MAT v.3

Task 6 Cybersecurity and Privacy RDS White Paper

Cybersecurity and Privacy Assessment and Best Practices for Reservations, Scheduling, and Dispatching for Paratransit, Demand Response, and On-Demand Transit

Tiffany Rad, ELCnetworks and ITE's MAT Subject Matter Experts

DRAFT September 2025

Published by:

ite
A Community of Transportation Professionals

Supported/Sponsored By: The United States Department of Transportation (USDOT)

U.S. Department of Transportation

Table of Contents

Introduction:

Reservations, Scheduling, and Dispatching (RSD) form the operational backbone of paratransit and demand-response transit services. These functions enable riders to request trips in advance, allow transit providers to coordinate and optimize vehicle routes, and ensure that drivers are dispatched efficiently to meet service demands. RSD systems are critical to maintaining reliability and accessibility in transportation for individuals who depend on flexible mobility-on-demand (MOD)[i]. Increasingly, these systems rely on digital platforms and interconnected networks to manage trip requests, scheduling algorithms, and real-time communication with drivers and riders. While these technological advancements have improved efficiency and service delivery, they have also introduced new cybersecurity challenges that could affect the safety, privacy, and reliability of transit operations. This paper focuses specifically on the intersection of cybersecurity and RSD functions within paratransit and mobility on demand transit systems.

Objectives:

The objective of this paper is to identify cybersecurity concerns associated with RSD systems in paratransit and demand-response transit. By analyzing the potential vulnerabilities and threats facing these functions, this report highlights the risks that could compromise service availability, passenger data privacy, and overall operational integrity. Additionally, the paper aims to provide a foundation for understanding how cybersecurity considerations can be integrated into the design and implementation of RSD systems.

This report is vendor-neutral; general cybersecurity and privacy practices will be recommended apart from specificity associated with particular 3rd party systems and vendors. Of primary importance is how transit users utilize technology to move through the transportation infrastructure by making reservations, scheduling transportation, and how that transportation is dispatched. There are cybersecurity and privacy concerns with enterprise-grade software managing sensitive personal and operational data. These

platforms manage highly sensitive information, including personally identifiable information (PII) for passengers including ePHI (Electronic Protected Health Information), their disability status, trip histories and real-time location data, driver information and schedules, payment or billing data, and Americans with Disabilities Act (ADA) compliance data and reporting. This report will evaluate cybersecurity and privacy concerns and recommend best practices and policies to be adopted to protect vulnerable road users using these services.

Research into the current state of cybersecurity and privacy within public transit systems has found significant shortcomings. [ii] Despite the growing frequency and severity of cyberattack -- particularly ransomware incidents and operational disruptions -- many transit agencies fail to fully understand the associated risks or prioritize cybersecurity at the executive or governance level. In many cases, even basic cybersecurity "hygiene" is lacking. A critical first step for agencies would be conducting a fundamental review of their digital infrastructure, including identifying the location of key assets such as databases, payment systems, and backup storage. Establishing this foundational awareness is essential before implementing more advanced cybersecurity policies and best practices.[iii]

This report focuses on cybersecurity best practices specific to transit systems that use reservations, scheduling, and dispatching for paratransit, and demand-response, and on-demand transit services dispatching. The definitions for these types of transit systems are as follows:

> **Paratransit** is a specialized transit service designed for people with disabilities or mobility challenges who cannot use regular fixed-route buses or trains. It operates under legal requirements such as the Americans with Disabilities Act (ADA) in the U.S. and is usually scheduled in advance, often through a reservation system. It is flexible, demand-responsive transportation services that operate outside the fixed-route, fixed-schedule model of conventional public transit.[iv]

Demand-Response Transit is a flexible transit service that responds to requests from passengers rather than following a fixed route or schedule. It is any system of transporting individuals, including the provision of designated public transportation service by public entities and the provision of transportation service by private entities, including but not limited to specified public transportation service, which is not a fixed route system.[v]

Mobility On-Demand (MOD) Transit represents a modern evolution of demand response services, often enabled by mobile apps or digital platforms. It offers real-time booking and dynamic routing, similar to ridesharing services. This service can cater to general transit users, paratransit riders, or both, emphasizing flexibility, efficiency, and real-time optimization through technology. MOD offers users personalized mobility and goods delivery options upon request, matched with coordinated network strategies of service providers and operations managers.[vi]

While the primary emphasis is on these functional areas, general cybersecurity recommendations applicable to the broader transit environment are also included in Appendix 1.

Scope:

The scope includes all mobility users who access on-demand and demand-responsive transportation services that operate through reservation, scheduling, and dispatching mechanisms provided by public or private transit operators. This encompasses platforms and services that allow users to plan and request trips in advance, receive real-time updates on vehicle status, and coordinate efficient pick-up and drop-off. The scope further extends to systems that integrate multiple modes of transportation, support accessible and inclusive travel for individuals with disabilities or limited mobility, and ensure seamless interaction between service providers, riders, and operational management platforms.

This graphic (below) is an example of reference architecture that is an overview of the RSD data flow and process.

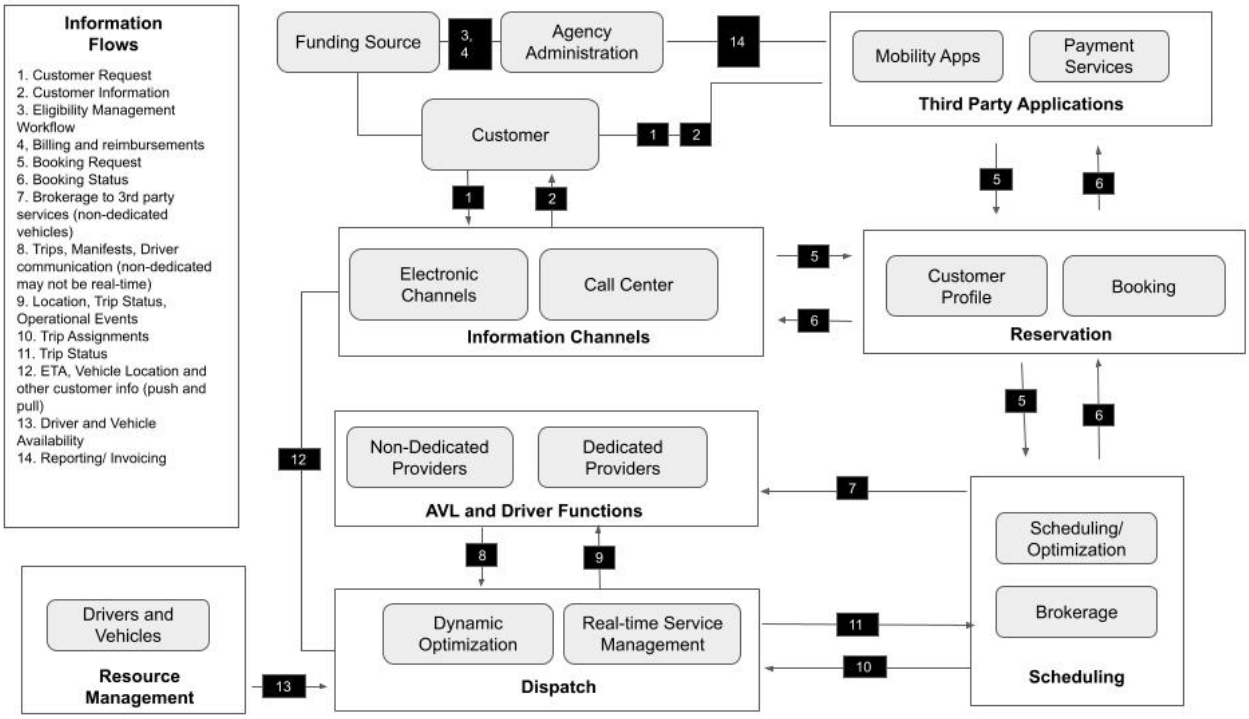

Figure One: RSD Data Flow. Graphic by Santosh Mishra.

