U^2C PROGRAM

Cybersecurity & Cyber Resilience Requirements

SEPTEMBER 2019

RS&H

CCS, LLC

Table of Contents

Executive Summary

The JTA is leading the development of a network of connected and autonomous vehicles (C/AVs) in Jacksonville's urban core on the street level and on the elevated Skyway automated people mover guideway. Coined the Ultimate Urban Circulator (U^2C) Program, this multi-year development process will serve the transportation needs of JTA customers in Jacksonville's urban core and surrounding neighborhoods.

The JTA is pursuing a timeline and preparatory activities that properly addresses safety, while keeping up with emerging technologies. One of the key preparatory activities is the adoption of this document, entitled "U^2C Program Cybersecurity and Cyber Resilience Requirements." The requirements identify the cybersecurity needs that apply systemwide (i.e., all U^2C Program work done by the JTA, vendors, and partners) and apply to four key U^2C Program components:

1. C/AVs
2. Supervisory systems
3. Sensors
4. Internet of Things (IoT) Networks and Devices

To safely and effectively serve the public and protect JTA's business enterprise, the U^2C Program must protect the cybersecurity of the above four technology-embedded components.

Currently, the JTA is developing the U^2C Program's C/AV network in the Bay Street Innovation Corridor. As the U^2C Program grows, the C/AV network will reach into adjacent neighborhoods—supporting the JTA's vision of a vibrant, revitalized, and better-connected urban center.

Because the U^2C Program's C/AV network will be highly technology-driven, the threat of cyber-based disruption and unauthorized system intrusion demands that the program's cybersecurity planning takes place *prior* to the insertion of assets into the C/AV network. The community of designers, manufacturers, suppliers, and other industry key contributors that collaborate with the JTA on the U^2C Program C/AV network must uphold these cybersecurity efforts. **For this requirements document, any non-JTA individual or organization working in the U^2C Program C/AV environment is defined as a "Stakeholder."**

What These Requirements Are Designed to Do

The U^{2}C Program Cybersecurity and Cyber Resilience Requirements have been developed to minimize risk to the JTA's U^{2}C Program, business enterprise, customers, and community. Specifically, the requirements are designed to:

- Identify areas of U^{2}C Program cybersecurity risk
- Show which requirements should be followed by JTA-selected AV and smart city Stakeholders to minimize risk
- Determine what cyber-related information is needed to build a common operating picture (COP)

How These Requirements Fit with the Physical Security Requirements of the U^{2}C Program

Because the U^{2}C Program will be a cyber-physical systems (CPS), these requirements are to be used in conjunction with the U^{2}C Program Security Requirements. CPSs are real-time and robust independent and interdependent systems with high performance requirements. Cybersecurity attacks are major threats to CPSs, as there are complexity and interdependencies among various system components (physical and cyber), communication integration, computing, and control technology.

The International Organization for Standardization (ISO) defines risk as the "*effect of uncertainty on objectives*" (ISO 31000, Risk management – Guidelines). Combining the cybersecurity and physical security requirements will support an integrated cybersecurity risk management approach that assesses and reduces U^{2}C Program security risks.

From a CPS standpoint, the U^{2}C Program's integrated risk management approach will be to understand, manage, monitor, and communicate risks during operation. Components of this should:

- Build upon existing frameworks, standards, and guidelines
- Integrate a Stakeholder model for risk management
- Measure cross-functional risks from an organizational context

Coordination of These Requirements with Current JTA Policies and Protocols

The U^{2}C Program Cybersecurity and Cyber Resilience Requirements are coordinated with and comply with the JTA Board-approved Digital Security Program (DSP) and Vendor Cybersecurity Compliance Policy. These are described below.

DSP: Based on the National Institute of Standards and Technology (NIST) Cybersecurity Framework, JTA's DSP provides definitive information on the prescribed measures used to establish and enforce digital security. JTA is committed to protecting its employees, partners, clients, and business from damaging acts that are intentional or unintentional.

