Cybersecurity Assessment and Best Practices for Truck Stop Technologies

Final Report — December 2021

Prepared for:
Intelligent Transportation Systems Joint Program Office
Office of the Assistant Secretary for Research and Technology
and
Federal Motor Carrier Safety Administration
Office of Analysis, Research, and Technology

U.S. Department of Transportation
1200 New Jersey Avenue, SE
Washington, D.C. 20590

U.S. Department of Transportation
Volpe Center

Notice

This document is disseminated under the sponsorship of the Department of Transportation in the interest of information exchange. The United States Government assumes no liability for the contents or use thereof.

The United States Government does not endorse products or manufacturers. Trade or manufacturers' names appear herein solely because they are considered essential to the objective of this report.

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. AGENCY USE ONLY (Leave blank)	2. REPORT DATE	3. REPORT TYPE AND DATES COVERED
	December 2021	

4. TITLE AND SUBTITLE
Cybersecurity Assessment and Best Practices for Truck Stop Technologies

5a. FUNDING NUMBERS
VN118

6. AUTHOR(S)
Daniel Chin

5b. CONTRACT NUMBER
51HWB1B120

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
Volpe National Transportation Systems Center
Advanced Vehicle Technology Division, V-337
55 Broadway
Cambridge, MA 02142

8. PERFORMING ORGANIZATION REPORT NUMBER
DOT-VNTSC-FHWA-22-02

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)
Intelligent Transportation Systems Joint Program Office
Office of the Assistant Secretary for Research and Technology
1200 New Jersey Avenue, SE
Washington, D.C. 20590

Federal Motor Carrier Safety Administration
Office of Analysis, Research, and Technology
1200 New Jersey Avenue, SE
Washington, D.C. 20590

10. SPONSORING/MONITORING AGENCY REPORT NUMBER

11. SUPPLEMENTARY NOTES

12a. DISTRIBUTION/AVAILABILITY STATEMENT

12b. DISTRIBUTION CODE

13. ABSTRACT (Maximum 200 words)
This report presents the results of a research study that identified nine current and emerging truck stop technologies. This study applied the STRIDE threat model to identify the most critical cybersecurity risks for each technology, and the HEAVENS methodology to assign an associated security level (low, medium, or high). With this information, truck stop operators and truck stop technology vendors could apply the Center for Internet Security 18 controls to develop operational best practices.

14. SUBJECT TERMS
Truck stop, Cybersecurity, Wi-Fi, gas pump, Automatic Tank Gauges, ATG, Anti-Idling Systems, Electric Vehicle Supply Equipment, ESVE, Truck Parking Availability Systems, Weigh Stations, Payment Systems, Video Surveillance Systems, Information Technology Enterprise Infrastructure, STRIDE, HEAVENS, NIST CIS 18 Controls

15. NUMBER OF PAGES
71

16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT	18. SECURITY CLASSIFICATION OF THIS PAGE	19. SECURITY CLASSIFICATION OF ABSTRACT	20. LIMITATION OF ABSTRACT

NSN 7540-01-280-5500

Standard Form 298 (Rev. 2-89)
Prescribed by ANSI Std. 239-18
298-102

Contents

List of Tables

List of Abbreviations

Abbreviation	Term
AAA	Authentication, Authorization, and Auditing
ATG	Automatic Tank Gauge
CIA	Confidentiality, Integrity, and Availability
CIS	Center for Internet Security
CONOPS	Concept of Operations
DHCP	Dynamic Host Configuration Protocol
DKIM	DomainKeys Identified Mail
DMARC	Domain-based Message Authentication, Reporting, and Conformance
DNS	Domain Name System
DOT	Department of Transportation
ELD	Electronic Logging Device
EVSE	Electric Vehicle Supply Equipment
FMCSA	Federal Motor Carrier Safety Administration
HEAVENS	Healing Vulnerabilities to Enhance Software Security and Safety
IDS	Intrusion Detection System
IoT	Internet of Things
IP	Internet Protocol
IPS	Intrusion Prevention System
IT	Information Technology
MFA	Multi-Factor Authentication
NIST	National Institute of Standards and Technology
OpenSSH	Open Secure Shell
PCI DSS	Payment Card Industry Data Security Standard
SCAP	Security Content Automation Protocol
SPF	Sender Policy Framework
SSO	Single Sign-On
STRIDE	Spoofing, Tampering, Repudiation, Information disclosure, Denial of service, and Elevation of privilege
TLS	Transport Layer Security
TOE	Target Of Evaluation
TSE	Truck Stop Electrification
URL	Uniform Resource Locator
WPA2	Wi-Fi Protected Access 2
XFC	Extreme Fast Charger

Executive Summary

This report presents the results of a research study that has two main objectives:

1. Identify current and emerging truck stop technologies and assess their cybersecurity risks.
2. Recommend cybersecurity best practices for truck stop operators and their technology providers based on these assessments.

Identification and Cybersecurity Assessment of Truck Stop Technologies

Interviews with industry subject matter experts and an open-source internet scan of current and emerging technologies available at commercial truck stops and state-run rest stops identified the following technologies:

- Wi-Fi Communications and Networks
- Gas Pumps and Automatic Tank Gauges
- Anti-Idling Systems and Truck Stop Electrification
- Electric Vehicle Supply Equipment (EVSE)
- Truck Parking Availability Systems
- Weigh Stations
- Electronic Logging Device (ELD) Support Equipment
- Payment Systems
- Video Surveillance Systems
- Information Technology (IT) Enterprise Infrastructure

These technologies provide services and conveniences for truck drivers, enable efficient and ecologically responsible operation, and provide security and information infrastructure.

The cybersecurity assessment of each technology employed Volvo's Healing Vulnerabilities to Enhance Software Security and Safety (HEAVENS) Analysis Methodology [1]. This research study chose the HEAVENS methodology because it can derive security requirements for different technologies and systems, and accounts for the safety, financial, and operational impact of a cyber-attack. The methodology is also closely aligned with some cybersecurity industry standards listed in Table ES-1.

Table ES-1. Cybersecurity Industry Standards

Industry Standard	Use
Common Criteria	Standard for IT security evaluation
Common Vulnerability Scoring System	Open and standardized method for rating IT vulnerabilities
Operationally Critical Threat, Asset, and Vulnerability Evaluation	Approach to assess an organization's information security needs
Open Web Application Security Project	Risk rating methodology suitable for web application security

Industry Standard	Use
European Telecommunications Standards Institute Threat Vulnerability and Risk Analysis	Threat, vulnerability, and risk analysis methodology for the telecommunications industry
Microsoft's Spoofing, Tampering, Repudiation, Information disclosure, Denial of service, Elevations of privilege (STRIDE) Threat Model	Threat modeling and risk assessment for software
European Union's E-safety Vehicle Intrusion Protected Applications	Risk rating approach for automotive industry, focused on passenger cars and is attack centric

HEAVENS uses Microsoft's STRIDE categories to define the types of threats a system may encounter [1]. STRIDE extends the confidentiality, integrity, and availability model and utilizes six categories that are either threat- or attacker-centric.

The STRIDE approach evaluates the three predominant threat types in this environment (tampering, denial of service, and information disclosure) for each technology and, if appropriate, assigns a threat level (low, medium, high) to each. The assessment resulted in the assignment of threat levels summarized in Table ES-2.

Table ES-2. HEAVENS Methodology – Truck Stop Cybersecurity Results

Use Case #	Asset	STRIDE Threat Type	HEAVENS Security Level
1	Wi-Fi/Internet	Denial of Service	High
2		Information Disclosure	High
3	Refueling Technologies	Denial of Service	High
4		Tampering	Medium
5	Anti-Idling/Electrification	Denial of Service	High
6		Information Disclosure	High
7		Tampering	Low
8	Weigh Station Equipment	Information Disclosure	Low
9		Tampering	Low
10	EVSE	Denial of Service	Medium
11		Information Disclosure	Medium
12		Tampering	Medium
13	Parking Availability Systems	Tampering	High
14	ELD Support Equipment	Information Disclosure	Low
15		Tampering	Low
16	Payment Systems	Tampering	High
17		Information Disclosure	High
18	Video Surveillance	Denial of Service	High
19		Information Disclosure	Low

Cybersecurity Best Practices

Using the results from the cybersecurity assessment, the research study recommended cybersecurity best practices for truck stop operators and truck stop technology vendors. The recommended best practices were derived from the Center for Internet Security's 18 controls [3]:

1. Inventory and Control of Enterprise Assets
2. Inventory and Control of Software Assets
3. Data Protection
4. Secure Configuration of Enterprise Assets and Software
5. Account Management
6. Access Control Management
7. Continuous Vulnerability Management
8. Audit Log Management
9. Email and Web Browser Protections
10. Malware Defenses
11. Data Recovery
12. Network Infrastructure Management
13. Network Monitoring and Defense
14. Security Awareness and Skills Training
15. Service Provider Management
16. Application Software Security
17. Incident Response Management
18. Penetration Testing

The 18 controls were reviewed and applied to the truck stop technologies enumerated in this report. In particular, they are customized for three different types of operations:

- Best Practices for Small Truck Stops and Rest Areas
- Recommendations for Large Truck Stop Operators
- Recommendations for Truck Stop Technology Vendors

1. Introduction

1.1 Background Information

The American Trucking Associations estimates that trucks transported 71.4 percent of domestic freight in 2018. The Federal Motor Carrier Safety Administration (FMCSA) develops data-driven regulations to balance the safety and efficiency of trucks throughout the United States. One of these regulations is FMCSA's Hours-of-Service that aims to prevent fatigued drivers from operating their vehicles on the road, which may lead to crashes. The regulation limits when and how long truck drivers may drive to ensure they are alert when operating their vehicle and to reduce the possibility of truck drivers driving fatigued.

When truck drivers reach their regulated amount of driving hours, they can stop at truck stops to rest. Some truck stops may have modern amenities, such as Wi-Fi and electric vehicle charging stations with information technology (IT) components. However, these IT components may carry a cybersecurity risk that has the potential to disrupt commerce.

The United States Department of Transportation (DOT) Volpe National Transportation Systems Center has conducted a research study, in conjunction with FMCSA and the Intelligent Transportation Systems Joint Program Office, which identified and evaluated the possible cybersecurity risk of truck stop technologies. This report presents the results of this research study, titled "Cybersecurity Assessment and Best Practices for Truck Stop Technologies".

1.2 Research Objectives

This research study has two main objectives:

1. Identify current and emerging truck stop technologies and assess their cybersecurity risks.
2. Recommend cybersecurity best practices for truck stop operators and their technology providers based on these assessments.

This study does not consider the potential effects of truck stop technologies on truck operations.

In order to identify common truck stop technologies, this study involved an open-source internet scan and interviews with both truck stop operators and truck stop technology vendors, and state DOTs. This was followed by a cybersecurity analysis of those technologies and recommendations of cybersecurity best practices for truck stop operators and truck stop technology vendors.

1.3 Report Content

This report contains the following sections:

- Section 2: Truck Stop Technology Scan
- Section 3: Truck Stop Stakeholder Feedback
- Section 4: Cybersecurity Analysis
- Section 5: Truck Stop Cybersecurity Best Practices

Sections 2 and 3 address information gathering of truck stop technologies via an open-source internet scan and interviews. Section 4 deals with cybersecurity analysis and assessment. Finally, Section 5 addresses best practices for small truck stops and rest areas, larger truck stops, and truck stop technology vendors.

2. Truck Stop Technology Scan

An open-source internet scan identified truck stop technologies, including critical applications or systems that could compromise the cybersecurity and safety of trucks and truck drivers. Specifically, the scan focused on technologies that could have cybersecurity implications, including:

- Wi-Fi Communications/Network
- Gas Pumps and Automatic Tank Gauges (ATGs)
- Anti-Idling Systems/Truck Stop Electrification (TSE)
- Electric Vehicle Supply Equipment (EVSE)
- Truck Parking Availability Systems
- Weigh Stations
- Payment Systems
- Video Surveillance
- IT Enterprise Infrastructure

Each technology is described by its technology maturity level, connection type, and potential cybersecurity criticality. A technology's maturity level is assessed as either a current technology in use or an emerging technology being looked into or tested at truck stops. A technology's connection type describes what important systems the technology may be connected to at the truck stops. A technology's criticality is based on its importance for a truck stop to function. If the technology is important for the truck stop's operation or a cyber-attack steals or compromises important information from the technology, then it is deemed critical. Otherwise, it is considered noncritical.

The technologies described in the following sections contain information found during the internet scan.

2.1 Wi-Fi Communications/Network

Technology Maturity: Current
Connections: Internet via truck stop infrastructure
Criticality: Critical for truck stops, but noncritical for customers.

There can be up to three different types of networks at a truck stop:

- Guest network for truck drivers in which guests/customers may use the internet for personal matters.
- Truck stop technology vendor network in which technologies provided by truck stop technology vendors communicate back to their own network or to another service or system.
- Truck stop operator network in which the truck stop operator's equipment, such as IT systems, communicate.

Truck drivers may choose to access the guest network via a Wi-Fi access point in order to minimize

cellular data use. Truck stop technology vendors may connect their technologies to the internet on a separate network from the truck stop. Truck stop operators may have a dedicated network for their own employees and IT systems. Some truck stops may only have one network for the combined use of truck stop operators, technology vendors, and truck drivers.

2.2 Gas Pumps and Automatic Tank Gauges

Technology Maturity: Current
Connection: Internet via truck stop infrastructure
Criticality: Critical

Truck drivers refuel at truck stop gas pumps. Attackers can attach credit card skimmers to gas pump payment devices.

ATGs monitor the fuel level in the tanks that feed the gas pumps. ATGs also monitor the fuel tanks for leaks. Some ATGs connect to the internet to provide truck stop operators with current data regarding fuel sales and remaining inventory.

2.3 Anti-Idling Systems/Truck Stop Electrification

Technology Maturity: Current and Emerging
Connections: Internet via truck stop infrastructure
Criticality: Critical

Anti-idling systems are TSE facilities that provide heating, ventilation, and air conditioning, power, internet, and other amenities directly to the truck, allowing operators to turn off their engines when parked while remaining powered and connected. There are two types of anti-idling systems:

- Single-system electrification
- Dual-system electrification

Single-systems use only off-board equipment to provide the amenities. The off-board equipment is typically mounted at the window of the truck to provide its amenities. Dual-systems require off-board and onboard equipment to provide the amenities. The onboard equipment must be pre-installed on the truck.

