Sector released a progress report on reaching security goals within the transportation sector. One of the goals highlighted in this report specifically speaks to the management of "risks to physical, human, and cyber elements of critical transportation infrastructure," or CISA. One important element that Transportation Departments across the nation have identified as problematic is physical security of traffic cabinets and roadside communication equipment.

Traffic Control Boxes

Traffic control boxes and digital signs are expensive pieces of equipment that are essential to the safe and smooth operation of roads and highways. Each traffic control box contains thousands of dollars in critical equipment, including networking devices, computers, expensive cabling and more.

EACH TRAFFIC CONTROL BOX CONTAINS THOUSANDS OF DOLLARS IN CRITICAL EQUIPMENT. THE SECURITY OF THIS EQUIPMENT IS OF THE UTMOST IMPORTANCE. TRAFFIC BOXES ARE ATTRACTIVE TARGETS FOR THIEVES.

The security of this equipment is essential to the safety and reliability of our transportation infrastructure. Traffic control boxes not only control the flow of traffic, they also house equipment used to control operations of other public systems. With thousands of dollars in critical equipment inside, traffic boxes are attractive targets for thieves. Numerous accounts illustrate the prevalence of theft in the traffic cabinet industry. Not only are traffic boxes targeted for theft of internal components, they are also susceptible to tampering. Whether malicious or not, tampering can create dangerous conditions for the public.

Roadside Equipment

Roadside equipment is a frequent target of tampering, particularly speed monitors and digital signs. Messages displayed on digital signs

are regularly altered by unauthorized individuals with intentions ranging from helpful to malicious. A routine web search reveals countless photographs and news stories illustrating unapproved changes that both DOT employees and members of the public have made to digital signs. Signs often get changed from important warnings, such as "Night Construction: Be Prepared to Stop," to trivial messages like "Marry Me Sally?" depriving drivers of critical information. Tampering is not only dangerous to motorists, it can be problematic for employees and engineers who service this equipment. Leaving their regular service route to resolve issues caused by tampering can delay important scheduled maintenance.

THE LACK OF CONTROL INHERENT IN THESE MECHANICAL KEY SYSTEMS JEOPARDIZES THE SECURITY AND SAFETY OF TRANSPORTATION INFRASTRUCTURE ACROSS THE GLOBE. MECHANICAL LOCKS AND KEYS ARE NOT SOPHISTICATED ENOUGH TO MEET THE DEMANDS OF THE DOT.

#2 Mechanical Keys

Regional and local Transportation Departments throughout the United States struggle to properly secure traffic cabinets and road communication equipment. The leading problems in transportation security are derived from a commonly used security element, the #2 mechanical key. For most traffic cabinet locks, a standard #2 key is issued to control access. #2 keys are extremely prevalent and easily duplicated. Additionally, there are limited variations in the cut of the key. A single #2 key can open a variety of traffic cabinets across the country. Transportation departments are tasked with finding a reliable security solution that eliminates the concerns and risks that #2 keys pose.

The #2 standard key is widely used to access traffic cabinets from many of the top manufacturers. Unfortunately, it is also one of the easiest mechanical keys to duplicate or purchase online. On any given day, an abundance of these #2 'skeleton' keys are available for purchase. Further yet, new technologies now enable accurate duplication of any mechanical key, using only a smartphone app and a consumer-friendly 3D printer. Despite these concerns, the #2 mechanical key often represents the only form of security preventing unauthorized access to critical roadside equipment; equipment that should only be accessible by trained, trusted individuals.

The lack of control inherent in these mechanical key systems jeopardizes the security and safety of transportation infrastructure across the globe, from small towns to the largest cities. In addition to critical issues with key control, mechanical locks are susceptible to picking and keyway vandalism, rendering them inoperable. Simply put, mechanical locks and keys are not sophisticated enough to meet the demands of the transportation industry.

KEY-CENTRIC ACCESS CONTROL PROVIDES THE IDEAL SECURITY SOLUTION TO MEET THE NEEDS OF TRANSPORTATION DEPARTMENTS ACROSS THE NATION.

Key-Centric Access Control

Key-centric access control systems combine the precision of electronic systems with the simple installation, affordability, and ease of use of mechanical locks and keys. Electronic locks and keys provide the ability to control access to critical equipment without installing cables to power the lock. Instead, the batteries in the smart keys energize the cylinders, which means there is no need to manage and replace batteries in the lock. Electronic cylinders are designed to the exact specifications of the mechanical cylinder, enabling a simple retrofit that takes just minutes.

Reducing key-control concerns, smart keys are programmed with access permissions for each individual user. If a key is lost or stolen, it can easily be deactivated in the system, eliminating the need to re-key. Simply mark the key as lost in the software and communicate that information to the locks, rendering the key inoperable if access is attempted. Each lock and key holds a memory of every access attempt, allowing

management to view an audit trail showing who accessed or attempted to access specific locations. Key centric access control provides the ideal security solution to meet the needs of Transportation Departments across the nation.

A number of state DOTs have turned to the CyberLock key-centric access control system to secure traffic cabinets and roadside equipment, as well as eliminate concerns associated with #2 keys. Georgia Department of Transportation (GDOT) found success with CyberLock in securing hub buildings and field equipment. They are now able to control subcontractor and employee access to restricted areas. Additionally, any attempt to access restricted areas is tracked in both the locks and the key, providing them peace of mind.

Securing critical infrastructure is of the utmost importance because even simple disruptions can create havoc. Mechanical locks and keys have significant limitations that simply do not suit this industry. CyberLock electronic locks and keys combine the benefits of both systems, providing an ideal solution for Transportation Departments.

CyberLock®

CyberLock, Inc. 1105 N.E. Circle Blvd., Corvallis, OR 97330
541-738-5500 • Fax 541-738-5501 • www.cyberlock.com • sales@cyberlock.com • support@cyberlock.com