Phase 2 Data Privacy Plan (DPP)

Buffalo, NY ITS4US Deployment Project

www.its.dot.gov/index.htm

Final– January 27, 2023

FHWA-JPO-22-969

ITS4US

IT'S TRANSPORTATION FOR ALL OF US

U.S. Department of Transportation

Produced by NFTA
U.S. Department of Transportation
Intelligent Transportation Systems Joint Program Office
Federal Highway Administration
Office of the Assistant Secretary for Research and Technology
Federal Transit Administration

Notice

Technical Report Documentation Page

1. Report No.	2. Government Accession No.	3. Recipient's Catalog No.
FHWA-JPO-22-969		

4. Title and Subtitle	5. Report Date
Phase 2 Data Privacy Plan (DPP) - Buffalo, NY ITS4US Deployment Project	January 27, 2023
	6. Performing Organization Code

7. Author(s)	8. Performing Organization Report No.
Adel W. Sadek (UB), Polly Okunieff (ICF), Nayel Urena Serulle (ICF), Deepak Gopalakrishna (ICF), Robert Jones (NFTA), Kelly Dixon (GBNRTC), Jamie Hamann-Burney (BNMC), Chunming Qiao (UB), Stephen Still (UB), Victor Paquet (UB), and Jordana Maisel (UB)	

9. Performing Organization Name and Address	10. Work Unit No. (TRAIS)
NFTA, 181 Ellicott Street, Buffalo, NY 14203 BNMC, 640 Ellicott Street, Buffalo, NY 14203 ICF International, 9300 Lee Highway, Fairfax, VA 22031 University at Buffalo, Amherst, NY 14228 RSG, 55 Railroad Row, Suite 101, White River Junction, VT 05001 ETCH, 4696 Smothers Road, Westerville, OH 43081	**11. Contract or Grant No.** 693JJ32250011

12. Sponsoring Agency Name and Address	13. Type of Report and Period Covered
U.S. Department of Transportation ITS Joint Program Office 1200 New Jersey Avenue, SE Washington, DC 20590	Final Draft
	14. Sponsoring Agency Code HOIT-1

15. Supplementary Notes

Elina Zlotchenko (USDOT ITS-JPO) is the Agreement Officer Representative (AOR) and Sarah Tarpgaard (USDOT) is the Agreement Officer (AO).

16. Abstract

The Buffalo NY ITS4US Deployment Project seeks to improve mobility to, from and within the Buffalo Niagara Medical Campus by deploying new and advanced technologies with a focus on addressing existing mobility and accessibility challenges. Examples of the technologies to be deployed are electric and self-driving shuttles, a trip planning app that is customized for accessible travel, intersections that use tactile and mobile technologies to enable travelers with disabilities navigate intersections, and Smart Infrastructure to support outdoor and indoor wayfinding. The deployment geography includes the 120-acre Medical Campus and surrounding neighborhoods with a focus on three nearby neighborhoods (Allentown, Fruit Belt and Masten Park) with underserved populations (low income, vision impaired, deaf or hard of hearing, wheeled mobility device users and older adults).

This document, the Data Privacy Plan (DPP), provides the plan to ensure sufficient data privacy controls to mitigate the risk of harm to individuals that would result in the improper handling or disclosure of the Personally Identifiable Information (PII) or Sensitive Personally Identifiable Information (SPII) collected from individuals in connection with the Buffalo ITS4US Deployment Project.

17. Keywords	18. Distribution Statement
ITS4US; Deployment; ITS; Intelligent Transportation Systems; participant training; stakeholder education, Data Privacy Plan	

19. Security Classif. (of this report)	20. Security Classif. (of this page)	21. No. of Pages	22. Price
Unclassified	**unclassified**	51	

Form DOT F 1700.7 (8-72) **Reproduction of completed page authorized**

Revision History

Name	Date	Version	Summary of Changes	Approver
NFTA	Nov 1, 2022	0.1	Initial Draft	Kelly Dixon
Buffalo ITS4US Phase 2 Data Privacy Plan	Dec 5, 2022	0.2	Responded to USDOT comments	Kelly Dixon
Buffalo ITS4US Phase 2 Data Privacy Plan	Jan 27, 2023	1	Apply configuration control to SOI section.	Kelly Dixon

Table of Contents

List of Tables

List of Figures

1 Introduction

1.1 Document Purpose

The Data Privacy Plan (DPP) provides the plan to ensure sufficient data privacy controls to mitigate the risk of harm to individuals that would result in the improper handling or disclosure of the Personally Identifiable Information (PII), or Sensitive Personally Identifiable Information (SPII) collected from individuals in connection with the Buffalo ITS4US Deployment Project. This document builds upon the information provided in the system's Concept of Operations (ConOps) (FHWA-JPO-21-860)[1], Data Management Plan (DMP) (FHWA-JPO-21-868)[2], Human Use Approval Summary (HUAS) (FHWA-JPO-21-898) [3], and Performance Measurement and Evaluation Support Plan (PMESP) (FHWA-JPO-21-878)[4].

1.1.1 Organization of this Document

The remainder of this document is organized as follows:

- **Section 2** describes the privacy approach, detailing requirements, and assessments.
- **Section 3** details the different security controls.
- **Appendix A** lists the acronyms used in this document.
- **Appendix B** provides the references used in this document.

1.2 Deployment Concept

Buffalo is moving toward a sustainable future at all levels of society, incorporating actions in the community, government, and private entities in the area. Providing access to the City's underserved populations to jobs and healthcare is the primary motivation for all the regional partners involved in this deployment. A lack of public transportation that adequately addresses "first/last mile" challenges is a major problem for community mobility, especially for people with disabilities. This often leads to compromised healthcare (e.g., rescheduled or missed appointments, delayed care) and/or dependence on paratransit service, which is much costlier for transit agencies and can be burdensome for riders. The ITS4US concept proposed here directly addresses these concerns by:

1. **Focusing on providing transit access to healthcare and jobs** to underserved residents or persons and allowing them to share in the economic development in downtown Buffalo.
2. **Putting technology to work in support of accessible transportation**, bringing leading edge researchers in accessible transportation, transit, and connected automation to solve a transportation need.

3. **Developing a scalable model** for considering accessibility and universal design in transportation technology projects

The deployment location is targeted around the downtown Buffalo area with a focus on travel to and from the Buffalo Niagara Medical Campus (BNMC). The deployment includes the 120-acre Medical Campus and surrounding neighborhoods with a focus on three nearby neighborhoods (Fruit Belt, Masten Park, and Allentown)—see Figure 1.

Figure 1. Buffalo Niagara Medical Campus Relative to the Neighborhoods of Focus.
Source: Buffalo, NT ITS4US

More than 16,000 people work or study at the BNMC and more than 1.5 million visit each year for health care and other services, generating significant transportation demand for the area, its visitors, and its employees. The demographics of the surrounding neighborhoods (see Table 1) are emblematic of a broader socioeconomic and racial divide in Buffalo along Main Street, which this deployment seeks to bridge. In Allentown (west of Main Street), the percentage of traditionally underserved populations is significantly less than other neighborhood east of Main Street, namely Fruit Belt and Masten Park. Table 1 indicates percentages for Allentown that are far below average of the Metropolitan Statistical Area (MSA) in many categories, and percentages for Fruit Belt and Masten Park that are above average for the MSA.

While the Allentown neighborhood is not characterized by underserved populations, it contains a high concentration of transit service and commercial activity, including health care offices. Allentown hosts several significant bus lines (including the #20-Elmwood, the #25-Delaware, the #11-Colvin, and the #8-Main) that connect the BNMC and Downtown Buffalo with neighborhoods to the north, carrying over 10,500 riders on an average weekday.

Table 1. Demographics of Neighborhoods of Focus

Geography (ACS 2018 tracts)	Percent 0-veh. house-holds	Percent population 65+	Percent poverty	Percent Black	Percent Hispanic / Latino	Percent limited English ability	Percent income <$25k	Percent with a disability (18 to 65 yrs old)	Percent veteran	Percent commute by transit	Total house-holds	Total pop.
Fruit Belt	47.0%	21.9%	28.0%	77.0%	8.9%	4.2%	39.5%	20.0%	6.7%	16.1%	976	2,435
Allentown	18.4%	6.2%	28.8%	7.2%	6.6%	0.0%	17.4%	8.0%	7.8%	4.8%	1978	3,143
Masten Park	35.0%	18.5%	34.7%	89.7%	3.1%	2.9%	38.9%	15.2%	6.6%	11.7%	1496	3,208
Buffalo MSA	**36.6%**	**12.0%**	**31.1%**	**36.6%**	**11.6%**	**4.8%**	**30.7%**	**9.7%**	**5.7%**	**11.5%**	**11,0701**	**255,423**

BNMC sits adjacent to the Fruit Belt neighborhood, which has a poverty rate of 28%, and 47% zero-car households. Several community and social services are found within the neighborhood, which is relatively close to the wider array of services and jobs offered in downtown Buffalo. Several bus lines serve the area, although headways are relatively infrequent, ranging between ½ hour and one hour. Access to dispersed jobs in the suburbs via public transportation tends to be difficult. Although accessible to the Fruit Belt residents, the Niagara Frontier Transportation Authority (NFTA) Metro Rail station is 0.25 – 0.75 miles away, a distance that becomes amplified during the winter and for travelers with physical difficulties. While BNMC continues to improve pedestrian accessibility, sidewalk quality and intersection crossings still are a challenge for wheelchair users and users with audible or visual impairments. The Fruit Belt struggles with aging infrastructure and infrastructure management issues, issues that have been consistently noted in community forums over the years.

This project seeks to improve transportation access for this population and utilize an innovative approach to support effective trip-making. BNMC's user population make it an ideal location to test accessibility features for safety and usability. The ITS4US Buffalo project focuses on two primary trip purposes: employee-related travel and patient/visitor travel to the campus from the three adjacent neighborhoods.

1.2.1 System Overview

The Greater Buffalo-Niagara Regional Transportation Council (GBNRTC) established its vision of the region for 2050 in its "Moving Forward 2050 – A Regional Transportation Plan for Buffalo Niagara" [6](GBNRTC; University at Buffalo Regional Institute, The SUNY at Buffalo School of Architecture and Planning; Cambridge Systematics; TyLin International, 2018).

The plan seeks to guide transportation investments to:

1. Raise the region's standard of living
2. Support efficient freight movement
3. Maximize infrastructure resiliency
4. Support focused growth in communities (urban, suburban, and rural)
5. Ensure access to opportunities and services
6. Support healthy and safe communities through targeted transportation investment
7. Strengthen the fiscal health of local governments
8. Preserve and protect a healthy environment and accessible open spaces and waterways
9. Create a fully integrated and seamless transportation environment

The Buffalo ITS4US project goals directly align with GBNRTC's goals 1, 4, 5, 6, and 9 by providing innovative tools and services to better enable travelers to make complete trips in and around the BNMC. Furthermore, the proposed system focuses on providing transit access to

healthcare and jobs to underserved citizens and allow them to share in the economic development in downtown Buffalo.