2.4 Electric Vehicle Supply Equipment

Technology Maturity: Emerging (with sparse current use)
Connections: Internet to back-end servers via truck stop infrastructure, electrical grid, and electric trucks
Criticality: Critical

EVSE and extreme fast chargers (XFCs) essentially "refuel" electric vehicles. EVSEs and XFCs typically have connections to their back-end systems via the internet. They also connect directly to the electrical grid and the trucks themselves. EVSE for passenger vehicles generally charge at a rate of about 3 kilowatts to 19 kilowatts with Level 2 charging or at a rate of 50 kilowatts to 350 kilowatts with direct current fast charge. Trucks will use XFCs as they charge at a rate of 300 kilowatts to 1 megawatt.

As there are relatively few electric trucks in service, EVSE technology is not currently widespread at truck stops. It is possible that truck stops may also install EVSEs for passenger cars for public use in the near future.

2.5 Truck Parking Availability Systems

Technology Maturity: Current
Connections: Internet via truck stop infrastructure
Criticality: Critical

Truck parking availability systems inform truck drivers about current parking availability at truck stops. These systems use sensors such as cameras to identify unused parking spots. They relay their information to operators via signage, smart phone applications, and/or web portals. Truck parking availability systems employ an internet connection to provide the information to truck drivers. Some private truck stop operators also use parking availability systems to offer reserved parking through a mobile application.

Truck parking availability systems are also found in rest areas and are generally managed by individual states.

2.6 Weigh Stations

Technology Maturity: Current
Connections: Internet via truck stop infrastructure or through a cellular connection
Criticality: Noncritical

Weigh stations assess the weight of a truck to ensure it is within legal limits. Most weigh stations are run by a state and found on or near major highways. Some truck stops may have a weigh station to allow drivers and companies to assess their current excess capacity. That is, they allow truck drivers discern how much additional cargo they can legally take on. The information provided to the freight company can be forwarded to various companies that might then buy the remaining capacity for their own cargo.

2.7 Payment Systems

Technology Maturity: Current
Connections: Internet via truck stop infrastructure
Criticality: Critical

Truck drivers use various payment systems for truck stop services. These systems are not unique to truck stop transactions and can include automated teller machines, smart phone applications, contactless credit cards, and retail point-of-sales systems. Most truck stop retail vendors use a separate network for transactions.

Some truck stops use point-to-point encryption for sales transaction. Encryption reduces the likelihood that a man-in-the-middle attack (i.e., an unauthorized user monitors transaction communications) could be used to steal credit card information. Credit card skimming reads credit card information before it is encrypted, so point-to-point encryption does not provide protection against it.

2.8 Video Surveillance Systems

Technology Maturity: Current
Connections: Internet via truck stop infrastructure to back-end server
Criticality: Critical

Many truck stops employ video surveillance for physical security purposes. These systems can be connected via the internet to an off-site physical server or to cloud-based storage. Some systems use closed networks to store videos on-site, so no internet connection is necessary.

2.9 Information Technology Enterprise Infrastructure

Technology Maturity: Current
Connections: Internet via truck stop infrastructure
Criticality: Critical

Truck stops with internet connections have varying degrees of IT infrastructure. Larger truck stop organizations may have a more in-depth IT enterprise infrastructure that includes firewalls, malware protections, local and remote servers, cloud-based services, web portals, and network access controls.

3. Truck Stop Stakeholder Feedback

After conducting the open-source internet scan to determine which technologies are or will soon be present at truck stops, this research study involved interviews with truck stop operators, truck stop technology vendors, state DOTs, and other truck stop stakeholders. The purpose of the interviews was to verify the technologies and assess what cybersecurity measures are used to protect their systems from cyber-attacks.

3.1 Truck Stop Technology Interview Topics

The following topics were discussed during the interviews with truck stop operators, truck stop technology vendors, and state DOTs:

- Prevalence of the following technologies at truck stops:
    - Wi-Fi communications for either infrastructure at a truck stop or its customers
    - Refueling technologies (i.e., gas pumps and ATGs)
    - Anti-idling systems/TSE
    - EVSE
    - Parking availability systems, including phone applications or signage on a road
    - Weigh station equipment
    - Electronic logging device (ELD) support equipment
    - Payment systems
    - Video surveillance
- Usage of the technologies mentioned above by customers
- IT systems utilized at truck stops for the truck stop itself and its customers
- IT infrastructure and cybersecurity standards

The ELD support equipment, as well as phone applications and road signage for parking availability systems, were added to the list of truck stop technologies after conducting initial interviews.

3.2 Truck Stop Technology Interview Responses

The interviewees were asked whether they used specific technologies and if so, how the technologies are operated.

3.2.1 Wi-Fi Communications/Network

Interviewees provided the following information about Wi-Fi Communications and Networks:

- Truck stops provide Wi-Fi communications to provide internet access.
- Third parties often provide Wi-Fi services to drivers separate from the internal network of the truck stop.
- Cellular communications can send parking availability information to backend systems.
- Cellular communications can provide internet access at truck stops.

3.2.2 Gas Pumps and Automatic Tank Gauges

Interviewees provided the following information about gas pumps and ATGs:

- ATG refueling technologies are available at many truck stops.
- New ATGs are generally on private networks behind a firewall.
- ATG systems typically have good physical security, but they do require a network connection.

3.2.3 Anti-Idling Systems/Truck Stop Electrification

Interviewees indicated that anti-idling/TSE systems are no longer operational at some truck stops, but might be brought back in the future.

3.2.4 Electric Vehicle Supply Equipment

Interviewees provided the following information about EVSE:

- A limited number of truck stops have installed EVSE. The industry has conducted internal studies to determine future requirements.
- There are plans to provide public charging facilities.

3.2.5 Parking Availability Systems

Interviewees provided the following information about parking availability systems:

- Some truck drivers use truck parking applications.
- Truck stop parking availability systems have been implemented that count empty stalls using cameras and display the number of empty stalls on signage.
- Some truck stops allow parking spot reservations using a penetration-tested mobile application.
- State data and crowd-sourced data are both used to assess truck parking availability, typically through mobile applications.
- There are ongoing tests of several parking availability technologies and an ongoing review of Concept of Operations (CONOPS) for parking availability systems at rest stops.
- A truck parking management platform uses smart road signs with a mobile application. The

mobile application provides information on how long a driver may park in a spot, allows the operator to check in and out of parking spaces, and allows the truck parking facility manager to monitor their spaces.

- Transponders are sometimes used to inform truck stop operators of trucks entering the facility.

3.2.6 Weigh Stations

Interviewees provided the following information about weigh stations:

- Some truck stops operate weigh stations, often connected to dedicated vendor networks.
- State-run weigh stations often use a closed and interconnected communications ring with dedicated servers.
- Some states have transitioned to mobile weighing equipment deployed by law enforcement.

3.2.7 Electronic Logging Device Support Equipment

The interviews with various truck stop operators and technology vendors provided no evidence that ELD support equipment (e.g., for data uploads or update downloads) were used at a significant number of truck stops.

3.2.8 Payment Systems

Interviewees provided the following information about payment systems:

- Payment for gas or retail transactions is generally via credit cards that are inherently protected by end-to-end encryption.
- Truck stop operators typically use good IT practices (e.g., data backup, regular physical checks for credit card skimmers) for their payment systems.
- Some stakeholders volunteered that they are compliant with the Payment Card Industry Data Security Standard (PCI DSS). [Note: No specific protocols were reviewed in this study.]

3.2.9 Video Surveillance

Interviewees provided the following information about video surveillance:

- Cameras connected to an internal network are often used for video surveillance and loss prevention.
- Video surveillance is also used to verify the data integrity of parking availability systems. Video feeds (e.g., with internet protocol (IP) cameras) may be available to the public via the internet.

3.2.10 Information Technology Systems

Interviewees mentioned that truck stop IT systems can be advanced and comprehensive.

3.3 Truck Stop Cybersecurity Interview Topics

The following topics were discussed during the interview to gather information about truck stop cybersecurity:

- Cybersecurity practices used at truck stops for each truck stop technology and IT technology
- Current and planned implementation of cybersecurity technologies at truck stops
- Associations or organizations looking into cybersecurity at truck stops

3.4 Truck Stop Cybersecurity Interview Responses

Interviewees were asked if they used cybersecurity at truck stops or for their technologies, and how they implemented cybersecurity.

3.4.1 Cybersecurity Practices

Interviewees provided the following information about cybersecurity practices:

- Some truck stops employ multiple cybersecurity frameworks such as the National Institute of Standards and Technology (NIST) Cybersecurity Framework and the Center for Internet Security (CIS) 18 controls. These truck stops may also conduct regular penetration tests on internal systems, external systems, wireless network, and/or web application.
- Some truck stops employ access management, application segmentation, security policies, data security and encryption, and a respond and recover service.
- Some truck stop payment systems are PCI DSS compliant.
- Some technology vendors perform penetration tests on their products, following best practices for cloud services and employing third-party cybersecurity assistance.
- State DOT IT departments are often responsible for the cybersecurity of systems and technologies at rest areas. Thus, parking availability system specifications for those rest areas often include specific cybersecurity requirements.
- Systems designers typically conduct risk assessments on the parking availability systems. The CONOPS for parking availability systems inherently contain high-level cybersecurity requirements. Clients can specify their own cybersecurity requirements for parking availability systems.

3.4.2 Cybersecurity Technologies

Interviewees provided the following information about cybersecurity technologies:

- Truck stops often use cybersecurity technologies such as network firewalls, intrusion prevention systems (IPS) (i.e., an automated system that monitors and blocks suspicious activities), intrusion detection systems (IDS) (i.e., an automated system that monitors for suspicious activities), vulnerability and patch management systems (i.e., a system for finding, reporting,

and responding to vulnerabilities by applying software updates to address vulnerabilities), security log monitoring, configuration management systems (i.e., a system that manages various IT services), and point-to-point encryption.

- Some truck stops employ anti-virus software, secure web gateways (i.e., filters unauthorized network traffic from the network), and application whitelisting (i.e., allowing access only to pre-approved software applications).
- Technology vendors typically offer IDS, firewalls, and anti-virus software to their clients.
- Technology vendors may use firewalls, private IPs over a private cloud, endpoint detection and response (i.e., automated system that monitors, analyzes, and responds to cybersecurity threats), IPS and IDS on their servers, and encryption on their network traffic.

4. Cybersecurity Analysis

This research study included a cybersecurity analysis on the technologies identified in the open-source internet scan and in interviews with truck stop stakeholders. The methodology utilized in this study is Volvo's Healing Vulnerabilities to Enhance Software Security and Safety (HEAVENS) Risk Analysis Methodology. The HEAVENS Risk Analysis Methodology was chosen because it can derive security requirements for different technologies and systems, and accounts for the safety, financial, and operational impact of a cyber-attack.

4.1 HEAVENS Risk Analysis Methodology Background

The HEAVENS methodology focuses on the systems, attackers, and cybersecurity threats. Volvo developed HEAVENS in 2017 as a generic model designed to map threats to security attributes and objectives [1]. The methodology is closely aligned with cybersecurity industry standards that are listed in Table 4-1:

Table 4-1. Cybersecurity Industry Standards

Industry Standard	Use
Common Criteria	Standard for IT security evaluation
Common Vulnerability Scoring System	Open and standardized method for rating IT vulnerabilities
Operationally Critical Threat, Asset, and Vulnerability Evaluation	Approach to assess an organization's information security needs
Open Web Application Security Project	Risk rating methodology suitable for web application security
European Telecommunications Standards Institute Threat Vulnerability and Risk Analysis	Threat, vulnerability and risk analysis methodology for the telecommunications industry
Microsoft's Spoofing, Tampering, Repudiation, Information disclosure, Denial of service, Elevations of privilege (STRIDE) Threat Model	Threat modeling and risk assessment for software
European Union's E-safety Vehicle Intrusion Protected Applications	Risk rating approach for automotive industry, focused on passenger cars and is attack centric

HEAVENS uses Microsoft's STRIDE categories to define the types of threats a system may encounter [1]. STRIDE extends the confidentiality, integrity, and availability (CIA) model and utilizes six categories that are either threat or attacker centric.

Table 4-2 lists the STRIDE categories.

Table 4-2. Microsoft's STRIDE Categories [1][2]

STRIDE Categories	Description	Security Attributes
Spoofing	Attackers pretend to be someone or something else	Authenticity, Freshness
Tampering	Attackers change data either in transit or in storage	Integrity
Repudiation	Attackers actions cannot be traced back to them	Non-repudiation
Information disclosure	Attackers gain access to data either in transit or in storage	Confidentially, Privacy
Denial of service	Attackers interrupt a system's operation	Availability
Elevation of privilege	Attackers perform actions they are not authorized to perform	Authorization

The HEAVENS methodology establishes a direct link between security attributes and threats [1]. Estimating the technical impacts (such as CIA) on a system provides a threat's impact on items such as safety, privacy and/or legislation, financial, and operational impact.

4.2 Use Cases and Potential Cyberattack Scenarios

Nineteen high-level use cases were developed and analyzed using the HEAVENS methodology for the technologies identified in the truck stop technology scan and in stakeholder interviews. Each use case contains a description of an attack, entry point, method of access, and its potential effects.

4.2.1 Wi-Fi/Internet

Use Case 1: Denial of Service

Description:	An attacker prevents truck drivers (customers) or truck stop operators from accessing the internet.
Entry Point(s):	Wi-Fi access point or internet
Method of Access:	Connecting to the Wi-Fi directly or remote access via the internet
Potential Effects:	Truck drivers who prefer using the truck stop's Wi-Fi/internet rather than their own cellular service (which may cost money) may be inconvenienced. Truck drivers may leave the truck stop to find another one with working internet services rather than remain at the current truck stop. If the same internet is used by the truck stop operator, any services at the truck stop requiring internet access will not be functional. If

services are not functioning, the truck stop will be inoperable.

Use Case 2: Information Disclosure

Description:	An attacker steals information from truck drivers or truck stop operators.
Entry Point(s):	Wi-Fi access point or internet
Method of Access:	Connecting to the Wi-Fi directly, remote access via the internet, or creation a rogue Wi-Fi access point
Potential Effects:	If the truck drivers or truck stop operators are sending sensitive information via the internet, their information may be stolen. Stolen sensitive information, such as payment or system login information, can hinder the truck drivers and truck stop operators from performing their duties as they try to resolve their data breach.

4.2.2 Refueling Technologies

Use Case 3: Denial of Service

Description:	An attacker prevents information about fuel levels from being sent to truck stop operators and prevents remote access to ATG maintenance ports.
Entry Point(s):	Internet
Method of Access:	Remote access via the internet
Potential Effects:	Truck stop operators will not be able to remotely check their fuel levels, and/or ATGs will be unable to warn truck stop operators of any issues with the fuel tank. If the fuel tank has a leak, truck stop operators will lose money as they are unable to provide fuel to trucks and may have to pay a fine or clean up services for any leaked fuel.

