# ITS AMERICA CYBERSECURITY FOR NOVICE CYBER PROFESSIONALS PRIMER

ITS America Cybersecurity Community of Practice

202.484.4847

www.itsa.org | info@itsa.org

1100 New Jersey SE Suite 850, Washington DC 20003

October
2024

# ITS America Cybersecurity for Novice Cyber Professionals Primer

This ITS America Cybersecurity for Novice Cyber Professionals Primer addresses the critical issue of cybersecurity within transportation systems at a level accessible to non-cybersecurity experts. This primer highlights the inherent vulnerabilities of current traffic systems and equipment to cyber threats, ranging from minor pranks to severe attacks perpetrated by professional hackers. It also emphasizes the increasing complexity and interconnectedness of modern transportation systems, which amplifies the potential risk landscape. This primer addresses the following critical areas:

- The distinction between Information Technology (IT) and Operational Technology (OT) requirements, and the significance of addressing cybersecurity from a comprehensive perspective that includes people, processes, and technology.
- The diverse types of physical and digital vulnerabilities in the transportation system and threat assessment considerations.
- A Zero Trust approach to cybersecurity; the importance of frameworks, standards, and governance; and the differences between requirements and best practices.
- Security architecture and operations, the need for patching, and additional considerations.
- USDOT policy resources, user education, and career development.

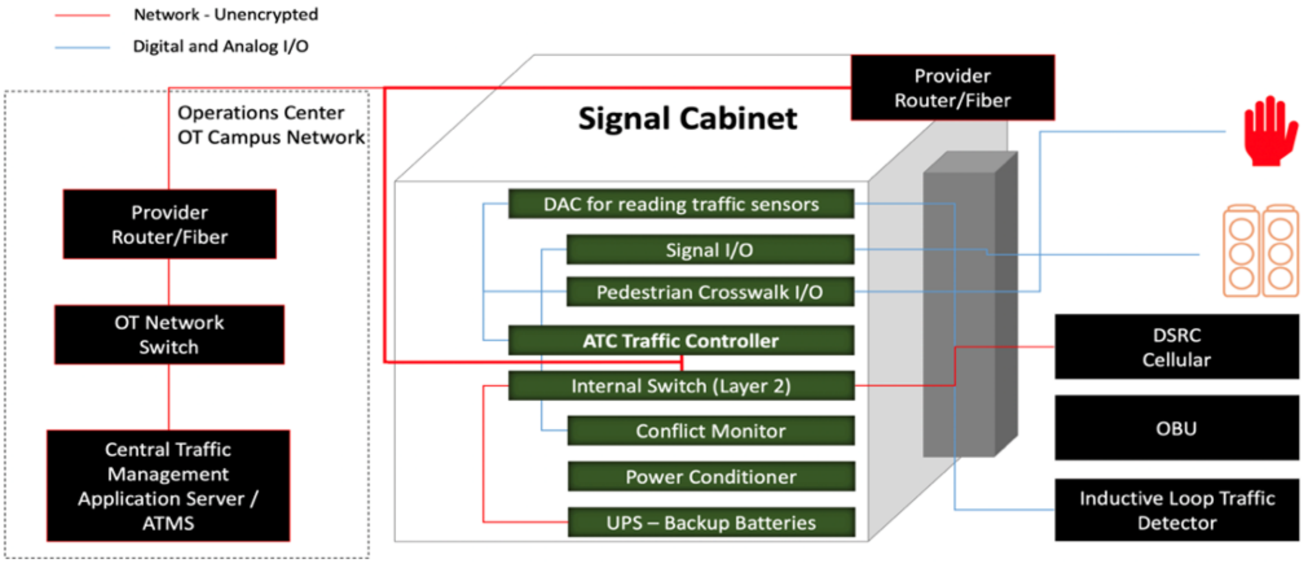
This document is a foundational guide for transportation cyber professionals to develop a basic awareness and understanding of cybersecurity issues within their field. It aims to foster a more secure and resilient transportation infrastructure, thereby protecting against the escalating threats posed by increasingly sophisticated cyber adversaries.

# Table of Contents

## Introduction

Many existing traffic systems and equipment are inherently unsecured and unprotected against cyber threats. From traffic operations centers and Advanced Traffic Management Systems (ATMS) to field signal cabinets and traffic control devices, transportation systems classically combine digital and automated components to manage physical processes – the flow and control of traffic, vehicles, and pedestrians. Transportation systems today present numerous attack vectors for increasingly sophisticated and bold adversaries. These adversaries can range from the pranksters updating electronic message boards on the side of the road to much more serious professional hackers seeking ransom or damage on the behalf of criminal enterprises, terrorists, or nation states. As depicted in Figure 1 below (shown via the red line which highlights the unencrypted and most vulnerable network), today's traffic systems and equipment typically lack visibility into and protection from cyber adversaries.