A few elements listed in "Information Flows," such as General Transit Feed Specification (GTFS) and General On-Demand Feed Specification (GOFS-lite), will not be addressed in detail in the paper because they were addressed in this project's first cybersecurity and RSD white papers. However, a brief summary of each will be provided for context.

GTFS is a standardized data format used by fixed route public transportation agencies to publish schedule, route, and geographic information in a way that is accessible by trip planning applications like Google Maps and Transit App. GTFS includes key details such as stop locations, route structures, trip schedules, service calendars, and fare information. It can also be extended with GTFS Flex to include live updates

about vehicle positions, service alerts, and arrival predictions. GTFS is essential for enabling fixed-route transit systems—such as buses, trains, and trams—to integrate with digital tools and inform riders efficiently.[vii]

	GTFS-flex	GOFS-lite
Primary services supported	Paratransit, dial-a-ride, deviated fixed-route sere	On-demand transit, paratransit, taxi, ridehail
Zone or pickup type	Zone-to-zone, point-to-zane, and other servicess onn be hailed on th street	Services that operate between or within zoness can be ordered in real-time
Primary purpose of data standard	Service information and trip planning	Service information and trip planning
Real-time pickup ETA	Not available. Static service information onyiy.	Supported
Fare and pricing information	Some support via GTFS files used for fixed-route	Supported directly in GOFS-lite
How booking or pickup requests are handled	Direct link to the demand-response provider's app,	Direct link to the demand-response or wbbce app

Figure 2: GTFS-flex vs GOFS-lite

GOFS-lite by contrast, is being designed to support -demand-responsive transportation services that do not operate on fixed routes or schedules. This includes services such as paratransit, demand response, microtransit/on-demand services. GOFS-lite provides a framework for sharing dynamic information like service areas, booking rules, vehicle availability, and response times. It enables these flexible services to be integrated into mobility platforms, helping agencies coordinate trips, improve accessibility, and offer first-mile/last-mile options.[viii]

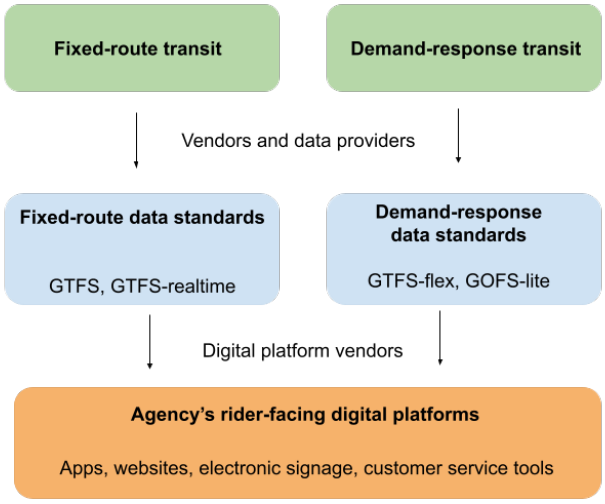

Figure 3: Fixed-Route vs Demand-Response Transit

Together, GTFS and GOFS-lite support a transit ecosystem by allowing both fixed-route and on-demand services to be represented in a standardized format. This enhances multimodal trip planning, improves operational efficiency, and makes transit more accessible and responsive to diverse rider needs.

Recommendations for addressing cybersecurity and privacy concerns related to GOFS-lite and GTFS align closely with the best practices outlined for reservations, scheduling, and dispatching in later sections of this report. The technologies associated with these data standards include application programming interfaces (APIs), the collection and storage of geospatial information, integration with proprietary booking platforms, and the use of OAuth2/Identity and Access Management (IAM) or API key management for secure access control.

- RESTful APIs**:** GOFS-lite services use RESTful web services for requesting, booking, and managing trips.
- Geospatial Data Standards**:** Uses GeoJSON or similar formats to define service zones, pickup/drop-off areas, and routing preferences.

- Integration with Booking Platforms**:** GOFS-lite is often integrated with backend platforms for demand-responsive services by proprietary companies. GOFS-lite has been used by proprietary demand-responsive/back-end vendors in real deployments, but it is mainly for publishing service-offering info (zones, hours, fares, basic rules). It is not a full booking/ops API, so deep integration (trip requests, dispatching, payments) still runs through each vendor's proprietary API.
- OAuth2/IAM or API Keys**:** For secure access and authentication when agencies or platforms share trip request APIs or user data.[ix]

Overview of Core Functions of VRU Reservations, Scheduling, and Dispatching Technologies

Cybersecurity and Privacy for Reservation Management

Booking transit rides via phone, web portals, mobile apps, or interactive voice response (IVR) systems introduces a range of cybersecurity and privacy vulnerabilities. Across all booking channels, there are significant risks related to the exposure of personal data such as names, addresses, phone numbers, trip histories, and payment details. For paratransit services, the risk is heightened due to the inclusion of sensitive health or disability information, which may be protected under regulations like the Health Insurance Portability and Accountability Act (HIPAA) or state privacy laws like the California Consumer Privacy Act (CCPA). Inadequate identity verification and weak authentication mechanisms further expose systems to unauthorized access.

Mobile apps, in particular, are vulnerable due to insecure APIs, over-permissioned access (e.g., to contacts or location data), and the potential for malicious app clones in the Apple and Android stores. Location tracking features can leak real-time user movements, while poorly secured APIs may allow attackers to

extract or manipulate ride data. Web portals are also susceptible to threats such as cross-site scripting (XSS), cross-site request forgery (CSRF), and weak encryption protocols if HTTPS is not properly enforced.

Phone-based systems and Interactive Voice Response (IVR) systems can be vulnerable to social engineering tactics, including call spoofing, where attackers impersonate riders to alter or view ride bookings. Voice calls may be recorded and stored without proper security controls, and some systems lack full audit logging or accountability. Automated attacks on IVR systems, such as bots flooding with fake bookings, can also degrade system reliability and security.

Artificial intelligence (AI) assistants and automated booking bots present newer concerns, including the vulnerability of voice-based authentication to spoofing via deepfake technologies. Additionally, algorithmic bias in automated decision-making systems can result in unfair ride prioritization or denial of service to certain groups. On a broader level, the integration of third-party tools, such as routing engines and payment platforms, introduces external vulnerabilities, especially if those services are not properly vetted or maintained. Many transit agencies also rely on legacy systems that lack regular patching which makes them inherently insecure due to outdated architecture.