To achieve these goals, the proposed system of interest is made of four major subsystems and a variety of data interfaces between them. The four major subsystems include:

- **Complete Trips Platform** – The complete trip platform (CTP) is the integrated trip planning function for travelers. It includes various modules that allow users to personalize their trip planning, execution, and navigation experience. Specific modules in this subsystem include:
    - User Profiles
    - Trip Booking
    - Trip Planning
    - Trip Monitoring and Notifications
    - Geolocation and Mapping
    - Navigation
    - Real-time situational monitoring
    - Performance metrics
    - Trip history/ledger
    - User Interface (UI): Mobile application
    - UI: Web
- **Community Shuttle Subsystem** – The Community Shuttle (CS) subsystem provides demand-responsive transit services within a specified zone of operations, using a mix of vehicles, including both human-driven (HDS) and self-driving shuttles (SDS). The SDS will operate on a predefined route(s), consisting of a set of streets within the zone and pick-up and drop-off locations, but will be responsive to travelers' demand (e.g., it can skip certain pick-up/drop-off locations if there is no demand). The HDS will provide door-to-door on demand service within the zone of operation. Modules within this subsystem include both types of vehicles, as well as a Shuttle Operations Center (SOC).
- **Smart Infrastructure Subsystem** – The smart infrastructure subsystem includes wayfinding and orientation for indoor and outdoor, provision of navigation and destination finding through information kiosks (Transportation Information Hub, TIH), augmented communications technologies (Smart Signs), and intersection treatment for hands-free, pedestrian signal requests.
- **Performance Dashboard Subsystem** – The performance measurement dashboard (PMD) subsystem measures and presents the performance of the system to the agency operating the system.

While not directly part of the project, the CS will be complemented by NFTA Paratransit Access Line (PAL) spontaneous (i.e., same day trip booking and execution) and regular services (i.e., trip reservation done by at least 8pm ET the day before the trip). Other NFTA services, such as bus and rail, will also provide complement to the CS.

The envisioned service area for the proposed CS fleet is shown in Figure 2. The services to be provided within this area are detailed in Figure 3.

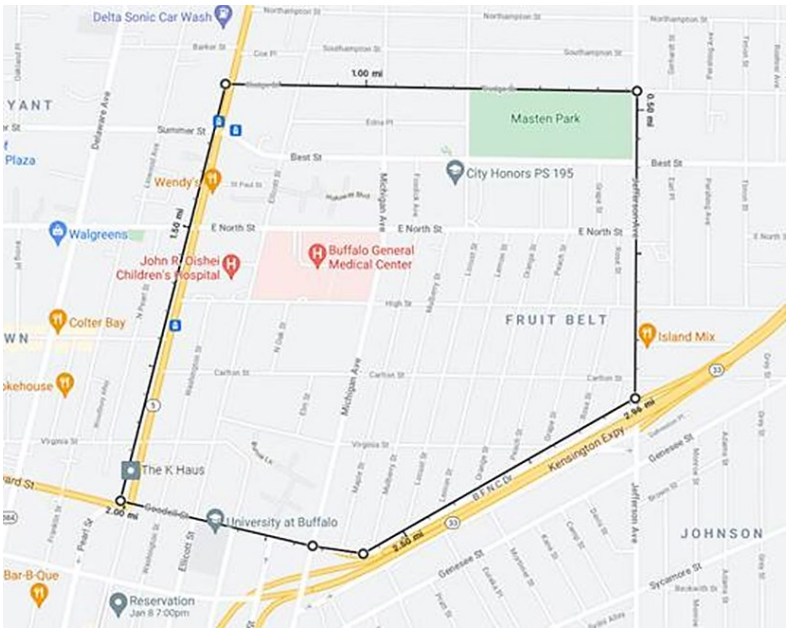

Figure 2. Proposed Service Area for the Community Shuttle
Source: Buffalo, NT ITS4US

	Services	Inside Area	Outside Area
Community Shuttle	HDS	CTP- PAL eligible, CTP - General Traveler	
Community Shuttle	SDS	CTP- PAL eligible, CTP - General Traveler	
	PAL (spontaneous)*	CTP- PAL eligible	
	PAL (regular)**	CTP- PAL eligible	CTP- PAL eligible
	Other NFTA Serv.	CTP- PAL eligible, CTP - General Traveler	CTP- PAL eligible, CTP - General Traveler

* PAL (spontaneous) refers to same-day service
**PAL (regular) reservation must be done by 8pm night before the trip

Figure 3. Community Shuttle Services
Source: Buffalo, NT ITS4US

1.2.2 System of Interest

This section describes a high-level description of the four subsystems of the Buffalo, NY ITS4US system. The following SOI diagrams are updated versions of the Context Diagrams described in the Concept of Operations (ConOps) (FHWA-JPO-21-860) and System Requirements Specification (SyRS) (FHWA-JPO-21-883)[7].

The high-level context diagram which includes the four subsystems are shown in Figure 4.

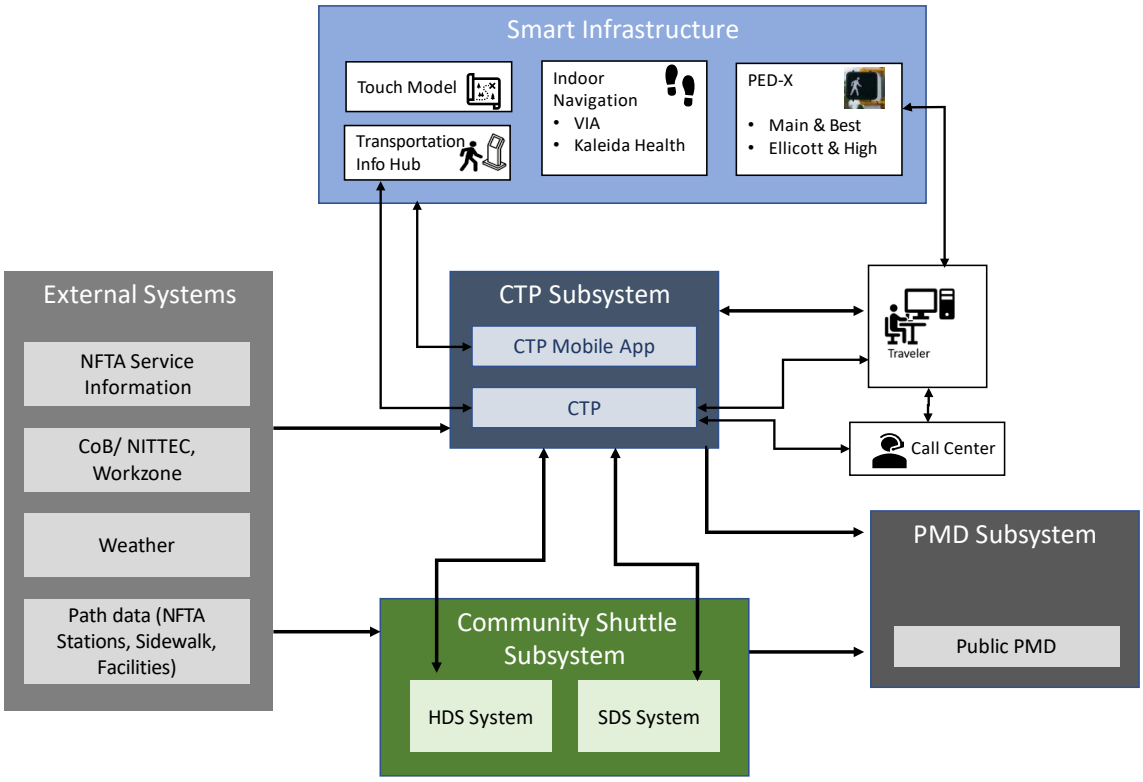

Figure 4. System of Interest: High-Level Context Diagram
Source: Buffalo, NT ITS4US

Some of the details in the high-level context diagram were refined from the Phase 1 system of interest to Phase 2. Justification for these changes will be documented in the Phase 2 Concept of Operations, which will be available prior to June 14, 2024. The detailed context diagrams for each subsystem and associated Smart Infrastructure modules are described in the following four sections (each corresponding to one of the four subsystems). Where detail is needed, for example, the CTP, the subsystem functions, and flows are documented. Where subsystems are deployed as a service, pre-existing systems, or turn-key, fewer details are provided (e.g., SDS and HDS).

The following subsections describe the key components of the SOI. The detailed diagrams include information flows within and between subsystems and functions. A complete set of these information flows (tagged in the diagrams as [I-n] where n is a number between 1 and 23), is listed in Table 2.

Table 2. Information Flows in System of Interest (detailed diagrams)

Information Flow #	Information Flow Name	Information Flow Description
I-1	UI Mobile App APIs	APIs and web services provisioned between the CTP mobile app and server
I-2	UI Web	APIs and web services provisioned to a thin client such as the web or TIH

Information Flow #	Information Flow Name	Information Flow Description
I-3	Service information	NFTA fixed route GTFS, GTFS-realtime
I-4	BNMC Facility Map Update	BNMC indoor facility pathways
I-5	NFTA Map Update	NFTA station pathways (GTFS-pathways)
I-6	(1) SDS Booking transactions (2) SDS Service Information	(1) Reservations, scheduling and status information to book a SDS service. (2) SDS Service information (GTFS-realtime)
I-7	(1) HDS Booking transactions (2) HDS Service Information	(1) Reservations, scheduling and status information to book a HDS service (2) HDS Service information (GTFS-realtime)
I-8	PED-X request transactions	(1) Information exchange between the CTP mobile app and PED-X gateway to request actuation of the pedestrian crossing (2) Location of PED-X enabled crossing
I-9	BNMC Facility waypoint sensor broadcast	Transactions between mobile app native comm and indoor navigation waypoint sensors (e.g., beacons)
I-10	CTP operational log	Operational and performance data monitored and collected by the CTP
I-11	PED-X operational log	A summary of the requests and their results
I-12	SDS operational log	Operational and performance information from SDS
I-13	HDS operational log	Operational and performance information from HDS
I-14	Performance measures	Performance Measurement results
I-15	Map services	APIs and web services that present performance measures
I-16	Direct access data files	APIs / links to access public data
I-17	API data (requires authentication)	APIs and web services that require authentication
I-18	External Data (NFTA Performance Data and OSM / path / map updates)	OSM / path / map updates: Map, sidewalk, indoor facility and asset data and updates from external sources NFTA Performance Data: Summary data for fixed route and PAL on time performance and other performance metrics
I-19	NITTEC Traffic Information	The static network data and dynamic information includes right of way (ROW) data feeds and situational awareness TRANSCOM data fusion engine SPATAL data feeds. The following data feeds are currently identified: -- mobile maps

Information Flow #	Information Flow Name	Information Flow Description
		-- situational awareness information (incidents, work zones, planned events)
I-21	Communications between support personnel	Communications to support travelers on the CS SDS
I-22	Signal Control Exchange	Message from the PED-X gateway to a local traffic signal controller. The information flow forwards a request made by a traveler to request signal actuation
I-23	CoB PROW WZ	Update of work zone information associated with the public right of way developed and disseminated by the City of Buffalo

1.2.2.1 Complete Trip Platform

The CTP provides trip planning and travel functions for travelers. The tool is available for registered and non-registered account users. Account holders will be able to interact (e.g., book a trip reservation, check estimated time of arrival, etc.) with other mobility partners for which they have accounts (e.g., Niagara Frontier Transportation Authority (NFTA) paratransit and community shuttle services), personalize their trip preferences and customize hands-free turn-by-turn notifications, and access wayfinding assets using components specified in the smart infrastructure subsystem. Non-registered travelers will be able to use the trip planning and travel tools to view accessible paths, transit services and alerts about asset status (e.g., elevator / escalator operations). The functions are described in the following sections.