*Figure 1 – Signal Cabinet*



Further, more intelligent transportation systems, increasing vehicle autonomy, and enhanced technological connectivity, all of which can provide significant benefits, expands the risk landscape for the controlled, safe, and reliable operation of transportation systems.

How do governments and public agencies secure transportation systems from cyber threats, and how do existing regulations and standards support or impede those efforts? Securing cyber-physical systems is a challenge not unique to the transportation industry, but rather one being dealt with throughout various sectors and at all levels of government. This primer provides a first step for transportation professionals to gain a basic awareness and understanding of the core cybersecurity issues, terminology, and simple actions that will help move your organization toward a more cyber-safe posture. For a more advanced review of this topic and additional resources, see *ITS America Cybersecurity for Connected Infrastructure.*

## Cyber Fundamentals

This section introduces the critical importance of cybersecurity in transportation systems, emphasizing that it is not solely an Information Technology (IT) responsibility but requires a comprehensive approach involving people, processes, and technology. It highlights the necessity of balancing perceived vulnerabilities, regulatory requirements, and risk tolerance to establish an effective cybersecurity program.

### Informational Technology and Operational Technology – A Basic Introduction

Cybersecurity is a current and expanding concern for transportation systems, but responsibility for it is often seen as strictly an IT function and assumed to be the sole responsibility of the IT staff. However, many operational technologies[1] introduce cyber risk into the transportation system and must also be addressed.

Traditional Information Technology (IT) focuses on the core business functions many businesses share, such as accounting, human resources, and public relations. These common business functions often incorporate cybersecurity practices that are (or should be) very standard. Establishing firewalls, educating end-users, implementing multi-factor authentication, installing malware protection, and patching software are standard IT cybersecurity practices. Organizations that implement these protections are often considered to have "good cyber hygiene."

In contrast, Operational Technology (OT) involves field networks, software, and equipment that monitor and control physical devices and processes, such as various sensors, traffic signal systems, Closed Circuit Television (CCTV), and Dynamic Messaging Signs (DMS), as well as electric vehicle charging infrastructure, have not always been developed with cybersecurity in mind. Early OT implementations were isolated, disconnected systems – so the perceived risk was minimal. As connectivity comes to the world of OT, especially in the transportation industry, the risk is more evident.

OT differs from IT systems in that these "cyber/physical" systems drive activities in the field and as such, pose a potential safety risk for transportation system users. The OT environment also differs from the IT environment in that it is a distributed environment reaching a variety of endpoint devices spread across an entire jurisdiction. These OT networks have typically evolved over time with additional devices being added by various parts of the transportation organization. Consequently, this network is usually a combination of fiber and wireless elements with multiple service providers from telecommunications companies to Internet Service Providers (ISPs) and the public entity's own communications assets. The complexity and diversity of this network provides different challenges to security. For example, there can be equipment running quite simple firmware all the way to end devices utilizing stripped down or full Window's operating systems. This requires a complex Vulnerability Management (VM) strategy.

[1] Operational technologies include hardware and software that detect or cause changes in systems that can affect the physical environment. These changes can be caused or detected through direct monitoring and control of physical devices, processes, and events. They are used in industries such as manufacturing, transportation, energy, and utilities.