From a compliance perspective, failure to adhere to strong state-mandated data protection regulations such as CCPA -- particularly in areas like consent, data deletion, and user transparency -- can expose agencies to legal penalties. Accessibility issues in booking systems may also violate ADA standards, especially for paratransit riders who depend on inclusive technology.

To mitigate these risks, transit agencies should implement multi-factor authentication (MFA), end-to-end encryption for all communication channels (including down to the application//presentation layer – not just the network and transport layers at which many vendors' systems operate), secure API gateways with authentication tokens and rate limiting, and role-based access controls. Regular vulnerability scanning, penetration testing, and data minimization audits are essential. Conducting Privacy Impact Assessments

(PIAs) and maintaining compliance with privacy laws should be standard practice -- especially in systems managing sensitive personal data or serving vulnerable populations.

Cybersecurity and Privacy for Scheduling and Optimization

Cybersecurity and privacy concerns become increasingly complex when transit systems incorporate automated reservations, dispatching, scheduling, and dispatching, especially when assignments are based on proximity, time windows, ride time limits, and vehicle accessibility. These functions rely on continuous access to sensitive user data, real-time location tracking, and automated decision-making, all of which can introduce vulnerabilities and ethical risks.

Transit systems that schedule and assign paratransit and demand-response rides are based on factors like rider proximity, requested time windows, trip duration limits, and vehicle accessibility must manage and process a large volume of sensitive, personally identifiable information (PII), including names, pickup/drop-off addresses, and disability-related accommodations. This information—if not properly secured—can be exploited in targeted attacks or unintentionally leaked due to weak data governance practices. The use of real-time geolocation data introduces significant privacy risks; for example, tracking rider movements may reveal patterns related to home addresses, healthcare visits, or religious affiliations, which can be exploited for surveillance or discrimination if misused.

Scheduling and dispatching systems are often linked with the global positioning system (GPS), mobile data terminals, and routing algorithms. If these systems are breached, attackers could hijack routes, cause intentional delays, or access real-time vehicle and rider locations. Additionally, optimization algorithms that prioritize scheduling efficiency could be exploited to manipulate resource allocation or discriminate against certain riders—particularly if bias exists in the data or model assumptions. For instance, if a system deprioritizes longer or more complex trips (such as those needing specific accessible vehicles), it may unintentionally discriminate against people with greater mobility challenges.

Cyber risks also arise from the integration of third-party scheduling engines and cloud-based platforms. For example, vendors often use external service -- such as for weather and mapping – and if scheduling programs are relying upon this ingested data for their operations, ensuring validity and accuracy of this data is important. Likewise, ff APIs or data pipelines are inadequately secured, attackers may intercept or manipulate dispatching commands or reservation data. Furthermore, unauthorized access to back-end systems could enable tampering with time windows, trip caps, or reservation limits—potentially resulting in service denial or manipulation of eligibility.

Automated scheduling and dispatching tools must also account for fairness, transparency, and accountability. If the algorithmic logic is opaque, affected riders and regulators may have little recourse to challenge unfair or inconsistent ride assignments. This becomes especially important in regulated paratransit services, where federal or state laws (e.g., ADA) mandate equal access and prohibit unjustified trip denials or excessive ride times. In 2022, the US Department of Justice found that Uber was violating the ADA by charging riders with disabilities extra fees, even when the need for extra time was due to a disability.[x]

Lastly, insufficient audit trails and logging mechanisms limit an agency's ability to detect security breaches or policy violations. If a system lacks logs showing how and why ride assignments were made, investigating disputes, errors, or malicious actions becomes difficult. Insecure storage or excessive retention of historical trip data also increases the risk of long-term exposure in a data breach.

Dispatching

Sending real-time assignments, trip updates, delays, and cancellations to paratransit drivers raises several cybersecurity and privacy concerns due to the sensitive nature of the data involved and the operational dependencies on mobile communication systems. Trip dispatching often contain personally identifiable information (PII) such as passenger names, pickup and drop-off addresses, phone numbers, and

accommodation needs related to mobility or health. If this information is not properly encrypted during transmission or storage, it can be intercepted by malicious actors, potentially leading to identity theft, stalking, or violations of regulations such as HIPAA or ADA, especially when medical or disability-related information is disclosed.

Many systems rely on mobile devices like tablets, smartphones, or mobile data terminals (MDTs), which may use public Wi-Fi or unsecured cellular networks for communication. Without proper security controls like end-to-end encryption, strong authentication, or secure VPN tunnels, these communication channels are vulnerable to eavesdropping or spoofing. Attackers could intercept or manipulate trip data, redirecting drivers, canceling rides, or creating system confusion. Compounding this risk are vulnerabilities in the mobile apps or devices themselves—unpatched software, inadequate access controls, or lack of encryption could allow unauthorized access to driver apps and the sensitive data they contain.

Vulnerabilities to cellular networks became evident in 2024 after the US government and private cybersecurity companies disclosed the discovery of a malicious hacking campaign named “Salt Typhoon.” While it was publicly identified at that time, security researchers found that the group had been covertly active since at least 2019 or 2020.[xi]

Salt Typhoon is a state-sponsored advanced persistent threat (APT) group believed to be affiliated with China’s Ministry of State Security (MSS), active since approximately 2019–2020. The group has engaged in extensive cyber espionage campaigns, particularly targeting the telecommunications infrastructure of the United States. Victims have included major telecom providers such as AT&T, Verizon, T-Mobile, and others.

Salt Typhoon uses highly advanced tools and techniques to maintain stealth and persistence. Their operations are considered among the most damaging cyberespionage campaigns targeting U.S. infrastructure, with the U.S. Senate Intelligence Committee labeling one of the campaigns “the worst

telecom hack in our nation's history." Up until the public disclosure of Salt Typhoon, the general consensus was that telecom was "safe" for transmission of data. In response, mitigation technique include adoption of zero-trust architectures, enforcing strict network segmentation, and implementing advanced anomaly detection. U.S. government has encouraged broader public-private collaboration to improve threat intelligence sharing and resilience against state-sponsored cyber threats like Salt Typhoon.

Real-time vehicle tracking also presents privacy risks. These systems constantly transmit GPS location data to ensure accurate dispatching, but if location data is stored without adequate protection or shared for unauthorized purposes, it can be misused for surveillance. A system breach could allow attackers to track vehicles in real time, compromising the safety of both passengers and drivers. Moreover, systems that allow real-time trip changes—such as cancellations, delays, or rerouting -- must be protected against unauthorized manipulation. Weak authentication or role-based access controls could allow insiders or hackers to disrupt services or intentionally deny rides, especially for vulnerable populations relying on paratransit.

Another concern lies in the lack of proper audit trails or logging. Without detailed records of who initiated trip adjustments and why, it becomes difficult to trace suspicious behavior or resolve disputes over missed rides. Furthermore, frequent updates or poorly designed real-time communication interfaces can distract drivers, posing a physical safety risk. If drivers must interact manually with unsecured devices while in motion, the likelihood of accidents increases.

