



ITS AMERICA CYBERSECURITY FOR CONNECTED ITS INFRASTRUCTURE

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 Connected ITS Infrastructure

Executive Summary

This Cybersecurity for Connected ITS Infrastructure Resource Guide is intended to be used as an ITS cybersecurity guide and to further assist professionals in the ITS industry to secure our digital infrastructure. This document is relevant for cyber-informed ITS practitioners, state, and local department of transportation (DOT) staff, and ITS America stakeholders. The paper was authored and reviewed by members of the ITS America Cybersecurity Community of Practice (COP).

Providing detailed information on how to secure all connected ITS infrastructure is a task worthy of a large technical book with annual revisions, and we encourage all ITS America members interested in this topic to utilize this guide as just a starting point in their journey in how to secure our digital infrastructure. This guide is a sampling of the most common ITS cybersecurity topics and current resources for additional exploration by the reader.

The members of the Cybersecurity Community of Practice appreciate the diverse background and perspectives of all members of ITS America and recognize that we all have different levels of cybersecurity knowledge. Because of this, we would like to highlight an additional resource published in 2024 by the ITS America Cybersecurity Community of Practice, [*ITS America Cybersecurity for Novice Cyber Professionals Primer*](#), which will be a better starting point for those just beginning their journey in cybersecurity.

The format of this Cybersecurity for Connected ITS Infrastructure document allows readers to quickly access resources for securing connected ITS infrastructure. As subject matter experts, we have vetted and included the most relevant and timely online resources across the cybersecurity and ITS industry. The content in this document is accurate as of publication. This high-level guide provides brief definitions, resource links, and concise narratives for practitioners and stakeholders. The content in this document is accurate as of publication.

Our Task Force has leveraged years of preceding work done by the U.S. Department of Transportation (USDOT) as part of the National ITS Reference Architecture program. That framework is the Architecture Reference for Cooperative and Intelligent Transportation (ARC-IT), and the most recent update is version 9.2, 2023, [National ITS Reference Architecture, v9.2](#). This framework presents the physical connectivity layer of the ITS Architecture Diagram for all connected ITS components.

This Cybersecurity for Connected ITS Infrastructure guide is not an exhaustive list of ITS and Internet of Things (IoT) cybersecurity resources in the U.S. or across the industry, but rather a cybersecurity reference catalog for the most commonly used systems. The constantly changing technology ecosystem necessitates frequent updates of cybersecurity best practices.

In terms of the overall methodology for securing connected ITS infrastructure, there are two simple recommended principles for practitioners to understand:

1. **Zero Trust Architecture** (ZTA). [NIST.SP.800-207 – Zero Trust Architecture](#) is key as the evolutionary reference architecture superseding defense-in-depth, which was used in previous decades. Our networks' perimeter has evolved due to edge computing, cloud services, software as a service (SaaS), artificial intelligence (AI), and other technological advancements. It is important to design our digital environment and secure ITS infrastructure using ZTA models.
2. **Security by Design**. The U.S. Department of Energy (DOE) [Cyber-Informed Engineering Implementation Guide v1.0](#) is one of the latest resources that ensures cybersecurity is built into the design of technologies. A similar effort led by the U.S. Department of Homeland Security (DHS), Cybersecurity and Infrastructure Security Agency (CISA) is the 2024 [Secure by Design](#). This resource outlines industry best practices for designing products, software, systems, and networks for critical infrastructure with security built into the design of Information Technology (IT) and Operational Technology (OT) systems.

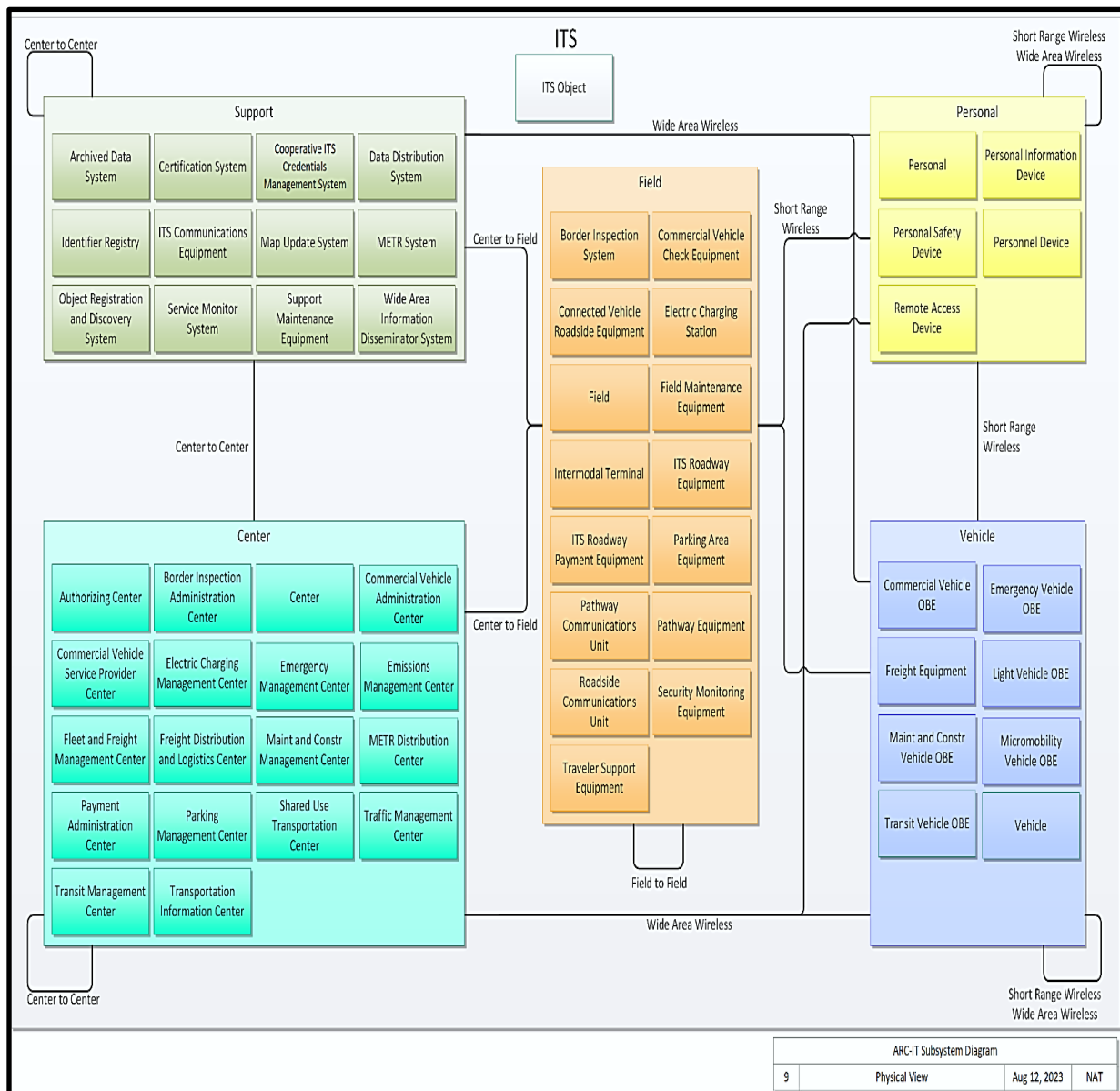
These methodologies are crucial to secure digital systems before they are placed into production and must be quickly and efficiently put into practice by the entire industry. For each topic, we have provided links, the date, and titles of documents to which we are referring, along with a brief narrative of content to assist in defining the subject matter. In some cases, we have included illustrations or infographics.

For brevity, clarity, and alignment with the National ITS Reference Architecture (ARC-IT) program, this paper is divided into three sections including:

1. Technology
2. Policy
3. People

The current ARC-IT physical view framework is illustrated in Figure 1 below.

Figure 1 - DOT ARC-ITv9.2 Physical Layer



Finally, we provide industry stakeholders with ten key recommendations based on this *Cybersecurity for Connected ITS Infrastructure* document. These are listed in priority order with the foremost being the need for a framework built around People, Process, and Technology for a secure ITS infrastructure. A more complete description of these ten key recommendations is included in the Conclusion section of this document.

- 1. The People, Process, Technology framework developed by Dr. Harold Leavitt in 1964** as a framework to help companies manage digital change is still relevant in 2024. This model emphasizes that successful organizational change and system implementation require an integrated approach, balancing the development of people (skillsets and culture), processes (workflows and methodologies), and technology (tools and systems).
- 2. Cyber-informed engineering and secure by design methodologies** both suggest that cybersecurity must be included incrementally throughout the entire lifecycle of any product, system, or network design in ITS.
- 3. Zero Trust Architecture** should be part of all system and network designs as our network perimeters have evolved and can no longer be supported by simple firewall or antivirus technologies.
- 4. Best practices and industry standards for securing connected infrastructure will continue to change in the near future.** Tracking this information must be an ongoing effort.
- 5. Internal OT, Internet of Things (IoT), and Intelligent Transportation Systems (ITS) cybersecurity policies and procedures must be developed by all transit and transportation agencies.** The most important of these policies and procedures is an Incident Response Plan. The time to develop an Incident Response Plan and practice using tabletop exercises is before you are attacked, not after.
- 6. Staffing levels and workforce retention will continue to be a challenge,** especially with OT, IoT, and ITS. The industry can advocate to include OT cybersecurity curriculum in accredited civil engineering, transportation engineering, and associated university and college programs.

7. **Collaboration is key to successfully secure connected ITS infrastructure.** Given the convergence of transportation and energy sector ecosystems in today's digital roadways, collaboration is a crucial component for success.
8. **Product vendors can be certified.** There is an option for vendors to purchase a test harness for internal testing through the [ISASecure Vendor Cybersecurity Certification Program](#). The ISASecure certification program is successfully delivering secure products in the ITS environment.
9. **Supply chain cybersecurity continues to be a concern across all critical infrastructure sectors including transportation.** DOE [Cybersecurity, Energy Security, and Emergency Response](#) (CESER) group has recently published a Call to Action to build cybersecurity throughout global supply chains in the energy sector which now includes EVSE. The ITS ecosystem should join in this DOE effort or establish a similar effort through the Joint Office of Energy and Transportation.
10. **Education and awareness must continue for the near future** to ensure securing our connected ITS infrastructure remains a safety priority for our digital roadways. Funding levels at the Federal, State, and local levels must not diminish as the cybersecurity challenge will remain.

Table of Contents

- Executive Summary..... 1
- 1. TECHNOLOGY 7
 - Vehicle 8
 - Field..... 14
 - Center..... 23
 - Personal 26
- 2. POLICY 27
 - Agency Cybersecurity Policies and Procedures 27
 - ISA/IEC 62443 29
 - National Electric Vehicle Infrastructure 29
 - National Institute of Standards and Technology..... 30
 - Federal Energy Regulatory Commission..... 31
 - Federal Highway Administration..... 32
 - ITE Traffic Signal Maintenance Manual 33
 - Manual on Uniform Traffic Control Devices for Streets and Highways 33
 - SAE International 35
 - SAE International 35
 - Cybersecurity Insurance 36
- 3. PEOPLE..... 37
 - Stakeholders..... 37
 - Roles and Responsibilities..... 38
 - Additional Staffing Considerations 41
 - Procurement Language Recommendations 45
 - Agency Maturity Level Considerations..... 45
- 4. SUMMARY & CONCLUSION 46
- 5. CREDITS..... 48

1. TECHNOLOGY

The Technology section provides an overview of the current state and considerations surrounding four of the six physical object classes listed in the USDOT National Reference Architecture v9.2. The four physical object classes discussed herein include vehicle, field, center, and personal as noted below. This is not intended to be a comprehensive list but a referential excerpt from ARC-IT v9.2.

Vehicles discussed include *autonomous and connected vehicles (AV and CV), electric vehicles, emergency vehicles, freight vehicles, drones, micromobility, and transit vehicles.* This is a small subset of the vehicles listed in the ARC-IT v9.2

Field objects refer to *infrastructure distributed near or along the transportation network, including 'intelligent' or 'smart' infrastructure which performs surveillance (e.g., traffic detectors, cameras), traffic control (e.g., signal controllers), information provision (e.g., Dynamic Message Signs (DMS)) and local transactions (e.g., tolling, parking) functions. Typically, their operation is governed by transportation management functions running in back offices.*

Center refers to *an entity that provides application, management, administrative, and support functions from a fixed location not in proximity to the road network. The terms "back office" and "center" are used interchangeably. Center is a traditionally a transportation-focused term, evoking management centers to support transportation needs, while back office generally refers to commercial applications. From the perspective of ARC-IT these are considered the same.*

Personal physical objects refer to *equipment used by travelers and others using personal devices to access transportation services pre-trip and en-route. This includes equipment that is owned and operated by the traveler/person as well as equipment that are owned by agencies and used/worn by staff/personnel.*

In summary, this technology section underscores the dynamic landscape of connected infrastructure that must be secured, emphasizing the importance of cybersecurity and evolving communication standards throughout the ITS landscape.

Vehicle

Vehicle technology is a rapidly evolving field characterized by significant advancements and complex challenges. This section explores these developments, particularly focusing on autonomous and connected vehicles. Autonomous vehicles (AVs) use technology to partially or entirely replace human drivers, navigating the vehicle and responding to traffic conditions.

According to the Society of Automotive Engineers (SAE), there are six levels of driving automation, ranging from Level 0, where the driver is responsible for all tasks, to Level 5, where the vehicle handles all driving tasks under all conditions. Automated vehicles (AVs) cover levels 1-4, where the vehicle can undertake some, but not all, driving tasks independently. This classification highlights the varying degrees of automation in modern vehicles and the technological advancements in autonomous driving.