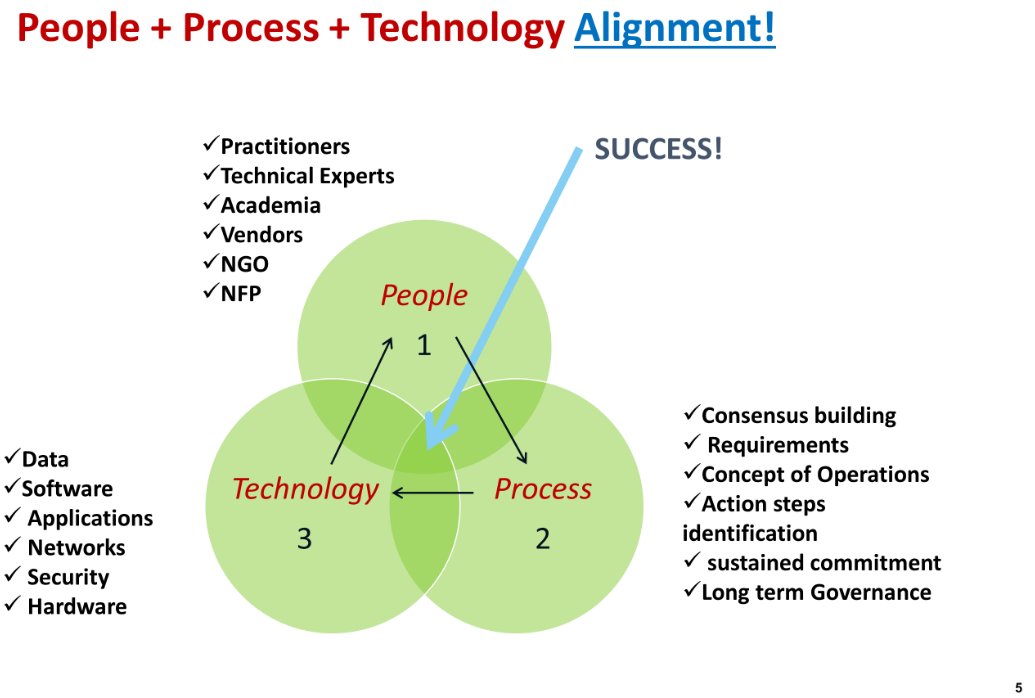
- Cyber threats target OT components such as Industrial Control Systems (ICS), Sensors and Actuators, Human Machine Interfaces (HMI), Real Time Operating Systems (RTOS), and Field Devices.

- OT cybersecurity focuses on protecting the OT components of an industry's operations and networks from cyber threats that could take control, damage, or cause disruption of physical processes and infrastructure.

**People, Process, and Technology**

An effective cybersecurity program addresses the three aspects of "People, Process, and Technology." Cybersecurity is not simply a technological issue, but rather there are human factors and policies/procedural issues that also need to be addressed to be successful. Addressing each of these aspects and bringing them into alignment is what will lead to increased cyber maturity. An example of "People, Process, and Technology" alignment is demonstrated in Figure 2 below.

*Figure 22– People, Process, Technology, Alignment*



People + Process + Technology Alignment!

✓Practitioners
✓Technical Experts
✓Academia
✓Vendors
✓NGO
✓NFP

SUCCESS!

People
1

Technology
3

Process
2

✓Data
✓Software
✓ Applications
✓ Networks
✓ Security
✓ Hardware

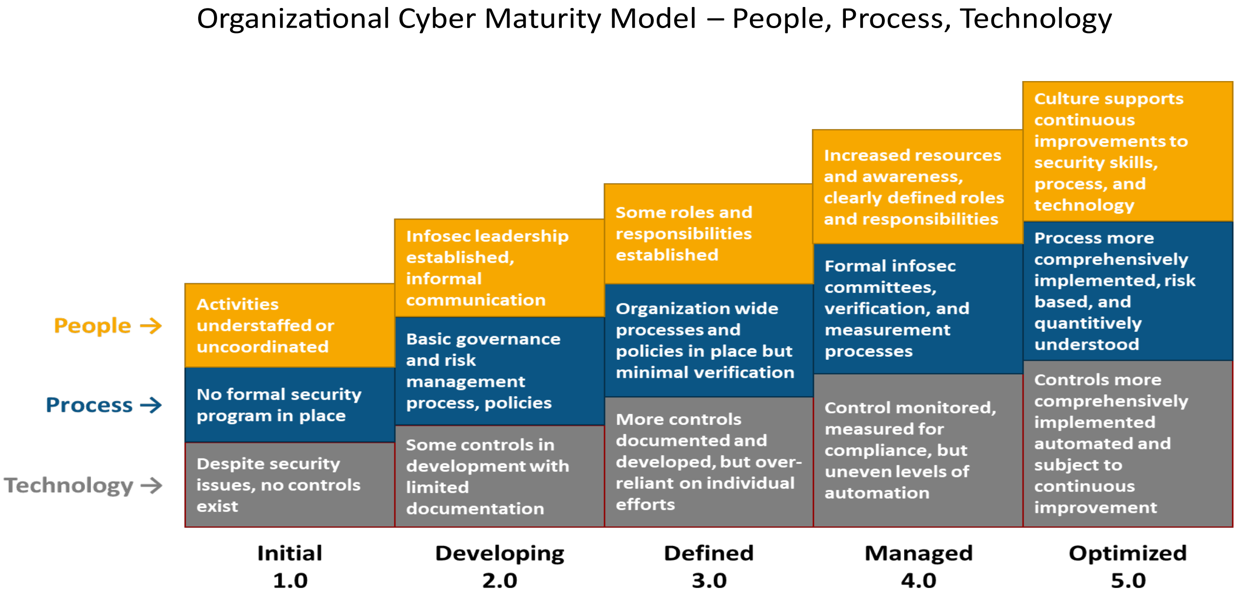
✓Consensus building
✓ Requirements
✓Concept of Operations
✓Action steps identification
✓ sustained commitment
✓Long term Governance