Data retention and over-collection present additional concerns. Some systems store large volumes of historical trip data, messages, and adjustment logs far beyond operational needs. There are significant data collection requirements for Federal, state, and local regulations for services such as Medicaid, this increases the impact of a potential breach. Over-collection of passenger metadata or internal notes may also violate privacy principles of data minimization and informed consent. Real-time communication

systems are often integrated with larger scheduling, billing, or reservation databases. If a vulnerability in the mobile interface or driver-side app is exploited, it could serve as a pivot point to access and compromise core back-end systems, escalating the breach's severity.

To mitigate these risks, agencies and vendors should implement end-to-end encryption for all communication between drivers and dispatch, require strong authentication protocols, and deploy mobile device management (MDM) tools to secure devices and remotely wipe data if needed. Logging and audit capabilities should be robust, allowing full traceability of all trip changes or cancellations. Similarly, dispatching software, mobile apps, and device operating systems must be regularly updated and patched. Additionally, drivers and dispatch should be trained to recognize social engineering tactics, and system design should limit the exposure of sensitive data to only what is strictly necessary for trip fulfillment. Strong data retention and destruction policies and minimal data exposure practices should be enforced to reduce long-term privacy risks.

Payment Systems and Processes

Payment processes for paratransit and on-demand mobility services vary considerably, and each method introduces unique considerations for cybersecurity protections as well as Payment Card Industry (PCI) and PCI DSS compliance obligations. Understanding the distinctions between these methods is critical, as the scope of required security provisions, risk management strategies, and vendor responsibilities changes depending on how payments are initiated, stored, validated, and paid.[xii]

One common approach is in app payments through mobile or web platforms, which are common in microtransit and on-demand services. In these cases, riders pay directly through an app, and most of the responsibility for securing financial data, maintaining PCI DSS compliance, and ensuring safe transactions rests with third party vendors that provide payment gateways. While this reduces the direct exposure of transit agencies to sensitive payment data, agencies must still conduct due diligence on vendors to ensure

that cybersecurity standards are met and that risks such as app cloning, phishing, or unauthorized data access are mitigated.

Another widely used approach is account based debiting after trip completion. Here, users maintain prepaid accounts or wallets, which are charged after each trip. These accounts require periodic replenishment, usually through bank card transactions or ACH transfers. Larger transit agencies increasingly rely on tokenization services which allows them to avoid storing cardholder data and thereby reduces PCI scope.[xiii] Smaller agencies, however, may still store sensitive payment card data locally, significantly increasing their compliance requirements and exposing them to risks such as data breaches or improper handling of personally identifiable information.

A third model involves on-board payment or validation of proof of payment. Riders may pay directly upon boarding using cash, contactless cards, or mobile wallets, or alternatively, they may present a pre purchased ticket, pass, or digital credential. In the latter case, the actual financial transaction takes place outside of the real time reservation, scheduling, and dispatching environment, and the boarding process serves only to validate proof of payment. While this reduces the scope of PCI DSS compliance during boarding itself, agencies must still consider the risks associated with counterfeit media, tampering with validation equipment, or fare evasion.

Finally, some systems operate through institutional billing and invoicing, where funding entities such as healthcare providers, social service agencies, or employers cover the costs of trips. In this model, the transit agency bills the entity electronically, often using Electronic Data Interchange (EDI) messages or other invoicing systems, and receives payment through electronic funds transfers or other mechanisms. While this method largely shifts financial responsibility away from riders, it introduces other cybersecurity considerations, such as the security of EDI transactions, the confidentiality of billing data, and compliance with privacy and data protection regulations governing sensitive information about users and their trips.

Considered together, these payment models illustrate the complexity of financial and data security in paratransit and demand responsive systems. Each model requires a tailored approach to cybersecurity and PCI compliance, with considerations ranging from vendor management and tokenization to transaction validation, fraud prevention, and secure handling of institutional data. Recognizing these distinctions is critical for agencies to manage risk effectively, safeguard user trust, and ensure that transit services remain both accessible and secure.

GPS Tracking and Automated Vehicle Location (AVL)

Providing real-time vehicle tracking for paratransit dispatch and customer updates offers clear operational benefits but also introduces a range of cybersecurity and privacy vulnerabilities. These systems rely on continuous GPS data from vehicles, which is transmitted to backend platforms for dispatch and sometimes shared with riders through apps, short message service (SMS), or web portals. Without strong encryption and secure communication protocols, this data is vulnerable to interception or tampering. Attackers could potentially eavesdrop on GPS transmissions, track vehicle movements, or inject false location data, leading to serious operational disruptions or even safety risks.

Privacy concerns are especially heightened in paratransit, or demand -response, and on-demand services, where ride data may reveal sensitive personal information. Vehicle tracking is often tied to identifiable rider information, including names, home addresses, appointment destinations (such as clinics or dialysis centers), and mobility needs. If this data is exposed -- whether through a breach, insecure system configuration, or insufficient access controls -- it can allow malicious actors to reconstruct personal routines or infer medical conditions and living situations. This raises serious concerns under privacy laws such as HIPAA and the ADA, which protect sensitive health-related data.

Dispatching platforms themselves may be vulnerable due to insecure login mechanisms, weak session management, or outdated software. A compromise of these administrative systems, whether through

phishing, credential stuffing, or software exploitation, could allow unauthorized users to access live vehicle locations, reroute drivers, or view sensitive passenger information. Additionally, these platforms often rely on third-party location APIs or cloud-based services, introducing supply chain risks and potential data-sharing practices that may not align with public sector privacy obligations.

Integration with third-party systems also presents significant concerns. These systems often need to connect with critical business functions such as human resources, payroll, billing, and accounting. It is essential to ensure that cybersecurity best practices are strictly followed during these integrations, especially since many third-party systems may be developed in-house and potentially lack rigorous security measures.

Customer-facing tracking updates bring further risks if systems do not enforce proper authentication. For instance, if riders can track a vehicle by entering a ride number without verifying their identity, others could impersonate them to monitor their location. Mistakenly sending notifications or messages to the wrong contact can also result in unintended data disclosures. These issues are compounded by the fact that many systems retain historical GPS and trip data for long periods without strong data minimization or anonymization policies. In the event of a breach, this data becomes a high-value target that reveals extensive movement and behavior patterns.

In many cases, riders have little visibility or control over how their location data is collected, stored, or shared. A lack of transparency and consent around GPS tracking can erode trust and potentially violate privacy regulations such as the California Consumer Privacy Act (CCPA). To address these concerns, transit agencies should implement end-to-end encryption, enforce role-based access controls, and authenticate all rider-facing systems. They should also minimize data retention, conduct regular audits of third-party services, and ensure that users are informed about how their location data is being used—with opt-out options available when feasible.

Customer Notifications

Sending estimated time of arrival (ETA), delay, and cancellation notifications to paratransit customers through SMS, phone calls, or app alerts enhances communication and service quality, but it also introduces a range of cybersecurity and privacy risks. These notifications typically include personal and location-based information such as the rider's name, pickup address, trip status, or driver details. If this data is intercepted, misdirected, or accessed by unauthorized individuals, it can reveal sensitive patterns about the rider's behavior or health status—particularly concerning for paratransit users traveling to medical appointments or facilities. Such exposures may also lead to violations of privacy laws, including the Health Insurance Portability and Accountability Act (HIPAA) and the Americans with Disabilities Act (ADA), when disability-related or healthcare information is involved.