Use Case 4: Tampering

Description:	An attacker alters the fuel level information sent to the truck stop operator.
Entry Point(s):	Internet
Method of Access:	Remote access via the internet
Potential Effects:	Truck stop operators may believe their ATGs are fully functional. If the fuel level is inaccurately reported as empty, the truck stop operator may temporarily close the truck stop as they refuel. If the fuel level is inaccurately reported as full, the attacker might steal fuel from the fuel tank (barring no other security measure). Either of these two scenarios could cause the truck stop operator to suffer financially.

4.2.3 Anti-Idling/Electrification

Use Case 5: Denial of Service

Description:	An attacker prevents truck drivers from using anti-idling/electrification systems such as internet, power, air conditioning, heat, etc.
Entry Point(s):	Anti-Idling/electrification system or internet
Method of Access:	Connected to the anti-idling/electrification system or remote access via the internet
Potential Effects:	Truck drivers who use anti-idling/electrification systems may be inconvenienced, especially if they paid for such services. Truck drivers may leave truck stop for another truck stop with an operational anti-idling/electrification system.

Use Case 6: Information Disclosure (Specifically the Internet Access)

Description:	An attacker steals information from truck drivers while using the anti-idling/electrification system's internet.
Entry Point(s):	Anti-Idling/electrification system or internet
Method of Access:	Connected to the anti-idling/electrification system or remote access via the internet
Potential Effects:	If truck drivers are sending sensitive information via the internet using the anti-idling/electrification systems, their information may be stolen. Sensitive information, such as payment or system login information being stolen can hinder the truck drivers.

Use Case 7: Tampering (Specifically the Electrification System)

Description:	An attacker alters the anti-idling/electrification system so the truck is either not being completely charged or being over-charged.
Entry Point(s):	Anti-Idling/electrification system, or internet
Method of Access:	Connected to the anti-idling/electrification system or remote access via the internet
Potential Effects:	The truck may not operate if the driver is unintentionally using the truck's electrical system rather than the nonfunctioning anti-idling/electrification system or if the truck's battery is overcharged and damaged. These situations could temporarily disable the truck in order to charge or replace the battery.

4.2.4 Weight Station Equipment

Use Case 8: Information Disclosure

Description:	An attacker steals weight data from weigh station users.
Entry Point(s):	Internet
Method of Access:	Remote access via the internet
Potential Effects:	Attackers may access proprietary or confidential information about freight shipments.

Use Case 9: Tampering

Description:	An attacker or truck driver alters the truck's reported weight with the weigh station system to bypass legal requirements.
Entry Point(s):	Internet
Method of Access:	Remote access via the internet
Potential Effects:	If an attacker alters the truck's reported weight at a weigh station, it could allow the truck driver to violate regulations. Overweight trucks may be more likely to be involved in serious crashes or damage roads/bridges.

4.2.5 Electric Vehicle Supply Equipment

Use Case 10: Denial of Service

Description:	An attacker prevents the EVSE from operating.
Entry Point(s):	EVSE or internet
Method of Access:	Physical access to the EVSE, hacked over-the-air update mechanism of EVSE or remote access via the internet
Potential Effects:	Electric truck drivers might be unable to safely charge their vehicle. If there are no other EVSEs nearby, the truck could be stranded.

Use Case 11: Information Disclosure

Description:	An attacker steals payment information from truck drivers using the EVSE.
Entry Point(s):	EVSE or internet
Method of Access:	Physical access to the EVSE or remote access via the internet
Potential Effects:	The truck driver truck operator may need to spend time to remove fraudulent charges from their compromised credit card. It will also require the truck driver to get new payment information, which may lead to some downtime for the truck driver.

Use Case 12: Tampering

Description:	An attacker alters the EVSE's charge rate resulting in an undercharged or overcharged electric truck
Entry Point(s):	EVSE or internet
Method of Access:	Physical access to the EVSE or remote access via the internet
Potential Effects:	If an attacker alters the EVSE's charge rate, the truck may be delayed, may have a reduced range, possibly leading to a disabled truck, or may induce damage to the battery, potentially leading to an unsafe condition or a time-consuming process to replace the battery.

4.2.6 Parking Availability System

Use Case 13: Tampering

Description:	An attacker alters the parking availability's information to provide incorrect data regarding available parking spaces for truck drivers.
Entry Point(s):	Internet
Method of Access:	Remote access via the internet
Potential Effects:	Incorrect parking availability information may have operational impacts for truck drivers who need to make on time deliveries of critical items. If a truck driver is informed that the truck stop has spaces but the truck stop is actually full, the truck driver will waste time and fuel looking for space before having to leave and find another truck stop. If truck drivers are told that the truck stop is full when it is not, truck drivers will bypass the truck stop in search of another. Both scenarios may prolong truck driver shifts beyond legal limits and could cause financial loss, and may cause major disruptions to heavily traveled corridors if trucks are backed onto the highway.

4.2.7 Electronic Logging Device Support Equipment

Use Case 14: Information Disclosure

Description:	An attacker steals information about the truck and/or truck driver through the ELD support equipment.
Entry Point(s):	ELD support equipment or internet
Method of Access:	Physical hacking of ELD support equipment or remote access via internet
Potential Effects:	The attack would compromise sensitive personal, operational, and/or cargo data, including contents, locations, route, and time sensitivity. This may facilitate cargo tracking and possibly theft. It may also be

possible to falsify credentials in order to gain elevated privileges in the device or the system or network it connects to.

Use Case 15: Tampering

Description:	An attacker gains access to the ELD support equipment
Entry Point(s):	ELD support equipment or internet
Method of Access:	Physical hacking of ELD support equipment or remote access via internet
Potential Effects:	If the truck's ELD is connected to the ELD support equipment at the truck stop, a compromised ELD may be able to send arbitrary controller area network messages to the truck, causing it to perform actions that can lead to an accident at the truck stop. The accident may cause operational and financial harm to the truck drivers, truck driver companies, and the truck stop.

4.2.8 Payment Systems

Use Case 16: Tampering

Description:	An attacker installs malware, such as ransomware, onto a truck stop's payment systems, which prevents operators from processing payments.
Entry Point(s):	Internet
Method of Access:	Remotely via internet
Potential Effects:	If payment systems are held hostage via ransomware, truck stop operators will need to either pay the attackers or lose significant revenue while they work with the payment system vendor to regain control of the system. In either case there may be significant financial implications.

Use Case 17: Information Disclosure

Description:	An attacker installs skimming devices on the gas pumps to read truck drivers' credit card information.
Entry Point(s):	Gas pump
Method of Access:	Physical access to the gas pump's payment system
Potential Effects:	Attackers gain access to truck drivers' credit card information and can use it to make fraudulent purchases. The truck drivers or their companies will need to spend time and effort to obtain new credit cards.

4.2.9 Video Surveillance

Use Case 18: Denial of Service

Description:	An attacker prevents truck stop operators from viewing their internet/cloud-based security cameras.
Entry Point(s):	Internet
Method of Access:	Remotely via internet
Potential Effects:	If the video surveillance system can be made inoperable, it may facilitate crimes such as theft at truck stops.

Use Case 19: Information Disclosure

Description:	An attacker views internet/cloud-based video surveillance cameras at a truck stop to identify a particular truck carrying specific items.
Entry Point(s):	Internet
Method of Access:	Remotely via internet
Potential Effects:	Attackers use the truck stop's video surveillance to identify specific trucks. This may allow attackers to track the route and location of specific trucks and facilitate theft or delay of particular cargo.

4.3 HEAVENS Risk Analysis Results

After developing use cases for the truck stop technologies, the HEAVENS methodology was applied to assess the threat level and impact level for each asset. The assets, STRIDE threat type, and security level from the HEAVENS methodology are given in Table 4-3 below.

Table 4-3. HEAVENS Methodology – Truck Stop Cybersecurity Results

Use Case #	Asset	STRIDE Threat Type	HEAVENS Security Level
1	Wi-Fi/Internet	Denial of Service	High
2		Information Disclosure	High
3	Refueling Technologies	Denial of Service	High
4		Tampering	Medium
5	Anti-Idling/Electrification	Denial of Service	High
6		Information Disclosure	High
7		Tampering	Low
8	Weigh Station Equipment	Information Disclosure	Low
9		Tampering	Low
10	EVSE	Denial of Service	Medium
11		Information Disclosure	Medium
12		Tampering	Medium
13	Parking Availability Systems	Tampering	High

Use Case #	Asset	STRIDE Threat Type	HEAVENS Security Level
14	ELD Support Equipment	Information Disclosure	Low
15		Tampering	Low
16	Payment Systems	Tampering	High
17		Information Disclosure	High
18	Video Surveillance	Denial of Service	High
19		Information Disclosure	Low

Table 4-4 lists the assets by their most critical HEAVENS security level with the associated STRIDE threat. Note that organizations with broader portfolios of technologies are generally more vulnerable to cyber-attacks.

Table 4-4. Truck Stop Assets by Most Critical HEAVENS Security Level

High	Medium	Low
• Wi-Fi/Internet (Denial of Service and Information Disclosure) • Refueling Technologies (Denial of Service) • Anti-Idling/Electrification (Denial of Service and Information Disclosure) • Parking Availability Systems (Tampering) • Payment Systems (Tampering and Information Disclosure) • Video Surveillance (Denial of Service)	• Refueling Technologies (Tampering) • EVSE (Denial of Service and Information Disclosure)	• Anti-Idling/Electrification (Tampering) • Weigh Station Equipment (Information Disclosure and Tampering) • ELD Support Equipment (Information Disclosure and Tampering) • Video Surveillance (Information Disclosure)

Note that some high-level threats could potentially risk the physical security of the drivers or the cargo.

5. Truck Stop Cybersecurity Best Practices

This section contains cybersecurity best practices for truck stop operators, truck stop technology vendors, and their related groups. The recommendations are based on the information obtained via the interviews and the cybersecurity analysis conducted in Section 4. The information obtained from the interviews and the cybersecurity analysis showed where there are possible cybersecurity gaps at truck stops and for truck stop technologies.

5.1 CIS 18 Controls Overview

The CIS 18 controls were selected to address the cybersecurity gaps for truck stops and truck stop technologies [3]. These CIS 18 controls are mapped to the NIST Cybersecurity Framework's five main functions (Identify, Protect, Detect, Respond, and Recover). The CIS 18 controls are also divided into three main categories based on an organization's size, and IT and cybersecurity expertise. At least two large truck stop operators already use this approach.

The CIS developed the CIS 18 controls using experience and knowledge from real world cyber-attacks to develop defenses for different types of attacks. The authors designed the controls to be a list of recommendations that organizations can follow to strengthen their cybersecurity rather than items they must implement.

The recommended CIS controls are tailored to the size and sophistication of an organization's IT and cybersecurity teams. The document defines three implementation groups:

1. Group 1 is comprised of small to medium size organizations with a main focus on business operations. The security recommendations are designed to prevent general, non-targeted attacks on low sensitivity data using small, home office off-the-shelf hardware and software.
2. Group 2 contains organizations with dedicated employees who are responsible for managing and protecting the organization's IT systems and sensitive data. The security recommendations are designed for a more complex IT system that uses enterprise-grade technology that is installed and managed with specialized expertise.
3. Group 3 contains larger organizations with employees who specialize in different areas of cybersecurity. Organizations with specialized employees generally have sensitive assets, data, and functions. The security recommendations for Group 3 are designed to lessen the impact of targeted attacks, and zero-day attacks. A zero-day attack is a cyber-attack using a vulnerability that the developer has yet to discover and patch.

Each Implementation Group inherits the safeguards from the previous group. That is, Implementation Group 1 is the foundational group, whereas Implementation Group 2 is subject to further

recommendations beyond those inherited from Group 1, and Implementation Group 3 is subject to the recommendations beyond those given for Group 2.

The document defines the following 18 functional controls that provide safeguards for different elements of the organization:

1. Inventory and Control of Enterprise Assets
2. Inventory and Control of Software Assets
3. Data Protection
4. Secure Configuration of Enterprise Assets and Software
5. Account Management
6. Access Control Management
7. Continuous Vulnerability Management
8. Audit Log Management
9. Email and Web Browser Protections
10. Malware Defenses
11. Data Recovery
12. Network Infrastructure Management
13. Network Monitoring and Defense
14. Security Awareness and Skills Training
15. Service Provider Management
16. Application Software Security
17. Incident Response Management
18. Penetration Testing

5.2 CIS 18 Controls Best Practices

This research study determined that members of the truck stop industry generally fall under Implementation Group 1 or 2 as defined in the CIS 18 controls. Therefore, the controls recommended for Implementation Group 3 are not included.

For truck stops, Implementation Group 1 would include small truck stop operators who maintain a small number of truck stops. These operators typically focus on providing services to truck drivers and are not usually concerned about IT systems or cybersecurity. Group 1 also includes rest areas, which are generally managed by state DOTs. Rest areas may use some technologies such as parking availability systems.

Implementation Group 2 would include the larger truck stops operators and their technology vendors. These groups generally have dedicated IT teams. Due to their size, members of Group 2 inherently serve more customers and are more likely to be targeted by cyber-attacks.

5.2.1 Best Practices for Small Truck Stops and Rest Areas

Small truck stop operators and rest areas are considered under Implementation Group 1. Small truck stop operators manage a small number of truck stops and focus on providing goods and services to truck drivers rather than IT systems or cybersecurity risks.

Table 5-1 lists CIS Control 1 recommendations for inventory and control of enterprise assets. Maintaining an inventory of the technologies installed and used at truck stops will inhibit the addition and use of unauthorized technologies that could compromise the cybersecurity of the facility.

A detailed asset inventory list can be created using database software or spreadsheet software. The database/spreadsheet can list each asset (e.g., Wi-Fi access point, gas pumps, EVSEs, payment systems, video cameras, or other technologies) at a truck stop with its serial number, item description, installation location, installation date, if the asset is currently in use, and its manufacturer, vendor and/or owner.

Table 5-1. CIS Control 1 (Inventory and Control of Enterprise Assets) for Small Truck Stops and Rest Areas [3]

Safeguard	Title	Description
1.1	Establish and Maintain Detailed Enterprise Asset Inventory	Establish and maintain an accurate, detailed, and up-to-date inventory of all enterprise assets with the potential to store or process data, to include: end-user devices (including portable and mobile), network devices, non-computing/Internet of Things (IoT) devices, and servers.
1.2	Address Unauthorized Assets	Ensure that a process exists to address unauthorized assets on a weekly basis. The enterprise may choose to remove the asset from the network, deny the asset from connecting remotely to the network, or quarantine the asset.

Table 5-2 lists CIS Control 2 recommendations for inventory and control of software assets. At small truck stops and rest areas, the range of hardware and software in use is not extensive. Operators should know how to periodically verify that only current versions of authorized software are operating on their systems.