5

Many factors play into the overall risk tolerance of an organization. Leadership determines their organization's consideration of several factors, including applicable regulations, perceived vulnerability, data sensitivity, criticality of the system, and potential scale of negative impact in combination with their overall risk tolerance. These characteristics of the organization help define how a cybersecurity program should be implemented.

An Organizational Cyber Maturity Model example can be seen in Figure 3 below.

*Figure 3 – Organization Cyber Maturity Model-People- Process, Technology*



Organizational Cyber Maturity Model – People, Process, Technology

| | Initial 1.0 | Developing 2.0 | Defined 3.0 | Managed 4.0 | Optimized 5.0 |
|---|---|---|---|---|---|
| People → | Activities understaffed or uncoordinated | Infosec leadership established, informal communication | Some roles and responsibilities established | Increased resources and awareness, clearly defined roles and responsibilities | Culture supports continuous improvements to security skills, process, and technology |
| Process → | No formal security program in place | Basic governance and risk management process, policies | Organization wide processes and policies in place but minimal verification | Formal infosec committees, verification, and measurement processes | Process more comprehensively implemented, risk based, and quantitively understood |
| Technology → | Despite security issues, no controls exist | Some controls in development with limited documentation | More controls documented and developed, but over-reliant on individual efforts | Control monitored, measured for compliance, but uneven levels of automation | Controls more comprehensively implemented automated and subject to continuous improvement |

## Physical and Digital Security Vulnerabilities

This section highlights critical risks to transportation systems, including weak physical locks, inadequate site security, and outdated firmware. It emphasizes the need for robust cabinet access control, equipment protection, and effective password management to ensure the integrity and resilience of transportation infrastructure.

### Physical and Digital Security - Examples of Low Hanging Fruit

- **Cabinet Access Control:** Weak physical locks, lack of access control systems, and infrequent inspections of locks and hinges can allow unauthorized access to traffic signal cabinets.
- **Equipment Protection:** Traffic signal equipment is vulnerable to physical damage due to inadequate protective covers, a lack of measures to prevent vandalism (like surveillance cameras), and irregular equipment inspections and maintenance.
- **Site Security:** Inadequate lighting around traffic signal cabinets and infrequent site inspections to identify potential hazards can compromise the overall security of traffic signal locations.
- **Environmental Hazards:** Environmental physical hazards such as extreme temperatures, high humidity, inadequate airflow, smoke, and electrical surges can damage hardware and disrupt IT infrastructure, posing significant risks to cybersecurity. A robust cybersecurity plan should

incorporate strategies to monitor and mitigate these conditions to ensure data integrity and system availability.

**Digital Security Vulnerabilities**

- **Network Segmentation:** Failing to isolate traffic signal controllers from the broader transportation and/or government network can increase the attack surface and allow attackers to move laterally within the network.
- **Password Management:** Weak password policies, such as not requiring complex passwords, infrequent password changes, and failure to disable default passwords pose a significant security risk.
- **Firmware Updates:** Outdated firmware in traffic signal controllers and components can leave known vulnerabilities unaddressed and weaken system resilience.
- **Intrusion Detection Systems (IDS):** The absence of IDS solutions to monitor traffic signal network traffic for suspicious activity can delay the detection of threats and increase potential damage.
- **Access Controls:** Weak access controls, including the lack of role-based access controls, infrequent access reviews, and absent audit logging of system access can allow unauthorized modifications to traffic signal system configurations.
- **Proxies and Data Flow Monitoring:** Limiting direct ingress and egress internet communication by routing traffic through a proxy enhances cybersecurity by controlling and monitoring data flow, reducing the risk of unauthorized access and compromises. This approach has been proven to significantly improve security posture, particularly by managing Internet of Things (IoT) communications more effectively.
- **Reduce Attack Surface:** Disabling unnecessary features or functionality reduces potential entry points for cyber-attacks, thereby enhancing the overall security of systems and applications. By minimizing the attack surface, organizations can better protect sensitive data and maintain system and application integrity.
- **Centralized Administration:** Implementing centralized administration for multiple devices streamlines security management by standardizing configurations and policies across the network. This approach reduces administrative effort and ensures consistent security measures are applied globally, enhancing overall protection.