The context diagram for the CTP is shown in Figure 5, where:

1) the subsystems are shown in blue boxes and boxes with icons;

2) functions depicted in white boxes contained in the blue boxes;

3) terminators which are source or destinations of the data are shown in various colored boxes and ovals as designated in the legend; and

4) information flows are shown as either green lines (designated as internal interfaces) or orange lines (designated as external interfaces) tagged with information flow indices [e.g., I-1]).

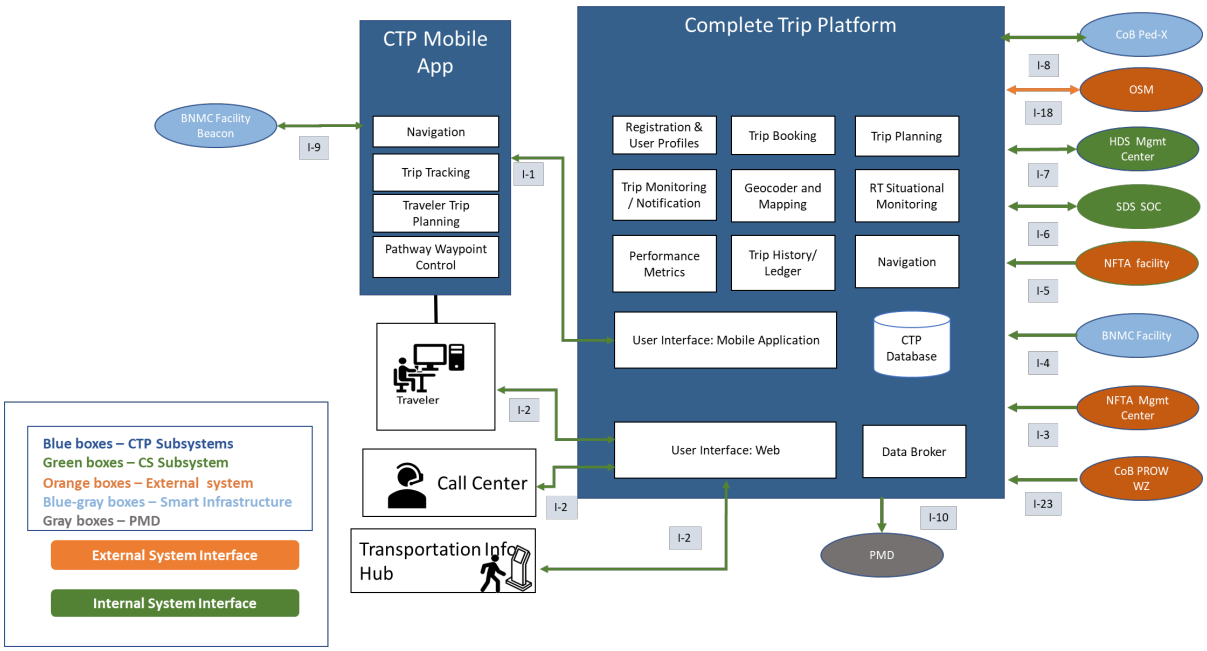

Figure 5. Complete Trip Platform Subsystem
Source: Buffalo, NY ITS4US

1.2.2.2 Community Shuttle Subsystem

The Community Shuttle (CS) subsystem will provide on-demand mobility services within the Fruit Belt, Masten Park and Allentown neighborhoods and BNMC. Although they share similar interfaces to external components/subsystems, the CS consists of two service types – Self Driving and Human Driven services, each designated as a system within this architecture description. The two systems include:

- **SDS System** is composed of two autonomous vehicles and the shuttle operations center (SOC). The SDS will provide microtransit service on a pre-defined set of road segments that satisfy the Operational Design Domain (ODD) of the SDS.

- **HDS System** is composed of wheelchair accessible vehicles, dispatch, and scheduling software (from the NFTA paratransit fleet) and reservations services from the NFTA PAL Direct software system. The HDS will provide door-to-door, on-demand service similar to current PAL paratransit service, but available for all registered CTP participants.

1.2.2.2.1 The Self-Driving Shuttle (SDS) System

The SDS System will be procured as a turn-key service exchanging prescribed information flows between the SDS services and System of Interest (SOI) subsystems (e.g., PMD, CTP) and external systems (e.g., NITTEC). The SDS is composed of the Autonomous Vehicle and Shuttle Operations Center (SOC) components. The shuttle will operate on an on-demand schedule constrained to travel over a pre-defined route (i.e., a set of streets that satisfy the SDS ODD) and pre-designated pick-up/drop-off locations. The SDS Operations Center (SOC) will receive all calls for services and will track the status of each vehicle in the SDS fleet. The SDS system will be

procured as a turn-key service exchanging prescribed information flows between the SDS services and SOI subsystems (e.g., PMD, CTP) and external systems (e.g., NITTEC).

Human actors include the SDS's Shuttle Operations personnel who will manage the SOC and manage incidents, Call Center Customer Support (who provide direct support to travelers) and SDS operators / stewards (who will be trained by the SDS vendor). Figure 6 provides a representation of the SDS information flows with other systems and subsystems Internal system interfaces are indicated by green oval identification numbers and external system interfaces are represented with orange oval identification numbers. The CS/SDS System is enclosed within a dark blue container.

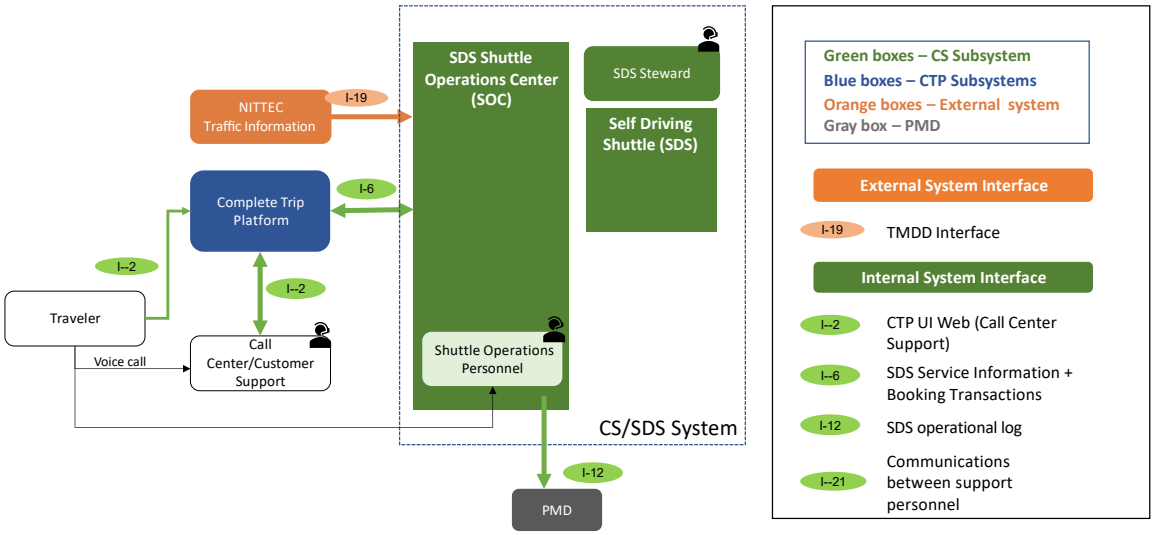

Figure 6. Community Shuttle SDS System
Source: Buffalo, NY ITS4US

1.2.2.2.2 The Human-Driven Shuttle (HDS) System

The HDS System (Figure 7) is composed of the NFTA Dispatch and Reservations System, HDS vehicle, and HDS operator. The HDS will use the NFTA PAL dispatch and software services and operate from the NFTA PAL dispatch and operations center. To that end, the major components are interfaces to and from the NFTA PAL Direct system. The CS/HDS System is enclosed within a dark blue container.

The HDS subsystem will use an existing NFTA system that already provides the appropriate services (APIs) needed to transact customer booking and mobility services.