SMS and voice calls are among the least secure forms of communication, as they are often unencrypted and vulnerable to SIM swapping, mobile device compromise, or carrier-level interception. If exploited, attackers could spoof legitimate notifications, mislead passengers, or harvest information for targeted phishing or harassment. Mobile apps, though generally more secure, still present risks, especially if they use insecure APIs, lack strong authentication mechanisms, or store sensitive information on devices without proper encryption. Poor session management and excessive permissions can further increase the risk of unauthorized access to trip histories and personal data. Call centers should evaluate their call recording systems for potential cybersecurity risks, ensuring that sensitive customer and operational data is adequately protected.[xiv]

Internet-based text messaging services such as Twilio[xv] and AWS Connect[xvi] provide strong encryption while data is stored and during transport between your application and their servers, typically using TLS/HTTPS and robust key management systems. Within these providers' environments, message data is protected by strict access controls and encryption standards. However, standard SMS messages are

inherently not end-to-end encrypted, meaning that once the message leaves Twilio's or AWS's secure infrastructure and traverses the public carrier network, it becomes susceptible to interception, such as through SIM swap attacks or other network-level compromises. While AWS Connect and similar services also encrypt call recordings, transcripts, and stored customer information at rest, these protections do not extend to the public SMS network once the message is delivered. For true end-to-end privacy in communications, encrypted chat channels or secure voice platforms should be considered over traditional SMS.

Another concern is the lack of identity verification mechanisms before dispatch alerts. Notifications sent to shared landlines, public phones, or devices used by caregivers may inadvertently disclose private ride information to unintended recipients. Mistakes in account records or data entry -- such as incorrect phone numbers or mismatched rider profiles -- can also result in alerts being delivered to the wrong person, posing both privacy and safety risks.

Moreover, notification systems often log and retain messages, phone numbers, and timestamps for operational purposes. Without strong data protection and retention policies, these logs may be subject to breaches or misuse, revealing behavioral or healthcare patterns about vulnerable populations. Some transit systems also rely on third-party providers for SMS, voice, or push notification services, and if those vendors lack rigorous privacy controls or data handling agreements, they can introduce additional vulnerabilities or misuse customer data for advertising or analytics purposes.

To address these concerns, transit agencies and service providers should avoid including sensitive information in plaintext communications and encrypt data wherever feasible. APIs and app infrastructure must be secured with proper authentication, token management, and audit logging. Rider preferences should be respected through secure opt-in mechanisms, and alerts should be configured to share only minimal necessary information. Contact information must be regularly verified, and caregivers should only

receive updates with explicit consent and role-based access control. Finally, agencies should audit and vet all third-party communication vendors for compliance with relevant data protection laws and implement strong data minimization and retention policies to limit long-term exposure in the event of a breach.

Compliance Reporting

Tracking paratransit customer rides to comply with ADA requirements—such as monitoring no-shows and on-time performance—is critical for ensuring service quality and regulatory adherence. However, this process raises several cybersecurity and privacy concerns due to the sensitive nature of the data collected and the potential risks of misuse or unauthorized access. Paratransit ride tracking involves gathering detailed information about riders' locations, trip histories, pickup and drop-off times, and service outcomes.

Because this data often correlates with visits to healthcare facilities or disability services, it may inadvertently expose protected health information (PHI) or details about a rider's mobility needs. Many systems rely on mobile data terminals, tablets, cloud databases, and scheduling software to record and transmit ride data in real time. Without proper encryption, strong authentication, and access controls, these systems are vulnerable to attacks or insider threats. Malicious actors with backend access could alter no-show records or falsify on-time performance data, undermining service integrity and potentially impacting rider eligibility.

Additionally, inadequate role-based access control (RBAC) can lead to excessive data exposure among dispatch, drivers, and third-party contractors, increasing the risk of misuse—whether through negligence or intentional wrongdoing. There are also concerns about data accuracy and bias; improper logging of no-shows or delays may unfairly penalize riders, especially those with disabilities, leading to discriminatory outcomes and ethical issues. Furthermore, retention of detailed ride logs for long periods can create

privacy risks if data is breached or repurposed beyond its original intent, such as for surveillance or profiling.

Many paratransit providers use a vendor's paratransit scheduling and dispatching software for tracking and scheduling, which introduces supply chain vulnerabilities if these vendors do not meet stringent cybersecurity standards or engage in improper data sharing. To mitigate these risks, agencies should secure tracking data with encryption, enforce strict access controls and multi-factor authentication, maintain accurate and auditable no-show logs, implement data minimization and retention policies with anonymization, and provide transparency to riders about data collection and usage. Staff and contractors must be trained on ethical data handling, and third-party vendors should be regularly reviewed to ensure compliance with privacy regulations.

Driver and Vehicle Management

Scheduling, certifications, and vehicle maintenance tracking for paratransit vehicles involve managing a broad range of operational and sensitive data, which presents several cybersecurity and privacy concerns. These systems store critical information such as vehicle locations, maintenance histories, driver certifications, compliance records, and operational schedules that are essential for safety and regulatory compliance. If not properly secured, these systems are vulnerable to cyberattacks that could disrupt transit operations or compromise sensitive data. Unauthorized access to maintenance and certification records is a significant risk, as attackers could manipulate logs, conceal vehicle defects, or alter driver certification information, potentially endangering passenger safety. Disruptions to scheduling systems might lead to improper vehicle assignments, missed maintenance, or the deployment of unsafe vehicles. Privacy issues also arise from the storage of personally identifiable information (PII) about drivers, including licensing and medical certifications, which, if exposed, could lead to identity theft or other

violations. Additionally, vehicle tracking data used in these systems can reveal patterns of driver behavior or movement that require protection against unwarranted surveillance.

The involvement of third-party vendors or cloud services further increases risks, as weaknesses in APIs, software vulnerabilities, or poor vendor security practices can lead to breaches. Insufficient patching, lack of encryption, and weak access management amplify these vulnerabilities. Moreover, inadequate audit trails and logging can make it difficult to detect unauthorized changes or tampering with critical data, potentially affecting compliance and safety. To mitigate these risks, transit agencies should enforce strong access controls and multi-factor authentication, ensure encryption of data both in transit and at rest, conduct regular security audits, maintain comprehensive logging with anomaly detection, and implement strict vendor management policies. Staff training on cybersecurity best practices and compliance with privacy regulations related to employee and operational data are also essential components of a robust security posture such as Zero Trust for devices and least-privilege access for application.

General Types of Data Transmission and Storage

When considering data transmission and storage deployment models, such as cloud/software as a service (SaaS) versus on-premise solutions, there are several cybersecurity and privacy advantages and disadvantages for each approach. Cloud and SaaS models offer scalability and flexibility, allowing organizations to manage varying data loads and rapidly deploy updates or security patches. Leading cloud providers invest heavily in advanced security features like encryption, intrusion detection, multi-factor authentication, and threat intelligence, often providing protections that smaller organizations might struggle to implement on their own. Additionally, cloud services typically include robust disaster recovery, backup, and geographic redundancy, enhancing data availability and resilience. They also support compliance efforts by offering automated reporting and adhering to industry standards such as ISO 27001,

SOC 2, and HIPAA. Moreover, outsourcing infrastructure to the cloud reduces the need for extensive on-site IT staff, allowing organizations to focus on core business functions.