## Threat Intelligence and Assessment

Hackers and cyber threats to operational technology can cause financial losses, organizational instabilities, and damage to staff, equipment, and the environment of an organization. Types of risks include software, hardware, technological indifference, cybersecurity related, and operational.

- **Software Risks:** This category includes risks related to software development and deployment, such as bugs, security vulnerabilities, and compatibility issues. Software risks can lead to system failures, data breaches, and operational disruptions.
- **Hardware Risks:** Risks associated with physical components of OT infrastructure, including servers, workstations, and networking equipment. Hardware malfunctions can result in data loss, downtime, and reduced operational capacity.
- **Technology Obsolescence Risks:** Outdated technology no longer maintained and supported well bears the risk of breaches, increased downtimes, and system crashes. Tackling these ensures business continuity from a technological perspective, invests available resources wisely and efficiently, and builds a tech stack that remains relevant, effective, and functional.
- **Cybersecurity Risks:** Encompasses threats from malicious cyber activities such as hacking, malware, ransomware, and phishing attacks. Cybersecurity risks can compromise sensitive data, disrupt business operations, and damage an organization's reputation.
- **Operational Risks:** Related to the day-to-day operation of technology systems and processes. Operational risks include system downtime, performance issues, and the failure of backup and recovery systems.

Scanning is a beneficial approach to identifying vulnerabilities and completing a threat assessment.

- **Scanning:** Scanning refers to the process of examining the network's topology, IP and MAC addresses, RAM, Operating Systems, and characteristics of devices used in the network. Scanning can identify vulnerabilities and weaknesses that cyber attackers can exploit to gain unauthorized access.
- **Port Scanning:** Port scanning involves checking open ports on a network or device to identify potential entry points for cyber-attacks. By scanning open TCP, UDP ports, and using pinging, attackers can find vulnerabilities to exploit and breach the network.
- **Pinging:** Pinging is a simple process that checks the reachability of a device within a network. Cyber attackers use Pinging to discover active devices and their network status, which can help them plan and execute further attacks.

## Defense in Depth

This section describes a comprehensive cybersecurity strategy that incorporates Zero Trust principles to enhance security. This strategy involves administrative measures such as strict access controls and continuous monitoring, as well as logical components like Policy Decision Points (PDPs) and Policy Enforcement Points (PEPs) to enforce security policies. Moreover, it includes physical safeguards to protect hardware and infrastructure, ensuring a layered and robust defense against potential threats.

### Zero Trust

Zero Trust security means that nothing is trusted by default from inside or outside the network, and verification is required from everything trying to gain access to anything on the network. This added layer of security has been shown to help prevent data breaches. The three principles of Zero Trust are: (1) Always Verify, (2) Least Privilege Access, and (3) Risk Mitigation.

The technologies behind Zero Trust include Identity and Access Management (IAM), Multifactor Authentication (MFA), micro-segmentation, and robust encryption. IAM ensures proper identification of users, while MFA adds an extra layer of authentication.

There are five important aspects of Zero Trust security: Identity; Device; Network; Application; and Workload and Data. Unlike a traditional VPN-based approach, which assumes that anyone or anything that passes network perimeter controls can be trusted, the zero-trust model takes the opposite approach. A Zero Trust security approach benefits from micro-segmentation of the network because once the secured area has been micro-segmented, it is better protected from threats. The firewall or filter that forms a barrier around the zone can also block threats from exiting the zone, which protects the rest of the network. Zero Trust models are built on this practice, which requires positive user identification for access to a network's resources. Identity and Access Management (IAM) uses features like MFA and Single Sign-On (SSO) to verify users and determine the level of access they will be granted.

One area where many security professionals run into difficulty with Zero Trust implementation is complexity. To set up Zero Trust architecture, organizations need to have a complete picture of their data and workflows. Every single resource and endpoint needs identifying, access control, and monitoring, so a common first step towards Zero Trust OT cybersecurity is to implement the capability to inventory assets on the OT network and monitor IP traffic.