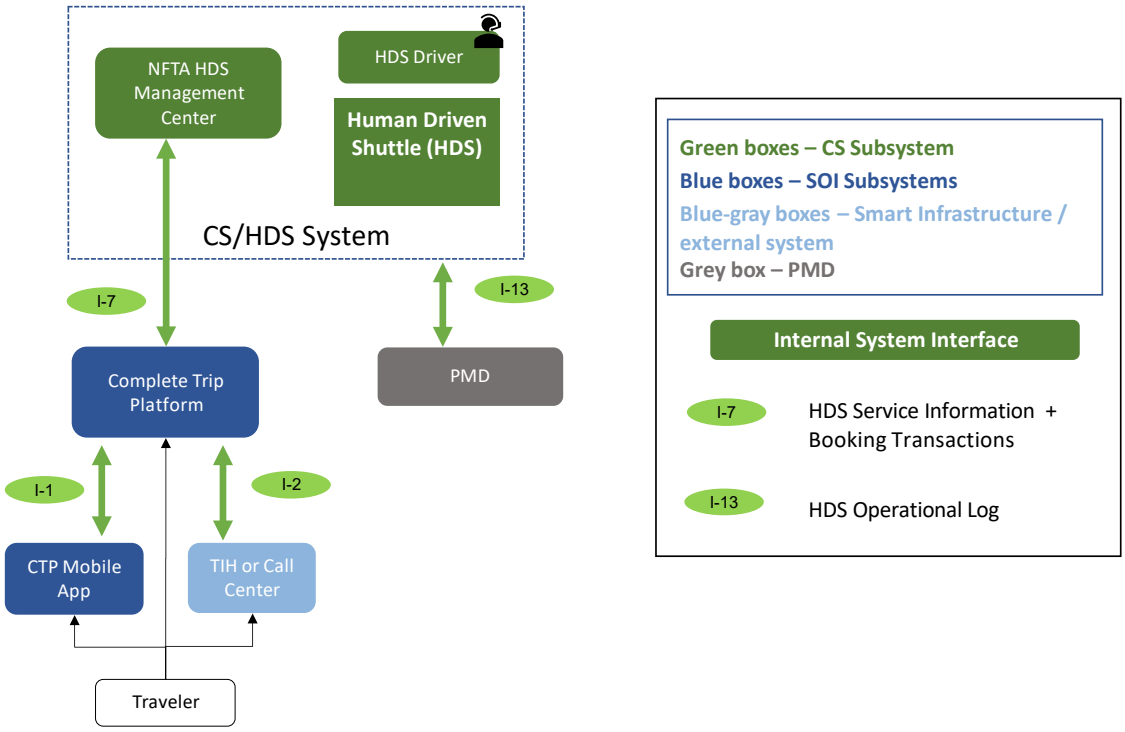

Figure 7. Community Shuttle HDS System Context Diagram
Source: Buffalo, NY ITS4US

1.2.2.3 Smart Infrastructure Subsystem

Smart Infrastructure (SI) supports personalized wayfinding capabilities for travelers. The technologies (subsystems) include:

- Transportation Information Hub (TIH) Subsystem
- Indoor Navigation Subsystem
- Pedestrian Intersection Crossing (PED-X) Subsystem

SI provides support technologies for trip planning and wayfinding. The SI will be used for public access to trip planning activities, supplementary sensors to support indoor navigation at building / facilities and Metro rail stations, and broker / gateway services for pedestrians to request pedestrian actuation at selected signalized intersections—Main St. & Best St. and Ellicott St. & High St.

The context diagrams for the indoor navigation component and the pedestrian signal crossing component are provided below.

1.2.2.3.1 Indoor Navigation Component

Using commonly available communications technologies already deployed in mobile handsets, low-cost beacons will be deployed in signs that support waypoint locations (for orientation) at two indoor spaces to provide indoor navigation (Figure 8). These beacons will provide waypoint (location) information for digital wayfinding integrated with the CTP mobile app navigation function.

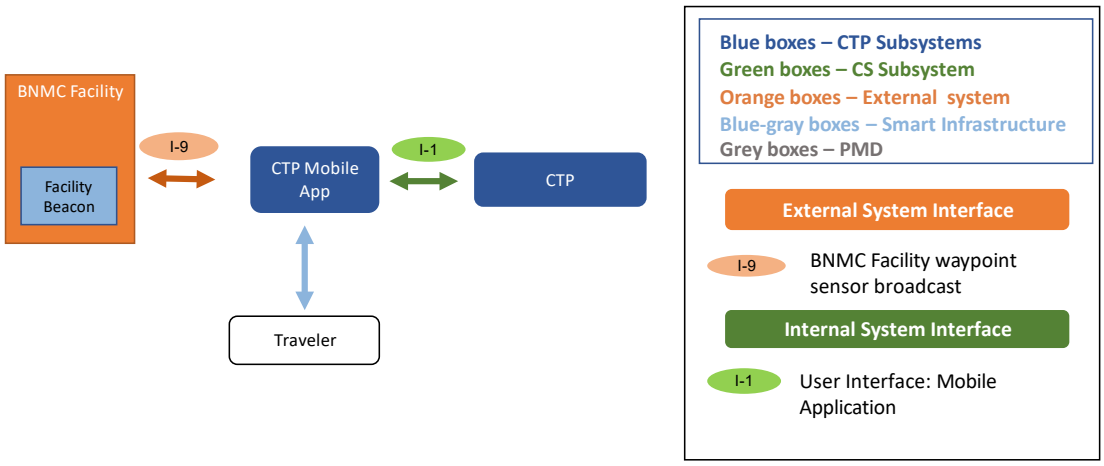

Figure 8. Indoor Navigation Module
Source: Buffalo, NY ITS4US

1.2.2.3.2 Pedestrian Signal Crossing Module

The PED-X module will be implemented as a PED-X Gateway. This gateway receives a CTP generated message triggered by their trip plan. The gateway serves as a conduit to authenticate and secure information exchange between the CTP and traffic signal system to actuate the pedestrian request. Information channeled from the pedestrian to the signal system includes the request information.

Note that the Traffic Signal System, using an audible pedestrian signal will display and annunciate *walk* and *don't walk* signals at the intersection. This link is not shown in the figure because it is not a physical communications message.

The Pedestrian Signal Crossing module is shown in Figure 9.

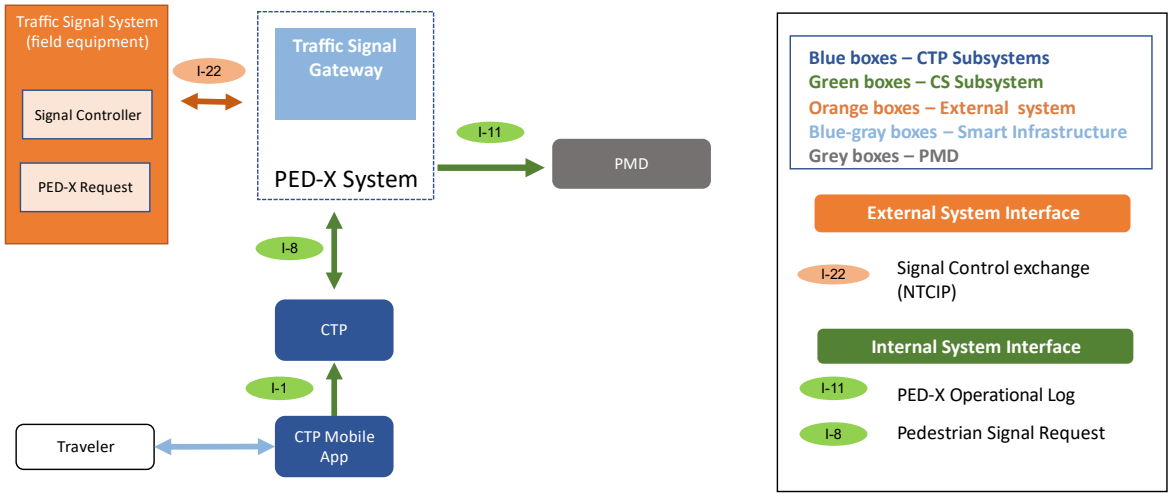

Figure 9. Pedestrian Signal Request (PED-X) Module
Source: Buffalo, NY ITS4US

1.2.2.4 Performance Measure Dashboard Subsystem

The Performance Measure Dashboard subsystem monitors, integrates, analyzes, and displays performance measures from other subsystems and external sources. The subsystem will include functions to ingest log files from the subsystems and external data sources, storage, analytic and visualization tools to display and access current and historic data sets produced from the integrated system. The PMD subsystem will be implemented using a three-tier architecture – data (data tier), analytic processes (processing tier), and access / visualization (presentation tier), see Figure 10.

Data Tier. The data tier will ingest and store data from the other subsystems and external systems as needed (defined in the Phase 1 PMESP (FHWA-JPO-21-878), Phase 1 Data Management Plan (DMP) (FHWA-JPO-21-868), and subsequent design documents). In addition, metadata management will be included to ensure data integrity as data is ingested and transformed for distribution. The data tier will ingest operational, maintenance, and performance summary data from each subsystem, as well as non-PII data from the performance measurement reports. The data will be ingested by the PMD and all PII will be removed.

Processing Tier. The processing tier will provide services to curate, transform, parse and query data stores to generate performance and aggregated measures. A user authentication function will provide access to users of different security levels. Security and privacy provisions will be implemented to protect, store and archive information.

Presentation Tier. The access and visualization channels will include a web-based dashboard showing key system performance measures as well as a data portal that will provide access via data feeds and APIs for authorized users.

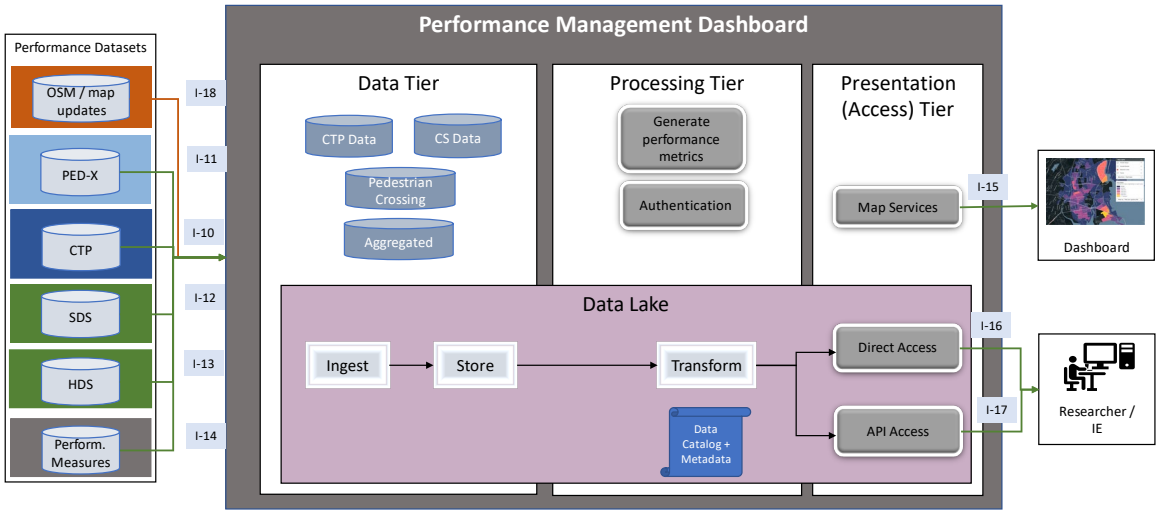

Figure 10. Performance Measure Dashboard
Source: Buffalo, NY ITS4US

2 Privacy Approach

2.1 Access Requirements

This section defines the data access requirements needed by the Buffalo ITS4US system to meet the overall user needs described in the SOI (Section 1.2.2). Basically, the security of the data will rely on four access levels, which combine levels of privacy and license restrictions (e.g., limited copying or redistribution). The four types of data access include:

- **Open** – Data that can be used by the public with no or limited licensing restrictions. This data is available to the public without needing to request permissions and will be provided to the USDOT-managed Public System. These may include anonymized or aggregated versions of private datasets to protect PII. Datasets that are considered open were anonymized or aggregated in such a way so as to make it impossible to derive any PII from them.