However, cloud solutions also come with drawbacks. Organizations often have limited direct control and visibility over their data, relying on vendors to enforce security and privacy measures, which can be concerning for sensitive or regulated information. The shared and complex nature of cloud environments introduces third-party risks, including potential supply chain vulnerabilities if providers are misconfigured or compromised. Data residency and jurisdiction issues may arise since cloud data can be stored across multiple geographic locations, potentially conflicting with local privacy laws requiring data to remain within specific boundaries. Additionally, organizations may face vendor lock-in challenges, making it difficult or costly to migrate data between providers or back on-premise. Cloud services also depend heavily on reliable internet connectivity, and outages can disrupt access to data and operations.

On the other hand, on-premise deployments provide organizations with full control over their hardware, software, and data, allowing for tailored security policies and direct oversight. This setup facilitates highly customizable security configurations to meet unique organizational or regulatory requirements. Keeping data within an organization's controlled environment simplifies compliance with strict data residency or privacy mandates and reduces exposure to third-party risks. On-premise systems can also operate offline, which may be critical for certain environments where internet connectivity is unreliable.

Despite these benefits, on-premise solutions involve significant upfront and ongoing costs for hardware, facilities, and skilled personnel. Organizations are responsible for all aspects of security management, including patching, monitoring, and incident response, which can be challenging without adequate expertise. Scalability is limited because increasing resources requires physical upgrades and procurement processes, reducing agility compared to cloud models. Disaster recovery may also be more difficult to implement effectively, increasing vulnerability to data loss from hardware failures or disasters.

Furthermore, budget and staffing constraints can lead to outdated infrastructure and delayed security updates, increasing exposure to cyber threats. Some public agencies may have purchased an on-premise proprietary system a long time ago, but do not pay for updates and some run outdated and unsupported operating systems which makes them non-compliant with current National Institute of Standards and Technology (NIST) or Federal Information Security Modernization Act (FISMA) standards.[xvii]

Ultimately, choosing between cloud/SaaS and on-premise deployments depends on factors such as organizational resources, regulatory requirements, data sensitivity, and risk tolerance. Many organizations adopt hybrid models to balance the benefits and drawbacks, leveraging cloud scalability while maintaining critical data on-premise for enhanced control.

Ransomware Attacks Affecting or Targeting RSD

On August 24, 2025, the Maryland Transit Administration (MTA) confirmed a cybersecurity incident that disrupted its Mobility paratransit service, which provides transportation for riders with disabilities.[xviii] The attack, described by some sources as ransomware though officially termed an “unauthorized access” event, disabled reservations and rebooking systems, leaving customers unable to request new rides, while previously scheduled trips continued as planned. Real-time tracking systems and some call center functions were also impacted, preventing riders from accessing current bus location and arrival information. While core transit services such as local bus, metro subway, light rail, MARC trains, commuter bus, and the Call-A-Ride program remained operational, the disruption created significant challenges for paratransit users.

In response, Maryland activated its emergency operations center and coordinated efforts between MTA, the Department of Information Technology, the Department of Emergency Management, law enforcement, and third-party cybersecurity experts to assess and contain the breach. At the writing of

this report, no more information has been relayed to the public. The identity of the attackers, whether data was stolen, and the full timeline for restoration remained unclear, though interim measures such as expanded call center hours and reliance on Call-A-Ride were put in place to maintain service continuity. As of September 12, 2025, MTA stated that Mobility paratransit services were still impaired by the attack.[xix]

There have been other reports of ransomware attacks on U.S. systems affecting RSD including Virginia, Missouri, and Kansas.[xx] On January 23, 2024, Kansas City Area Transportation Authority (KCATA / RideKC) disclosed a ransomware attack that primarily affected communications and call-center operations, limiting the ability of regional call centers to receive calls and complicating scheduling for paratransit and on-demand services. Core vehicle operations continued because KCATA established additional call centers to compensate for those that were compromised.[xxi] Similar to MTA's response to the ransomware attack, KCATA did not publicly disclose whether or how much sensitive data was exfiltrated or stolen or which internal systems were affected beyond the communications. In both cases, it is unclear if the attack compromised RSD systems and if those systems were directly targeted or instead collateral damage related to connected targeted systems.

Future Trends for RSD

Integrated Mobility-as-a-Service (MaaS), Mobility on Demand (MOD) and Automated Vehicles

Mobility as a Service (MaaS) emphasizes integrated, service-oriented offerings that package multiple transportation options for the end user, whereas Mobility on Demand (MOD) primarily focuses on providing flexible, on-demand transportation services for passengers and goods. From a cybersecurity perspective, a key concern is ensuring that multiple vendors and systems adhere to a common framework covering the customer experience—planning, booking, payment, and connectivity—as well as multimodal

operations management on the operator side. Standardized security protocols and interoperability are essential to protect sensitive user data and maintain secure, efficient service delivery across diverse platforms.

There is a research goal to tie paratransit into broader multimodal apps.[xxii] However, before that is done, researchers determined that there is a crucial gap in understanding how MaaS platforms must tackle cybersecurity, data trust, and policy governance if they're going to be resilient and user-adoptable in the long term.

Automated vehicles are the future for transit. The goMARTI (Grand Rapids Mobility and Autonomous Rural Transit Initiative) program is a pioneering autonomous shuttle service launched in Grand Rapids, Minnesota, in September 2022. The provides free, on-demand transportation, particularly in rural areas where traditional transit options are limited. The service operates a fleet of autonomous vehicles, including three wheelchair-accessible, ADA-compliant vans, covering a 5.13-square-mile area with approximately 70 pick-up and drop-off points.[xxiii] Riders can request a ride through a dedicated app or by phone.[xxiv]

Non-Emergency-Paratransit Convergence (NEMT)

Non-Emergency Paratransit Convergence (NEMT Convergence) refers to the integration or coordination of two traditionally separate transportation services: Non-Emergency Medical Transportation (NEMT) and paratransit. NEMT provides rides to individuals—often Medicaid beneficiaries—for medical appointments and healthcare-related travel that is not urgent. Paratransit, typically mandated under the Americans with Disabilities Act (ADA), serves people with disabilities and the general public over the age of 60 who cannot use fixed-route public transit systems. Convergence involves aligning operations, technologies, and policies to share resources such as vehicles, dispatching systems, and drivers, with the goal of improving efficiency and rider experience.

The primary objectives of NEMT convergence include reducing operational costs, increasing vehicle utilization, improving service quality, and leveraging technology for more efficient routing and real-time monitoring. However, several challenges can hinder convergence efforts. Regulatory differences exist between ADA paratransit and Medicaid-funded NEMT, and HIPAA compliance requirements for medical data add complexity when integrating systems. Scheduling can be difficult to align due to the varied nature of NEMT and paratransit trips, and funding silos often separate the two services. Moreover, cybersecurity and privacy concerns become more prominent when data systems are integrated, requiring safeguards to protect sensitive medical and personal information.