### Administrative

Since Zero Trust is an approach to cybersecurity that goes beyond “trust but verify” and treats all networks and traffic as potential threats, access is denied by default. A Zero Trust Architecture (ZTA) helps agencies build Zero Trust principles into industrial and enterprise infrastructure and workflows. For example, when a new service account is defined, or a new employee joins a company, they initially do not have access to any systems. Administrators need to explicitly approve specific permissions and access levels for the new account.

### Logical

As defined by NIST SP 800-207: Zero Trust Architecture, the three core logical components of the ZTA are the Policy Decision Point (PDP), the Policy Information Points (PIPs), and the Policy Enforcement Point (PEP). These components may be operated as an on-premises service or through a cloud-based service.

Zero Trust Network Access (ZTNA) is an IT security solution that provides secure remote access to an organization's applications, data, and services based on clearly defined access control policies. ZTNA is not meant to replace firewalls but rather complement them. Firewalls are still essential to a comprehensive security solution and provide the first line of defense against external threats.

**Physical**

Zero Trust emphasizes the importance of refraining from trusting someone or something, a device or service, just because of their physical location whether they are in the office or on a network. The Zero Trust model suggests every user, every device, and every system should be untrusted until proven otherwise.

One disadvantage of Zero Trust is that it can be costly to implement. This is because it requires a larger workforce and additional security measures – such as multi-factor authentication – which can add to the overall cost of the system. A common failing in Zero Trust implementations is the failure to fully commit. It is a lot of work to turn from a legacy intranet to full SaaS/IaaS (Software as a Service/Infrastructure as a Service) cloud solutions. As a result, implementations are often done in stages, which can lead to interim exposure of workload and data.

## Framework, Standards, and Governance

Organizations can use cybersecurity frameworks, standards, and governance to help identify and implement appropriate measures to protect their systems and data from cyber threats. Governance plays a crucial role in establishing clear policies and procedures to oversee the effective implementation and ongoing management of cybersecurity initiatives. Cybersecurity frameworks are applicable to all organizations, regardless of their size, industry, or sector. Standards can provide guidance on how to respond to and recover from cybersecurity incidents.

As an organization implements cybersecurity measures for their OT, it is essential that the agency or organization have the resources to identify and assess OT assets as well as resources to develop and implement a security plan and foster a culture of security. User security awareness and training is an essential part of any plan. In addition, resources are needed to provide day-to-day operations and oversight for the security of the OT network. Some organizations may approach this by partnering with their own internal Enterprise IT department while others may prefer to establish their own OT Cybersecurity team.

A Cybersecurity framework is a set of documents that will define and provide guidelines, standards, and best practices for the agency. The goal of the framework should be to reduce the agency’s exposure to vulnerabilities that could be exploited.

The framework should include industry best practice and any regulatory guidelines and standards the agency must follow. There are various cybersecurity frameworks available that were developed by national and international organizations. Basics of the various frameworks include assets and users identification, access control, network monitoring, incident response, and recovery plans.

Some of the most well-known frameworks include:

- NIST Cybersecurity Framework: The NIST Cybersecurity Framework is a high-level framework that provides a set of best practices for managing cybersecurity risk.
- ISA/IEC 62443: The ISA/IEC 62443 is a set of international standards that specifically address the security of industrial automation and control systems.
- MITRE ATT&CK ICS Framework: The MITRE ATT&CK ICS Framework is a knowledge base of adversary tactics, techniques, and procedures for ICS. This can be used to help organizations identify and defend against cyber-attacks.
- CISA Cybersecurity Best Practices for Industrial Control Systems (ICS): The CISA Cybersecurity Best Practices for Industrial Control Systems (ICS) is from the Cybersecurity and Infrastructure Security Agency and provides a set of best practices for securing ICS.

**Delineation Between Requirements and Best Practices**

The difference between requirements and best practices in cybersecurity can be understood as follows:

- **Requirements** are mandatory rules or standards that organizations must follow to comply with laws, regulations, or policies. These are often enforced by regulatory bodies and failure to comply can result in legal penalties, fines, or other consequences. Requirements are designed to ensure a minimum level of security and are often specific to certain industries or types of data.
- **Best Practices**, on the other hand, are recommended guidelines or strategies that organizations can follow to enhance their cybersecurity posture. These are not mandatory but are considered highly effective in protecting against cyber threats. Best practices are often based on industry standards, expert recommendations, and lessons learned from past incidents. They provide a higher level of security beyond the minimum requirements and help organizations stay ahead of emerging threats.