- **Private**

    - **Research** – Data that is available for research, but users of the data must meet IRB requirements before gaining access to the data. While efforts will be made to strip off research data from PII, some remnants of such information may still be available (e.g., trace data). The data remaining may allow a person to derive some PII by linking to other datasets for example. Because PII may be derived from research datasets, users of such data need to meet IRB requirements.

    - **Operational (Proprietary)** – Data stewards and operational personnel can access data for operations purposes only. This includes both third party (licensed) datasets and protected data. A subset of the data may be proprietary data that is licensed by third party or commercial business interests (CBI). Access to CBI data is determined by usage agreements between the parties.

    - **Protected (PII)** – Data that has PII included in the dataset. Access to this data is restricted to protect the PII based on IRB-approved processes. Data in this category should have an operational purpose that justifies its storage.

The complete set of information flows are listed in Table 2. The inputs into the SOI (i.e., external information flows) are listed in Table 3 where the column labeled “source” identifies the external source.

Table 3. External Data Inputs to the SOI

Flow #	Information Flow Name	Source	Destination	Description
I-3	Service Information	NFTA Management Center	CTP	NFTA Fixed Route GTFS, GTFS-realtime
I-4	BNMC Facility Map Update	BNMC Facility	CTP	BNMC Indoor Facility Pathways
I-5	NFTA Map Update	NFTA Facility Map Update	CTP	NFTA station pathways (GTFS-pathways)
I-8	PED-X Request Transactions	CoB PED-X	CTP Mobile App	1. Information exchange between the CTP mobile app and PED-X gateway to request actuation of the pedestrian crossing 2. Location of PED-X enabled crossing
I-9	BNMC Facility Waypoint Sensor Broadcast	BNMC Facility	CTP Mobile App	Transactions between mobile app native comm and indoor navigation waypoint sensors (e.g., beacons)
I-14	Performance Measures *	PM team	PMD	Performance measurement results
I-18	OSM / Path / Map Updates	External partners or data sets	PMD	Map, sidewalk, indoor facility and asset data and updates from external sources
I-19	NITTEC Traffic Information	NITTEC	SDS	The static network data and dynamic information includes right of way (ROW) data feeds and situational awareness TRANSCOM data fusion engine SPATAL data feeds. The following data feeds are currently identified: -- mobile maps -- situational awareness information (incidents, work zones, planned events)
I-22	Signal Control Exchange	CoB local traffic signal controller	PED-X Gateway	Message from the PED-X gateway to a local traffic signal controller. The information flow forwards a request made by a traveler to request signal actuation

* A number of performance measures will be derived from survey data completed by travelers of the system. Such survey data are input to the system.

Table 4 lists the outputs from the SOI where the column labeled “destination” identifies the destination of the information flow and the column labeled “source” defines the SOI subsystem which disseminates the flow.

Table 4. Data Outputs from SOI

Flow #	Information Flow Name	Source	Destination	Description
I-9	BNMC Facility Waypoint Sensor Broadcast	BNMC Facility	CTP Mobile App	Transactions between mobile app native comm and indoor navigation waypoint sensors (e.g., beacons)
I-15	Map Services	PMD	Thin Client	APIs and web services that present performance measures
I-16	Direct Access Data Files	PMD	Public Links	APIs / links to access public data
I-17	API Data (requires authentication)	PMD	Public Access	APIs and web services that require authentication
I-22	Signal Control Exchange	PED-X Gateway	CoB Local Traffic Signal Controller	Message from the PED-X gateway to a local traffic signal controller. The information flow forwards a request made by a traveler to request signal actuation

2.2 Security Assessments

This section will focus on conducting security assessments for the Buffalo ITS4US project datasets. The section will start with a description of those datasets that are private and will not be released to the public; those include datasets that fall under the Research, Operational and Protected access levels (section 2.2.1). Some datasets will be available for research and summarization purposes once they are anonymized although they may still contain trace data. Other datasets will not be made available because they are protected and may contain PII and HIPAA information.

2.2.1 Private Datasets

The Phase 2 Data Management Plan (DMP) has provided a comprehensive listing of all the Buffalo ITS4US project datasets, as well as the mapping between the datasets and the corresponding information flows (see Table 4 in the DMP). Four private levels were described in the DMP. These levels are: (1) open; (2) private - research; and (3) private – operational; and (4) private - protected. The private research includes anonymized data where the level of detail may include remnants of trace data; the private operational data are log files that have not been scrubbed of identifiers that may trace back to the request-response; finally, the protected level include identifiable information that is directly tied to a person. These categories are also described in Section 2.1 above. In this section, we identify the datasets that will be private (i.e., not shared with the public) in Table 5 below. For each private dataset, the table provides the access level type (i.e., research, operational or protected), the reason why the data is private, and

the security or safeguarding methods and processes. It is important to note that the access level of that dataset may change as additional information becomes available.

Table 5. List of Private Datasets

Dataset ID	Dataset Title	Access Level	Reason(s) the Data is Private	Security Methods and Processes
1	Pedestrian Signal Request Summary	Research	May contain PII (see explanation in section 2.1)	Anonymize and stored on secure server
9	Shuttle Booking Summary	Research	Contains PII	Encryption and store on secure server
10	PAL Direct Reservations Summary	Research	May contain PII	Encryption and store on secure server
11	CTP Usage Log Files	Research	May contain PII / HIPAA and even anonymized may still contain trace data.	Encryption and store on secure server
12	SOC Dispatch Log Files	Research	May contain PII	Anonymize and stored on secure server
15	Trip Planning Summary Usage Data	Research	Contains PII	Encryption and store on secure server
16	Customer Comment Forms	Research	May contain PII	Encryption and store on secure server
24	Intersection Crossing Assets	Operational	May be subject to security provisions	Security protocols (TBD during the design phase)
31	Researcher-accessible ITS4US Dataset	Research	May contain PII	Encryption and store on secure server

2.2.2 Access Request

Access to all datasets is expected to be managed by the data steward in close coordination with the data owner. The data steward and data owner for each dataset in the Buffalo ITS4US project were previously identified in the accompanying Data Management Plan (DMP). This information is included herein as well, for the convenience of the reader (see Table 6 below). However, management of access to research data will be determined after a full IRB process is completed, and detailed procedures and application forms developed. Individuals accessing datasets which may contain PII will be required to take and pass a training course provided through University at Buffalo's (UB) IRB office.

Table 6. Data Owner and Steward Information (from DMP)

Dataset ID	Dataset Title	Data Owner	Data Steward	Federal Sponsor
1	Pedestrian Signal Request Summary	COB	CTP	USDOT ITS JPO
2	Community Shuttle (SDS/HDS) GTFS	NFTA	CS Operator	USDOT ITS JPO
3	NFTA Fixed Route	NFTA	CTP	Not applicable, External data source
4	GTFS Flex for PAL	NFTA	CTP	Not applicable, External data source
5	Public right of way (PROW) information in the project region	OSM	CTP	Not applicable, External data source
6	PROW Work Zone Data	COB	CTP	Not applicable. External data source
7	Community Shuttle real time information	CS Operator	CS Operator	USDOT ITS JPO
8	NFTA GTFS-realtime	NFTA	NFTA	Not applicable, External data source
9	Shuttle Booking Summary	CS Operator, Traveler	CS Operator, CTP	USDOT ITS JPO
10	PAL Direct Reservations Summary	PAL Direct	PAL Direct	Not applicable, External data source
11	CTP Usage log files	CTP	CTP	USDOT ITS JPO
12	SOC Dispatch log summary files	CS Operator	CS Operator	USDOT ITS JPO
13	DEPRECATED			
14	CS Vehicle Performance Data	CS Operator	CS Operator	USDOT ITS JPO

Dataset ID	Dataset Title	Data Owner	Data Steward	Federal Sponsor
15	Trip Planning Summary Usage Data	COB, traveler	CTP	USDOT ITS JPO
16	Customer Comment Forms	COB, traveler	CTP	USDOT ITS JPO
17	Beacon Messages	IOO of asset	Project data steward	USDOT ITS JPO
18	Beacon message log file	IOO of asset	IOO of asset	USDOT ITS JPO
21	NFTA Conveyance Data Feed	NFTA	NFTA	USDOT ITS JPO
22	NFTA Conveyance Status	NFTA	NFTA	USDOT ITS JPO
23	NITTEC Traffic Information	NITTEC	NITTEC	Not applicable. External data source
24	Intersection Crossing Assets	COB	COB	Not applicable. External data source
25	Beacon asset location	IOO of asset	IOO of asset	USDOT ITS JPO
29	OpenStreetMap	OSM	CTP	Not applicable. External data source
30	Performance Measures	USDOT	Project Team	USDOT ITS JPO
31	Researcher-accessible ITS4US Dataset	USDOT	Project Team	USDOT ITS JPO
32	BNMC Facility Map	IOO of asset	IOO of asset	USDOT ITS JPO

2.2.3 Related Tools, Software and/or Code

No special tools or software will be required to process or access the datasets, beyond securing datasets containing PII in a secure server, accessible only to members of the research team which will be password protected. Identities of research participants will be kept confidential. This information will be securely stored in password protected files in 309 Hayes on the University of Buffalo Campus.

2.2.4 Relevant Privacy and/or Security Agreements

A formal set of data privacy and security agreements will be developed that incorporates all the datasets. The agreement will include existing privacy and security agreements issued from stakeholder data providers (i.e., NFTA which will be providing the Buffalo ITS4US system with PAL data). This section will be updated once the appropriate agreements are in place.

2.2.5 Confidentiality, Integrity, and Availability (CIA) Assessment

The datasets to be used within the Buffalo ITS4US project were assessed to determine their security requirements. In this project, we adopted the approach used by the Federal Government for classifying potential impacts and resulting security requirements, as defined in FIPS PUBS 199[8] and 200[9], to assess the confidentiality, integrity, and availability (CIA assessment) of each data set. FIPS PUBS 199 defines confidentiality, integrity and availability (CIA) as follows:

> *"CONFIDENTIALITY refers to Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information.*
>
> *INTEGRITY refers to Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity. A loss of integrity is the unauthorized modification or destruction of information.*
>
> *AVAILABILITY refers to Ensuring timely and reliable access to and use of information. A loss of availability is the disruption of access to or use of information or an information system."*

Table 7 below shows the results of assessing the confidentiality, integrity and availability of each dataset used in the Buffalo ITS4US project. A brief description of the three levels of high, moderate, and low for each of the three dimensions of confidentiality, integrity and availability is provided below.