In practice, convergence can be seen in efforts by regional mobility managers, shared software platforms, and state pilot programs that unify NEMT and paratransit services. Examples include real-time scheduling systems and broker models that streamline trip coordination. These efforts demonstrate the potential of convergence to improve service delivery while highlighting the need for careful planning, robust technology infrastructure, and strong data governance policies to protect user information is secure and private and within regulatory compliance guidelines.

Large Language Models (LLM) and Artificial Intelligence Agents (AI) Using Reservations, Scheduling, and Dispatching Transit Requests

A key cybersecurity and privacy concern when using natural language data from people requesting rides—especially data that reveals their medical or mobility needs—is the risk of sensitive personal information being exposed or misused. Since such requests often contain detailed, identifiable information about an individual's health conditions, disabilities, or mobility requirements, if this data is used to train AI models without proper anonymization and security controls, it could lead to unauthorized access or data breaches.

This exposure could result in discrimination, stigma, or violations of privacy rights. Moreover, if AI models inadvertently memorize or reproduce this sensitive information, it could be leaked in future interactions, further compromising individuals' confidentiality and trust. Ensuring robust data protection, strict anonymization, and compliance with privacy regulations (like HIPAA) is critical to mitigate these risks.

Conclusion

This report provides a targeted cybersecurity and privacy assessment of transit technologies used for reservations, scheduling, and dispatching services, with a focus on systems serving vulnerable road users (VRUs), including individuals with disabilities, older adults, and those with mobility or medical needs. As transit agencies increasingly adopt digital platforms to manage trip bookings and service delivery, these systems must balance access and operational efficiency with robust protections for sensitive user data.

The report identifies key risks associated with common transit software platforms and data exchange standards, such as the General Transit Feed Specification (GTFS) and the General On-Demand Feed Specification (GOFS-lite) for both on-demand and fixed route transit. It highlights vulnerabilities related to data collection, third-party integration, real-time location tracking, and authentication protocols. Particular attention is given to risks posed by the storage and transmission of information that may reveal a passenger's health status, travel behavior, or eligibility for specialized services.

Building on this assessment, the report offers best-practice recommendations tailored to transit agencies, technology vendors, and mobility managers. These include implementing multi-factor authentication, encrypting sensitive data in transit and at rest, conducting regular access audits, and following the principles of least privilege and zero trust. It also emphasizes the importance of staff training, cybersecurity governance, and inclusive design that safeguards both functionality and privacy for transit

users. Recent ransomware attacks have revealed that RSD systems have been affected and possibly directly targeted resulting in changes to and disruptions in transit services.

By integrating technical, operational, and policy perspectives, the report supports transit agencies in building secure, privacy-conscious systems that maintain public trust and regulatory compliance while delivering equitable and reliable mobility services.

Appendix 1: Cybersecurity Best Practices for Transit Agencies

1. Strengthen Access Controls
- Implement multi-factor authentication (MFA) for all administrative and operational systems.
- Use role-based access control (RBAC) to restrict system access based on job responsibilities.
- Regularly review and update user permissions, especially for control systems like SCADA and fare collection.

2. Keep Vehicle and Operational Systems Updated
- Ensure transit vehicle systems (e.g., Automatic Vehicle Location, communication units) receive timely firmware and software patches.
- Coordinate with vendors to apply security updates on embedded devices and IoT sensors.
- Maintain patch management for scheduling, dispatching, and customer service platforms.

3. Segment Networks and Isolate Critical Infrastructure
- Separate corporate networks from operational technology (OT) networks controlling vehicles, signaling, and station systems.
- Use firewalls and virtual LANs (VLANs) to minimize lateral movement within systems.
- Restrict remote access to operational control centers with secure VPNs and strict authentication.

4. Enforce Least Privilege Across Systems
- Limit administrative privileges to essential personnel only.
- Regularly audit access rights to fare payment systems, passenger data, and vehicle control interfaces.
- Apply strict controls on third-party contractors accessing sensitive systems.

5. Perform Regular Backups and Test Recovery Plans
- Backup critical operational data, including scheduling, vehicle telemetry, and payment records.
- Store backups securely, preferably offline or with encryption.
- Conduct disaster recovery drills focusing on ransomware and system outages.

6. Deploy Endpoint Protection and Real-Time Monitoring
- Protect desktops, servers, and mobile devices with updated antivirus and anti-malware solutions.
- Use intrusion detection systems (IDS) and Security Information and Event Management (SIEM) tools to monitor for suspicious activity.
- Monitor network traffic for anomalies indicating cyber threats.

7. Encrypt Data in Transit and at Rest
- Encrypt passenger payment data, personally identifiable information (PII), and operational communications.
- Use secure communication protocols (TLS/SSL) for ticketing and mobile apps.
- Ensure encryption keys are managed securely with access controls.

8. Conduct Regular Employee Training
- Provide targeted cybersecurity awareness training focused on phishing, social engineering, and operational security.
- Train frontline staff on recognizing cyber threats affecting fare systems and vehicle controls.
- Simulate attack scenarios like phishing campaigns to increase staff vigilance.

9. Develop and Maintain an Incident Response Plan
- Create a transit-specific incident response plan covering cyberattacks, system failures, and data breaches.
- Establish clear communication channels with law enforcement, vendors, and emergency responders.
- Regularly test the plan with tabletop exercises involving operations, IT, and management teams.

10. Log and Monitor System Activity
- Enable logging for vehicle control systems, fare payment platforms, and network devices.
- Review logs regularly for unauthorized access or operational anomalies.
- Correlate data using SIEM to detect coordinated attacks or insider threats.

11. Manage Third-Party and Vendor Security
- Conduct cybersecurity assessments of technology vendors, including fare payment providers and vehicle system manufacturers.

- Include cybersecurity requirements in contracts and service level agreements (SLAs).
- Limit third-party access to only necessary systems and monitor their activities continuously.

12. Adopt Zero Trust Principles

- Assume no user or device is trusted by default, especially for remote access and IoT devices.
- Continuously verify user identities and device health before granting access.
- Use micro-segmentation to control access to critical transit systems.

13. Conduct Risk Assessments and Regular Audits

- Identify and prioritize critical assets such as control centers, payment systems, and vehicle networks.
- Perform regular cybersecurity risk assessments focusing on emerging threats.
- Engage independent auditors for penetration testing and compliance checks.

14. Comply with Transit and Transportation Cybersecurity Standards

- Align cybersecurity practices with NIST Cybersecurity Framework, TSA guidelines, and FTA cybersecurity directives.
- Stay updated on federal and state regulations impacting transit cybersecurity and data privacy.
- Document compliance efforts and risk mitigation activities.

15. Promote a Culture of Security Across the Agency

- Encourage reporting of suspicious activities without fear of reprisal.
- Integrate cybersecurity into daily operational decision-making and employee performance metrics.
- Foster collaboration between IT, operations, and executive leadership on cybersecurity initiatives.