Connected vehicles (CVs) are defined by SAE as those equipped with wireless communication devices, enabling real-time data exchange with other vehicles, infrastructure, and networks. The technology supporting connected vehicles includes cellular vehicle-to-everything (C-V2X) facilitating enhanced safety and mobility services.

Furthermore, this section addresses the vital issue of vehicle cybersecurity, referencing authoritative resources such as DHS-CISA, SAE, and NIST. The overview illustrates the complexity of modern vehicles and underscores the need for the consideration of additional vehicle cybersecurity measures.

- **Autonomous Vehicles and Automated Vehicles** - Autonomous vehicles equipped with technology can perform real-time operational and tactical functions required to operate a vehicle with and without human intervention or supervision. The Society of Automotive Engineers (SAE) provides a detailed classification system for levels of driving automation, ranging from Level 0 to Level 5.
 - Level 0: No Automation - The driver is responsible for all aspects of driving.
 - Level 1: Driver Assistance - The vehicle can assist with either steering or acceleration/deceleration using information about the driving environment. The driver must remain engaged and monitor the vehicle.
 - Level 2: Partial Automation - The vehicle can control both steering and acceleration/deceleration but requires the driver to remain attentive and take over

if necessary.

- Level 3: Conditional Automation - The vehicle can handle all aspects of driving under certain conditions, but the driver must be ready to intervene when requested by the system.
- Level 4: High Automation - The vehicle can perform all driving tasks in specific conditions or environments, with no intervention required from the driver.
- Level 5: Full Automation - The vehicle can handle all driving tasks under all conditions, eliminating the need for a driver.

This classification underscores the varying degrees of automation present in modern vehicles, highlighting the complexity and the technological advancements in the field of autonomous driving.

1. [DHS-CISA Vehicle Ground Vehicle Security Guide, 2024](#)
2. [Society for Automotive Engineering, ISO/SAE DIS 21434 Road Vehicle Cybersecurity Engineering, 2020](#)
3. [NIST Automated Vehicle Communications Overview, 2023](#)

- **Connected Vehicle** - A connected vehicle is one equipped with wireless communication devices integrated within the vehicle as manufactured or installed aftermarket. Vehicles typically use multiple modes of wireless communication to support many different use cases, including cellular vehicle to everything (C-V2X) technology which allows vehicles to communicate with roadside sensors and other technologies for enhanced safety and some local mobility services. The primary controller allowing for this communication is the Electronic Control Unit (ECU). Some of the first connected vehicles had one or two ECUs, but today connected vehicles contain 150 or more ECUs. There is also a Controller Area Network (CAN) topology allowing ECUs in a vehicle to communicate with each other. This is further defined in the SAE J1939 standard and in the On-board Diagnostics (OBD) standard.

1. [National Highway Traffic Safety Administration, Vehicle Cybersecurity, 2022](#)
2. [ISO/SAE 21434, Road vehicles, Cybersecurity engineering, 2021](#)
3. [ISO 11898-1 Road vehicles, Controller area network \(CAN\), Part 1: Data link layer and physical coding sublayer, 2024](#)

- **Cellular Vehicle-to-Everything (C-V2X)** - Cybersecurity plays a vital role in ensuring the safe and reliable operation of Cellular Vehicle-to-Everything (C-V2X) technology, which enables vehicles to communicate with each other, road infrastructure, pedestrians, and networks. As C-V2X continues to evolve, the security challenges it faces are becoming more complex. Key concerns include data integrity, privacy, and protection against cyber threats such as denial-of-service attacks, unauthorized access, and man-in-the-middle exploits. To counter these risks, strong authentication and encryption protocols are essential, ensuring that only legitimate entities can access the network and that all data exchanges remain confidential. Regular software updates, intrusion detection systems, and privacy-preserving techniques are also critical components of a comprehensive cybersecurity strategy. The adoption of secure boot processes, hardware security modules, and adherence to industry standards such as those set by ETSI and 3GPP further bolsters the defense of C-V2X systems. These represent standard practices among current C-V2X deployments and should remain top implementation priorities in future projects. Collaborative efforts between automotive manufacturers, telecommunications providers, regulatory bodies, and research institutions are necessary to create a resilient and secure C-V2X ecosystem, ensuring the safety and privacy of users in the increasingly connected transportation landscape. One example of this is the work being done by Omniair Consortium, an industry association which provides certification and interoperability testing to ensure that cybersecurity considerations are being fully addressed in C-V2X deployments. Industry collaboration through groups like Omniair Consortium and ITS America represents one significant way in which robust cybersecurity practices and standards can be maintained within the broader ITS community.

1. [FCC History of DSRC Service, 2022](#)
2. [ITS-America-Future-of-V2X-in-5.9-GHz-Report, 2024](#)
3. [ITS-America-V2X-Decoded-Final, 2024](#)
4. [C-V2X Use Cases: Methodology, Examples, and Service Level Requirements, 2019 \(5GAA\)](#)
5. [On-Board System Requirements for LTE-V2X V2V Safety Communications, J3161/1, 2022 \(SAE International\)](#)

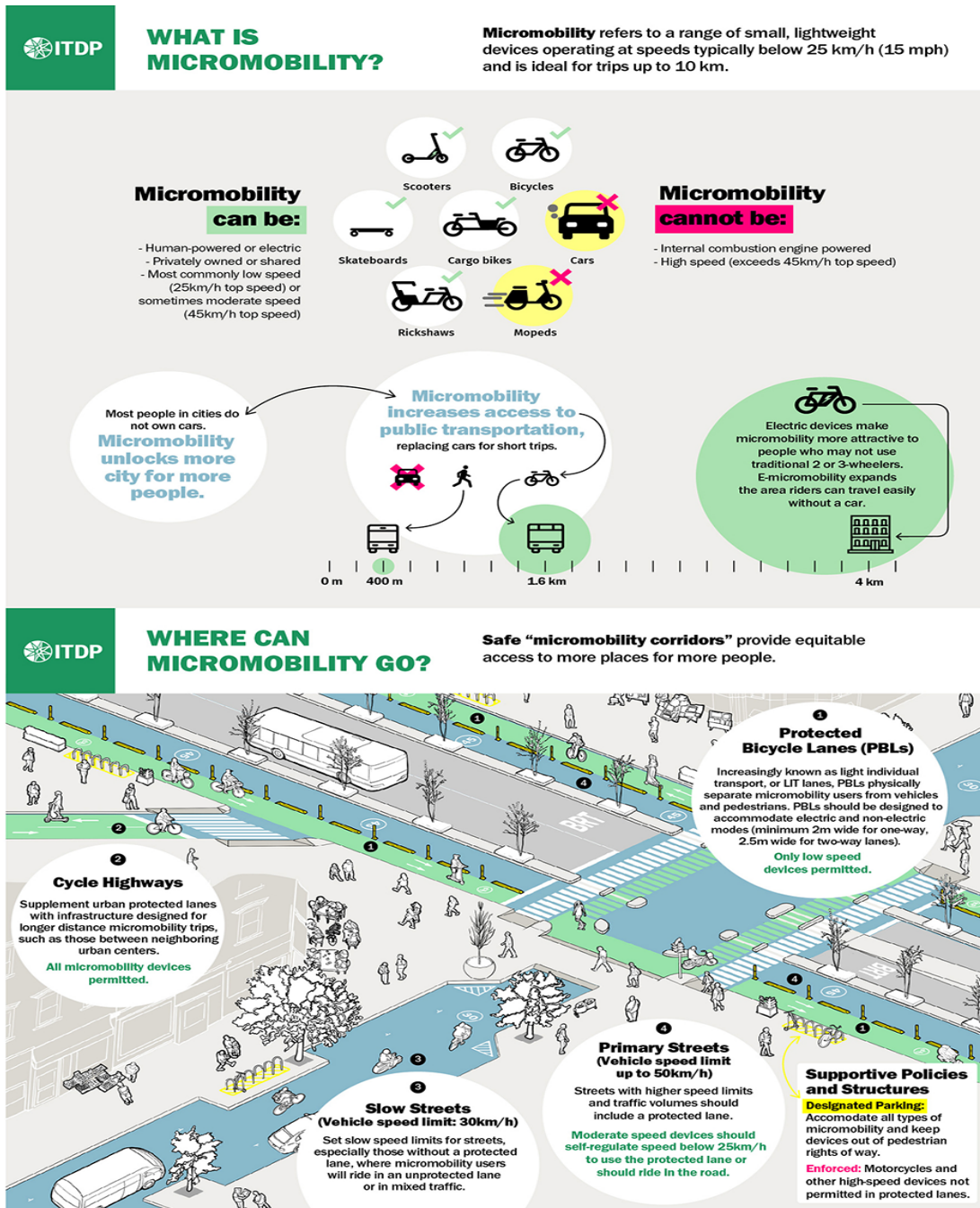
- **Drones** - Drones and Advanced Air Mobility (AAM) of many types will play a significant role in the future of our nation's transportation ecosystem. While cybersecurity for this technology is not yet fully regulated.

1. [DHS/CISA, Physical-Security/Be-Air-Aware, 2024](#)
 2. [NIST Uncrewed Aircraft Systems Working Group, 2024](#)
 3. [NIST UAS Standard Test Methods, 2020](#)
- **Electric Vehicles** - DOE defines electric vehicles as a vehicle that can be powered by an electric motor that draws electricity from a battery and is capable of being charged from an external source.
 1. [DEFCON CarHackingVillage.com, 2023](#)
 2. [IEEE Spectrum EV-Hacks, 2023](#)
 3. [Society for Automotive Engineering EV Safety and Security Training, 2024](#)
 - **Emergency Vehicles** - Generally speaking, an emergency vehicle is defined as an authorized ambulance, police, fire, rescue, recovery, or towing vehicle responding to an incident. Emergency Vehicles and related on-board equipment (OBE) must be secured such that radio communications used in these vehicles are encrypted and transmitted in a manner to ensure integrity and availability. Further information can be found in the [ARC-IT Emergency Vehicle object definition online](#).
 1. [IEEE1609.2 IEEE Standard for Wireless Access In Vehicular Environments— Security Services for Application and Management Messages, 2023](#)
 2. [FIPS 140-3 Encryption for Communications, 2019](#)
 3. [DOT-National Highway Traffic Safety Administration, Cybersecurity Best Practices for the Safety of Modern Vehicles, 2022](#)
 - **Freight Vehicle** - Referenced as Commercial Vehicles in the ARC-IT reference architecture, freight vehicles are vulnerable on multiple levels such as remote access to electronic logging devices, EVSE charging vulnerabilities, and other OBE communications via various non-secured RF frequencies.
 1. [National Motor Freight Traffic Association \(NMFTA\) Cybersecurity, 2024](#)
 2. [Federal Motor Carrier Safety Administration, Cybersecurity Best Practices, Updated, 2024](#)
 3. [NMFTA Trucking Cybersecurity, Stopping Hackers from Directly Attacking Our Trucks, 2024](#)
-

- **Micromobility** - USDOT defines Micromobility as any small, low-speed, electric-powered transportation device, including electric-assist bicycles (e-bikes), electric scooters (e-scooters), and other small, lightweight, wheeled electric-powered conveyances. Examples of Micromobility are illustrated in Figure 2 below. Micromobility devices sometimes operate on a pay-per-use basis, which could introduce cybersecurity risks within their backend payment systems. These systems, however, are subject to Payment Card Industry Data Security Standards (PCI DSS) regulations.

1. [U.S. DOT Electric Micro-mobility Website, 2024](#)
2. [PCI-DSS Website, 2024](#)
3. [Underwriter's Laboratory Micro-Mobility Device Evaluation, Testing, and Certification, 2024](#)

Figure 2 - Sourced from Institute of Transportation and Development Policy, www.itdp.org



- **Transit Vehicle** - The USDOT ARC-IT definition of transit vehicle is as follows:

“The 'Basic Transit Vehicle' represents the transit vehicle that hosts the on-board equipment that provides ITS functions. It includes a specialized and extended databus that is subject to different vehicle databus standards and hosts a broad

range of components that are unique to a transit vehicle including the farebox and associated electronics, passenger counters, and transit security systems. The Transit Vehicle may represent a bus, paratransit vehicle, light rail vehicle, or other vehicle designed to carry passengers.”

To better understand cyber vulnerabilities on transit vehicles, it is important to understand that all transit vehicles include a vehicular communications network of some type. Similar to physical building networks, vehicle networks are subject to many of the same types of attacks.

For buses, the “data bus” is often a Controller Area Network (CAN). For light rail and heavy rail systems, this is sometimes referred to as a Multi-function Vehicle Bus (MVB), a Wire Train Bus (WTB), or a Train Communication Network (TCN). There are multiple International Electrotechnical Commission (IEC), Institute of Electronics and Electrical Engineers (IEEE), and other standards for bus and rail communications.