For *Confidentiality:*

- A rating of "low" is assigned to public data which do not include any PII, or that had any PII anonymized or aggregated to make it impossible for anyone to derive PII from the dataset.
- A rating of "moderate" is assigned to datasets that may allow a person accessing the dataset to derive some PII when linking to other datasets (e.g., trace data). In other words, PII in such datasets have either been anonymized or aggregated and are not readily accessible.
- A rating of "high" is assigned to datasets that has sensitive PII.

For *Integrity:*

- A rating of "low" is assigned to datasets where inaccuracies and errors can be tolerated, or where data integrity is not important (note that none of the datasets in this project met such a condition, and hence no low integrity level was assigned to any dataset).

- A rating of “moderate” is assigned to cases where data integrity and accuracy are important but not safety-critical.

- A rating of “high” is assigned to safety-critical applications, and where the integrity of data is very important.

For *Availability:*

- A rating of “low” is assigned to datasets which will only be accessible to the ITS4US project team or the independent evaluator for performance measurement and reporting. Only IRB-trained individuals will be allowed to access such data, and hence a “low” rating is appropriate for the availability of such data.

- A rating of “moderate” is assigned to data which are needed for the operations of the system, and hence reliable and timely access is important. However, some delays may be allowable for such datasets and hence the rating of “moderate” availability.

- A rating of “high” is assigned to data which need to be available all the time and to everyone on a near real-time basis.

NOTE: Several datasets were deprecated in the Phase 2 DMP (FHWA-JPO-22-973)[5]. These include dataset ID: 13, 19, 20, 26, 27, and 28. The Change Control Log (included in Appendix C of the DMP) describes all the changes from Phase 1 to Phase 2).

Table 7. Confidentiality, Integrity, and Availability (CIA) Assessment of the Buffalo ITS4US Project Datasets

Dataset ID	Name	Confidentiality	Integrity	Availability
1	Pedestrian Signal Request Summary	Moderate	High	Moderate
2	Community Shuttle (SDS / HDS) GTFS	Low	Moderate	Moderate
3	NFTA Fixed Route	Low	Moderate	Moderate
4	GTFS Flex for PAL	Low	Moderate	Moderate
5	Public right of way (PROW) information in the project region	Low	Moderate	Moderate
6	PROW Work Zone Data	Low	Moderate	Moderate
7	Community Shuttle real time information	Low	Moderate	Moderate
8	NFTA GTFS-realtime	Low	Moderate	Moderate
9	Shuttle Booking Summary	Moderate	Moderate	Low
10	PAL Direct Reservations Summary	Moderate	Moderate	Low
11	CTP Usage Log	Moderate	Moderate	Low
12	SOC Dispatch Log Summary Files	Moderate	Moderate	Low
14	CS Vehicle Performance Data	Low	Moderate	Moderate

Dataset ID	Name	Confidentiality	Integrity	Availability
15	Trip Planning Summary Usage Data	Moderate	Moderate	Low
16	Customer Comment Forms	Moderate	Moderate	Low
17	Beacon Messages	Low	Moderate	Moderate
18	Beacon message Log File	Low	Moderate	Low
21	NFTA Conveyance Data Feed	Low	Moderate	Moderate
22	NFTA Conveyance Status	Low	Moderate	Moderate
23	NITTEC Traffic Information	Low	Moderate	Moderate
24	Intersection Crossing Assets	Low	High (the integrity of data is very important for the safety of users especially those needing additional crossing time)	Moderate
25	Beacon asset locations	Low	Moderate	Moderate
29	OpenStreetMap	Low	Moderate	Moderate
30	Performance Measures	Low	Moderate	Moderate
31	Researcher-accessible ITS4US Dataset	Low	Moderate	Low
32	BNMC Facility Map	Low	Moderate	Moderate

2.3 Data Security Requirements

FIPS PUBS 200 defines an approach for identifying the appropriate types of security controls (high-level requirements) for each security level in the three impact areas defined in FIPS PUBS 199. The document defines minimum requirements for Federal information and information processing systems. The first step is to identify the specific security and privacy controls of each type that the system will require. These are defined in Security and Privacy Controls for Federal Information Systems and Organizations.

In this document, we utilize the concept of a device class, or more precisely, a device security class, inspired by the approach defined in the National ITS Reference Architecture [10] (Architecture Reference for Co-operative and Intelligent Transportation or ARC-IT 9.1). According to ARC-IT a device security level is a statement of a storage system's security requirements for its confidentiality, integrity, and availability. The storage systems and access methods supported by the various SOI subsystem elements are described in the Phase 2 DMP (Section 2.2). These storage systems are identified as the "devices" against which the Security and Privacy control are assessed.

Because there are three security levels (low, moderate, or high) for each of the dimensions of confidentiality, integrity and availability, there are potentially 27 different device security classes. To simplify the process and to leverage the economies of scale, ARC-IT reduced the 27 classes into only five classes, based on the following two principles:

1. Every subsystem storage system is covered by a device class that matches or exceeds its security requirements
2. Every subsystem storage system is covered by a device class that exceeds its security requirements under no more than two headings

The five physical object device security classes are defined as in Table 8 below, which defines how the data security requirements levels in terms of confidentiality, integrity, and availability are related to the device security classes and their controls.

Table 8. Relationship between Data Security Requirements and Security Class Level.

Class	Confidentiality	Integrity	Availability	Detailed Controls
Class 1	Low	Moderate	Moderate	Class 1 Controls
Class 2	Moderate	Moderate	Moderate	Class 2 Controls
Class 3	Moderate	High	Moderate	Class 3 Controls
Class 4	High	High	Moderate	Class 4 Controls
Class 5	High	High	High	Class 5 Controls

The defined definitions of the class controls associated with each class can be found at: https://www.arc-it.net/html/security/deviceclasses.html

Table 9 below shows the device security class corresponding to the level of confidentiality, integrity and availability required for each storage system (and related dataset) in the Buffalo ITS4US project (security Class 2 is highlighted in bold and italics and security Class 3 are underlined and in bold and italics).

Table 9. Device Security Class for the Buffalo ITS4US Datasets

Data Storage	Dataset ID	Name	Confidentiality	Integrity	Availability	Security Class
CoB / GIS data storage	6	PROW Work Zone Data	Low	Moderate	Moderate	Class 1
CoB Server	24	Intersection Crossing Assets	Low	High	Moderate	***Class 3***
CTP	15	Trip Planning Summary Usage Data	Moderate	Moderate	Low	***Class 2***
CTP	16	Customer Comment Forms	Moderate	Moderate	Low	***Class 2***
CTP	25	Beacon asset locations	Low	Moderate	Moderate	Class 1
CTP	29	OpenStreetMap	Low	Moderate	Moderate	Class 1
Facility Owner	17	Beacon Messages	Low	Moderate	Moderate	Class 1
Facility Owner	18	Beacon message log file	Low	Moderate	Low	Class 1
NFTA	3	NFTA Fixed Route	Low	Moderate	Moderate	Class 1
NFTA	4	GTFS Flex for PAL	Low	Moderate	Moderate	Class 1
NFTA	8	NFTA GTFS-realtime	Low	Moderate	Moderate	Class 1
NFTA	21	NFTA Conveyance Data Feed	Low	Moderate	Moderate	Class 1
NFTA	22	NFTA Conveyance Status	Low	Moderate	Moderate	Class 1
NFTA PAL Server	10	PAL Direct Reservations Summary	Moderate	Moderate	Low	***Class 2***

Data Storage	Dataset ID	Name	Confidentiality	Integrity	Availability	Security Class
NITTEC	23	NITTEC Traffic Information	Low	Moderate	Moderate	Class 1
OSM	5	PROW information in the project region	Low	Moderate	Moderate	Class 1
PMD	1	Pedestrian Signal Request Summary	Moderate	High	Moderate	***Class 3***
PMD	2	Community Shuttle (SDS / HDS) GTFS	Low	Moderate	Moderate	Class 1
PMD	7	Community Shuttle real time information	Low	Moderate	Moderate	Class 1
PMD	9	Shuttle Booking Summary	Moderate	Moderate	Low	***Class 2***
PMD	11	CTP Usage Log files	Moderate	Moderate	Low	***Class 2***
PMD	12	SOC Dispatch log summary files	Moderate	Moderate	Low	***Class 2***
PMD	14	CS Vehicle Performance Data	Low	Moderate	Moderate	Class 1
PMD	30	Performance Measures	Low	Moderate	Low	Class 1
PMD	31	Researcher-accessible ITS4US Dataset	Low	Moderate	Low	Class 1

2.4 Risk Assessment of Threats

There are three major categories of security threats to the Buffalo ITS4US project. These are:

1. Intentional threats: both internal and external
2. Accidental threats: both internal and external
3. Acts of nature

The methodology used for risk assessment of these threats we are proposing here closely follows the NIST SP 800-30 [11]. However, instead of using five levels as was proposed by NIST SP800-30, we use three levels for both impact and likelihood: low, moderate, and high. To do this, we combine the lowest level into the low level, and the highest level into high level. The corresponding risk matrix is as shown in Figure 11 [see references: 12, 13].

		Level of Impact		
		Low	**Moderate**	**High**
Level of Likelihood	**High**	Low	Moderate	High
	Moderate	Low	Moderate	Moderate
	Low	Low	Low	Low

Figure 11. Risk Assessment Matrix.
Source: 12, 13.

The best way to protect computer systems and software from attacks is to first estimate the likely level of impact and the level of likelihood of potential threats. The associated level of risk may then be estimated based on Figure 11. Counter-measures then need to be developed for those potential threats with moderate/high risk rating.

To define the levels of impact, the guidelines outlined in in NIST SP 800-30 were utilized. The guidelines provide the following definitions for the ratings of “high”, “moderate” or “low” for level of impact.

- ***High:*** A high impact threat would be expected to have a ***severe or catastrophic*** adverse effect on organizational operations, organizational assets, individuals, other organizations, or the Nation. A severe or catastrophic adverse effect means that the threat event might: (i) cause a severe degradation in or loss of mission capability to an extent and duration that the organization is not able to perform one or more of its primary functions; (ii) result in major damage to organizational assets; (iii) result in major financial

loss; or (iv) result in severe or catastrophic harm to individuals involving loss of life or serious life-threatening injuries.

- ***Moderate:*** The threat event could be expected to have a ***serious adverse*** effect on organizational operations, organizational assets, individuals, other organizations, or the Nation. A serious adverse effect means that, for example, the threat event might: (i) cause a significant degradation in mission capability to an extent and duration that the organization is able to perform its primary functions, but the effectiveness of the functions is significantly reduced; (ii) result in significant damage to organizational assets; (iii) result in significant financial loss; or (iv) result in significant harm to individuals that ***does not*** involve loss of life or serious life-threatening injuries.