Appendix 2: Privacy Recommendations for Public Transit Users

- **Use Official Platforms**: Transit agencies should clearly identify their official websites and mobile apps for trip planning and ticketing. Users should be cautioned against using third-party services that do not clearly disclose their data collection, storage, and sharing practices. Agencies should also monitor app stores for fraudulent or misleading transit apps and report them, as necessary.
- **Minimize Data Sharing**: Encourage users to provide only the minimum personal information required to access transit services. Data such as medical status, travel history, or precise location should not be shared unless essential. Additionally, users should easily be able to access a statement or notice regarding with whom their data is shared.
- **Adjust Privacy Settings**: Advise users to review and modify app permissions to restrict unnecessary access to location data, contacts, and other personal information. Promote the use of strong, unique passwords and recommend enabling two-factor authentication to secure accounts.
- **Stay Alert to Scams**: Agencies should implement public awareness campaigns to help users recognize and avoid phishing attempts, suspicious emails, and unofficial QR codes that offer fake ticket discounts or account support. Clear guidance should be provided on how to verify legitimate communications from transit providers.

Appendix 3: Cybersecurity and Privacy Standards, Reference Documents, White Papers, and Frameworks Referenced in this Report

NIST Cybersecurity Framework Version 2: https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf

NIST 800-53 Security and Privacy Controls for Information Systems and Organizations: https://csrc.nist.gov/pubs/sp/800/53/r5/upd1/final

NIST Privacy Framework Version 2: https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.40.ipd.pdf

Health Insurance Portability and Accountability Act (HIPAA): https://www.hhs.gov/hipaa/for-professionals/index.html

Federal Information Security Modernization Act (FISMA): https://www.cisa.gov/topics/cyber-threats-and-advisories/federal-information-security-modernization-act

California Consumer Privacy Act (CCPA): https://oag.ca.gov/privacy/ccpa

ISO/IEC 27701 Privacy Information Management Systems (PIMS): https://www.iso.org/standard/71670.html

ISO/IEC 27018 Cloud privacy standard, focusing on protecting PII in public cloud environments: https://www.iso.org/standard/76559.html

NIST 800-171 Version 3, Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations: https://csrc.nist.gov/pubs/sp/800/171/r3/final

RSD Glossary: TBD

“Multimodal for All Travelers White Paper on Reservations, Scheduling, and Dispatching”: TBD

Endnotes

[i] "*On demand is a concept envisioning an interconnected and coordinated mobility ecosystem to meet the needs of all users by providing the safe, reliable, and efficient movement of travelers and goods. MOD offers users personalized mobility and goods delivery options upon request, matched with coordinated network strategies of service providers and operations managers. NOTE: MOD is based on the principle that transportation is a commodity where options have distinguishable values*." RSD Glossary.

[iiii] Belcher, S., & Belcher, T. (2025, April 1). *Does the transit industry understand the risks of cybersecurity and are the risks being appropriately prioritized?* (Tech. Rep. No. DOT 83460) [White paper]. U.S. Department of Transportation, Bureau of Transportation Statistics. https://rosap.ntl.bts.gov/view/dot/83460

[iii] Belcher, S. (2025, July 3). *Interview.*

[iv] "Paratransit." RSD Glossary.

[v] "Demand Response." RSD Glossary.

[vi] "Mobility on Demand." RSD Glossary.

[vii] Google. (n.d.). *General Transit Feed Specification (GTFS)* [Source code]. GitHub. https://github.com/google/transit

[viii] Google. (n.d.). *General On Demand Format Specification (GOFS)* [Source code]. GitHub. https://github.com/GOFS-lite/GOFS-lite

[ix] Hardt, D. (Ed.). (2012). *The OAuth 2.0 authorization framework* (RFC 6749). Internet Engineering Task Force. https://datatracker.ietf.org/doc/html/rfc6749

[x] U.S. Department of Justice, Office of Public Affairs. (2022, July 18). *Uber commits to changes and pays millions to resolve Justice Department lawsuit for overcharging people with disabilities* [Press release]. https://www.justice.gov/archives/opa/pr/uber-commits-changes-and-pays-millions-resolve-justice-department-lawsuit-overcharging-people-with-disabilities

[xi] U.S. Cybersecurity and Infrastructure Security Agency; U.S. Department of Homeland Security. (2025, January 16). *CISA first detected Salt Typhoon on federal networks prior to telecom intrusions* [Press release]. Cybersecurity & Infrastructure Security Agency. https://www.cybersecuritydive.com/news/salt-typhoon-federal-networks-easterly/737552/?utm_source=chatgpt.com

[xi] Federal Transit Administration. (2018). *Automatic Passenger Counter (APC) system validation and usage*. U.S. Department of Transportation. https://www.transit.dot.gov/sites/fta.dot.gov/files/docs/apc-validation-and-usage_0.pdf

[xi] Belcher, S., Belcher, T., Seckman, K., Thomas, B., & Yaqub, H. (2022, July). *Aligning the transit industry and their vendors in the face of increasing cyber risk: Recommendations for identifying and addressing cybersecurity challenges* (Project 2113) [White paper]. Mineta Transportation Institute, San José State University.

[xii] Seckman, K., Belcher, H., Belcher, S., & Thomas, B. (2021). *Personal data protection as a driver for improved cybersecurity practices in U.S. public transit* (Project 2113-WP2). Mineta Transportation Institute. https://transweb.sjsu.edu/sites/default/files/2113WP2-Belcher-Cybersecurity-PII-Transit.pdf

[xiii] Rourke, T. (2020, October 15). *A primer on tokens, tokenization, payment tokens, and merchant tokens*. ACI Worldwide. https://www.aciworldwide.com/blog/a-primer-on-tokens-tokenization-payment-tokens-and-merchant-tokens

[xiv] CallCabinet. (2024, December 3). *Understanding PCI DSS call recording requirements*. CallCabinet. Retrieved from https://www.callcabinet.com/blog/understanding-pci-dss-call-recording-requirements/

[xv] https://www.twilio.com/en-us/legal/security-overview

[xvi] https://docs.aws.amazon.com/sms-voice/latest/userguide/data-protection.html

[xviii] "MTA: 'Cybersecurity incident' affecting Mobility paratransit services, real-time tracking information," *WBAL-TV*, Aug. 25, 2025. https://www.wbaltv.com/article/mta-cybersecurity-incident-mobility-paratransit-real-time-information/65882568

[xix] Maryland Transit Administration. (2025, August). *Impacts from cybersecurity incident*. Maryland.gov. https://www.mta.maryland.gov/cybersecurity-incident

[xx] The Record. (2025, August 27). *Cyberattack on Maryland transit system affects services for people with disabilities*. The Record by Recorded Future. https://therecord.media/maryland-cyberattack-transit-disabled-people

[xxi] RideKC. (2024, January 24). Cyber-attack hits KCATA. Communications affected. https://ridekc.org/news/cyber-attack-hits-kcata-communications-affected

[xxii] Candel, L., van der Heijden, R., Feitsma, J., & van den Hoven, J. (2024). *The road not taken yet: A review of cyber security risks in mobility-as-a-service (MaaS) ecosystems and a research agenda*. Research in Transportation Business & Management, 56, 100971. https://doi.org/10.1016/j.rtbm.2024.100971

[xxiii] MinnPost. (2025, August 12). *Grand Rapids autonomous transit expanding to nearby cities, tribal stops*. Retrieved August 15, 2025, from https://www.minnpost.com/greater-minnesota/2025/08/grand-rapids-autonomous-transit-expanding-to-nearby-cities-tribal-stops/

[xxiv] goMARTI. (n.d.). *How to ride*. Retrieved August 15, 2025, from https://gomarti.com/ride-with-us/