Table 5-2. CIS Control 2 (Inventory and Control of Software Assets) for Small Truck Stops and Rest Areas [3]

Safeguard	Title	Description
2.1	Establish and Maintain a Software Inventory	Establish and maintain a detailed inventory of all licensed software installed on enterprise assets.
2.2	Ensure Authorized Software is Currently Supported	Ensure that only currently supported software is designated as authorized in the software inventory for enterprise assets.
2.3	Address Unauthorized Software	Ensure that unauthorized software is either removed from use on enterprise assets or receives a documented exception. Review monthly, or more frequently.

Table 5-3 lists CIS Control 3 recommendations for data protection. Small truck stops and rest areas may process and store data about users of their facilities including payment information, video surveillance,

license plate numbers, or other personally identifiable information. Appropriate protection and disposal of confidential customer data is important.

Table 5-3. CIS Control 3 (Data Protection) for Small Truck Stops and Rest Areas [3]

Safeguard	Title	Description
3.1	Establish and Maintain a Data Management Process	Establish and maintain a data management process. In the process, address data sensitivity, data owner, handling of data, data retention limits, and disposal requirements, based on sensitivity and retention standards for the enterprise.
3.2	Establish and Maintain a Data Inventory	Establish and maintain a data inventory, based on the enterprise's data management process. Inventory sensitive data, at a minimum.
3.3	Configure Data Access Control Lists	Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.
3.4	Enforce Data Retention	Retain data according to the enterprise's data management process. Data retention must include both minimum and maximum timelines.
3.5	Securely Dispose of Data	Securely dispose of data as outlined in the enterprise's data management process. Ensure the disposal process and method are commensurate with the data sensitivity.
3.6	Encrypt Data on End-User Devices	Encrypt data on end-user devices containing sensitive data.

Table 5-4 lists CIS Control 4 recommendations for secure configuration of enterprise assets and software. Proper configuration and management of software at small truck stops and rest areas can help prevent unauthorized access to the systems at the facility. As some components will require access to the facility network, strong network access authorization protocols will strengthen the cybersecurity of the system.

Table 5-4. CIS Control 4 (Secure Configuration of Enterprise Assets and Software) for Small Truck Stops and Rest Areas [3]

Safeguard	Title	Description
4.1	Establish and Maintain a Secure Configuration Process	Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile; non-computing/IoT devices; and servers) and software (operating systems and applications).
4.2	Establish and Maintain a Secure Configuration Process for Network Infrastructure	Establish and maintain a secure configuration process for network devices.
4.3	Configure Automatic Session Locking on Enterprise Assets	Configure automatic session locking on enterprise assets after a defined period of inactivity
4.4	Implement and Manage a Firewall on Servers	Implement and manage a firewall on servers, where supported.
4.5	Implement and Manage a Firewall on End-User Devices	Implement and manage a host-based firewall or port-filtering tool on end-user devices, with a default-deny rule that drops all traffic except those services and ports that are explicitly allowed.
4.6	Securely Manage Enterprise Assets and Software	Securely manage enterprise assets and software.

Safeguard	Title	Description
4.7	Manage Default Accounts on Enterprise Assets and Software	Manage default accounts on enterprise assets and software, such as root, administrator, and other pre-configured vendor accounts.

Table 5-5 lists CIS Control 5 recommendations for account management. Cautious management of customer and employee accounts will help ensure security for the system and, ultimately, individual users. Multi-Factor Authentication (MFA) is a security enhancement that requires the account holder to provide multiple credentials, usually two, to login.

Table 5-5. CIS Control 5 (Account Management) for Small Truck Stops and Rest Areas [3]

Safeguard	Title	Description
5.1	Establish and Maintain an Inventory of Accounts	Establish and maintain an inventory of all accounts managed in the enterprise. The inventory must include both user and administrator accounts.
5.2	Use Unique Passwords	Use unique passwords for all enterprise assets. Best practice implementation includes, at a minimum, an 8-character password for accounts using MFA and a 14-character password for accounts not using MFA.
5.3	Disable Dormant Accounts	Delete or disable any dormant accounts after a period of 45 days of inactivity, where supported.
5.4	Restrict Administrator Privileges to Dedicated Administrator Accounts	Restrict administrator privileges to dedicated administrator accounts on enterprise assets. Conduct general computing activities, such as internet browsing, email, and productivity suite use, from the user's primary, nonprivileged account.
5.5	Establish and Maintain an Inventory of Service Accounts	Establish and maintain an inventory of service accounts. The inventory, at a minimum, must contain department owner, review date, and purpose.
5.6	Centralize Account Management	Centralize account management through a directory or identity service.

Table 5-6 lists CIS Control 6 recommendations for access control management. Access control is an important aspect of account management for both employees and customers. The safeguards listed will help effectively manage account access.

Table 5-6. CIS Control 6 (Access Control Management) for Small Truck Stops and Rest Areas [3]

Safeguard	Title	Description
6.1	Establish an Access Granting Process	Establish and follow a process, preferably automated, for granting access to enterprise assets upon new hire, rights grant, or role change of a user.
6.2	Establish an Access Revoking Process	Establish and follow a process, preferably automated, for revoking access to enterprise assets, through disabling accounts immediately upon termination, rights revocation, or role change of a user. Disabling accounts, instead of deleting accounts, may be necessary to preserve audit trails.
6.3	Require MFA for Externally-Exposed Applications	Require all externally-exposed enterprise or third-party applications to enforce MFA, where supported. Enforcing MFA through a directory service or Single Sign-On (SSO) provider is a satisfactory implementation of this Safeguard.
6.4	Require MFA for Remote Network Access	Require MFA for remote network access.

Safeguard	Title	Description
6.5	Require MFA for Administrative Access	Require MFA for all administrative access accounts, where supported, on all enterprise assets, whether managed on-site or through a third-party provider.

Table 5-7 lists CIS Control 7 recommendations for continuous vulnerability management. A vulnerability management plan and a remediation process are important for any technology or system that is discovered to have or is otherwise susceptible to a vulnerability. Automatic patching of operating systems and application will ease system maintenance and reduce the likelihood of impacts from vulnerabilities.

Table 5-7. CIS Control 7 (Continuous Vulnerability Management) for Small Truck Stops and Rest Areas [3]

Safeguard	Title	Description
7.1	Establish and Maintain a Vulnerability Management Process	Establish and maintain a documented vulnerability management process for enterprise assets. Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.
7.2	Establish and Maintain a Remediation Process	Establish and maintain a risk-based remediation strategy documented in a remediation process, with monthly, or more frequent, reviews.
7.3	Perform Automated Operating System Patch Management	Perform operating system updates on enterprise assets through automated patch management on a monthly, or more frequent, basis.
7.4	Perform Automated Application Patch Management	Perform application updates on enterprise assets through automated patch management on a monthly, or more frequent, basis.

Table 5-8 lists CIS Control 8 recommendations for audit log management. Audit logs are important for managing technologies and systems at a truck stop or rest area. These logs can inform employees if a technology or system is operating normally or if there is an issue that needs to be addressed. Audit logs can also contain information on how employees or guests are using the different systems.

Table 5-8. CIS Control 8 (Audit Log Management) for Small Truck Stops and Rest Areas [3]

Safeguard	Title	Description
8.1	Establish and Maintain an Audit Log Management Process	Establish and maintain an audit log management process that defines the enterprise's logging requirements. At a minimum, address the collection, review, and retention of audit logs for enterprise assets.
8.2	Collect Audit Logs	Collect audit logs. Ensure that logging, per the enterprise's audit log management process, has been enabled across enterprise assets.
8.3	Ensure Adequate Audit Log Storage	Ensure that logging destinations maintain adequate storage to comply with the enterprise's audit log management process.

Table 5-9 lists CIS Control 9 recommendations for email and web browser protections. These recommendations apply specifically to operators who manage their own email systems.

Table 5-9. CIS Control 9 (Email and Web Browser Protections) for Small Truck Stops and Rest Areas [3]

Safeguard	Title	Description
9.1	Ensure Use of Only Fully Supported Browsers and Email Clients	Ensure only fully supported browsers and email clients are allowed to execute in the enterprise, only using the latest version of browsers and email clients provided through the vendor.
9.2	Use Domain Name System (DNS) Filtering Services	Use DNS filtering services on all enterprise assets to block access to known malicious domains.

Table 5-10 lists CIS Control 10 recommendations for malware defenses. Small truck stops and rest areas generally have some technologies or systems that require an internet network connection. Appropriate anti-virus and malware protections can reduce or mitigate many cyber-attacks, such as ransomware.

Table 5-10. CIS Control 10 (Malware Defenses) for Small Truck Stops and Rest Areas [3]

Safeguard	Title	Description
10.1	Deploy and Maintain Anti-Malware Software	Deploy and maintain anti-malware software on all enterprise assets.
10.2	Configure Automatic Anti-Malware Signature Updates	Configure automatic updates for anti-malware signature files on all enterprise assets.
10.3	Disable Autorun and Autoplay for Removable Media	Disable autorun and autoplay auto-execute functionality for removable media.

Table 5-11 lists CIS Control 11 recommendations for data recovery. An effective robust method for backup and recovery of sensitive data can be critical for both protection against cyber-attacks as well as IT equipment malfunctions.

Table 5-11. CIS Control 11 (Data Recovery) for Small Truck Stops and Rest Areas [3]

Safeguard	Title	Description
11.1	Establish and Maintain a Data Recovery Process	Establish and maintain a data recovery process. In the process, address the scope of data recovery activities, recovery prioritization, and the security of backup data.
11.2	Perform Automated Backups	Perform automated backups of in-scope enterprise assets. Run backups weekly, or more frequently, based on the sensitivity of the data.
11.3	Protect Recovery Data	Protect recovery data with equivalent controls to the original data. Reference encryption or data separation, based on requirements.
11.4	Establish and Maintain an Isolated Instance of Recovery Data	Establish and maintain an isolated instance of recovery data. Example implementations include version controlling backup destinations through offline, cloud, or off-site systems or services.

Table 5-12 lists CIS Control 12 recommendations for network infrastructure management. Maintaining and upgrading hardware as necessary to keep network infrastructure up-to-date can inhibit many cyber-attacks as newer versions often fix vulnerabilities in the system.

Table 5-12. CIS Control 12 (Network Infrastructure Management) for Small Truck Stops and Rest Areas [3]

Safeguard	Title	Description
12.1	Ensure Network Infrastructure is Up-to-Date	Ensure network infrastructure is kept up-to-date.

There are no recommended safeguards for Control 13 (Network Monitoring and Defense) for Implementation Group 1.

`

Table 5-13 lists CIS Control 14 recommendations for security awareness and skills training. Regardless of the number and sophistication of operational staff, training staff with privileged access to IT systems about cyber-attacks and good cybersecurity habits is beneficial.

Table 5-13. CIS Control 14 (Security Awareness and Skills Training) for Small Truck Stops and Rest Areas [3]

Safeguard	Title	Description
14.1	Establish and Maintain a Security Awareness Program	Establish and maintain a security awareness program.
14.2	Train Workforce Members to Recognize Social Engineering Attacks	Train workforce members to recognize social engineering attacks, such as phishing, pre-texting, and tailgating.
14.3	Train Workforce Members on Authentication Best Practices	Train workforce members on authentication best practices.
14.4	Train Workforce on Data Handling Best Practices	Train workforce members on how to identify and properly store, transfer, archive, and destroy sensitive data.
14.5	Train Workforce Members on Causes of Unintentional Data Exposure	Train workforce members to be aware of causes for unintentional data exposure.
14.6	Train Workforce Members on Recognizing and Reporting Security Incidents	Train workforce members to be able to recognize a potential incident and be able to report such an incident.
14.7	Train Workforce on How to Identify and Report if Their Enterprise Assets are Missing Security Updates	Train workforce to understand how to verify and report out-of-date software patches or any failures in automated processes and tools.

Safeguard	Title	Description
14.8	Train Workforce on the Dangers of Connecting to and Transmitting Enterprise Data Over Insecure Networks	Train workforce members on the dangers of connecting to, and transmitting data over, insecure networks for enterprise activities.

Table 5-14 lists CIS Control 15 recommendations for service provider management. Maintaining an inventory of IT infrastructure components as well as who installs and services them, will facilitate troubleshooting and repair if the system is under attack or otherwise malfunctions.

Table 5-14. CIS Control 15 (Service Provider Management) for Small Truck Stops and Rest Areas [3]

Safeguard	Title	Description
15.1	Establish and Maintain an Inventory of Service Providers	Establish and maintain an inventory of service providers.

There are no recommended safeguards for Control 16 (Application Software Security) for Implementation Group 1.

Table 5-15 lists CIS Control 17 recommendations for incident response management. No technology or system can be fully protected from cybersecurity incidents. Truck stop operators who control their own IT infrastructure need an incident response plan so that employees know what to do and whom to contact if a cyber-attack or other serious malfunction occurs. If employee responsibilities are clearly delineated in advance, negative impact of a cyber-attack can be greatly reduced.

Table 5-15. CIS Control 17 (Incident Response Management) for Small Truck Stops and Rest Areas [3]

Safeguard	Title	Description
17.1	Designate Personnel to Manage Incident Handling	Designate one key person, and at least one backup, who will manage the enterprise's incident handling process.
17.2	Establish and Maintain Contact Information for Reporting Security Incidents	Establish and maintain contact information for parties that need to be informed of security incidents.
17.3	Establish and Maintain an Enterprise Process for Reporting Incidents	Establish and maintain an enterprise process for the workforce to report security incidents. The process includes reporting timeframe, personnel to report to, mechanism for reporting, and the minimum information to be reported.

There are no recommended safeguards for Control 18 (Penetration Testing) for Implementation Group 1.

5.2.2 Best Practices for Large Truck Stop Operators

Larger truck stop operators fall under Implementation Group 2. They may manage truck stops in multiple states across the country with dedicated IT teams and typically have their own internal networks.

Table 5-16 lists CIS Control 1 recommendations for inventory and control of enterprise assets. Maintaining an inventory of the technologies installed and used at each truck stop in an operator's network will inhibit the addition and use of unauthorized technologies that could compromise the cybersecurity of any facility or the network as a whole. A large network may benefit from automating the inventory process.