1. [Rail Transit Systems Standards - American Public Transportation Association \(apta.com\), 2024 updates](#)
2. [Securing Control and Communications Systems in Transit Bus Systems \(apta.com\), 2019](#)
3. [Transportation Security Administration Rail Cybersecurity Mitigation Actions and Testing, 2022 with 2023 Updates](#)

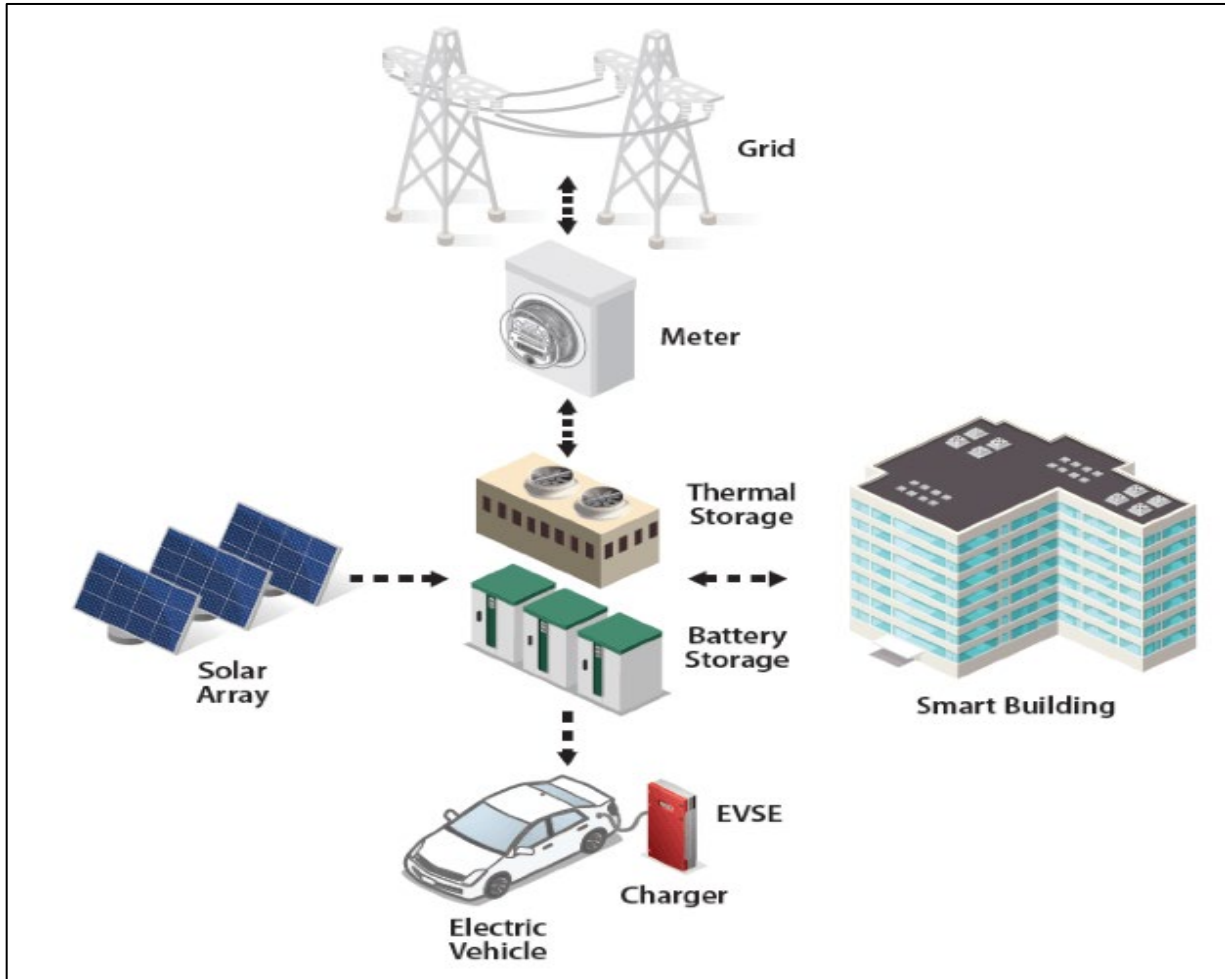
Field

The Field section outlines the standards and protocols necessary for cybersecurity considerations and data security measures for EV environments and intelligent transportation systems. Key resources and standards mentioned include FIPS 140-3, NTCIP, RFC 3410, ISO 15118-3, and IEEE 1547. The text emphasizes the importance of encryption and secure communication protocols to protect data at rest and in transit.

- **Data Security** - A detailed discussion about securing data at rest, data in transit, and data exchanges from vehicle to field and field to center and work zone data protection is beyond the scope of this document. Listed below are some links that describe securing this data. The data in ITS can be secured in much the same way other types of data in the IT environment are secured. Encryption at rest and in transit are key to secure communication protocols.

1. [FIPS 140-3 Security Requirements for Cryptographic Modules, 2019](#)
 2. [NTCIP | The NTCIP is part of a larger effort to develop a family of ITS standards, 2024 updates](#)
 3. [Internet Engineering Task Force Request for Comment \(RFC\) 3410, Introduction and Applicability Statements for Simple Network Management Protocol \(SNMP\) version 3, 2002](#)
- **Electric Vehicle Supply Equipment (EVSE)** (including meters and smart inverters) - EVSE is the commonly used acronym referring to Electric Vehicle Charging Systems and the components inside of each type. This includes the vehicle, the charging cable, and the charging stations themselves. There are many current vulnerabilities with all EVSE. An exhaustive list is not possible within the scope of this document. For more resources, please see the Policy section of this paper for IEEE, IEC, SAE, NREL, and other resources.
 1. [Open Charge Alliance Develops and Distributes the Open Charge Point Protocol, 2024 Updates](#)
 2. [ITS America White Paper, Considerations for a secure electric vehicle charging ecosystem, 2023](#)
 3. [NIST Guidance document on Cybersecurity for Electric Vehicle Fast Charging Infrastructure, 2023](#)
 - **Distributed Energy Resources (DERs)** - In a Vehicle-to-Grid environment with bi-directional charging from the EVSE/Vehicle back to the power grid, the EVSE/Vehicle becomes a DER. There are significant cybersecurity considerations which must be mitigated in these scenarios. An illustration from the National Renewable Energy Laboratory (NREL) is shown below in Figure 3 below.
 1. [ISO 15118-3, Vehicle to Grid Communication Interface, 2015](#)
 2. [IEEE 1547, Connecting Distributed Energy Resources, 2018](#)
 3. [National Renewable Energy Laboratory, Distributed Energy Resource Cybersecurity Framework Version 2, 2024 Updates](#)

Figure 3 - Sourced from NREL, EV Charging as DER



- Roadside Unit (RSU)** - A Roadside Unit is a transportation infrastructure communications device that enables communication between infrastructure and vehicles and among infrastructure. The devices are not “set and forget” devices and require firmware and other updates on a regular basis as do all network enabled devices. Some resources for understanding cybersecurity risks are included below. Individual vendors are responsible for tracking their own Common Vulnerabilities and Exposures (CVE) through the National Vulnerability Database (NVD).
 - [Ohio Department of Transportation DRAFT AV/CV Concept of Operations Guidebook, 2021](#)
 - [Institute of Transportation Engineers \(ITE\) Draft RSU Standard V01, 2021](#)
 - [U.S. DOT ARC-IT v9.2 National ITS Reference Architecture, 2023](#)

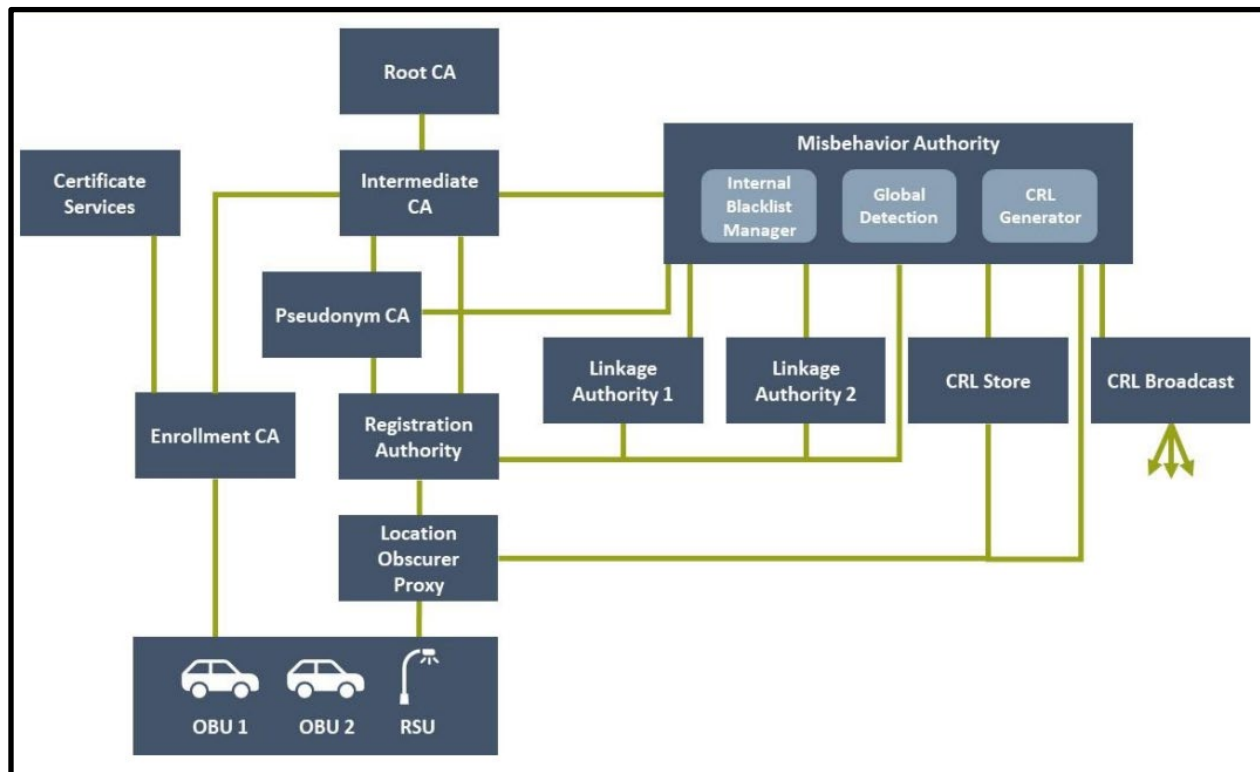
- **Roadway Payment Equipment** - This equipment includes roadway tolling systems, parking payment systems, rail and bus fare payment systems, and any other system that collects individual or group funds for transportation systems.
 1. [Payment Card Industry Data Security Standard, PCI-DSS, 2024 Updates](#)
 2. [International Bridge Tunnel and Turnpike Association, 2024 Updates](#)
 3. [Secure Technology Alliance for Transit Open Payment Systems and Smart Card, 2024 Updates](#)

- **Security Credentialed Management System (SCMS)** - The SCMS spans vehicle, field, and center subsystems. It is explained here in the Field subsystem section. The SCMS is implemented to provide a level of security for a specialized communications system that requires near-zero latency due to its safety-of-life applications. Traditional methods of securing communications such as encryption are not feasible in this case due to the latency added by the encryption overhead. This serves the baseline needs of a viable Vehicle to Everything (V2X) system, a method to establish a chain of trust among V2X end entities. The SCMS then ensures:
 1. Messages originate from another trusted device within the V2X ecosystem.
 2. Messages were not modified between sender and recipient.
 3. Misbehaving devices are detected and removed from the system.
 4. Verification of a message sender's trusted status is accomplished through security certificates assigned to the sending unit, "signing" the message and the recipient unit recognizing the certificate as valid according to the current library. These certificates used to sign messages are encrypted as they minimally impact latency.
 5. A mathematical algorithm similar to a checksum is used to verify the payload of the message has not been altered during transmission.
 6. Misbehavior detection, reporting and device removal are implemented but the maturity level continues to advance. While the system is improving the methods of detection, there are still weaknesses in the system, one of which is that the certificate revocation list (bad devices to drop from trust) is only sent out once daily. An illustration of the SCMS Ecosystem can be seen in Figure 4 below.

- 1. [U.S. DOT Intelligent Transportation Systems Joint Program Office, SCMS, 2020](#)

2. [U.S. DOT Connected Vehicle Deployment Technical Assistance: Security Credential Management System \(SCMS\) Technical Primer \(bts.gov\), 2019](#)
3. [U.S. DOT ITS Fact Sheets, SCMS, 2020](#)

Figure 4 - SCMS Ecosystem (Source: USDOT)



Connected vehicles communicating with traffic control devices such as RSUs and signal controllers represent an entry point to traffic control networks, and the SCMS, which provides the discussed assurances for the limited communication over V2X, does not additionally provide holistic cybersecurity protection for the attached ITS networks. A recommended Risk Management Framework (RMF) as described in other sections of this guide should be applied for all assets to be protected for an organization, and vulnerability scans should extend to V2X elements.

- **Security Monitoring Equipment** - This mostly refers to Closed Circuit Television (CCTV) cameras but also includes Intrusion Protection and Intrusion Detection Systems (IPS/IDS) and other physical security monitoring devices. Much has been written about the many cybersecurity vulnerabilities in CCTV systems, particularly since the onset of IP based cameras.

1. [American Society of Industrial Security \(ASIS\), 2024](#)
2. [NIST SP 800-82r3, 2023](#)
3. [FHWA Telecommunications Handbook, 2004](#)

- **Sensor Technologies** - Also sometimes referred to generically as Internet of Things (IoT) devices, sensor technologies are not unique to ITS but there are some applications which are more commonly seen in ITS digital infrastructure including but not limited to the following:
 - Radar sensors include LiDAR and speed sensors.
 - Traffic flow sensors include inductive loops.
 - Weigh In Motion Sensors.

Some of the challenges in securing these roadside sensor devices include authentication, insecure wireless network services, non-updated firmware, governance ambiguity, data privacy, and inability to install client-side monitoring due to processing constraints.