For example, the NIST Cybersecurity Framework provides a set of best practices for managing cybersecurity risks, while specific regulations like the EU's General Data Protection Regulation (GDPR) or the Health Insurance Portability and Accountability Act (HIPAA) outline mandatory requirements for protecting personal data.

### Center for Internet Security (CIS) Top 18

The Center for Internet Security (CIS) Top 18 Top 18, also known as the CIS Critical Security Controls, is a set of best practices for securing IT systems and data against cyber threats. These controls are designed to help organizations improve their cybersecurity posture by providing a prioritized and simplified set of actions. The CIS Controls were formerly known as the SANS Critical Security Controls (SANS Top 20) but have been updated and streamlined to 18 controls in the latest version.

1. Inventory and Control of Enterprise Assets: Maintain a detailed inventory of all hardware devices within the organization to ensure only authorized devices are given access.

2. Inventory and Control of Software Assets: Keep an exhaustive list of all software in use to prevent unauthorized or vulnerable applications.

3. Data Protection: Implement measures to safeguard sensitive data from theft, loss, or unauthorized access.

4. Secure Configuration of Enterprise Assets and Software: Ensure all hardware and software configurations are secure and adhere to industry standards.

5. Account Management: Manage user accounts and their permissions to minimize unauthorized access.

6. Access Control Management: Restrict access to critical systems and data based on user roles and responsibilities.

7. Continuous Vulnerability Management: Regularly scan for vulnerabilities and apply patches to mitigate risks.

8. Audit Log Management: Maintain and review logs to detect suspicious activities and anomalies.

9. Email and Web Browser Protections: Implement security measures to protect email and web browsers from phishing and malware.

10. Malware Defenses: Deploy anti-malware tools to detect and block malicious software.

11. Data Recovery Capabilities: Ensure systems are backed up regularly and can be restored after an incident.

12. Network Infrastructure Management: Secure and manage network devices to prevent unauthorized access and cyber-attacks.

13. Security Awareness and Skills Training: Educate employees on cybersecurity practices and provide training to enhance their security skills.

14. Service Provider Management: Evaluate and monitor third-party service providers to ensure they comply with security requirements.

15. Application Software Security: Incorporate security measures throughout the software development lifecycle to protect applications from vulnerabilities.

16. Incident Response Management: Develop and maintain an incident response plan to quickly address and mitigate security incidents.

17. Penetration Testing: Regularly conduct penetration tests to identify and address security weaknesses.

18. Security Audit: Perform regular audits to assess and ensure compliance with security policies and procedures.

These controls are designed to help organizations defend against today's top threats by simplifying their approach to threat protection, complying with industry regulations, achieving essential cyber hygiene, and translating information into actionable steps.

## Security Architecture and Security Operations

Security architecture is the strategic design of systems, policies, and technologies to protect organizations OT from cyberthreats. A well-designed security architecture aligns cybersecurity with the unique business goals and risk management profile of the organization. A robust security architecture ensures that organizations have the infrastructure to properly prevent, detect, and respond to attacks. It also helps determine when and which technologies to implement, giving security decision-makers the ability to add new capabilities as the threat landscape evolves.

The first three steps are similar in many cybersecurity frameworks and are critical: (1) Map out your existing state, (2) describe your target state (and align it with the organization's risk profile), and (3) prioritize opportunities for improvement.

Security teams and hackers are often locked in an arms race – competing to outmaneuver each other. But for organizations to win this battle, they must shift their risk management approach from reactive to proactive. That means building in security from the beginning instead of fixing breaches only when they occur. A unified console that integrates management and orchestration across all the key components of cybersecurity architecture is necessary and should include:

- Network Security

- Cloud Security (on-premises, at edge locations, and across multiple public clouds)
- Endpoint Security (including IoT)
- Identity and Access Management (IAM)
- Data Protection
- Security Monitoring and Incident Response
- Security Governance, Compliance, and Risk Management

Security operations require clear communication of the plan across the organization, establishment of education and training programs and will use the architecture as a tool for building a cybersecurity culture within the enterprise.

## The Need for and Basics of Patching

Patching, in the context of IT security, refers to the application of software updates to address vulnerabilities and enhance both digital and physical security. Given the vulnerabilities outlined, patching is crucial for several reasons:

**Addressing Digital Vulnerabilities**

- Firmware Updates: Patching outdated firmware is fundamental to closing security gaps exploited by attackers.
- Segmentation: While not a direct patch, it's often a result of system updates and configuration changes, which are part of the patching process.
- Password Management: Password policies and enforcement mechanisms are often part of system updates and configuration changes.
- Intrusion Detection Systems: IDS software requires regular updates to maintain effectiveness.
- Access Controls: Patching can involve updating access control systems and implementing role-based access controls.