Table 5-16. CIS Control 1 (Inventory and Control of Enterprise Assets) for Large Truck Stop Operators [3]

Safeguard	Title	Description
1.1	Establish and Maintain Detailed Enterprise Asset Inventory	Establish and maintain an accurate, detailed, and up-to-date inventory of all enterprise assets with the potential to store or process data, to include: end-user devices (including portable and mobile), network devices, noncomputing/IoT devices, and servers.
1.2	Address Unauthorized Assets	Ensure that a process exists to address unauthorized assets on a weekly basis. The enterprise may choose to remove the asset from the network, deny the asset from connecting remotely to the network, or quarantine the asset.
1.3	Utilize an Active Discovery Tool	Utilize an active discovery tool to identify assets connected to the enterprise's network. Configure the active discovery tool to execute daily, or more frequently.
1.4	Use Dynamic Host Configuration Protocol (DHCP) Logging to Update Enterprise Asset Inventory	Use DHCP logging on all DHCP servers or IP address management tools to update the enterprise's asset inventory.

Table 5-17 lists CIS Control 2 recommendations for inventory and control of software assets. Large truck stop operators may implement a more extensive array of hardware and software. The operator's IT team should regularly verify that only authorized and up-to-date software is running on their systems. Automation of this process may be economically justifiable.

Table 5-17. CIS Control 2 (Inventory and Control of Software Assets) for Large Truck Stop Operators [3]

Safeguard	Title	Description
2.1	Establish and Maintain a Software Inventory	Establish and maintain a detailed inventory of all licensed software installed on enterprise assets.
2.2	Ensure Authorized Software is Currently Supported	Ensure that only currently supported software is designated as authorized in the software inventory for enterprise assets.
2.3	Address Unauthorized Software	Ensure that unauthorized software is either removed from use on enterprise assets or receives a documented exception. Review monthly, or more frequently.
2.4	Utilize Automated Software Inventory Tools	Utilize software inventory tools, when possible, throughout the enterprise to automate the discovery and documentation of installed software.

Safeguard	Title	Description
2.5	Allowlist Authorized Software	Use technical controls, such as application allowlisting, to ensure that only authorized software can execute or be accessed. Reassess bi-annually, or more frequently.
2.6	Allowlist Authorized Libraries	Use technical controls to ensure that only authorized software libraries, such as specific .dll, .ocx, .so, etc., files are allowed to load into a system process.

Table 5-18 lists CIS Control 3 recommendations for data protection. A great deal of sensitive and confidential data is processed and stored at truck stops, and on the operator's network, including payment information, video surveillance, license plate numbers, or other personally identifiable information. Appropriate protection and disposal of confidential customer data is particularly important for larger networks and may justify more elaborate protection such as encryption and data segmentation.

Table 5-18. CIS Control 3 (Data Protection) for Large Truck Stop Operators [3]

Safeguard	Title	Description
3.1	Establish and Maintain a Data Management Process	Establish and maintain a data management process. In the process, address data sensitivity, data owner, handling of data, data retention limits, and disposal requirements, based on sensitivity and retention standards for the enterprise.
3.2	Establish and Maintain a Data Inventory	Establish and maintain a data inventory, based on the enterprise's data management process. Inventory sensitive data, at a minimum.
3.3	Configure Data Access Control Lists	Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.
3.4	Enforce Data Retention	Retain data according to the enterprise's data management process. Data retention must include both minimum and maximum timelines.
3.5	Securely Dispose of Data	Securely dispose of data as outlined in the enterprise's data management process. Ensure the disposal process and method are commensurate with the data sensitivity.
3.6	Encrypt Data on End-User Devices	Encrypt data on end-user devices containing sensitive data.
3.7	Establish and Maintain a Data Classification Scheme	Establish and maintain an overall data classification scheme for the enterprise. Enterprises may use labels, such as "Sensitive," "Confidential," and "Public," and classify their data according to those labels.
3.8	Document Data Flows	Document data flows. Data flow documentation includes service provider data flows and should be based on the enterprise's data management process.
3.9	Encrypt Data on Removable Media	Encrypt data on removable media.
3.10	Encrypt Sensitive Data in Transit	Encrypt sensitive data in transit. Example implementations can include: Transport Layer Security (TLS) and Open Secure Shell (OpenSSH).
3.11	Encrypt Sensitive Data at Rest	Encrypt sensitive data at rest on servers, applications, and databases containing sensitive data. Storage-layer encryption, also known as server-side encryption, meets the minimum requirement of this Safeguard.
3.12	Segment Data Processing and Storage Based on Sensitivity	Segment data processing and storage based on the sensitivity of the data. Do not process sensitive data on enterprise assets intended for lower sensitivity data.

Table 5-19 lists CIS Control 4 recommendations for secure configuration of enterprise assets and software. Proper configuration and management of software at truck stops can help prevent

unauthorized access to the systems at the facility. As some components will require access to operator's network, strong network access authorization protocols will strengthen the cybersecurity of the system. This is even more important for access to networks with access to data for multiple facilities.

Table 5-19. CIS Control 4 (Secure Configuration of Enterprise Assets and Software) for Large Truck Stop Operators [3]

Safeguard	Title	Description
4.1	Establish and Maintain a Secure Configuration Process	Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile; non-computing/IoT devices; and servers) and software (operating systems and applications).
4.2	Establish and Maintain a Secure Configuration Process for Network Infrastructure	Establish and maintain a secure configuration process for network devices.
4.3	Configure Automatic Session Locking on Enterprise Assets	Configure automatic session locking on enterprise assets after a defined period of inactivity
4.4	Implement and Manage a Firewall on Servers	Implement and manage a firewall on servers, where supported.
4.5	Implement and Manage a Firewall on End-User Devices	Implement and manage a host-based firewall or port-filtering tool on end-user devices, with a default-deny rule that drops all traffic except those services and ports that are explicitly allowed.
4.6	Securely Manage Enterprise Assets and Software	Securely manage enterprise assets and software.
4.7	Manage Default Accounts on Enterprise Assets and Software	Manage default accounts on enterprise assets and software, such as root, administrator, and other pre-configured vendor accounts.
4.8	Uninstall or Disable Unnecessary Services on Enterprise Assets and Software	Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.
4.9	Configure Trusted DNS Servers on Enterprise Assets	Configure trusted DNS servers on enterprise assets.
4.10	Enforce Automatic Device Lockout on Portable End-User Devices	Enforce automatic device lockout following a predetermined threshold of local failed authentication attempts on portable end-user devices, where supported.
4.11	Enforce Remote Wipe Capability on Portable End-User Devices	Remotely wipe enterprise data from enterprise-owned portable end-user devices when deemed appropriate such as lost or stolen devices, or when an individual no longer supports the enterprise.

Table 5-20 lists CIS Control 5 recommendations for account management. Cautious management of customer and employee accounts will help ensure security for the system and, ultimately, individual users.

Table 5-20. CIS Control 5 (Account Management) for Large Truck Stop Operators [3]

Safeguard	Title	Description
5.1	Establish and Maintain an Inventory of Accounts	Establish and maintain an inventory of all accounts managed in the enterprise. The inventory must include both user and administrator accounts.
5.2	Use Unique Passwords	Use unique passwords for all enterprise assets. Best practice implementation includes, at a minimum, an 8-character password for accounts using MFA and a 14-character password for accounts not using MFA.
5.3	Disable Dormant Accounts	Delete or disable any dormant accounts after a period of 45 days of inactivity, where supported.
5.4	Restrict Administrator Privileges to Dedicated Administrator Accounts	Restrict administrator privileges to dedicated administrator accounts on enterprise assets. Conduct general computing activities, such as internet browsing, email, and productivity suite use, from the user's primary, nonprivileged account.
5.5	Establish and Maintain an Inventory of Service Accounts	Establish and maintain an inventory of service accounts. The inventory, at a minimum, must contain department owner, review date, and purpose.
5.6	Centralize Account Management	Centralize account management through a directory or identity service.

Table 5-21 lists CIS Control 6 recommendations for access control management. Access control to large operator networks is an important aspect of account management for both employees and customers. The safeguards listed will help effectively manage account access.

Table 5-21. CIS Control 6 (Access Control Management) for Large Truck Stop Operators [3]

Safeguard	Title	Description
6.1	Establish an Access Granting Process	Establish and follow a process, preferably automated, for granting access to enterprise assets upon new hire, rights grant, or role change of a user.
6.2	Establish an Access Revoking Process	Establish and follow a process, preferably automated, for revoking access to enterprise assets, through disabling accounts immediately upon termination, rights revocation, or role change of a user. Disabling accounts, instead of deleting accounts, may be necessary to preserve audit trails.
6.3	Require MFA for Externally-Exposed Applications	Require all externally-exposed enterprise or third-party applications to enforce MFA, where supported. Enforcing MFA through a directory service or SSO provider is a satisfactory implementation of this Safeguard.
6.4	Require MFA for Remote Network Access	Require MFA for remote network access.
6.5	Require MFA for Administrative Access	Require MFA for all administrative access accounts, where supported, on all enterprise assets, whether managed on-site or through a third-party provider.
6.6	Establish and Maintain an Inventory of Authentication and Authorization Systems	Establish and maintain an inventory of the enterprise's authentication and authorization systems, including those hosted on-site or at a remote service provider.
6.7	Centralize Access Control	Centralize access control for all enterprise assets through a directory service or SSO provider, where supported.
6.8	Define and Maintain Role-Based Access Control	Define and maintain role-based access control, through determining and documenting the access rights necessary for each role within the enterprise to successfully carry out its assigned duties.

Table 5-22 lists CIS Control 7 recommendations for continuous vulnerability management. A vulnerability management plan and a remediation process are important for any technology or system that is discovered to have or is otherwise susceptible to a vulnerability. Automatic patching of operating systems and applications will ease system maintenance and reduce the likelihood of impacts from vulnerabilities.

Table 5-22. CIS Control 7 (Continuous Vulnerability Management) for Large Truck Stop Operators [3]

Safeguard	Title	Description
7.1	Establish and Maintain a Vulnerability Management Process	Establish and maintain a documented vulnerability management process for enterprise assets. Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.
7.2	Establish and Maintain a Remediation Process	Establish and maintain a risk-based remediation strategy documented in a remediation process, with monthly, or more frequent, reviews.
7.3	Perform Automated Operating System Patch Management	Perform operating system updates on enterprise assets through automated patch management on a monthly, or more frequent, basis.
7.4	Perform Automated Application Patch Management	Perform application updates on enterprise assets through automated patch management on a monthly, or more frequent, basis.
7.5	Perform Automated Vulnerability Scans of Internal Enterprise Assets	Perform automated vulnerability scans of internal enterprise assets on a quarterly, or more frequent, basis. Conduct both authenticated and unauthenticated scans, using a Security Content Automation Protocol (SCAP)-compliant vulnerability scanning tool.
7.6	Perform Automated Vulnerability Scans of Externally-Exposed Enterprise Assets	Perform automated vulnerability scans of externally-exposed enterprise assets using a SCAP-compliant vulnerability scanning tool. Perform scans on a monthly, or more frequent, basis.
7.7	Remediate Detected Vulnerabilities	Remediate detected vulnerabilities in software through processes and tooling on a monthly, or more frequent, basis, based on the remediation process.

Table 5-23 lists CIS Control 8 recommendations for audit log management. Audit logs are important for managing technologies and systems at a truck stop. These logs can inform employees if a technology or system is operating normally or if there is an issue that needs to be addressed. Audit logs can also contain information on how employees or guests are using the different systems.

Table 5-23. CIS Control 8 (Audit Log Management) for Large Truck Stop Operators [3]

Safeguard	Title	Description
8.1	Establish and Maintain an Audit Log Management Process	Establish and maintain an audit log management process that defines the enterprise's logging requirements. At a minimum, address the collection, review, and retention of audit logs for enterprise assets.
8.2	Collect Audit Logs	Collect audit logs. Ensure that logging, per the enterprise's audit log management process, has been enabled across enterprise assets.
8.3	Ensure Adequate Audit Log Storage	Ensure that logging destinations maintain adequate storage to comply with the enterprise's audit log management process.
8.4	Standardize Time Synchronization	Standardize time synchronization. Configure at least two synchronized time sources across enterprise assets, where supported.
8.5	Collect Detailed Audit Logs	Configure detailed audit logging for enterprise assets containing sensitive data. Include event source, date, username, timestamp, source addresses, destination addresses, and other useful elements that could assist in a forensic investigation.

Safeguard	Title	Description
8.6	Collect DNS Query Audit Logs	Collect DNS query audit logs on enterprise assets, where appropriate and supported.
8.7	Collect Uniform Resource Locator (URL) Request Audit Logs	Collect URL request audit logs on enterprise assets, where appropriate and supported.
8.8	Collect Command-Line Audit Logs	Collect command-line audit logs. Example implementations include collecting audit logs from PowerShell®, BASH™, and remote administrative terminals.
8.9	Centralize Audit Logs	Centralize, to the extent possible, audit log collection and retention across enterprise assets.
8.10	Retain Audit Logs	Retain audit logs across enterprise assets for a minimum of 90 days.
8.11	Conduct Audit Log Reviews	Conduct reviews of audit logs to detect anomalies or abnormal events that could indicate a potential threat. Conduct reviews on a weekly, or more frequent, basis.

Table 5-24 lists CIS Control 9 recommendations for email and web browser protections. These recommendations apply specifically to operators who manage their own email systems. Ensuring that the email services are filtered and supported can prevent attackers from gaining access to internal or otherwise confidential email messages.

Table 5-24. CIS Control 9 (Email and Web Browser Protections) for Large Truck Stop Operators [3]

Safeguard	Title	Description
9.1	Ensure Use of Only Fully Supported Browsers and Email Clients	Ensure only fully supported browsers and email clients are allowed to execute in the enterprise, only using the latest version of browsers and email clients provided through the vendor.
9.2	Use DNS Filtering Services	Use DNS filtering services on all enterprise assets to block access to known malicious domains.
9.3	Maintain and Enforce Network-Based URL Filters	Enforce and update network-based URL filters to limit an enterprise asset from connecting to potentially malicious or unapproved websites.
9.4	Restrict Unnecessary or Unauthorized Browser and Email Client Extensions	Restrict, either through uninstalling or disabling, any unauthorized or unnecessary browser or email client plugins, extensions, and add-on applications.
9.5	Implement Domain-based Message Authentication, Reporting, and Conformance (DMARC)	To lower the chance of spoofed or modified emails from valid domains, implement DMARC policy and verification, starting with implementing the Sender Policy Framework (SPF) and the DomainKeys Identified Mail (DKIM) standards.
9.6	Block Unnecessary File Types	Block unnecessary file types attempting to enter the enterprise's email gateway.

Table 5-25 lists CIS Control 10 recommendations for malware defenses. Truck stops generally have technologies and systems that require an internet network connection. Appropriate anti-virus and malware protections can reduce or mitigate many cyber-attacks, such as ransomware. Configuration management should be used to inhibit unauthorized access.