1. [NIST Cybersecurity for IoT Program | NIST, 2024](#)
2. [NIST SP 800-213, IoT Device Cybersecurity Guidance, 2021](#)
3. [DHS CISA Securing the Internet of Things, 2021](#)

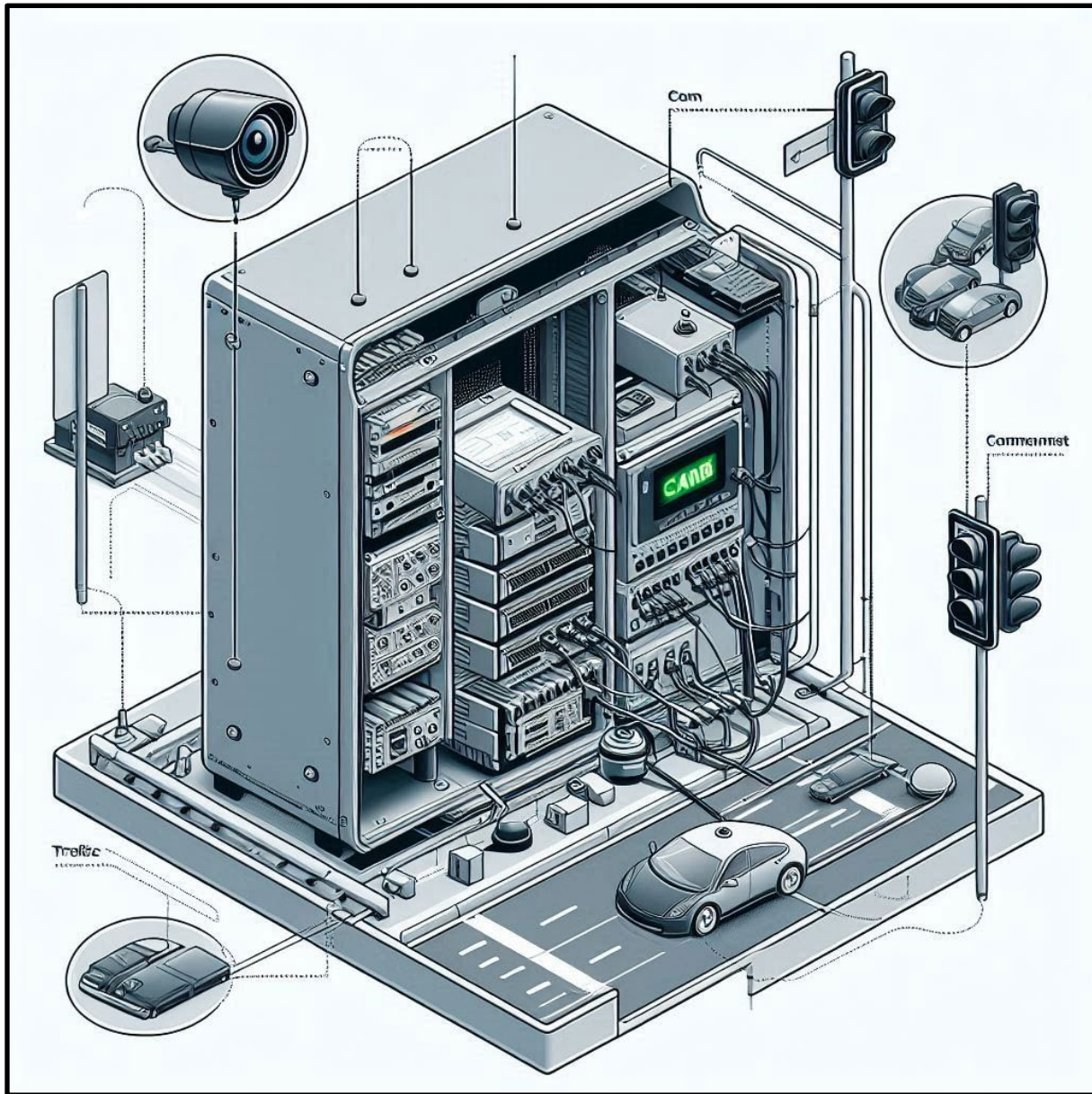
- **Traffic Management Systems, Advanced Traffic Management Systems (ATMS)** – ATMS consist of a multitude of technologies designed to make our traffic systems smarter and more efficient. Undoubtedly, artificial intelligence will continue to play a larger role in ATMS in the future. The connectivity of these systems requires additional protection against cybersecurity attacks. Currently the following components may be included in a traffic management system:
 - Real time, adaptive traffic signal timings using AI algorithms.
 - Environment adaptive timings based on weather or conditions.
 - Internet of Things devices such as sensors, cameras, and drones to collect and process data for predictive analysis.
 - Edge device computing (processing data at the device vs. a server).
 - Cloud based computing.

Securing ATMS requires multiple methods which can be reviewed here:

1. [National Cooperative Highway Research Program \(NCHRP\) Cybersecurity of Traffic Management Systems, 2024](#)
 2. [Transportation Review Board Cybersecurity of Traffic Management Systems, 2019](#)
 3. [IEC 61508, Functional Safety of Electrical, Electronic, Programmable Electronic Safety Related Systems, 2010](#)
- **Traffic Signal Controllers and Cabinets** - Traffic Signal Controllers and Traffic Cabinets, also referred to as Advanced Traffic or Transportation Controllers (or Cabinets), have evolved in the past 20 years. Some key considerations about traffic signal controllers and cabinets are below:
 1. In many cases, access into the traffic cabinets requires International Municipal Signal Association (IMSA) Level II certification [IMSA Level II Certification, 2024](#) which sometimes presents delays in mitigating physical network cybersecurity mitigations for OT/IoT/ITS cybersecurity.
 2. Primary components for an Advance Traffic Signal Controller Cabinet may include the following at a minimum:
 - **Controller Unit:** The brain of the traffic signal system. It processes data from sensors and determines signal timings. The unit provides a serial or ethernet connected interface for engineers to configure and monitor the system. There are Application Program Interfaces (APIs) [ITE Advanced Transportation Controller Unit API, 2022](#) that allow for proper management and monitoring of the device. This can be easily misconfigured such that a cyber-attack would be quite easy. Much care should be given to all API development.
 - **Cabinet Enclosure:** Protects the components from weather, vandalism, and other external factors.
 - **Traffic Signal Heads:** The actual signal lights (red, yellow, green) mounted on poles at intersections.
 - **Loop Detectors:** Inductive loops embedded in the road surface to detect vehicles and adjust signal timings. Today, these are largely replaced by CCTV.
 - **Pedestrian Signal Heads:** Separate lights for pedestrians, indicating when it is safe to cross.

- **Communication Module:** Connects to a central traffic management system for coordination and updates.
- **Conflict Monitor:** Detects faults or conflicts in the system.
- **Managed Ethernet Switch:** Facilitates communication between components.
- **Modem/Cellular Module:** Provides remote access and reporting capabilities.
- **CCTV Traffic Camera:** Monitors traffic flow and captures images for surveillance and analysis.
- **Traffic/Transit Signal Priority:** There are generally two types of transit signal priority mechanisms, passive and active. Passive transit signal priority uses traffic signal controller configuration and programming to achieve the most effective signal timing for transit vehicles. Active transit signal priority contains four primary components:
 1. Vehicle Onboard Equipment (OBE) to emit Radio Frequency (RF) priority request to traffic signal controller.
 2. Traffic Controller receiver/detector to receive RF request from vehicle and send to Discriminator unit.
 3. Discriminator receives a request from traffic controller and relays it to the backend Traffic Management software.
 4. Traffic Management software implements the transit signal priority, stores the data, and creates a log entry.
- **Traffic/Transit Signal Preemption:** Traffic controllers can be equipped with RF receivers to activate signal preemption by Emergency Vehicles with RF transmitters for this system.

Figure 5 - Diagram of ATC generated by Microsoft Co-Pilot DALL-E



As figure 5 illustrates, modern traffic signal cabinets are analogous to small data centers today. Managing cybersecurity vulnerabilities in this environment is increasingly challenging. From the technology perspective, there are systems like Artificial Intelligence, live video intelligence and heuristics, Application Programming Interfaces (APIs), and Software Defined Networking (SDN) for ethernet switches, among others, that can help mitigate cybersecurity concerns.

The challenge, however, lies with resources. The staff from maintenance, IT, ITS, OT, and management divisions, along with organized labor and budgetary considerations,

present challenges for responsibly managing and mitigating cybersecurity in these Advanced Traffic Controller Cabinets. As noted above, when physical access to the cabinet itself is limited across the organization, virtual and software defined management must be executed flawlessly.

1. [Advanced Transportation Controller \(ATC\) Standards - Institute of Transportation Engineers, 2018-2022](#)
 2. [ITE Cybersecurity for the ATC Standards, 2024](#)
 3. [U.S. DOT FHWA Traffic Signal Controller Handbook, Chapter 7, Local Controllers, 2022](#)
- **Traveler Equipment** - may include wayfinding signs, digital signage, passenger information systems, traveler information kiosks, 511 systems and others.
 1. [NIST SP 800-82r3 Guide to Operational Technology Cybersecurity, 2023](#)
 2. [NIST SP 800-53 Rev. 5, Security and Privacy Controls for Information Systems and Organizations, 2020](#)
 3. [DHS/CISA Securing Network Infrastructure Devices, 2024 updates](#)

Center

In today's rapidly evolving technological landscape, the cybersecurity of traffic management systems is paramount. This section delves into the various cybersecurity software tools and platforms that are integral to safeguarding these systems, highlighting their evolving nature and the critical role of AI in enhancing their effectiveness.

- **Cybersecurity Software Tools and Platforms** - This refers to the many diverse types of cybersecurity software tools and platforms that should be used in any type of traffic management center or security operations center, or combination of both. These software platforms change frequently so what may be a value-add today could be superseded tomorrow by something more powerful. AI algorithms will continue to make these cybersecurity software tools and platforms more effective at an increasing rate. Listed below are several types of cybersecurity software and tools:
 1. **Asset Management:** Software is essential to good cybersecurity hygiene. There are many now which are included in service desk packages and can be expanded to

include a Configuration Management Database (CMDB). The problem has not been with software, but with keeping software updated with limited resources.

2. **Certificate Management:** Software is also essential in any system which has Public Key Infrastructure (PKI). Certificate management software can be well worth the investment in ensuring certificates on web-enabled devices do not lapse and render part of your critical infrastructure unusable.
3. **Endpoint Detection and Response (EDR):** EDR requires a supplicant, or software agent, to be placed on the endpoint being monitored. This is not always possible for OT/IoT/ITS devices.
4. **Intrusion Detection and Intrusion Prevention Systems (IDS/IPS):** IDS/IPS have gained much popularity in the past decade. They are easier to manage and use than a SIEM (described below) and there are several platforms specifically built for OT/IoT/ITS devices.
5. **Managed Detection and Response (MDR):** MDR is closely related to Security as a Service (SaaS). As with Endpoint Detection and Response (EDR) and Extended Detection and Response (XDR), this service typically requires a supplicant (client) software on the end device. This is not feasible with many OT/IoT/ITS devices.
6. **Scanning Software:** This can be mobile to be used on laptops ad-hoc, or permanently installed on an appliance to continuously scan the entire IP-enabled environment. All software of this type uses some version of the original Network mapping tool (Nmap) as a backend, and some combine Simple Network Management Protocol (SNMP) capabilities. Common drawbacks for OT/IoT/ITS devices are that these solutions can only scan IP-enabled devices and many OT devices do not speak IP nor are they connected via Ethernet. There is no uncomplicated way to scan serial connected devices.
7. **Security Information and Event Management (SIEM):** once highly sought after, now with questionable value in a flooded market. Each agency must determine usefulness in an ITS environment for themselves. These platforms are expensive and require a lot of fine tuning to be effective. Artificial Intelligence has begun to help simplify this process.
8. **Extended Detection and Response (XDR):** is an expanded version of EDR which allows for monitoring in large multi-domain environments. This solution still requires a supplicant or agent to be installed on all devices being monitored, which is not feasible for many OT/IoT/ITS devices.

Additional information can be found at these links:

1. [DHS/CISA Free Cybersecurity Services and Tools for Critical Infrastructure Including Transit and Transportation Agencies, 2024 updates](#)
 2. [DHS/CISA Continuous Diagnostic and Mitigation Approved Product List, 2024](#)
 3. [Center for Internet Security Tools, 2024](#)
- **Transportation or Traffic Management Center (TMC)** - is defined by the Federal Highway Administration (FHWA) as:

“The hub or nerve center of most freeway management systems. It is where the data about the freeway system is collected and processed, fused with other operational and control data, synthesized to produce “information,” and distributed to stakeholders such as the media, other agencies, and the traveling public. TMC staff uses the information to monitor the operation of the freeway and to initiate control strategies that affect changes in the operation of the freeway network. It is also where agencies can coordinate their responses to traffic situations and incidents. The role of a TMC often goes beyond the freeway network and the responsible agency, functioning as the key technical and institutional hub to bring together the various jurisdictions, modal interests, and service providers to focus on the common goal of optimizing the performance of the entire surface transportation system. Because of its critical role in the successful operation of a freeway management system (and perhaps the broader surface transportation network), it is essential that the TMC be planned for, designed, commissioned and maintained to allow operators and other practitioners to control and manage the functional elements of the freeway management system, and possibly beyond.”

The TMC is evolving and many state DOTs are designing hybrid virtual/physical TMCs. It is possible that TMCs in the future will be entirely virtual.

It is important to consider how cybersecurity platforms and solutions will be integrated with the TMC. Will these continue to be separate and managed by IT, or will cybersecurity platforms become more fully integrated into the TMCs of the 21st century?