- ***Low:*** The threat event could be expected to have a ***limited adverse effect*** on organizational operations, organizational assets, individuals, other organizations, or the Nation. A limited adverse effect means that, for example, the threat event might: (i) cause a degradation in mission capability to an extent and duration that the organization is able to perform its primary functions, but the effectiveness of the functions is noticeably reduced; (ii) result in minor damage to organizational assets; (iii) result in minor financial loss; or (iv) result in minor harm to individuals.

Based on the CIA analysis of the Buffalo ITS4US project's datasets presented in Table 6 above, it can be seen that the datasets and applications where potential threats may present the highest risk are those related to:

1. The pedestrian crossing application;

2. Datasets that may contain PII (i.e., the private datasets listed in Table 5 above); and

3. Threats against the SDS component of the CS.

The threats and risk associated with each of the above-mentioned three applications/datasets are briefly discussed below.

2.4.1 Pedestrian Crossing Application

Potential threats to the pedestrian crossing applications are perhaps the most serious since the application is designed to allow vulnerable travelers to request the green phase for crossing without the need to press the pedestrian-crossing button. As such, malicious attacks or system failures that could result in the application failing to function as intended, may expose vulnerable travelers to unsafe crossing maneuvers (e.g., a traveler with a visual impairment crossing during the wrong phase, or crossing the wrong street). This potentially could result in life-threatening injuries, and hence the impact of such threat should be rated as **"high"**. However, we anticipate that the likelihood of this happening is **"low",** especially since there are already standards, appropriate design procedures, communications and cyber-security protocols which will be followed. Given this and based on the risk assessment matrix (Figure 11), the overall risk would be rated as **"low."**

2.4.2 Datasets Containing PII

As discussed in more detail in section 3 below, the Buffalo ITS4US project will implement a series of Security Controls to ensure the protection of all PII and to preserve privacy. In fact, datasets stored in the PMD and the CTP will be anonymized or encrypted while at rest. Data in transit will be encrypted and transmitted over the network using Transport Level Security (TLS) protocol. These safeguards should help lower the level of likelihood of any threat of data breaches to PII to the **"low"** level. In terms of level of impact, it was determined that a rating of "moderate" is appropriate for such types of threats. Based on the assessment and using the risk assessment matrix of Table 5, the overall risk here is also **"low."**

2.4.3 Threats Against the SDS Component of the CS Subsystem

The SDS will be procured as a turn-key solution, and therefore issues related to cyber security and guarding against malicious attacks on the SDS software and hardware will be the responsibility of the vendor. To verify this, the RFP process will request the vendors who respond to the RFP to describe their system security features. Once the SDS vendor is selected, the team plans to update this section of the DPP.

Also, it should be noted that for the duration of this project we will require a human safety steward onboard the vehicle during operation. The safety steward will be trained to take over the control of the shuttle whenever an emergency occurs, or whenever a software/hardware component of the SDS fails. The presence of the onboard safety steward will significantly reduce the impact of potential threats, and hence the overall risk has been determined to be **"low"** (as can be seen from Figure 11, for an impact level of "low", the overall risk is also "low", regardless of the likelihood level).

It should be noted, however, that long-term (beyond the duration of Phases 2 and 3 of the ITS4US project), the presence of a human safety steward onboard the shuttle may not be practical. This is especially true for the business case for automation. If the human steward is to be removed, we expect that the steward would be replaced by a control center which can remotely monitor (and even, in the future, control) the shuttle, therefore also helping lower the risk of the SDS operations. In that case, however, it would be imperative to protect the communications and the remote-control systems against cyber-attacks.

2.5 Data Sharing and Provision

All dataset identified so far in this project are expected to be open licensed, as detailed in Table 10. This section will be updated in Phase 2 when more design details are known. Note that some datasets, although not subject to a license restriction, are subject to access level provisions (e.g., no redistribution of the data). The access level drives restrictions on the data.

Table 10. Re-Use, Redistribution, and Derivative Products Policies

Data ID	Dataset Title	Access Level	License Used	Reason(s) for Non-Open License
1	Pedestrian Signal Request Summary	Research	Open	n/a
2	Community Shuttle GTFS and GTFS Flex	Open	Open	n/a
3	NFTA Fixed Route GTFS	Open	Open	n/a
4	NFTA GTFS-Flex for PAL	Open	Open	n/a
5	PROW Data	Open	Open	n/a
6	PROW Work Zone Data	Open	Open	n/a
7	Community Shuttle Realtime Information	Operational	Open	n/a
8	NFTA GTFS-realtime	Open	Open	n/a
9	Shuttle Trip Booking Summary	Protected (PII)	Open	n/a
10	PAL Direct Reservations Summary	Protected (PII)	Open	n/a
11	CTP Usage Log Files	Research	Open	n/a
12	SOC Dispatch Log Files	Research	Open	n/a
14	CS Vehicle Performance Data	Open	Open	n/a
15	Trip Planning Data	Research	Open	n/a
16	Customer Comment Forms	Protected (PII)	Open	n/a
17	Smart Sign Messages	Open	Open	n/a
18	Smart Sign Message Log File	Research	Open	n/a
21	NFTA Conveyance Data Feed	Open	Open	n/a

Data ID	Dataset Title	Access Level	License Used	Reason(s) for Non-Open License
22	NFTA Conveyance Status	Open and research	Open	n/a
23	NITTEC Traffic Information	Open and research	Open	n/a
24	Intersection Crossing Assets	Open	Open	n/a
25	Smart Sign Assets	Open	Open	n/a
29	OpenStreetMap	Open	Open	n/a
30	Performance Measures	Open	Open	n/a
31	Researcher-accessible ITS4US Dataset	Research	Open	n/a
32	BNMC Facility Map	Open	Open	n/a

2.6 Specific System Hardware Security Analysis

For the Buffalo ITS4US deployment project, the following key system hardware components are identified: (1) The SDS subsystem (i.e., the shuttle itself, the onboard equipment (OBE) on the SDS and the hardware in the SDS SOC); (2) the HDS subsystem (i.e., the human-driven shuttle itself and the hardware in the HDS reservation system); (3) the CTP servers; (4) UB servers hosting PII data; (5) the traffic cameras supporting PED-X Gateway; and (6) the indoor navigation beacons used within the indoor navigation application. Table 11 below provides a high-level analysis of the specific system hardware security.

Table 11. System Hardware Security Analysis

System Hardware Components	Security Analysis
SDS subsystems and its different components (i.e., the shuttle, OBE, and hardware in the SDS SOC)	This subsystem will be procured as a turn-key solution, as previously mentioned, and therefore the system hardware security analysis will be the responsibility of the vendor including the responsibility to provide the required cyber security protocols. As previously mentioned, the RFP process will request the vendors who respond to the RFP to describe their system security features. With this, and once the SDS vendor is selected, the team plans to update this section of the DPP and to make the security analysis of the SDS subsystems and its different components available to the stakeholders.

System Hardware Components	Security Analysis
HDS subsystem (i.e., shuttle and the hardware in the HDS reservation system)	The HDS will be a vehicle that satisfies all Federal Motor Vehicle Safety Standards (FMVSS), and as such, we do not foresee the need for conducting specific system hardware security analysis for the HDS vehicles. Also, for the HDS reservation system, the security of any hardware will be guided by the security protocols and procedures of NFTA IT department.
CTP and UB servers	The hardware will be selected based on the CIA analysis discussed in section 2.2 and section 2.3 above. Specifically, the security level of the server will be selected to match the confidentiality, integrity and availability requirements of the datasets hosted on that server.
Traffic cameras supporting PED-X Gateway	Hardware for these components are required to satisfy the security requirements specified in the relevant industry standards. The hardware will be compliant with NEMA rated enclosure. In addition, secure communications will meet the following provisions: • shall provide a Virtual Private Network (VPN) for secure data transmission between the Communications Interface and Server • shall create a private network where IP traffic can be transmitted from a traffic cabinet directly into the traffic management center and any central software systems • shall use authentication using public key infrastructure (PKI) and encryption using PKI and the TLS/DTLS1.0+ protocol • shall support HTTPS/SSL communication to the Server from the public internet for access of the User Interface • shall support revoking of all authenticated usernames, passwords, or keys at anytime
Indoor Navigation Beacons	Beacons will adhere to the system requirements and industry security standards as described in the SyRS and ICD.

3 Security Controls

3.1 Cybersecurity Policies

Cybersecurity polices will be developed that cover data (at rest), operations and networks of all the subsystem back-office systems, vehicles, field devices and their interactions. The policies will include existing cybersecurity policies issued from stakeholder data providers including NFTA and City of Buffalo. This section will be updated once the procurement agreements with the vendors who will be providing components or subsystems of the Buffalo ITS4US project (e.g., the SDS vendor, the vendor for the way-finding elements of the smart infrastructure) are in place.

3.2 Data Security Policies and Procedures

The data security policies and procedures developed during the system design phase will provide layered security to protect data storage while at rest and data exchange while in transit. The policies and procedures will address:

1. **Confidentiality** requirements to ensure that information is not made available or disclosed to unauthorized persons or systems.

2. **Availability** to ensure that data is accessible, functioning, and able to meet the needs of the system. The types of procedures include addressing Denial of Service attacks and other ransom attacks and corruption of data.

3. **Integrity** to preserve the quality of the data including accuracy and consistency. Integrity also includes protecting against unauthorized modification to prevent unauthorized modification.

4. **Authenticity and non-repudiation** to ensure that data and information is authentic, the user is confirmed, and the message exchange can be audited. The procedures include identity management and role-based access provisions.

3.3 Back-up and Recovery Policies and Procedures

Back-up and recovery policies and procedures will be developed that cover all datasets including operational data of all the subsystem back-office systems, vehicles, field devices and their interactions will be developed as part of the Agile process. The policies will incorporate existing back-up, recovery and retention policies issued from stakeholder data providers including NFTA and City of Buffalo.

3.4 Technical Controls

This section will describe the technical controls proposed for the Buffalo ITS4US system. These include those related to access, logging and monitoring, encryption and database controls [13].

3.4.1 Access

Access to the Buffalo ITS4US project's datasets and applications will be restricted by identity role-based authorization and authentication and will be consistent with the requirements set out in section 2.1 and which support data privacy. Authorized administrators and registered users will access applications using minimum access privileges needed in order to perform a given task. All user accounts accessing the system applications will require users to login using a password to a registered mobile device, email, or telephone confirmation for the specified user. Passwords will be required to meet complexity requirements (upper and lower-case letters with at least 1 special character and a minimum of 8 characters in length) and shall not be shared with others. The approach will apply best practices based on industry standards, and will be updated once more information is available (e.g., solicited from our stakeholders during Agile Demos), in order to meet user privacy needs.

Within an active session user content is restricted to the minimum amount of data needed to perform an action. Likewise, the independent evaluator chosen to work on the evaluation of the Buffalo ITS4US deployment will also be restricted to the minimum amount of data needed to adequately evaluate the performance of the project.