Table 5-25. CIS Control 10 (Malware Defenses) for Large Truck Stop Operators [3]

Safeguard	Title	Description
10.1	Deploy and Maintain Anti-Malware Software	Deploy and maintain anti-malware software on all enterprise assets.
10.2	Configure Automatic Anti-Malware Signature Updates	Configure automatic updates for anti-malware signature files on all enterprise assets.
10.3	Disable Autorun and Autoplay for Removable Media	Disable autorun and autoplay auto-execute functionality for removable media.
10.4	Configure Automatic Anti-Malware Scanning of Removable Media	Configure anti-malware software to automatically scan removable media.
10.5	Enable Anti-Exploitation Features	Enable anti-exploitation features on enterprise assets and software, where possible.
10.6	Centrally Manage Anti-Malware Software	Centrally manage anti-malware software.
10.7	Use Behavior-Based Anti-Malware Software	Use behavior-based anti-malware software.

Table 5-26 lists CIS Control 11 recommendations for data recovery. An effective robust method for backup and recovery of sensitive data can be critical for both protection against cyber-attacks as well as IT equipment malfunctions. Regular backup testing is recommended for large and complex networks.

Table 5-26. CIS Control 11 (Data Recovery) for Large Truck Stop Operators [3]

Safeguard	Title	Description
11.1	Establish and Maintain a Data Recovery Process	Establish and maintain a data recovery process. In the process, address the scope of data recovery activities, recovery prioritization, and the security of backup data.
11.2	Perform Automated Backups	Perform automated backups of in-scope enterprise assets. Run backups weekly, or more frequently, based on the sensitivity of the data.
11.3	Protect Recovery Data	Protect recovery data with equivalent controls to the original data. Reference encryption or data separation, based on requirements.
11.4	Establish and Maintain an Isolated Instance of Recovery Data	Establish and maintain an isolated instance of recovery data. Example implementations include version controlling backup destinations through offline, cloud, or off-site systems or services.
11.5	Test Data Recovery	Test backup recovery quarterly, or more frequently, for a sampling of in-scope enterprise assets.

Table 5-27 lists CIS Control 12 recommendations for network infrastructure management. Maintaining and upgrading hardware and software as necessary to keep network infrastructure up-to-date can inhibit many cyber-attacks as newer versions often fix vulnerabilities in the system.

Table 5-27. CIS Control 12 (Network Infrastructure Management) for Large Truck Stop Operators [3]

Safeguard	Title	Description
12.1	Ensure Network Infrastructure is Up-to-Date	Ensure network infrastructure is kept up-to-date.

Safeguard	Title	Description
12.2	Establish and Maintain a Secure Network Architecture	Establish and maintain a secure network architecture.
12.3	Securely Manage Network Infrastructure	Securely manage network infrastructure.
12.4	Establish and Maintain Architecture Diagram(s)	Establish and maintain architecture diagram(s) and/or other network system documentation.
12.5	Centralize Network Authentication, Authorization, and Auditing (AAA)	Centralize network AAA.
12.6	Use of Secure Network Management and Communication Protocols	Use secure network management and communication protocols (e.g., 802.1X, Wi-Fi Protected Access 2 (WPA2) Enterprise or greater).
12.7	Ensure Remote Devices Utilize a VPN and are Connecting to an Enterprise's AAA Infrastructure	Require users to authenticate to enterprise-managed VPN and authentication services prior to accessing enterprise resources on end-user devices.

Table 5-28 lists CIS Control 13 recommendations for network monitoring and defense. Complex networks can benefit from intrusion detection systems, security alerts, and network filtering. An effective IDS can greatly increase the likelihood that a cyber-attack can be mitigated.

Table 5-28. CIS Control 13 (Network Monitoring and Defense) for Large Truck Stop Operators [3]

Safeguard	Title	Description
13.1	Centralize Security Event Alerting	Centralize security event alerting across enterprise assets for log correlation and analysis.
13.2	Deploy a Host-Based Intrusion Detection Solution	Deploy a host-based intrusion detection solution on enterprise assets, where appropriate and/or supported.
13.3	Deploy a Network Intrusion Detection Solution	Deploy a network intrusion detection solution on enterprise assets, where appropriate.
13.4	Perform Traffic Filtering Between Network Segments	Perform traffic filtering between network segments, where appropriate.
13.5	Manage Access Control for Remote Assets	Manage access control for assets remotely connecting to enterprise resources.
13.6	Collect Network Traffic Flow Logs	Collect network traffic flow logs and/or network traffic to review and alert upon from network devices.

Table 5-29 lists CIS Control 14 recommendations for security awareness and skills training. Regardless of the number and sophistication of operational staff, training staff with privileged access IT systems about cyber-attacks and good cybersecurity habits is beneficial.

Table 5-29. CIS Control 14 Security Awareness and Skills Training) for Large Truck Stop Operators [3]

Safeguard	Title	Description
14.1	Establish and Maintain a Security Awareness Program	Establish and maintain a security awareness program.
14.2	Train Workforce Members to Recognize Social Engineering Attacks	Train workforce members to recognize social engineering attacks, such as phishing, pre-texting, and tailgating.
14.3	Train Workforce Members on Authentication Best Practices	Train workforce members on authentication best practices.
14.4	Train Workforce on Data Handling Best Practices	Train workforce members on how to identify and properly store, transfer, archive, and destroy sensitive data.
14.5	Train Workforce Members on Causes of Unintentional Data Exposure	Train workforce members to be aware of causes for unintentional data exposure.
14.6	Train Workforce Members on Recognizing and Reporting Security Incidents	Train workforce members to be able to recognize a potential incident and be able to report such an incident.
14.7	Train Workforce on How to Identify and Report if Their Enterprise Assets are Missing Security Updates	Train workforce to understand how to verify and report out-of-date software patches or any failures in automated processes and tools.
14.8	Train Workforce on the Dangers of Connecting to and Transmitting Enterprise Data Over Insecure Networks	Train workforce members on the dangers of connecting to, and transmitting data over, insecure networks for enterprise activities.
14.9	Conduct Role-Specific Security Awareness and Skills Training	Conduct role-specific security awareness and skills training.

Table 5-30 lists CIS Control 15 recommendations for service provider management. Maintaining an inventory of IT infrastructure components as well as who installs and services them, will facilitate troubleshooting and repair if the system is under attack or otherwise malfunctions.

Table 5-30. CIS Control 15 (Service Provider Management) for Large Truck Stop Operators [3]

Safeguard	Title	Description
15.1	Establish and Maintain an Inventory of Service Providers	Establish and maintain an inventory of service providers.
15.2	Establish and Maintain a Service Provider Management Policy	Establish and maintain a service provider management policy.

Safeguard	Title	Description
15.3	Classify Service Providers	Classify service providers.
15.4	Ensure Service Provider Contracts Include Security Requirements	Ensure service provider contracts include security requirements.

Table 5-31 lists CIS Control 16 recommendations for application software security. Some large truck stop operators have mobile applications that provide information and services about individual locations. These applications should be securely developed and maintained.

Table 5-31. CIS Control 16 (Application Software Security) for Large Truck Stop Operators [3]

Safeguard	Title	Description
16.1	Establish and Maintain a Secure Application Development Process	Establish and maintain a secure application development process.
16.2	Establish and Maintain a Process to Accept and Address Software Vulnerabilities	Establish and maintain a process to accept and address reports of software vulnerabilities, including providing a means for external entities to report.
16.3	Perform Root Cause Analysis on Security Vulnerabilities	Perform root cause analysis on security vulnerabilities.
16.4	Establish and Manage an Inventory of Third-Party Software Components	Establish and manage an updated inventory of third-party components used in development, often referred to as a "bill of materials," as well as components slated for future use.
16.5	Use Up-to-Date and Trusted Third-Party Software Components	Use up-to-date and trusted third-party software components.
16.6	Establish and Maintain a Severity Rating System and Process for Application Vulnerabilities	Establish and maintain a severity rating system and process for application vulnerabilities that facilitates prioritizing the order in which discovered vulnerabilities are fixed.
16.7	Use Standard Hardening Configuration Templates for Application Infrastructure	Use standard, industry-recommended hardening configuration templates for application infrastructure components.
16.8	Separate Production and Non-Production Systems	Maintain separate environments for production and non-production systems.
16.9	Train Developers in Application Security Concepts and Secure Coding	Ensure that all software development personnel receive training in writing secure code for their specific development environment and responsibilities.
16.10	Apply Secure Design Principles in Application Architectures	Apply secure design principles in application architectures.

Safeguard	Title	Description
16.11	Leverage Vetted Modules or Services for Application Security Components	Leverage vetted modules or services for application security components, such as identity management, encryption, and auditing and logging.

Table 5-32 lists CIS Control 17 recommendations for incident response management. No technology or system can be fully protected from cybersecurity incidents. Truck stop operators who control their own IT infrastructure need an incident response plan so that employees know what to do and whom to contact to if a cyber-attack or other serious malfunction occurs. If employee responsibilities are clearly delineated in advance, negative impact of a cyber-attack can be greatly reduced.

Table 5-32. CIS Control 17 (Incident Response Management) for Large Truck Stop Operators [3]

Safeguard	Title	Description
17.1	Designate Personnel to Manage Incident Handling	Designate one key person, and at least one backup, who will manage the enterprise's incident handling process.
17.2	Establish and Maintain Contact Information for Reporting Security Incidents	Establish and maintain contact information for parties that need to be informed of security incidents.
17.3	Establish and Maintain an Enterprise Process for Reporting Incidents	Establish and maintain an enterprise process for the workforce to report security incidents. The process includes reporting timeframe, personnel to report to, mechanism for reporting, and the minimum information to be reported.
17.4	Establish and Maintain an Incident Response Process	Establish and maintain an incident response process that addresses roles and responsibilities, compliance requirements, and a communication plan.
17.5	Assign Key Roles and Responsibilities	Assign key roles and responsibilities for incident response, including staff from legal, IT, information security, facilities, public relations, human resources, incident responders, and analysts, as applicable.
17.6	Define Mechanisms for Communicating During Incident Response	Determine which primary and secondary mechanisms will be used to communicate and report during a security incident. Mechanisms can include phone calls, emails, or letters.
17.7	Conduct Routine Incident Response Exercises	Plan and conduct routine incident response exercises and scenarios for key personnel involved in the incident response process to prepare for responding to real-world incidents.
17.8	Conduct Post-Incident Reviews	Conduct post-incident reviews. Post-incident reviews help prevent incident recurrence through identifying lessons learned and follow-up action.

Table 5-33 lists CIS Control 18 recommendations for penetration testing. Penetration testing is an important method for identifying vulnerabilities in technologies, systems, or networks. Conducting regular penetration tests basis can improve an organization's overall cybersecurity.

Table 5-33. CIS Control 18 (Penetration Testing) for Large Truck Stop Operators [3]

Safeguard	Title	Description
18.1	Establish and Maintain a Penetration Testing Program	Establish and maintain a penetration testing program appropriate to the size, complexity, and maturity of the enterprise.
18.2	Perform Periodic External Penetration Tests	Perform periodic external penetration tests based on program requirements, no less than annually. External penetration testing must include enterprise and environmental reconnaissance to detect exploitable information.
18.3	Remediate Penetration Test Findings	Remediate penetration test findings based on the enterprise's policy for remediation scope and prioritization.

5.2.3 Best Practices for Truck Stop Technology Vendors

Truck stop technology vendors fall under Implementation Group 2 in the CIS controls. The vendors may design, build, install, maintain, and/or write software for these systems. Technology vendors provide the systems to truck stops that may then connect them back to the vendor's own networks. Truck stop technology vendors and truck stop operators should coordinate early on regarding who is responsible for the operation and cybersecurity of each system.

Table 5-34 lists CIS Control 1 recommendations for inventory and control of enterprise assets. Keeping track of the technologies installed and utilized at truck stops will help prevent and remove unauthorized technologies from compromising the cybersecurity of the facility. A list of technologies each vendor installs at a truck stop would help ensure their technology or system is not compromising the truck stop's system.

Table 5-34. CIS Control 1 (Inventory and Control of Enterprise Assets) for Truck Stop Technology Vendors [3]

Safeguard	Title	Description
1.1	Establish and Maintain Detailed Enterprise Asset Inventory	Establish and maintain an accurate, detailed, and up-to-date inventory of all enterprise assets with the potential to store or process data, to include: end-user devices (including portable and mobile), network devices, noncomputing/IoT devices, and servers.
1.2	Address Unauthorized Assets	Ensure that a process exists to address unauthorized assets on a weekly basis. The enterprise may choose to remove the asset from the network, deny the asset from connecting remotely to the network, or quarantine the asset.
1.3	Utilize an Active Discovery Tool	Utilize an active discovery tool to identify assets connected to the enterprise's network. Configure the active discovery tool to execute daily, or more frequently.
1.4	Use DHCP Logging to Update Enterprise Asset Inventory	Use DHCP logging on all DHCP servers or IP address management tools to update the enterprise's asset inventory.

Table 5-35 lists CIS Control 2 recommendations for inventory and control of software assets. Truck stops implement many technologies from different vendors utilizing an assortment of different software. Helping truck stop operators by maintaining a software list for each individual truck stop technology vendor can assist truck stop operators in ensuring their technology is up to date and no unwanted software is installed on any systems.

Table 5-35. CIS Control 2 (Inventory and Control of Software Assets) for Truck Stop Technology Vendors [3]

Safeguard	Title	Description
2.1	Establish and Maintain a Software Inventory	Establish and maintain a detailed inventory of all licensed software installed on enterprise assets.
2.2	Ensure Authorized Software is Currently Supported	Ensure that only currently supported software is designated as authorized in the software inventory for enterprise assets.
2.3	Address Unauthorized Software	Ensure that unauthorized software is either removed from use on enterprise assets or receives a documented exception. Review monthly, or more frequently.
2.4	Utilize Automated Software Inventory Tools	Utilize software inventory tools, when possible, throughout the enterprise to automate the discovery and documentation of installed software.
2.5	Allowlist Authorized Software	Use technical controls, such as application allowlisting, to ensure that only authorized software can execute or be accessed. Reassess bi-annually, or more frequently.
2.6	Allowlist Authorized Libraries	Use technical controls to ensure that only authorized software libraries, such as specific .dll, .ocx, .so, etc., files are allowed to load into a system process.

Table 5-36 lists CIS Control 3 recommendations for data protection. A great deal of sensitive and confidential data is processed and stored at truck stops, and often on the technology vendor's network, including payment information, video surveillance, license plate numbers, or other personally identifiable information. Appropriate protection and disposal of confidential customer data is particularly important for larger networks and may justify more elaborate protection such as encryption and data segmentation.