1. [U.S. DOT/FHWA Transportation Management Center, 2020](#)
2. [U.S. DOT/FHWA Transportation Management Center IT Security Considerations, 2019](#)

3. [Transportation Research Board \(TRB\), Cybersecurity of Traffic Management Systems, 2019](#)
- **Building Automation Systems** - While not listed in the ARC-IT v9.2, they have been added here as these systems which include Heating, Ventilation, and Air Conditioning (HVAC), meters, lighting systems, fire systems, elevators, and others are smart and IP-enabled. Any Traffic Management Center or transportation facility should include secure Building Automation Systems.
 1. [ISA/IEC 62443 Series of Standards – ISA, 2024 Updates](#)
 2. [3 Steps to Building Automation System Cybersecurity - Facilities Management Insights \(facilitiesnet.com\), 2024 Updates](#)
 3. [American Society of Heating, Refrigeration, and Air Conditioning \(ASHRAE\) Building Automation Systems Addressing The Cybersecurity Threat, 2024 Updates](#)

Personal

This section delves into the cybersecurity considerations for personal devices and systems within the context of transportation management. By examining the integration of these technologies, we can ensure a more secure and resilient transportation infrastructure.

- **Remote Access Devices** - These devices can include any device which is remotely connected into an ITS subsystem. In this paper, we are including smart phones. Application Program Interfaces (API) cybersecurity is also included in this category as APIs often enable more effective use of mobile applications in transportation.
 1. [Open Worldwide Application Security Project \(OWASP\), 2023](#)
 2. [NIST SP 800-77r1 Guide to IPSEC VPNs, 2020](#)
 3. [NIST SP 800-124r2, Guidelines for Managing the Security of Mobile Devices in the Enterprise, 2023](#)

2. POLICY

This section delves into the major policy initiatives that address the integration of cybersecurity within transportation technologies. It highlights the contributions of various standards bodies and provides insights into the development of comprehensive cybersecurity policies and procedures for transit and transportation agencies.

This section also contains the major policy initiatives surrounding the technologies addressed above as published by specific U.S. stakeholder groups. Any known gaps, shortcomings, or recommendations for each policy, standard, or program initiative have been identified. There are too many standards bodies involved in cybersecurity to include in this document because of the convergence of the energy and transportation industries. For those seeking more detailed information, here is a partial list of additional standards stakeholder groups:

- International Electrotechnical Commission (IEC)
- Institute of Electrical and Electronics Engineers (IEEE)
- International Standards Organization (ISO)
- United Nations Economic Commission for Europe (UNECE)

In terms of cybersecurity policy, the first step is the requirement for any transit or transportation agency to develop their own individual cybersecurity policies and procedures.

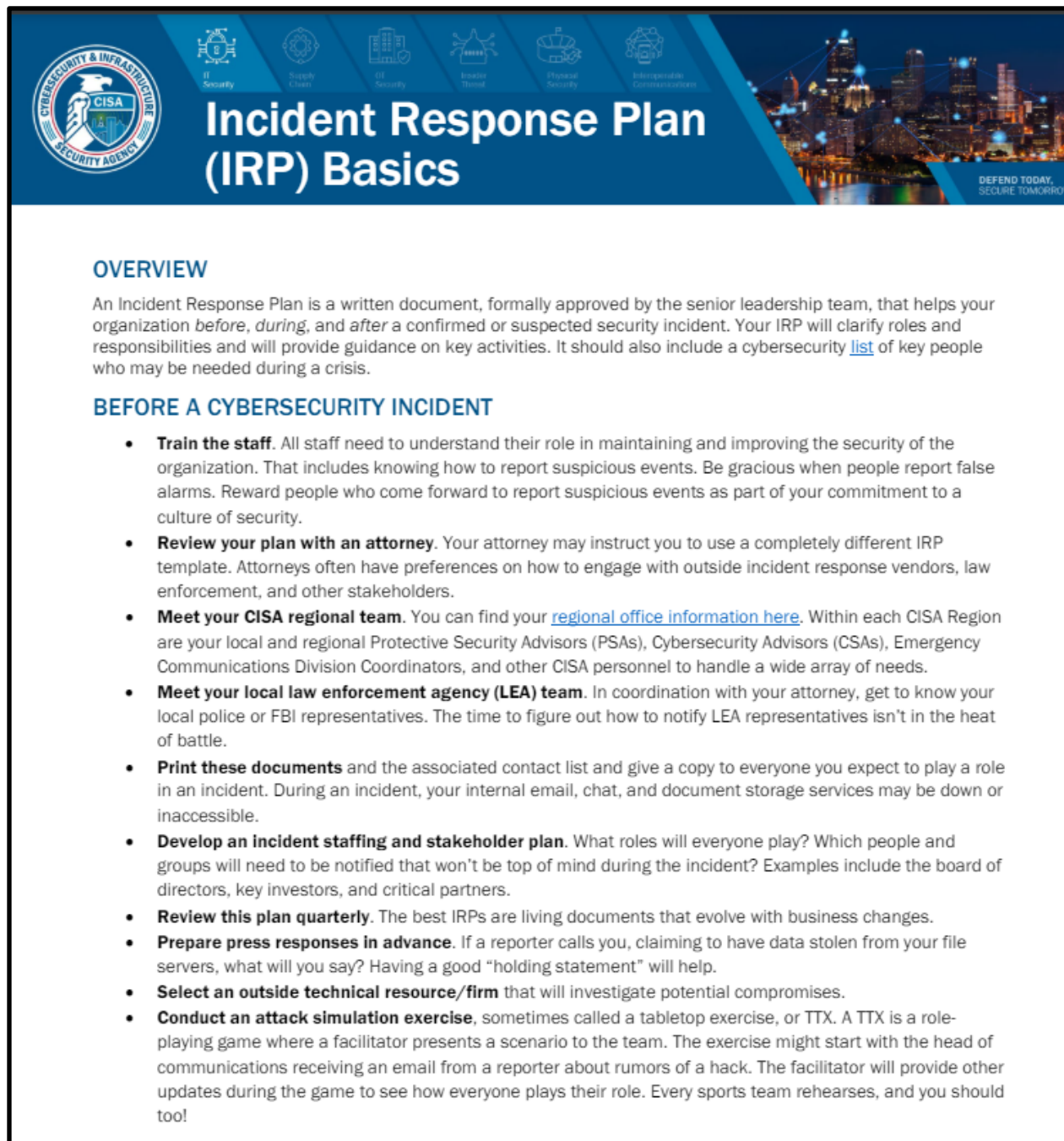
Agency Cybersecurity Policies and Procedures

When developing internal cybersecurity policies and procedures for non-IT infrastructure such as ITS, refer to NIST SP 800-82r3, which was recently updated in 2023 and renamed to “[Guide to Operational Technology \(OT\) Cybersecurity](#)”. OT is the term used for all things that are cyber-physical and use controllers, sensors, actuators, or other control systems to operate. In ITS, this includes things like traffic signal controllers, reversible lanes controls and gates, rail crossing gates, Autonomous and Connected Vehicles, Electric Vehicle Supply Equipment (EVSE), and all the other components listed in the Technology section of this paper in Vehicle, Field, Center, or Personal subsystems.

NIST SP 800-82r3 can be used effectively to develop ITS/OT/IoT cybersecurity policies and procedures. The most important policy and procedure an agency has is the Incident Response Policy. DHS/CISA has developed an extensive library of training, samples, and playbooks for incident response plans some of which can be found here: [DHS-CISA Incident Response Planning Strategies](#).

Additionally, NIST published a Computer Security Incident Handling Guide in 2012, [NIST.SP.800-61r2](#) and released a draft revision three for comment in 2024, [Considerations for Cybersecurity Risk Management](#). An illustration of NIST Response Basics resources can be seen in Figure 6 below.

Figure 6 - NIST Incident Response Basics



The infographic is titled "Incident Response Plan (IRP) Basics" and features the CISA logo on the left. At the top, there are six icons representing different security domains: IT Security, Supply Chain, IT Security, Insider Threat, Physical Security, and Interoperable Communications. The background shows a city skyline at night with the slogan "DEFEND TODAY, SECURE TOMORROW".

OVERVIEW

An Incident Response Plan is a written document, formally approved by the senior leadership team, that helps your organization *before, during, and after* a confirmed or suspected security incident. Your IRP will clarify roles and responsibilities and will provide guidance on key activities. It should also include a cybersecurity [list](#) of key people who may be needed during a crisis.

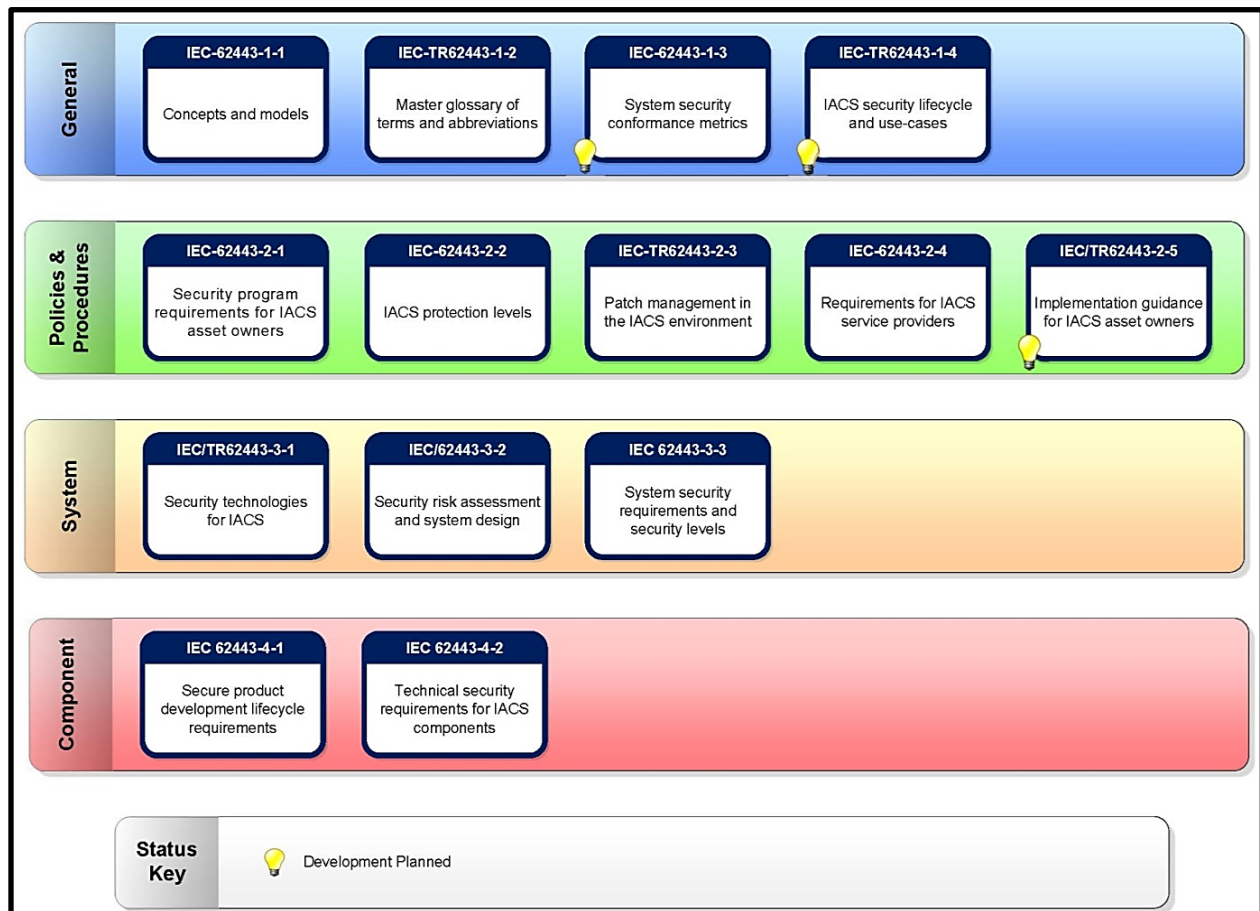
BEFORE A CYBERSECURITY INCIDENT

- **Train the staff.** All staff need to understand their role in maintaining and improving the security of the organization. That includes knowing how to report suspicious events. Be gracious when people report false alarms. Reward people who come forward to report suspicious events as part of your commitment to a culture of security.
- **Review your plan with an attorney.** Your attorney may instruct you to use a completely different IRP template. Attorneys often have preferences on how to engage with outside incident response vendors, law enforcement, and other stakeholders.
- **Meet your CISA regional team.** You can find your [regional office information here](#). Within each CISA Region are your local and regional Protective Security Advisors (PSAs), Cybersecurity Advisors (CSAs), Emergency Communications Division Coordinators, and other CISA personnel to handle a wide array of needs.
- **Meet your local law enforcement agency (LEA) team.** In coordination with your attorney, get to know your local police or FBI representatives. The time to figure out how to notify LEA representatives isn't in the heat of battle.
- **Print these documents** and the associated contact list and give a copy to everyone you expect to play a role in an incident. During an incident, your internal email, chat, and document storage services may be down or inaccessible.
- **Develop an incident staffing and stakeholder plan.** What roles will everyone play? Which people and groups will need to be notified that won't be top of mind during the incident? Examples include the board of directors, key investors, and critical partners.
- **Review this plan quarterly.** The best IRPs are living documents that evolve with business changes.
- **Prepare press responses in advance.** If a reporter calls you, claiming to have data stolen from your file servers, what will you say? Having a good "holding statement" will help.
- **Select an outside technical resource/firm** that will investigate potential compromises.
- **Conduct an attack simulation exercise**, sometimes called a tabletop exercise, or TTX. A TTX is a role-playing game where a facilitator presents a scenario to the team. The exercise might start with the head of communications receiving an email from a reporter about rumors of a hack. The facilitator will provide other updates during the game to see how everyone plays their role. Every sports team rehearses, and you should too!