**Indirect Impact on Physical Security**

- Equipment Protection: Software updates can sometimes include features that improve equipment diagnostics, allowing for earlier detection of potential physical damage.
- Site Security: While not related, a robust digital infrastructure can support advanced physical security measures like video surveillance and remote monitoring.

## Additional Considerations

This section provides additional insight into the necessity of securing the supply chain, maintaining data backups, developing and testing incident response plans, and providing thorough employee training.

These measures are essential for enhancing the overall cybersecurity posture and ensuring robust protection against potential threats.

- **Supply Chain Security:** A lack of security measures in the supply chain for traffic signal components could allow the introduction of malicious hardware.
- **Data Backup and Recovery:** The absence of regular backups of traffic signal system configurations and data could hinder rapid recovery in a cyberattack or equipment failure.
- **Incident Response Planning:** Failing to develop and test an incident response plan could lead to ineffective management of security incidents.
- **Employee Training:** Inadequate security awareness training for employees involved in traffic signal operations and maintenance could increase the risk of security breaches.

## USDOT Policy Resources

Three policy resources for assistance in cybersecurity from the U.S. Department of Transportation (USDOT) are described below. These documents help grantees understand and comply with USDOT's cybersecurity requirements, as well as best practices for enhancing cybersecurity measures within the transportation sector.

1. Cybersecurity Resources | US Department of Transportation: The Office of Sector Cyber Coordination has developed a technical assistance guide to outline the USDOT's cybersecurity approach for its grant-funded projects. This guide helps grantees understand when they may be subject to DOT cybersecurity requirements, what DOT's current cybersecurity requirements are, and what informational resources are available to help grantees meet the cybersecurity requirements.
2. Cybersecurity, Privacy and Information Assurance Technology Operations and Infrastructure | US Department of Transportation: This resource outlines the DOT's cybersecurity priorities, including standards, policies, directives, situational awareness, incident response, independent verification and validation, certification and accreditation, and privacy.
3. USDOT ITS Research - General Cybersecurity References and Guides: This resource supports the transportation workforce by conducting research that adopts or adapts implementation practices from other industries or develops new approaches specific to transportation if needed.

## User Education and Career Development

Three important resources to help develop cybersecurity professionals are described below. These resources should provide a comprehensive view of the current state and future needs of workforce development for cybersecurity professionals.

1. Cybersecurity Education & Career Development | CISA: The Cybersecurity and Infrastructure Security Agency (CISA) is committed to strengthening the nation's cybersecurity workforce through standardizing roles and helping to ensure we have well-trained cybersecurity workers today, as well as a strong pipeline of future cybersecurity leaders for tomorrow. CISA provides a

wide range of opportunities for quality cybersecurity education and training, including the Cybersecurity Education and Training Assistance Program (CETAP).

2. Workforce Framework for Cybersecurity (NICE Framework) | NICCS: The NICE Framework is a nationally focused resource to help employers develop their cybersecurity workforce. It establishes a common lexicon that describes cybersecurity work and workers regardless of where or for whom the work is performed. The framework includes work role categories, competency areas, and tasks, knowledge, and skill statements.
3. Cybersecurity Workforce Training Guide | CISA: This guide helps professionals develop a training plan based on their current skill level and desired career opportunities. With over 100 training resources and certification prep courses, CISA's new guide can help cybersecurity professionals of all levels stay current and advance their careers.

## Conclusion

This primer underscores the multifaceted risks associated with operational technology, including software, hardware, technological obsolescence, cybersecurity threats, and operational risks. Cybersecurity is crucial as the digital landscape becomes increasingly complex and interconnected, amplifying the potential for cyber threats to disrupt essential services. We urge organizations to proactively address these vulnerabilities by adopting robust cybersecurity measures and staying abreast of technological advancements.  It is our hope with this primer that non-cybersecurity experts in the ITS and transportation industry writ large are able to improve their knowledge and understanding of cybersecurity best practices and associated threats. We must commit to making cybersecurity a top priority, fostering an environment where technological progress and safety go hand in hand.

*We would like to extend our gratitude to the ITS America Cybersecurity Community of Practice and AASHTO Transportation Cybersecurity Community of Practice for their contributions to this resource.*