Table 5-36. CIS Control 3 (Data Protection) for Truck Stop Technology Vendors [3]

Safeguard	Title	Description
3.1	Establish and Maintain a Data Management Process	Establish and maintain a data management process. In the process, address data sensitivity, data owner, handling of data, data retention limits, and disposal requirements, based on sensitivity and retention standards for the enterprise.
3.2	Establish and Maintain a Data Inventory	Establish and maintain a data inventory, based on the enterprise's data management process. Inventory sensitive data, at a minimum.
3.3	Configure Data Access Control Lists	Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.
3.4	Enforce Data Retention	Retain data according to the enterprise's data management process. Data retention must include both minimum and maximum timelines.
3.5	Securely Dispose of Data	Securely dispose of data as outlined in the enterprise's data management process. Ensure the disposal process and method are commensurate with the data sensitivity.
3.6	Encrypt Data on End-User Devices	Encrypt data on end-user devices containing sensitive data.
3.7	Establish and Maintain a Data Classification Scheme	Establish and maintain an overall data classification scheme for the enterprise. Enterprises may use labels, such as "Sensitive," "Confidential," and "Public," and classify their data according to those labels.
3.8	Document Data Flows	Document data flows. Data flow documentation includes service provider data flows and should be based on the enterprise's data management process.
3.9	Encrypt Data on Removable Media	Encrypt data on removable media.

Safeguard	Title	Description
3.10	Encrypt Sensitive Data in Transit	Encrypt sensitive data in transit. Example implementations can include: TLS and OpenSSH.
3.11	Encrypt Sensitive Data at Rest	Encrypt sensitive data at rest on servers, applications, and databases containing sensitive data. Storage-layer encryption, also known as server-side encryption, meets the minimum requirement of this Safeguard.
3.12	Segment Data Processing and Storage Based on Sensitivity	Segment data processing and storage based on the sensitivity of the data. Do not process sensitive data on enterprise assets intended for lower sensitivity data.

Table 5-37 lists CIS Control 4 recommendations for secure configuration of enterprise assets and software. Proper configuration and management of software at truck stops can help prevent unauthorized access to the systems at the facility. As some components may require access to vendor's network, strong network access authorization protocols will strengthen the cybersecurity of the system. This is even more important for access to networks that hold data from multiple facilities.

Table 5-37. CIS Control 4 (Secure Configuration of Enterprise Assets and Software) for Truck Stop Technology Vendors [3]

Safeguard	Title	Description
4.1	Establish and Maintain a Secure Configuration Process	Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile; non-computing/IoT devices; and servers) and software (operating systems and applications).
4.2	Establish and Maintain a Secure Configuration Process for Network Infrastructure	Establish and maintain a secure configuration process for network devices.
4.3	Configure Automatic Session Locking on Enterprise Assets	Configure automatic session locking on enterprise assets after a defined period of inactivity
4.4	Implement and Manage a Firewall on Servers	Implement and manage a firewall on servers, where supported.
4.5	Implement and Manage a Firewall on End-User Devices	Implement and manage a host-based firewall or port-filtering tool on end-user devices, with a default-deny rule that drops all traffic except those services and ports that are explicitly allowed.
4.6	Securely Manage Enterprise Assets and Software	Securely manage enterprise assets and software.
4.7	Manage Default Accounts on Enterprise Assets and Software	Manage default accounts on enterprise assets and software, such as root, administrator, and other pre-configured vendor accounts.
4.8	Uninstall or Disable Unnecessary Services on Enterprise Assets and Software	Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.
4.9	Configure Trusted DNS Servers on Enterprise Assets	Configure trusted DNS servers on enterprise assets.
4.10	Enforce Automatic Device Lockout on Portable End-User Devices	Enforce automatic device lockout following a predetermined threshold of local failed authentication attempts on portable end-user devices, where supported.

Safeguard	Title	Description
4.11	Enforce Remote Wipe Capability on Portable End-User Devices	Remotely wipe enterprise data from enterprise-owned portable end-user devices when deemed appropriate such as lost or stolen devices, or when an individual no longer supports the enterprise.

Table 5-38 lists CIS Control 5 recommendations for account management. The networks for truck stop technology vendors may have accounts for large operators, small operators, numerous customers, as well as employees. Cautious management of customer and employee accounts will help ensure security for the system and, ultimately, individual users.

Table 5-38. CIS Control 5 (Account Management) for Truck Stop Technology Vendors [3]

Safeguard	Title	Description
5.1	Establish and Maintain an Inventory of Accounts	Establish and maintain an inventory of all accounts managed in the enterprise. The inventory must include both user and administrator accounts.
5.2	Use Unique Passwords	Use unique passwords for all enterprise assets. Best practice implementation includes, at a minimum, an 8-character password for accounts using MFA and a 14-character password for accounts not using MFA.
5.3	Disable Dormant Accounts	Delete or disable any dormant accounts after a period of 45 days of inactivity, where supported.
5.4	Restrict Administrator Privileges to Dedicated Administrator Accounts	Restrict administrator privileges to dedicated administrator accounts on enterprise assets. Conduct general computing activities, such as internet browsing, email, and productivity suite use, from the user's primary, nonprivileged account.
5.5	Establish and Maintain an Inventory of Service Accounts	Establish and maintain an inventory of service accounts. The inventory, at a minimum, must contain department owner, review date, and purpose.
5.6	Centralize Account Management	Centralize account management through a directory or identity service.

Table 5-39 lists CIS Control 6 recommendations for access control management. Access control to technology vendor networks is an important aspect of account management for vendors, operators, customers, and employees. The operators and vendors must determine strategically who bears what responsibility for equipment operation and maintenance as well as data security. The safeguards listed will help effectively manage account access.

Table 5-39. CIS Control 6 (Access Control Management) for Truck Stop Technology Vendors [3]

Safeguard	Title	Description
6.1	Establish an Access Granting Process	Establish and follow a process, preferably automated, for granting access to enterprise assets upon new hire, rights grant, or role change of a user.
6.2	Establish an Access Revoking Process	Establish and follow a process, preferably automated, for revoking access to enterprise assets, through disabling accounts immediately upon termination, rights revocation, or role change of a user. Disabling accounts, instead of deleting accounts, may be necessary to preserve audit trails.
6.3	Require MFA for Externally-Exposed Applications	Require all externally-exposed enterprise or third-party applications to enforce MFA, where supported. Enforcing MFA through a directory service or SSO provider is a satisfactory implementation of this Safeguard.

Safeguard	Title	Description
6.4	Require MFA for Remote Network Access	Require MFA for remote network access.
6.5	Require MFA for Administrative Access	Require MFA for all administrative access accounts, where supported, on all enterprise assets, whether managed on-site or through a third-party provider.
6.6	Establish and Maintain an Inventory of Authentication and Authorization Systems	Establish and maintain an inventory of the enterprise's authentication and authorization systems, including those hosted on-site or at a remote service provider.
6.7	Centralize Access Control	Centralize access control for all enterprise assets through a directory service or SSO provider, where supported.
6.8	Define and Maintain Role-Based Access Control	Define and maintain role-based access control, through determining and documenting the access rights necessary for each role within the enterprise to successfully carry out its assigned duties.

Table 5-40 lists CIS Control 7 recommendations for continuous vulnerability management. A vulnerability management plan and a remediation process are important for any technology or system that is discovered to have or is otherwise susceptible to a vulnerability. Automatic patching of operating systems and application will ease system maintenance and reduce the likelihood of impacts from vulnerabilities.

Table 5-40. CIS Control 7 (Continuous Vulnerability Management) for Truck Stop Technology Vendors [3]

Safeguard	Title	Description
7.1	Establish and Maintain a Vulnerability Management Process	Establish and maintain a documented vulnerability management process for enterprise assets. Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.
7.2	Establish and Maintain a Remediation Process	Establish and maintain a risk-based remediation strategy documented in a remediation process, with monthly, or more frequent, reviews.
7.3	Perform Automated Operating System Patch Management	Perform operating system updates on enterprise assets through automated patch management on a monthly, or more frequent, basis.
7.4	Perform Automated Application Patch Management	Perform application updates on enterprise assets through automated patch management on a monthly, or more frequent, basis.
7.5	Perform Automated Vulnerability Scans of Internal Enterprise Assets	Perform automated vulnerability scans of internal enterprise assets on a quarterly, or more frequent, basis. Conduct both authenticated and unauthenticated scans, using a SCAP-compliant vulnerability scanning tool.
7.6	Perform Automated Vulnerability Scans of Externally-Exposed Enterprise Assets	Perform automated vulnerability scans of externally-exposed enterprise assets using a SCAP-compliant vulnerability scanning tool. Perform scans on a monthly, or more frequent, basis.
7.7	Remediate Detected Vulnerabilities	Remediate detected vulnerabilities in software through processes and tooling on a monthly, or more frequent, basis, based on the remediation process.

Table 5-41 lists CIS Control 8 recommendations for audit log management. Audit logs are important for managing technologies and systems at a truck stop. These logs can inform employees if a technology or system is operating normally or if there is an issue that needs to be addressed. Audit logs can also

contain information on how employees or guests are using the different systems.

Table 5-41. CIS Control 8 (Audit Log Management) for Truck Stop Technology Vendors [3]

Safeguard	Title	Description
8.1	Establish and Maintain an Audit Log Management Process	Establish and maintain an audit log management process that defines the enterprise's logging requirements. At a minimum, address the collection, review, and retention of audit logs for enterprise assets.
8.2	Collect Audit Logs	Collect audit logs. Ensure that logging, per the enterprise's audit log management process, has been enabled across enterprise assets.
8.3	Ensure Adequate Audit Log Storage	Ensure that logging destinations maintain adequate storage to comply with the enterprise's audit log management process.
8.4	Standardize Time Synchronization	Standardize time synchronization. Configure at least two synchronized time sources across enterprise assets, where supported.
8.5	Collect Detailed Audit Logs	Configure detailed audit logging for enterprise assets containing sensitive data. Include event source, date, username, timestamp, source addresses, destination addresses, and other useful elements that could assist in a forensic investigation.
8.6	Collect DNS Query Audit Logs	Collect DNS query audit logs on enterprise assets, where appropriate and supported.
8.7	Collect URL Request Audit Logs	Collect URL request audit logs on enterprise assets, where appropriate and supported.
8.8	Collect Command-Line Audit Logs	Collect command-line audit logs. Example implementations include collecting audit logs from PowerShell®, BASH™, and remote administrative terminals.
8.9	Centralize Audit Logs	Centralize, to the extent possible, audit log collection and retention across enterprise assets.
8.10	Retain Audit Logs	Retain audit logs across enterprise assets for a minimum of 90 days.
8.11	Conduct Audit Log Reviews	Conduct reviews of audit logs to detect anomalies or abnormal events that could indicate a potential threat. Conduct reviews on a weekly, or more frequent, basis.

Table 5-42 lists CIS Control 9 recommendations for email and web browser protections. These recommendations apply specifically to operators who manage their own email systems. Ensuring that the email services are filtered and supported can prevent attackers from gaining access to internal or otherwise confidential email messages.

Table 5-42. CIS Control 9 (Email and Web Browser Protections) for Truck Stop Technology Vendors [3]

Safeguard	Title	Description
9.1	Ensure Use of Only Fully Supported Browsers and Email Clients	Ensure only fully supported browsers and email clients are allowed to execute in the enterprise, only using the latest version of browsers and email clients provided through the vendor.
9.2	Use DNS Filtering Services	Use DNS filtering services on all enterprise assets to block access to known malicious domains.
9.3	Maintain and Enforce Network-Based URL Filters	Enforce and update network-based URL filters to limit an enterprise asset from connecting to potentially malicious or unapproved websites.
9.4	Restrict Unnecessary or Unauthorized Browser and Email Client Extensions	Restrict, either through uninstalling or disabling, any unauthorized or unnecessary browser or email client plugins, extensions, and add-on applications.

Safeguard	Title	Description
9.5	Implement DMARC	To lower the chance of spoofed or modified emails from valid domains, implement DMARC policy and verification, starting with implementing the SPF and the DKIM standards.
9.6	Block Unnecessary File Types	Block unnecessary file types attempting to enter the enterprise's email gateway.

Table 5-43 lists CIS Control 10 recommendations for malware defenses. Truck stops generally have technologies and systems that require an internet network connection. Appropriate anti-virus and malware protections can reduce or mitigate many cyber-attacks, such as ransomware. Configuration management should be used to inhibit unauthorized access.

Table 5-43. CIS Control 10 (Malware Defenses) for Truck Stop Technology Vendors [3]

Safeguard	Title	Description
10.1	Deploy and Maintain Anti-Malware Software	Deploy and maintain anti-malware software on all enterprise assets.
10.2	Configure Automatic Anti-Malware Signature Updates	Configure automatic updates for anti-malware signature files on all enterprise assets.
10.3	Disable Autorun and Autoplay for Removable Media	Disable autorun and autoplay auto-execute functionality for removable media.
10.4	Configure Automatic Anti-Malware Scanning of Removable Media	Configure anti-malware software to automatically scan removable media.
10.5	Enable Anti-Exploitation Features	Enable anti-exploitation features on enterprise assets and software, where possible.
10.6	Centrally Manage Anti-Malware Software	Centrally manage anti-malware software.
10.7	Use Behavior-Based Anti-Malware Software	Use behavior-based anti-malware software.

Table 5-44 lists CIS Control 11 recommendations for data recovery. An effective robust method for backup and recovery of sensitive data can be critical for both protection against cyber-attacks as well as IT equipment malfunctions. Regular backup testing is recommended for large and complex networks.

Table 5-44. CIS Control 11 (Data Recovery) for Truck Stop Technology Vendors [3]

Safeguard	Title	Description
11.1	Establish and Maintain a Data Recovery Process	Establish and maintain a data recovery process. In the process, address the scope of data recovery activities, recovery prioritization, and the security of backup data.
11.2	Perform Automated Backups	Perform automated backups of in-scope enterprise assets. Run backups weekly, or more frequently, based on the sensitivity of the data.
11.3	Protect Recovery Data	Protect recovery data with equivalent controls to the original data. Reference encryption or data separation, based on requirements.
11.4	Establish and Maintain an Isolated Instance of Recovery Data	Establish and maintain an isolated instance of recovery data. Example implementations include version controlling backup destinations through offline, cloud, or off-site systems or services.

Safeguard	Title	Description
11.5	Test Data Recovery	Test backup recovery quarterly, or more frequently, for a sampling of in-scope enterprise assets.

Table 5-45 lists CIS Control 12 recommendations for network infrastructure management. Maintaining and upgrading hardware as necessary to keep network infrastructure up-to-date can inhibit many cyber-attacks as newer versions often fix vulnerabilities in the system. Truck stop technology vendors should verify with the truck stop operator who bears responsibility for maintenance, operation and cybersecurity of each aspect of the infrastructure and networks.