ISA/IEC 62443

The ISA 62443 as it is commonly called is an evolution of the ISA99 committee on cybersecurity developed by the International Society of Automation (ISA) 20 years ago. This suite of standards is gaining momentum in the United States and Europe as the de facto cybersecurity standards for OT. An Illustration of [ISA/IEC 62443](#) can be seen in Figure 7 below.

Figure 7 - ISA/IEC 62443 Cybersecurity Standards



National Electric Vehicle Infrastructure

The National Electric Vehicle Infrastructure (NEVI) Standards and Requirements were codified in 2023 as Title 23, Chapter I (FHWA/DOT), subchapter G Engineering and Traffic Operations), Part 680. These have been updated as of June 2024 and the updated version can be found [here](#).

ITS America released [Considerations for a Secure Electric Vehicle Charging Ecosystem](#)

technical exchange panel white paper in August 2023. This white paper discussed cybersecurity considerations for electric vehicle charging infrastructure and brought specific attention to the immediate problems that cybersecurity is not being consistently implemented across the U.S. in accordance with any one framework for design, installation, or maintenance.

The FHWA ITS Cybersecurity Research Program, [USDOT ITS Research - About ITS Cybersecurity](#), was developed to meet the urgent need to protect ITS from cyber-attacks. The stated goal for this program is to provide resources and tools to ITS stakeholder communities in support of cyber-resilient, secure ITS implementations. Emerging from this research was the Request for Information (RFI) on the J3400 Connector and Potential Options for Performance-Based Charging Standards published on March 6, 2024. The top ten current recommendations for FHWA's NEVI cybersecurity guidance are noted below:

1. Update requirement for OCPP version to 2.1 minimum.
2. Update TLS requirements to TLS 1.3 or latest version.
3. Increase the use of Artificial Intelligence to monitor anomalies across the Bulk Electric System (BES) before enabling bi-directional charging at scale.
4. Do not rely solely on TLS for end-to-end OCPP security. Think Zero Trust i.e., Third party MFA and VPN solutions.
5. Prohibit the use of hard-coded credentials in OEM charging station firmware.
6. Mandate both client and server certificates.
7. Inform system integrators not to connect Commercial EV Charging Stations directly to the Internet without some form of perimeter defense.
8. Update the requirements to include ISO 15118-2
9. Include a newly developed U.S. national standardized reference architecture.
10. Update charging standard to incorporate the new North American Charging Standard (NACS), SAE J3400.

National Institute of Standards and Technology

The National Institute of Standards and Technology (NIST) has released two interagency reports regarding electric vehicle infrastructure:

- [NIST Interagency Report 8473, Cybersecurity Framework for Electric Vehicle Extreme Fast Charging Infrastructure, 2023](#)

- [NIST Interagency Report 8294, Symposium on Federally Funded Research on Cybersecurity of Electric Vehicle Supply Equipment \(EVSE\), 2020](#)

Notably, the NIST 800 series special publications on cybersecurity are written for Federal agency compliance. For private sector companies that are not contracted to the Federal government, NIST is not enforceable, but merely a recommendation. There is one NIST 800 series special publication that provides guidelines for OT of which ITS is often a subset, and that is [NIST SP 800-82r3, Guide to Operational Technology Security](#).

Recommendations for NIST regarding EVSE and cybersecurity include:

1. Develop and publish an EVSE reference architecture for the United States.
2. Use NIST SP 800-82r3 as guideline for OT/IoT controls vs. 800-53r5 which is IT focused.
3. Update NIST 8473 and 8294 Interagency Reports to include OT control criteria.

Federal Energy Regulatory Commission

The U.S. Federal Energy Regulatory Commission (FERC) approved the first North American Electric Reliability Corporation Critical Infrastructure Protection (NERC CIP) set of standards in 2008 used to regulate cybersecurity functions of entities that are connected to the Bulk Electric System (BES) in North America. Most recently, NERC CIP Version 5 was approved in May 2024.

NERC CIP standards do not currently apply to Distributed Energy Resources (DERs). However, since EVSE or EV charging systems will have bi-directional power capabilities as part of V2G, efforts are underway to enhance cybersecurity for the EV infrastructure of the future. NERC is currently developing strategies to manage Distributed Energy Resources (DERs). In January 2024, NERC published a “[Preliminary Findings and Recommendations](#)” document. Prior to that publication, in 2023, NERC published its “EV Modeling and Parameterization” white paper found here: [Electric Vehicle Technical Reference Report](#). Of these two documents, only the 2024 release mentions cybersecurity to any extent, stating that this white paper:

“...does not discuss the cyber security risk associated with EV charging in detail (e.g., reviewing threat intelligence), but the electric industry, through ongoing activities, seeks to analyze EV and charging system vulnerabilities and recommend areas of research to enhance security by design for the equipment.”

FERC issued a final rule on January 19, 2023, requiring NERC to develop new reliability standards. These standards will mandate internal network security monitoring for high and medium impact bulk electric system (BES) cyber systems with external routable connectivity within trusted Critical Infrastructure Protection networks. This is an important ruling for EV charging stations for the following reasons:

1. As EV adoption increases, charging stations, integral to the electric grid, may fall under the Critical Infrastructure Protection (CIP). The CIP standards developed by NERC would ensure these stations have strong cybersecurity measures.
2. High and medium impact BES cyber systems may encompass EV charging stations due to their significant power draw. This would mean reliability standards directly influence the cybersecurity of these stations.
3. The NERC directive mandates network security monitoring within trusted environments, meaning that connections to and from EV charging stations must be monitored for cybersecurity threats, aiding in early threat detection and mitigation.
4. EV charging stations are currently internet-connected to support functions like remote monitoring and billing. Without appropriate perimeter protection, the charging stations remain vulnerable to cyber-attacks. For this reason, the directive's inclusion of "medium-impact BES cyber systems with external routable connectivity" should include EV infrastructure cybersecurity measures.

Further reading can be found at these links below:

1. [North American Electric Reliability Corporation Potential Bulk Power System Impact of Vehicle Chargers, 2024](#)
2. [Federal Energy Regulatory Commission Directs North American Electric Reliability Corporation to Update Cybersecurity Standards | Environmental and Energy Brief, 2024](#)
3. [American Public Power Association, NERC Sees Need for Greater Cross Sector Collaboration, 2024](#)

Federal Highway Administration

The Federal Highway Administration (FHWA) provides guidance and approves plans related to EV infrastructure, leaving the actual implementation of cybersecurity measures to be conducted by state and local agencies, as well as private sector partners. For FHWA

updates on NEVI, see the [NEVI section above](#).

FHWA announced it has adopted the Cyber Security Evaluation Tool (CSET) now distributed by DHS/CISA. This tool was originally developed by DOE Idaho National Laboratory more than a decade ago and its current version is 12.x, which includes many new features.

1. [FHWA adopts the CSET tool, 2024](#)
2. [DHS/CISA CSET Tool Download Instructions, 2024](#)
3. [FHWA Cybersecurity Handbook, 2017](#)

ITE Traffic Signal Maintenance Manual

The risk management chapter of the first edition of this ITE Traffic Signal Maintenance manual focused only on legal liability avoidance through physical maintenance of the equipment and roadway. The second edition recognizes that service disruptions, equipment damage, and unauthorized access to full OT and IT networks can be achieved via cyber-attacks, added a high-level section on best practices and external references available.

ITE has included cybersecurity in the March 2023 Second Edition of the ITE Traffic Signal Maintenance Handbook for the first time since original publication. The handbook is available for a small fee to both ITE members and non-members here: [ITE Traffic Signal Maintenance Handbook, 2023](#).

Manual on Uniform Traffic Control Devices for Streets and Highways

[The Manual on Uniform Traffic Control Devices for Streets and Highways](#) (MUTCD) does not contain any information regarding cybersecurity for traffic control devices as of the current 2023 edition. It is highly recommended that the next version of MUTCD includes cybersecurity considerations for traffic control devices. The FHWA website states the following about the MUTCD:

“The Manual on Uniform Traffic Control Devices for Streets and Highways—the MUTCD—defines the standards used by road managers nationwide to install and maintain traffic control devices on all streets, highways, pedestrian and bicycle facilities, and site roadways open to public travel. The MUTCD is published by the

Federal Highway Administration (FHWA) under [23 Code of Federal Regulations \(CFR\), Part 655, Subpart F](#).

The MUTCD, which has been administered by the FHWA since 1971, is a compilation of national standards for all traffic control devices, including road markings, highway signs, and traffic signals. It is updated periodically to accommodate the nation's changing transportation needs and address new safety technologies, traffic control tools, and traffic management techniques.

On December 19, 2023, a Final Rule adopting the 11th Edition of the MUTCD was published in the Federal Register with an effective date of January 18, 2024. States must adopt the 11th Edition of the National MUTCD as their legal State standard for traffic control devices within two years from the effective date. The Federal Register notice, which provides detailed discussion of the final dispositions of major changes from the 2009 edition, can be viewed at [Federal Register: National Standards for Traffic Control Devices](#).

FHWA does not print copies of the MUTCD. The PDF version of the [11th Edition of the MUTCD](#) is the most current edition of the official FHWA publication.”

MUTCD is the most trusted source of information for traffic and highway engineers. Cybersecurity guidance for these critical infrastructure devices should be added in coming editions.

SAE International

SAE International, originally established as the Society of Automotive Engineers, is a global association committed to advancing mobility knowledge and solutions for the benefit of humanity. Founded in 1905, SAE brings together engineers, technical experts, and professionals from various industries, including aerospace, automotive, and commercial vehicles. Their mission is to provide a platform for the development of standards, foster innovative technologies, and support lifelong learning for engineers and other technical professionals worldwide.

SAE plays a crucial role in the development of industry standards that ensure safety, reliability, and efficiency in transportation systems. Their standards cover a wide range of areas including vehicle design, manufacturing processes, and cybersecurity measures. SAE's J2945/5 standard, for instance, provides specific permissions and security guidelines for connected vehicle applications, highlighting their commitment to addressing the challenges posed by emerging technologies. Additionally, their J3061 Cybersecurity Guidebook for Cyber-Physical Vehicle Systems offers comprehensive guidance on securing vehicle systems against cyber threats, showcasing their pivotal role in safeguarding modern transportation infrastructure.

By fostering collaboration among industry stakeholders, SAE facilitates the development and adoption of best practices that enhance both innovation and safety. Their work ensures that as technology evolves, it does so within a framework that prioritizes the well-being of society. Their emphasis on cybersecurity is particularly significant in today's digital age, where the integration of cyber-physical systems poses new risks and opportunities. With cyber threats becoming increasingly sophisticated, SAE's standards play a vital role in setting the foundation for secure and resilient transportation systems. Through their standards and educational initiatives, SAE International continues to be a cornerstone in driving progress and ensuring the resilience of critical transportation systems.

SAE International

Service Specific Permissions and Security Guidelines for Connected Vehicle Applications

J2945/5_202002, available for purchase/download at SAE website: [SAE J2945/5_202002: Service Specific Permissions and Security Guidelines for Connected Vehicle Applications - SAE International, 2020.](#)

Security Specification through the Systems Engineering Process for SAE V2X Standards, available for purchase at: [SAE Security Specification Through the Systems Engineering Process, 2020.](#)

Cybersecurity Guidebook for Cyber-Physical Vehicle Systems J3061_20160, available for purchase at: [SAE J3061, Cybersecurity Guidebook for Cyber-Physical Systems, 2020.](#)

Cybersecurity Insurance

Cybersecurity insurance continues to be an active topic at the Federal, State, and local levels as insurance companies are faced with unprecedented numbers of claims by cybersecurity insurance holders. Agencies and insurance clients should be prepared to demonstrate cybersecurity measures such as incident response plans, continuous monitoring, and other implemented measures as insurers typically require certain standards to be met for coverage.

In June 2024, the U.S. House Homeland Security Committee's Subcommittee on Cybersecurity and Infrastructure Protection convened a hearing to examine the vulnerabilities of the U.S. critical infrastructure. The hearing also focused on the role of [cyber insurance](#) in planning, response, and recovery efforts to ensure [critical infrastructure resilience](#). Details can be found here: [US House Subcommittee examines critical infrastructure vulnerabilities, role of cyber insurance in resilience efforts - Industrial Cyber.](#)

The recent release of the National Security Memorandum-22 (NSM-22), [National Security Memorandum on Critical Infrastructure Security and Resilience | The White House](#), confirms that transportation remains one of the Department of Homeland Security (DHS) 16 critical infrastructure sectors [DHS 16 Critical Infrastructure Sectors](#). DHS CISA has begun a re-write of Sector-Specific Plans for Sector Risk Management Agencies (SRMAs) and created a new organizational structure to accommodate each of the sectors within CISA. Overall, for the transportation sector and ITS, cybersecurity insurance can be particularly unique in its challenges. Some areas which must be considered are:

1. Data Breach Coverage
2. Business Interruption

3. Ransomware Protection
4. Third-Party Liability
5. IoT Device Security
6. Regulatory Compliance
7. Cyber Extortion
8. Social Engineering Fraud
9. Reputational Damage
10. Incident Response Services
11. System Upgrade and Patch Management
12. Supply Chain Risk

A review of current cybersecurity insurance concerns for the transportation industry is beyond this document's scope. However, below are some current resources with more information.

1. [Mineta Transportation Institute White Paper, Is There Light at End of Tunnel Outlook for Cybersecurity Insurance and Transit, 2024](#)
2. [DHS/CISA Cybersecurity Insurance Working Group, 2023](#)
3. [National Association of Insurance Commissioners, Cybersecurity Insurance Update Report, 2023](#)

The Cybersecurity Association of Maryland recently published a 2024 cyber insurance market outlook online [here](#).