3.4.2 Logging and Monitoring

Logging and monitoring will be required/performed to maintain the security of the Buffalo ITS4US system and its associated data. Accesses or attempted access to data within the system will be logged and recorded to a secure database location or file within the system and made available for routine automated or manual review. Servers within the system will record all API requests to REST services and will include information about the resources requested, accessed, and the source of the request to local log files. Log files will be replicated within the system and backed up on a routine basis.

3.4.3 Encryption

Data encryption will be implemented to maintain security and protect privacy. Specifically, data stored within the CTP Platform and within the PMD will be encrypted using Transparent Data Encryption. Transparent Data Encryption ensures data-at-rest encryption in the database layer. Data in transit will be encrypted and transmitted over the network using Transport Level Security (TLS) protocol.

3.4.4 Database

Data fields within the Buffalo ITS4US datasets which may contain PII will be identified, marked and any data added or stored to the field will be required to be encrypted. Symmetric-key locking using Advanced Encryption Standard (AES) or Triple Data Encryption Standard (3DES) at the column level or table space will be required of any database that stores PII. All server systems

within the data center, including the systems that support the Buffalo ITS4US databases, will have operating system and application software patches applied on a regular basis.

Developers who access the project's databases must have a reason to access the data and sign a Computer Environment Access and Non-Disclosure Agreement with NFTA. Developers and consultants will be assigned unique database accounts with appropriately restricted access to information. Databases will implement audit logging for appropriate PII-related information.

3.5 Policy Controls

The Buffalo ITS4US project will employ industry accepted best practices for ensuring a safe computing environment. The partner organizations collaborating on the ITS4US deployment (i.e., NFTA, GBNRTC, BNMC and UB) all have policies and procedures in place that require their employees to review periodic online training materials. These training courses discuss cyber security issues such as phishing scams, protection of sensitive information, and proper use of computing systems. In addition, the project will put in place policies and policies to ensure the protection of all PII and to preserve privacy. Below we summarize some of those procedures.

3.5.1 Protection of Data Collected

PII can be derived from a number of data sources. This section will describe a few data elements that either: (1) contain explicit PII; or (2) could allow a user to derive PII by linking to other datasets. This section will also describe the measures which the ITS4US project will take to maintain a privacy-secured data environment. As listed in Table 5 above, we have identified a total of 9 different datasets which may contain PII. Before these data are stored within the PMD databases, the data will be anonymized (e.g., by removing data points at the beginning, end of a trip for trip trajectory data). PII data will be encrypted for storage as well as in transit. Some specific details follow.

3.5.1.1 Survey Data

Data collected directly through participant surveys will contain PII and will need to be secured. This information is important to collect for the performance measures part of the Buffalo ITS4US project and may contain information such as address, telephone number and name, which will not be released to the general public. Surveys will include other types of information, such as opinions about the deployment itself, general travel experiences, or familiarity with the area, that can also be of a sensitive nature, such as opinions about the deployment itself, travel experiences, or familiarity with the area. These pieces of information will only be linked to the participant's PII through a privately held code that is not released to outside agencies. By doing this, outside agencies will not be able to link information such as age, gender, income, education level, etc. back to an individual. Since the link between the user and their information is kept securely away from the dataset, PII will not be released to individuals acquiring the data after a large-scale data release.

3.5.1.2 GPS Trajectories

GPS location data can be acquired through a number of different means, the most prominent for the Buffalo ITS4US project is through trace data of individuals making trips while utilizing the subsystems of the ITS4US deployment (e.g., a traveler utilizing the CTP mobile app for

navigation). There are a few ways that this sensitive data can get into the wrong hands. The expected primary way for this data to be obtained is through data released after the completion of the initial deployment for general research. Measures will be in place to reduce the level of PII that is included in large time-series GPS files. These measures include techniques such as aggregating the start and end points of a trip to a larger zone, or not including the time of day for the trace.

3.5.1.3 De-Identification

De-identification is a method of security control that allows one to transition from a complete GPS travel data to secure GPS traces. These methods generally remove any data that can lead to someone being able to determine through statistical methods important locations or predict future travel from the historic GPS data. It is also important to keep the information that would be useful (to the fullest extent possible) for future research. Any points within a certain distance threshold of a destination would also be removed, as the destination can be easily estimated from the trajectory of the approaching points. By removing points from GPS traces based upon land use type (residential or school), it is easier to remove those that may have privacy considerations.

3.5.2 Breach Plan

In the event of a breach in data security, the policies and procedures adopted by NFTA cyber security team will be followed. These procedures define: (1) who needs to be contacted when a breach occurs and when; (2) the actions followed after the breach occurs including periodic updates; (4) laws that need to be followed in such cases; (4) mitigation strategies to minimize the impact of the breach; and (5) after-action analysis to identify the cause of the breach and how to guard against it occurring in the future. The breach mitigation plan, timing, stakeholders, roles, and responsibilities will be described in detail in the Operations and Maintenance Plan (Phase 2 Comprehensive Operations and Maintenance Plan, TBD).

Appendix A. Acronyms

Table 12 describes the acronyms used in this document.

Table 12. Acronyms

Acronym	Description
AES	Advanced Encryption Standard
API	Application Programming Interface
ARC-IT	Architecture Reference for Co-operative and Intelligent Transportation
BNMC	Buffalo Niagara Medical Campus
CIA	Confidentiality, Integrity, and Availability Assessment
CoB	City of Buffalo
ConOps	Concept of Operations
CS	Community Shuttle
CTP	Complete Trip Platform
DMP	Data Management Plan
DPP	Data Privacy Plan
ET	Eastern Time
FHWA	Federal Highway Administration
FIPS	Federal Information Processing Standards
FMVSS	Federal Motor Vehicle Safety Standards
FTA	Federal Transit Administration
GBNRTC	Greater Buffalo-Niagara Regional Transportation Council
GPS	Global Positioning System
GTFS	General Transit Feed Specification
HDS	Human Driven Shuttle
HIPAA	Health Insurance Portability and Accountability Act
HUAS	Human Use Approval Summary
IRB	Institutional Review Board
IT	Information Technology
ITS	Intelligent Transportation System
ITS4US	Intelligent Transportation Systems for Underserved Communities
JPO	Joint Program Office
MSA	Metropolitan Statistical Area
NFTA	Niagara Frontier Transportation Authority
NIST	National Institute of Standards and Technology
NITTEC	Niagara International Transportation Technology Coalition
OBE	Onboard Equipment
ODD	Operations Design Domain
OSM	OpenStreetMap
PAL	Paratransit Access Line
PED-X	Pedestrian Signal Request
PII	Personally Identifiable Information

Acronym	Description
PMD	Performance Measurement Dashboard
PMESP	Performance Measurement and Evaluation Support Plan
PROW	Public Right of Way
PUB	Publication
REST	Representational State Transfer
ROW	Right of Way
SDS	Self-Driving Shuttle
SMS	Short Message Service
SOC	Shuttle Operations Center
SOI	System of Interest
SP	Special Publication
SPII	Sensitive Personally Identifiable Information
SUNY	School of New York
SyRS	System Requirements Specification
TBD	To Be Determined
TIH	Transportation Information Hub
TLS	Transport Level Security
UB	University of Buffalo
UI	User Interface
USDOT	United States Department of Transportation
3DES	Triple Data Encryption Standard

Appendix B. References

[1] [ConOps] Gopalakrishna, D., et al. (2021). *Phase 1 Concept of Operations (ConOps) – Buffalo, NY ITS4US Deployment Project (FHWA-JPO-21-860)*. Federal Highway Administration. https://rosap.ntl.bts.gov/view/dot/57571.

[2] [DMP] Gopalakrishna, D., et al. (2021). Phase 1 Data Management Plan (DMP) – Buffalo, NY ITS4US Deployment Project (FHWA-JPO-21-868). Federal Highway Administration.

[3] [HUAS] Gopalakrishna, D., et al. (2021). *Phase 1 Human use Approval Summary (HUAS) – Buffalo, NY ITS4US Deployment Project (FHWA-JPO-21-898)*. Federal Highway Administration.

[4] [PMESP] Gopalakrishna, D., et al. (2021). *Phase 1 Performance Measurement and Evaluation Support Plan (PMESP) – Buffalo, NY ITS4US Deployment Project (FHWA-JPO-21-878)*. Federal Highway Administration.

[5] [DMP] Gopalakrishna, D., et al. (TBD 2022). *Phase 2 Data Management Plan (DMP) – Buffalo, NY ITS4US Deployment Project (FHWA-JPO-22-973)*. Federal Highway Administration.

[6] GBNRTC; University at Buffalo Regional Institute, The SUNY at Buffalo School of Architecture and Planning; Cambridge Systematics; TyLin International, 2018.

[7] [SyRS] Gopalakrishna, D., et al. (2021). *Phase 1 System Requirements Specification (SyRS) – Buffalo, NY ITS4US Deployment Project (FHWA-JPO-21-883)*. Federal Highway Administration.

[8] US Department of Commerce, National Institute of Standards and Technology (NIST). (2004). Federal Information Processing Standards (FIPS) Publication 199: Standards for Security Categorization of Federal Information and Information Systems. U.S. Department of Commerce.

[9] US Department of Commerce, National Institute of Standards and Technology (NIST). (2006). Federal Information Processing Standards (FIPS) Publication 200: Minimum Security Requirements for Federal Information and Information Systems.

[10] The National ITS Reference Architecture (ARC-IT 9.1). 2022. Device Classes. Available online at: https://www.arc-it.net/html/security/deviceclasses.html.

[11] US Department of Commerce, National Institute of Standards and Technology (NIST). (2020). NIST Special Publication (SP) 800-30, Revision 1, Guide for Conducting Risk Assessments.

[12] Zumpf, S., English, T., Ahmed, M.A., Gopalakrishna, D., and Garcia, V. (2017). Connected Vehicle Pilot Deployment Program Phase 2: Data Privacy Plan, Version 2 – Wyoming. US Department of Transportation. Report No.: FHWA-JPO-17-469.

[13] Gopalakrishna, D., Garcia, G. Ragan, A., English, T., Zumpf, S., Young, R., Ahmed, M., Kitchener, F., Ureña Serulle, N. and Hsu, E. (2016). Connected Vehicle Pilot Deployment Program Phase 1, Security Management Operational Concept – ICF/Wyoming. US Department of Transportation. Report No.: FHWA-JPO-16-288.

U.S. Department of Transportation
ITS Joint Program Office-HOIT
1200 New Jersey Avenue, SE
Washington, DC 20590

Toll-Free “Help Line” 866-367-7487
www.its.dot.gov

FHWA-JPO-22-969

U.S. Department of Transportation