Table 5-45. CIS Control 12 (Network Infrastructure Management) for Truck Stop Technology Vendors [3]

Safeguard	Title	Description
12.1	Ensure Network Infrastructure is Up-to-Date	Ensure network infrastructure is kept up-to-date.
12.2	Establish and Maintain a Secure Network Architecture	Establish and maintain a secure network architecture.
12.3	Securely Manage Network Infrastructure	Securely manage network infrastructure.
12.4	Establish and Maintain Architecture Diagram(s)	Establish and maintain architecture diagram(s) and/or other network system documentation.
12.5	Centralize Network AAA	Centralize network AAA.
12.6	Use of Secure Network Management and Communication Protocols	Use secure network management and communication protocols (e.g., 802.1X, WPA2 Enterprise or greater).
12.7	Ensure Remote Devices Utilize a VPN and are Connecting to an Enterprise's AAA Infrastructure	Require users to authenticate to enterprise-managed VPN and authentication services prior to accessing enterprise resources on end-user devices.

Table 5-46 lists CIS Control 13 recommendations for network monitoring and defense. Complex networks can benefit from intrusion detection systems, security alerts, and network filtering. An effective IDS can greatly increase the likelihood that a cyber-attack can be mitigated.

Table 5-46. CIS Control 13 (Network Monitoring and Defense) for Truck Stop Technology Vendors [3]

Safeguard	Title	Description
13.1	Centralize Security Event Alerting	Centralize security event alerting across enterprise assets for log correlation and analysis.
13.2	Deploy a Host-Based Intrusion Detection Solution	Deploy a host-based intrusion detection solution on enterprise assets, where appropriate and/or supported.

Safeguard	Title	Description
13.3	Deploy a Network Intrusion Detection Solution	Deploy a network intrusion detection solution on enterprise assets, where appropriate.
13.4	Perform Traffic Filtering Between Network Segments	Perform traffic filtering between network segments, where appropriate.
13.5	Manage Access Control for Remote Assets	Manage access control for assets remotely connecting to enterprise resources.
13.6	Collect Network Traffic Flow Logs	Collect network traffic flow logs and/or network traffic to review and alert upon from network devices.

Table 5-47 lists CIS Control 14 recommendations for security awareness and skills training. Regardless of the number and sophistication of operational staff, training staff with privileged access IT systems about cyber-attacks and good cybersecurity habits is beneficial.

Table 5-47. CIS Control 14 (Security Awareness and Skills Training) for Truck Stop Technology Vendors [3]

Safeguard	Title	Description
14.1	Establish and Maintain a Security Awareness Program	Establish and maintain a security awareness program.
14.2	Train Workforce Members to Recognize Social Engineering Attacks	Train workforce members to recognize social engineering attacks, such as phishing, pre-texting, and tailgating.
14.3	Train Workforce Members on Authentication Best Practices	Train workforce members on authentication best practices.
14.4	Train Workforce on Data Handling Best Practices	Train workforce members on how to identify and properly store, transfer, archive, and destroy sensitive data.
14.5	Train Workforce Members on Causes of Unintentional Data Exposure	Train workforce members to be aware of causes for unintentional data exposure.
14.6	Train Workforce Members on Recognizing and Reporting Security Incidents	Train workforce members to be able to recognize a potential incident and be able to report such an incident.
14.7	Train Workforce on How to Identify and Report if Their Enterprise Assets are Missing Security Updates	Train workforce to understand how to verify and report out-of-date software patches or any failures in automated processes and tools.
14.8	Train Workforce on the Dangers of Connecting to and Transmitting Enterprise Data Over Insecure Networks	Train workforce members on the dangers of connecting to, and transmitting data over, insecure networks for enterprise activities.

Safeguard	Title	Description
14.9	Conduct Role-Specific Security Awareness and Skills Training	Conduct role-specific security awareness and skills training.

Table 5-48 lists CIS Control 15 recommendations for service provider management. Truck stop technology vendors may implement third-party technologies or systems into their products. Vendors should assure that suppliers are aware of and meet the cybersecurity requirements of their systems. Maintaining a list of the suppliers can be indispensable when troubleshooting and repairing a complex system that is under attack or otherwise malfunctions.

Table 5-48. CIS Control 15 (Service Provider Management) for Truck Stop Technology Vendors [3]

Safeguard	Title	Description
15.1	Establish and Maintain an Inventory of Service Providers	Establish and maintain an inventory of service providers.
15.2	Establish and Maintain a Service Provider Management Policy	Establish and maintain a service provider management policy.
15.3	Classify Service Providers	Classify service providers.
15.4	Ensure Service Provider Contracts Include Security Requirements	Ensure service provider contracts include security requirements.

Table 5-49 lists CIS Control 16 recommendations for application software security. Some truck stop technology vendors may design proprietary systems and/or mobile applications. These systems and applications should be securely developed and maintained.

Table 5-49. CIS Control 16 (Application Software Security) for Truck Stop Technology Vendors [3]

Safeguard	Title	Description
16.1	Establish and Maintain a Secure Application Development Process	Establish and maintain a secure application development process.
16.2	Establish and Maintain a Process to Accept and Address Software Vulnerabilities	Establish and maintain a process to accept and address reports of software vulnerabilities, including providing a means for external entities to report.
16.3	Perform Root Cause Analysis on Security Vulnerabilities	Perform root cause analysis on security vulnerabilities.
16.4	Establish and Manage an Inventory of Third-Party Software Components	Establish and manage an updated inventory of third-party components used in development, often referred to as a "bill of materials," as well as components slated for future use.
16.5	Use Up-to-Date and Trusted Third-Party Software Components	Use up-to-date and trusted third-party software components.

Safeguard	Title	Description
16.6	Establish and Maintain a Severity Rating System and Process for Application Vulnerabilities	Establish and maintain a severity rating system and process for application vulnerabilities that facilitates prioritizing the order in which discovered vulnerabilities are fixed.
16.7	Use Standard Hardening Configuration Templates for Application Infrastructure	Use standard, industry-recommended hardening configuration templates for application infrastructure components.
16.8	Separate Production and Non-Production Systems	Maintain separate environments for production and non-production systems.
16.9	Train Developers in Application Security Concepts and Secure Coding	Ensure that all software development personnel receive training in writing secure code for their specific development environment and responsibilities.
16.10	Apply Secure Design Principles in Application Architectures	Apply secure design principles in application architectures.
16.11	Leverage Vetted Modules or Services for Application Security Components	Leverage vetted modules or services for application security components, such as identity management, encryption, and auditing and logging.

Table 5-50 lists CIS Control 17 recommendations for incident response management. No technology or system can be fully protected from cybersecurity incidents. When a cybersecurity incident does occur, it is helpful to have a plan in place to deal with the incident swiftly. Having an incident response management plan allows employees to act swiftly and alert the responsible party to fix the incident. Truck stops who use the technology can also easily reach out to truck stop technology vendors to disclose vulnerabilities discovered.

Table 5-50. CIS Control 17 (Incident Response Management) for Truck Stop Technology Vendors [3]

Safeguard	Title	Description
17.1	Designate Personnel to Manage Incident Handling	Designate one key person, and at least one backup, who will manage the enterprise's incident handling process.
17.2	Establish and Maintain Contact Information for Reporting Security Incidents	Establish and maintain contact information for parties that need to be informed of security incidents.
17.3	Establish and Maintain an Enterprise Process for Reporting Incidents	Establish and maintain an enterprise process for the workforce to report security incidents. The process includes reporting timeframe, personnel to report to, mechanism for reporting, and the minimum information to be reported.
17.4	Establish and Maintain an Incident Response Process	Establish and maintain an incident response process that addresses roles and responsibilities, compliance requirements, and a communication plan.

Safeguard	Title	Description
17.5	Assign Key Roles and Responsibilities	Assign key roles and responsibilities for incident response, including staff from legal, IT, information security, facilities, public relations, human resources, incident responders, and analysts, as applicable.
17.6	Define Mechanisms for Communicating During Incident Response	Determine which primary and secondary mechanisms will be used to communicate and report during a security incident. Mechanisms can include phone calls, emails, or letters.
17.7	Conduct Routine Incident Response Exercises	Plan and conduct routine incident response exercises and scenarios for key personnel involved in the incident response process to prepare for responding to real-world incidents.
17.8	Conduct Post-Incident Reviews	Conduct post-incident reviews. Post-incident reviews help prevent incident recurrence through identifying lessons learned and follow-up action.

Table 5-51 lists CIS Control 18 recommendations for penetration testing. Penetration testing is an important method for identifying vulnerabilities in technologies, systems, or networks. Conducting regular penetration tests basis can improve an organization's overall.

Table 5-51. CIS Control 18 (Penetration Testing) for Truck Stop Technology Vendors [3]

Safeguard	Title	Description
18.1	Establish and Maintain a Penetration Testing Program	Establish and maintain a penetration testing program appropriate to the size, complexity, and maturity of the enterprise.
18.2	Perform Periodic External Penetration Tests	Perform periodic external penetration tests based on program requirements, no less than annually. External penetration testing must include enterprise and environmental reconnaissance to detect exploitable information.
18.3	Remediate Penetration Test Findings	Remediate penetration test findings based on the enterprise's policy for remediation scope and prioritization.

6. Conclusion

This report delineated the results of a research study that evaluated possible cybersecurity risks of truck stop technologies. This study involved an open-source internet scan of truck stop technologies and information gathering via interviews with truck stop operators, truck stop technology vendors, state DOTs, and other truck stop stakeholders. After gathering information on the various technologies at a truck stop, a cybersecurity assessment was conducted on the various truck stop technologies discovered. Finally, this research study applied the CIS 18 controls to the various truck stop stakeholder organizations based on their size and their truck stop IT infrastructure size.

7. References

1. A. Lautenbach, and M. Islam, *HEAVENS* (Gothenburg, Sweden: Chalmers University of Technology, and Gothenburg, Sweden: Volvo AB, 2016).
2. F. Swiderski and W. Snyder. *Threat Modeling* (Microsoft Press, 2004).
3. Center for Internet Security, *CIS Controls Version 8* (Center for Internet Security, 2021).

Appendix A: HEAVENS Risk Analysis Methodology

The HEAVENS methodology requires the development of use cases with the system assets (i.e., truck stop technologies) in mind. The use cases contain details of the cyberattack, such as the entry point of the attack, attack type, and potential effects from the attack. With the use cases established, the HEAVENS methodology requires input about the threat level and impact level on the assets. Once the threat and impact levels are determined, HEAVENS uses the data to calculate the security level of the asset. Security levels range from quality management to low, medium, high, and critical.

A.1 Threat Level Parameters

In the HEAVENS methodology, there are four different parameters for threat levels: attacker expertise, window of opportunity, knowledge of the target of evaluation (TOE), and equipment.

Expertise describes the general knowledge of the relevant underlying principles, product type, or attack methods that are required to carry out an attack. The levels of expertise are:

Layman	No particular expertise and lacks knowledge when compared to an expert or proficient person.
Proficient	Has general knowledge about cybersecurity and is involved in the business. A proficient person would know about simple and popular attacks and can mount these types of attacks. They are also capable of using available tools and if required, can improvise to a degree in order to achieve the desired results.
Expert	Familiar with all cyber components of the system such as underlying algorithms, protocols, hardware, and system structures. In addition, Experts have in-depth knowledge of the techniques and tools, cryptography, classical attacks, and the ability to create new attacks.
Multiple Experts	Different fields of experts are required to carry out an attack.

Window of opportunity combines access type and access duration that an attacker would be expected to have to carry out an attack. The levels of windows of opportunity are:

Low	Low availability of time with the asset to conduct an attack. These attacks require physical access to the asset and with a complex disassembly.
Medium	Low physical and/or logical access availability of the asset to conduct an attack. The attack would require physical access to the asset but does not require any special tools.

High	The asset is highly available, but there is a limit on the amount of access time. These attacks are logical or remote access and do not require a physical presence.
Critical	High availability through public/untrusted networks without any time limitation on system access. These attacks are logical or remote access and do not require a physical presence.

Knowledge of the Target of Evaluation describes the availability of information about the TOE and the community size that possesses that knowledge. The levels of knowledge are:

Public	Information regarding the asset can be gained from public sources such as the Internet.
Restricted	Information regarding the system is controlled and is usually found within the developer organization and shared only with other select organizations.
Sensitive	Information regarding the asset is only shared between distinct teams in the developer organization. Access to this level of information is limited to only certain members of specified teams.
Critical	Information regarding the asset is more tightly controlled than at the sensitive level and would be on a strict need-to-know basis.

Equipment is the equipment required to identify/exploit a vulnerability and/or mount an attack. The levels of equipment are:

Standard	Readily available to the attacker for either the identification of a vulnerability or for an attack. The equipment may be a part of the TOE itself such as a debugger in an operating system, or can be readily obtained.
Specialized	Not readily available to the attacker, but could be acquired without much effort. This could include the development of more extensive attack scripts or programs.
Bespoke	Not readily available to the public as it may need to be specially produced, the distribution is controlled or restricted, or is very expensive.
Multiple Bespoke	Information regarding the asset is more tightly controlled than at the sensitive level and would be on a strict need-to-know basis.

After inputting the four threat level parameters, the values are summed by the HEAVENS methodology to determine the threat level on the asset at either none, low, medium, high, or critical.

A.2 Impact Level Parameters

The HEAVENS methodology has four different impact parameters: safety, privacy and/or legislation, financial, and operational.

Safety estimates the safety impact of a successful attack and is adopted from ISO 26262. The levels of safety are no injury, light and moderate injuries, severe and life-threatening injuries (survival probable), and life-threatening injuries (survival uncertain) and fatal injuries.

Privacy/Legislation includes damages caused by privacy violation of stakeholders and/or violation of legislations or regulations. Privacy and legislation are merged into a single parameter because privacy may be enforced via legislation, and there are legislation that are not related to privacy. Damages from privacy/legislation do not have a direct injury, financial, or operational effects, but may cause financial or operational damages to stakeholders. The impact of privacy or legislation is lower, with respect to safety and financial parameters.

Financial considers all financial losses or damages that occur directly or indirectly. Direct financial damages include product liability issues, legislation issues, or product features. Indirect financial damages include damage to the original equipment manufacturer's (OEM) reputation, loss of market share, or IP infringement. The financial damage is the sum of direct and indirect costs for the OEM.

Operational includes operational damages caused by unwanted or unexpected incidents. In certain situations, operational damage may yield safety and financial damages. The impact of the operational category is lower, with respect to safety and financial parameters.

After inputting the four impact level parameters, the values are summed by the HEAVENs methodology to determine the impact level on the asset at either none, low, medium, high, or critical.

U.S. Department of Transportation
John A. Volpe National Transportation Systems Center
55 Broadway
Cambridge, MA 02142-1093

617-494-2000
www.volpe.dot.gov

DOT-VNTSC-FHWA-22-02