3. PEOPLE

This section delves into the critical role of human factors in ensuring the cybersecurity of a connected Intelligent Transportation Systems (ITS) ecosystem. It highlights the importance of clearly defined roles and responsibilities for all stakeholders, particularly in the context of IT and OT convergence. This section also addresses considerations, gaps, and recommendations regarding people factors as part of the cybersecurity of a connected ITS ecosystem.

Stakeholders

The continued progression of technology has led and is leading to the concept known as IT

/ OT convergence. IT traditionally referred to computer information systems, while OT was mainly hardware and machines responsible for physical processing. IT includes things like servers, networking devices, and endpoint devices, while OT devices generally include industrial computing equipment like IoT gateways and control systems. A connected ITS infrastructure is expected to encompass various departments within an agency by clearly outlining the roles and responsibilities of all parties involved.

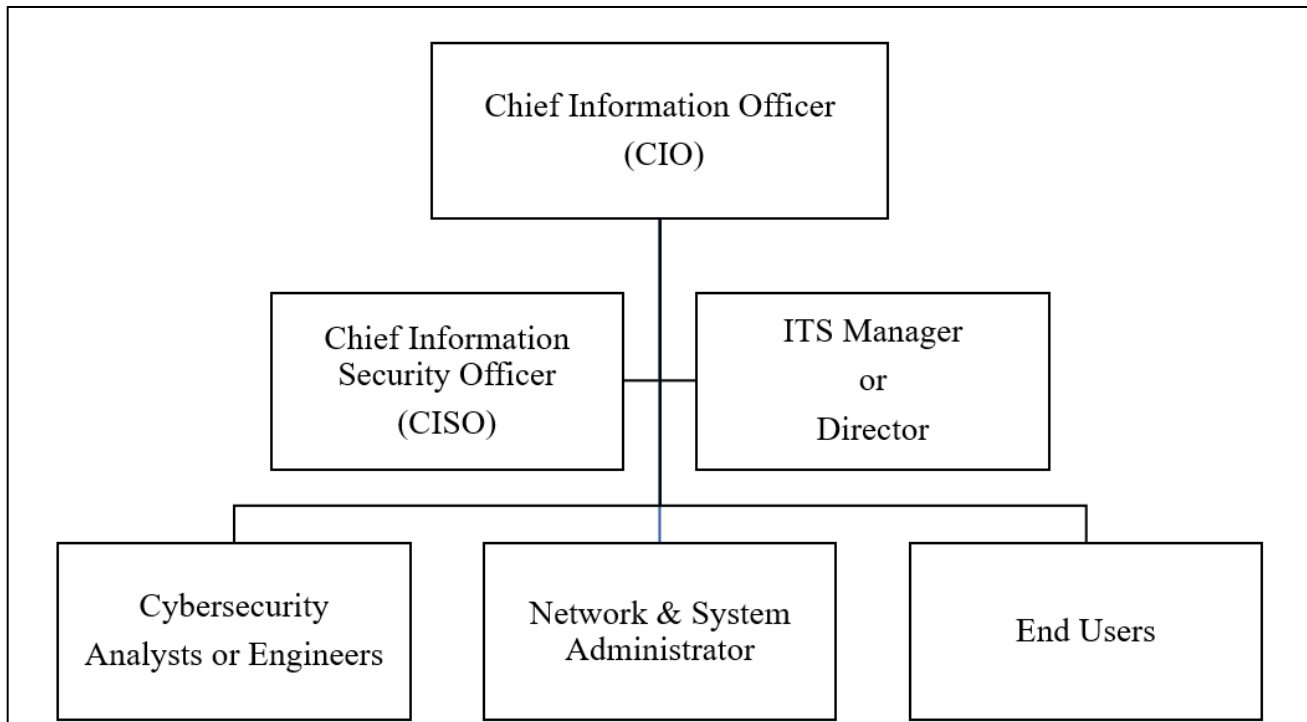
An organization's Chief Information Officer (CIO) can establish a structured approach to cybersecurity governance within the ITS environment, ensuring that all stakeholders understand their roles in safeguarding critical transportation infrastructure and data. A sample of a Cybersecurity Organizational Structure can be seen in Figure 9 below.

Roles and Responsibilities

Some legacy OT systems may not have the necessary features to keep your system secure and may be vulnerable to cyber-attacks. Because of this, security analysts within IT should be involved early and often in the convergence process. When looking at OT applications, a security-first mindset should be applied.

Individuals in the following key roles have specific responsibilities to ensure cybersecurity for Intelligent Transportation Systems (ITS), assuring the integrity to the agency's resources when they are deployed, managed, and retired while mitigating cyber risks effectively.

Figure 8 - Sample Cybersecurity Organizational Structure



Listed below are commonly found key roles and responsibilities in ITS cybersecurity:

1. Chief Information Officer (CIO):

- Serves as the authorizing official, and thus, runs the overall ITS cybersecurity strategy.
- Ensures alignment of ITS initiatives with agency goals and objectives.
- Approves IT policies, standards, and procedures for ITS.
- Provides oversight of cybersecurity budget and resource allocation.
- Monitors compliance with regulatory requirements and industry standards.
- Represents cybersecurity interests at the executive level and communicates with other stakeholders.
- Grants approval, with the CISO and ITS Manager/Director, of information exchange of agency data with third-party entities.

2. Chief Information Security Officer (CISO) or equivalent:

- Respond to inquiries regarding interpretation of ITS Cybersecurity policies.

- Develop, disseminate, and perform periodic reviews of the assessment, authorization, and monitoring policies and procedures specific to ITS.
 - Manages cybersecurity risk assessment and mitigation efforts.
 - Leads incident response and recovery activities in the event of cybersecurity incidents.
 - Conducts regular cybersecurity training and awareness programs for ITS staff.
 - Collaborates with other departments to ensure cybersecurity controls are integrated into ITS projects and operations.
 - Reports regularly to the CIO and other senior executives on cybersecurity posture and challenges.
 - Grants approval, with the CIO and ITS Manager/Director, of information exchange of data with third-party entities.
3. ITS Manager or Director:
- Ensures that ITS infrastructure, systems, and applications adhere to cybersecurity and privacy protections standards and best practices.
 - Collaborates with the CISO and other stakeholders to identify and address cybersecurity risks specific to ITS.
 - Participates in incident response and recovery efforts as needed.
 - Provides input to the CIO and CISO on cybersecurity requirements for ITS projects and initiatives.
 - Grants approval, with the CIO and CISO, information exchange data with third-party entities.
4. Cybersecurity Analysts or Engineers:
- Conduct architecture designs review for integration of ITS systems.
 - Monitor and analyze ITS networks, systems, and applications for cybersecurity threats and vulnerabilities.
 - Conduct regular security assessments and penetration tests to identify weaknesses in ITS infrastructure and applications.
 - Implement and manage cybersecurity tools and technologies, such as SIEM (Security Information and Event Management) systems, endpoint protection solutions, and vulnerability scanning tools.

- Investigate and respond to cybersecurity incidents and breaches in a timely manner.
- Assist in the development of cybersecurity policies, standards, and procedures specific to ITS.

5. Network and System Administrators:

- Configure and maintain ITS networks, servers, and other infrastructure components in accordance with cybersecurity best practices.
- Develop configuration baseline for ITS equipment.
- Implement access controls, encryption, and other security measures to protect ITS data and resources.
- Monitor system logs and alerts for signs of unauthorized access or malicious activity.
- Apply security patches and updates to ITS systems and applications in a timely manner.
- Work closely with cybersecurity analysts and engineers to remediate security vulnerabilities and incidents.

6. End Users

- Follow cybersecurity policies, standards, and procedures when using ITS systems and applications.
- Participate in cybersecurity training and awareness programs to recognize and report potential security threats.
- Promptly report any suspected security incidents or breaches to the ITS manager or cybersecurity team.
- Exercise caution when managing sensitive information and adhere to data protection guidelines.

Additional Staffing Considerations

Frequent questions from transit and transportation agencies evolving their IT and OT cybersecurity programs involve the number of staff, job descriptions, certifications, and average salary requirements for cybersecurity resources. You can find some key information in this section related to each consideration:

- Proper staffing levels for cybersecurity resources will depend on the size, funding, organizational structure, and complexity of ITS infrastructure for each agency. There is no single standard approach for how many staff an agency should have, but rather illustrations above and below on roles and responsibilities for each.
- The following is a sample list of cybersecurity industry certification bodies that have information on their websites regarding their offerings. Certifications can cost a few hundred to many thousand dollars. Individuals typically incur these costs on their own, but there is a growing trend for employees to request certification funding from employers.
 - [GIAC: The Highest Standard in Cyber Security Certifications](#)
 - [CompTIA: Industry Leading Certifications](#)
 - [ISC2: Cybersecurity Certifications](#)
 - [NICCS: Cybersecurity Certifications](#)
 - [EC-Council: Build Cybersecurity Skills that Matter](#)
 - [ISACA: Certifications](#)
- Work role descriptions, task knowledge, and skillset descriptions for cybersecurity staff were initially published in NIST SP 800-181r1, Workforce Framework for Cybersecurity in 2020. The associated National Initiative for Cybersecurity Education Workforce Framework for Cybersecurity (NICE Framework):
 1. [NIST.SP.800-181r1, Workforce Framework for Cybersecurity, 2020](#)
 2. [NICE Framework Components v1.0.0: Summary of Changes](#)
 3. [NICE Framework Components v1.0.0 Summary of Changes, 2024](#)
 4. [NICE Framework Users Group-Become a Member, 2023](#)
- Salaries for cybersecurity staff, both IT and OT, normalized from peak industry highs just a few years ago but continue to remain incredibly competitive. Staff recruiting and retention remain a challenge for government agencies at all levels. NIST standards and testing, CompTIA certification standards, and Lightcast, a private sector organization, have formed a public-private research coalition to assist both cybersecurity employers and employees in salary and placement determination. That consortium is called [Cyberseek.org](#). A sample with salary for the Washington, DC, area from Cyberseek is included below. This sample shows IT skillsets, generally those with OT or ITS skillsets require higher annual compensation.

An illustration of each is provided in figures 10,11, and 12 below:

Figure 9- NICE Framework

Workforce Framework for Cybersecurity (NICE Framework)

WHAT?

The NICE Workforce Framework for Cybersecurity (NICE Framework) (NIST SP 800-181r1) establishes a common language that defines and categorizes cybersecurity Competency Areas and Work Roles, including the Knowledge and Skills needed to complete Tasks in those roles. It is a fundamental resource in the development and support of a prepared and effective cybersecurity workforce that enables consistent organizational and sector communication for cybersecurity education, training, and workforce development.

WHO?

The NICE Framework considers the cybersecurity workforce as those whose primary focus is on cybersecurity as well as those in the workforce who need specific cybersecurity-related knowledge and skills in order to perform their work in a way that enables organizations to properly manage the cybersecurity-related risks to the enterprise. It is used by:

Employers: Employers use the NICE Framework to support cybersecurity workforce assessment, planning, recruitment, and development. It is a key tool that helps employers identify critical gaps in cybersecurity staffing and capabilities; determine and communicate position responsibilities and job descriptions; and provide staff training and career pathways.

Learners: Students, job-seekers, and employees can use the NICE Framework to explore the wide variety of cybersecurity-related Work Roles available and learn about top Competency Areas valued by employers for in-demand cybersecurity jobs. Staffing specialists and guidance counselors can also use the NICE Framework as a resource to support learners.

Education, Training, and Credential Providers: These providers can use the NICE Framework to create learning content and curriculum. By aligning with the NICE Framework, providers can leverage the common language to communicate with and support employer needs and describe learner capabilities.

LEARN MORE

The NICE Framework, tools, guidance, and other resources can be found in the NICE Framework Resource Center at: nist.gov/nice/framework

WHY?

The NICE Framework grew from the need to better define, develop, and assess the cybersecurity workforce in both the public and private sectors. More than 20 governmental departments and agencies, along with representatives from the private sector and academia, came together to address this challenge resulting in the creation of two early versions of the NICE Framework, followed by its release as NIST Special Publication 800-181 in 2017 and the first revision in 2020. The NICE Framework now provides an evolving resource that is agile, flexible, interoperable, and modular and continues to draw from engagement between the government, private sector, and academia.

HOW?

Task, Knowledge, and Skill (TKS) statements serve as the foundational building blocks of the NICE Framework. The NICE Framework organizes these statements into Work Roles and Competency Areas that can be used to improve practices around identifying, recruiting, developing, and retaining cybersecurity talent.

GLOSSARY

Task, Knowledge, and Skill (TKS) Statements: The core building blocks of the NICE Framework.

Task: An activity directed toward the achievement of organizational objectives. Task statements define the work to be done, and include associated Knowledge and Skill statements that represent learners' potential to perform those Tasks.

Knowledge: A retrievable set of concepts within memory. Knowledge statements define what a learner knows.

Skill: The capacity to perform an observable action. Skill statements define what a learner is able to do.

Competency Area: A cluster of related Knowledge and Skill statements that correlates with one's capability to perform Tasks in a particular domain. Competency Areas can help learners discover areas of interest, inform career planning and development, identify gaps for knowledge and skills development, and provide a means of assessing or demonstrating a learner's capabilities in the domain.

Work Role: A grouping of work for which an individual or team is responsible or accountable. They comprise a group of Tasks that define the work to be done.

nist.gov/nice
updated May 2023

Figure 10 - NICE Work Roles

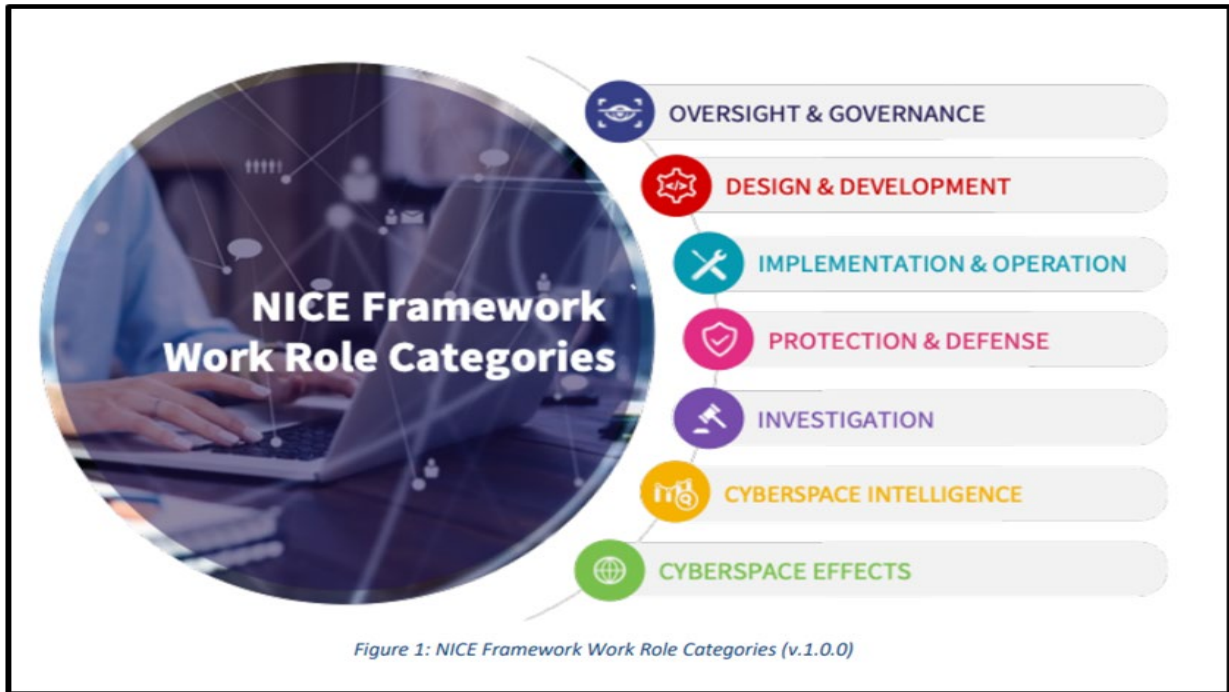
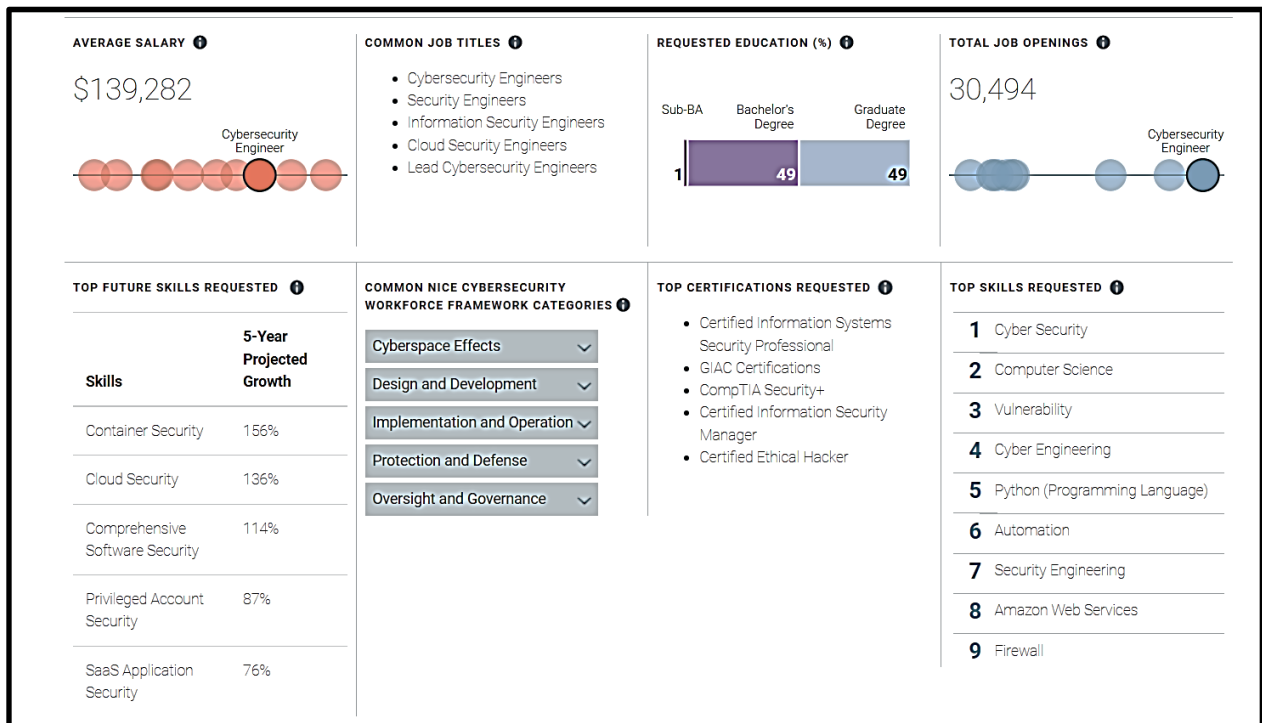


Figure 11 - Cyberseek Salary Report



Procurement Language Recommendations

Often, it is challenging for procurement departments to use the right cybersecurity language for Request for Proposals (RFPs) and other bid documents. There are several industry resources for agency purchasing and procurement departments publicly available. Below is a link originally published by the DOE's Pacific Northwest National Laboratory (PNNL) and adopted by the Joint Office of Energy and Transportation.

The document was last updated in 2023 as PNNL document number 34454, and the current link is included below:

1. [PNNL Document Number 34454 Sample Cybersecurity Clauses for EV Charging Infrastructure, 2023](#)

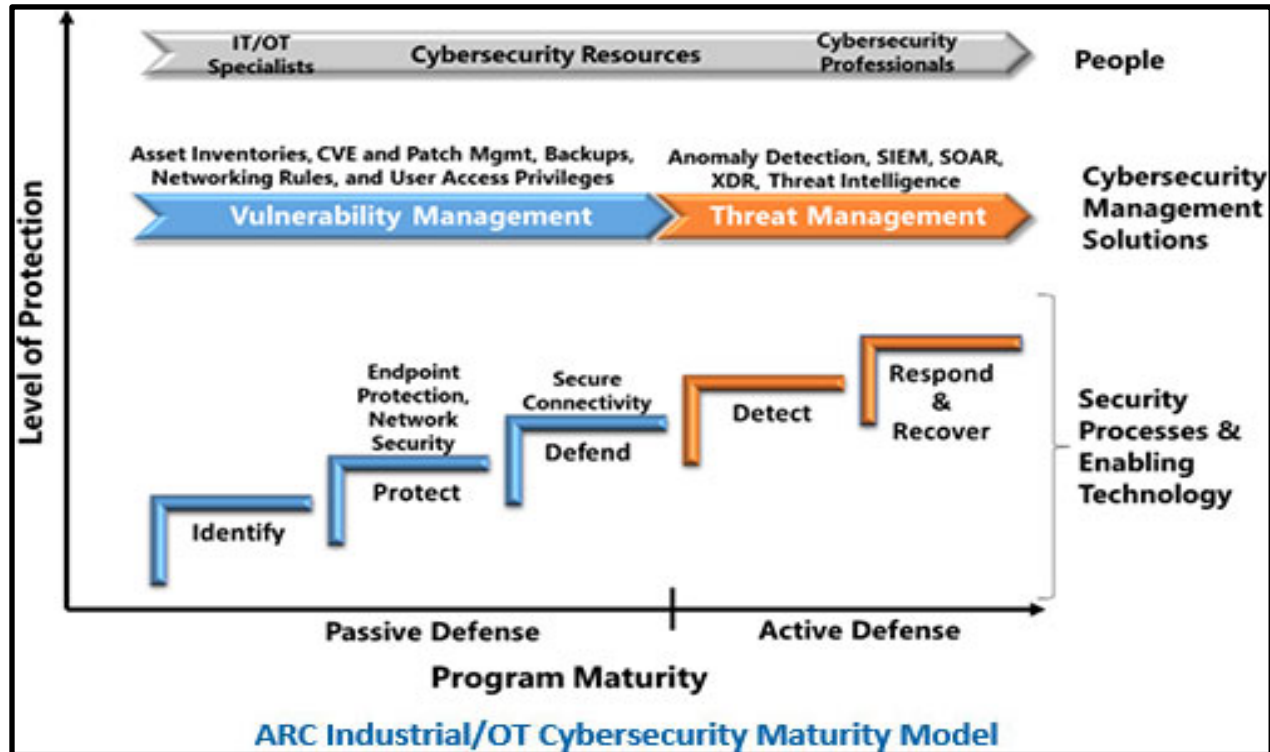
The Joint Office of Energy and Transportation has enhanced the procurement language process, links to resources:

1. [Joint Office of Energy and Transportation Cybersecurity Procurement Language, 2024](#)

Agency Maturity Level Considerations

Maturity models in IT and OT cybersecurity are not new but have evolved over time to encompass both IT and OT. The ARC Advisory Group [ARC Advisory Group](#) maturity model was one of the first in the industry to focus on the OT side of cybersecurity and has evolved as shown below in figure 13 and online at [ARC Advisory Group ICS/OT Maturity Model](#) 2024.

Figure 12 - ARC Advisory OT Cyber Maturity Model



4. SUMMARY & CONCLUSION

In summary, there are ten key recommendations based on this *Cybersecurity for Connected ITS Infrastructure* document. These are listed in priority order with the foremost being the need for a framework built around People, Process, and Technology for a secure ITS infrastructure. Technology alone cannot and will not prevent cyber-attacks. People and Process play the most significant role as this is where the largest opportunity lies for significant impact to any organization’s ecosystem.

1. **The People, Process, Technology framework developed by Dr. Harold Leavitt in 1964** as a framework to help companies manage digital change is still relevant in 2024. This model emphasizes that successful organizational change and system implementation require an integrated approach, balancing the development of people (skillsets and culture), processes (workflows and methodologies), and technology (tools and systems). Today, securing connected ITS infrastructure and our digital roadways must be done by using this comprehensive approach involving people, processes, and technology. Public-Private Partnerships (PPP or P3) between public transportation agencies and technology companies will be key to maintaining secure

infrastructure.

2. **Cyber-informed engineering and secure by design methodologies** both suggest that cybersecurity must be included incrementally throughout the entire lifecycle of any product, system, or network design in ITS. Two key methodologies to do this include:
 1. [DOE Cyber-Informed Engineering](#)
 2. [DHS/CISA Secure By Design](#)
3. **Zero Trust Architecture** should be part of all system and network designs as our network perimeters have evolved and can no longer be supported by simple firewall or antivirus technologies. The NIST Zero Trust Architecture publication can be found here: [NIST.SP.800-207](#).
4. **Best practices and industry standards for securing connected infrastructure will continue to change in the near future.** Tracking this information must be an ongoing effort. Therefore, this document should be updated regularly.
5. **Internal OT, Internet of Things (IoT), and Intelligent Transportation Systems (ITS) cybersecurity policies and procedures must be developed by all transit and transportation agencies.** The most important of these policies and procedures is an Incident Response Plan. The time to develop an Incident Response Plan and practice using tabletop exercises is before you are attacked, not after. For guidance on how to write an Incident Response Plan, visit the following site: [DHS-CISA](#).
6. **Staffing levels and workforce retention will continue to be a challenge,** especially with OT, IoT, and ITS. The industry can advocate to include OT cybersecurity curriculum in accredited civil engineering, transportation engineering, and associated university and college programs. Successful execution of this advocacy was seen in early 2000s to increase the number of cyber-informed engineering graduates available.
7. **Collaboration is key to successfully secure connected ITS infrastructure.** Given the convergence of transportation and energy sector ecosystems in today's digital roadways, collaboration is a crucial component for success. This is evident by the newly formed and highly relevant [Joint Office of Energy and Transportation](#). It is

recommended the Joint Office increase ITS cybersecurity education and awareness for the quickly converging energy and transportation sectors.

8. **Product vendors can be certified.** There is an option for vendors to purchase a test harness for internal testing through the [ISASecure Vendor Cybersecurity Certification Program](#). The ISASecure certification program is successfully delivering secure products in the ITS environment. We recommend using ITS products on the list of vendor certified products.
9. **Supply chain cybersecurity continues to be a concern across all critical infrastructure sectors including transportation.** DOE [Cybersecurity, Energy Security, and Emergency Response](#) (CESER) group has recently published a Call to Action to build cybersecurity throughout global supply chains in the energy sector which now includes EVSE. Information on this effort can be found here: [Supply Chain Cybersecurity Principles \(energy.gov\), 2024](#). The ITS ecosystem should join in this DOE effort or establish a similar effort through the Joint Office of Energy and Transportation.
10. **Education and awareness must continue for the near future** to ensure securing our connected ITS infrastructure remains a safety priority for our digital roadways. Funding levels at the Federal, State, and local levels must not diminish as the cybersecurity challenge will remain. Innovative technologies like AI will be used by both cyber-attackers and cybersecurity protectors. We must continually learn how best to secure our digital roadways and infrastructure from future cybersecurity threats and maintain a safe transportation system for all users.

5. CREDITS

This document was authored and reviewed by members of the ITS America Cybersecurity Community of Practice.