Vendor Cybersecurity Compliance Policy: JTA's Vendor Compliance Program is designed to enforce data protection controls, regardless of the location of the party responsible for those controls. All vendors are expected to meet the minimum controls that are identified in this policy that states: *"Vendors must protect the confidentiality, integrity and availability of JTA's data and systems, regardless of how the data is created, distributed or stored. Vendor's security controls must be tailored accordingly so that cost-effective controls can be applied commensurate with the risk and sensitivity of the data and system, in accordance with all legal obligations."*

Document Structure

This document is structured into four main sections:

1.0 Introduction

The introduction includes **1.1 Purpose**, **1.2 Scope**, and **1.3 Key Considerations** sections, as well as a **1.4 Primer** on how to use this document. The document's overarching purpose is to outline and communicate the U^{2}C Program's cybersecurity and cyber resilience requirements. The requirements are the essential U^{2}C cybersecurity features and behaviors (i.e., WHAT the U^{2}C Program is required to provide—not how those requirements are met). As described in the primer, each requirement is mapped to the DSP and the Center for Internet Security (CIS) Control Version 7.1 (released April 2019). CIS Controls are internationally recognized cybersecurity best practices for defense against common threats. Each requirement also has the following timeline allocation: short-term, mid-term (may be identified as "elevated" or "at-grade"), or long-term; *the JTA is to decide internally the time-horizon of each requirement*. Finally, each requirement has a unique identifying number for easier reference.

2.0 U^{2}C Program Basic Cybersecurity & Cyber Resilience Requirements

In a tabular format, this section provides the desired cybersecurity & cyber resilience requirements for:

- 2.1 U^{2}C Program: Systemwide
- 2.2 C/AVs
- 2.3 Supervisory Systems
- 2.4 Sensors
- 2.5 Internet of Things (IoT) Networks and Devices

3.0 Acronyms and Definitions

- Critical Acronyms (**Section 3.1**) and Definitions (**Section 3.2**) are presented in tables in this section.

4.0 Appendix

Subsections 4.1 through **4.7** provide references and resources to support and supplement this document and the U^{2}C Program.

1.0 Introduction

The introduction of connected and autonomous vehicles (C/AVs) at the JTA will usher in a new era of transportation innovation that requires specific cybersecurity and safety measures. The JTA is enhancing its security posture to minimize risk as these new functions and conveyances are launched. The JTA understands that although the U^{2}C Program will provide new service opportunities, it can increase risks as legacy networks will be connected with leading-edge sensors, control units, and vehicles; for this reason, the JTA is performing due diligence to prepare for differential and increasing cybersecurity risks.

Because the C/AV network of the U^{2}C Program will be so highly technology-driven, **the JTA is requiring that the community of designers, manufacturers, suppliers, and other industry key contributors that collaborate with the JTA on the U^{2}C Program C/AV network upholds these cybersecurity requirements.** For this document, any non-JTA individual or organization working in the U^{2}C Program C/AV environment is defined as a "Stakeholder." Stakeholders may be vendors, partners, or their supply chains.

The JTA U^{2}C Program Cybersecurity and Cyber Resilience Requirements are designed to maintain the confidentiality, integrity, availability, and safety (CIAS) of systems and promote a layered approach to vehicle cybersecurity to reduce the probability of a successful cyber-attack. These requirements will help the JTA identify risks, reduce vulnerabilities, and minimize consequences—should an attack be successful. **The JTA is ensuring that all Stakeholders contribute to meeting JTA's cybersecurity goals by clearly communicating these requirements to Stakeholders and obtaining documentation from Stakeholders that show that Stakeholders are following these requirements.**

U^{2}C Program Stakeholders must comply with this document that aligns to the JTA's Digital Security Program (DSP) and Vendor Cybersecurity Compliance Policy. Stakeholder compliance will harden the electronic architecture, networked systems, and electronic mechanisms associated with the U^{2}C Program C/AV environment.

1.1 Purpose

This document is designed to define the cybersecurity and cyber resilience requirements for the JTA U^{2}C Program. All Stakeholders have the responsibility to be in compliance with these requirements as a key element of the JTA's enterprise risk management approach to protect the public and the U^{2}C Program.

1.2 Scope

These cybersecurity and resilience requirements are to minimize risk of the U^{2}C Program for the JTA, its customers, and its community. The requirements:

- Identify areas of cybersecurity risk for the U^{2}C Program
- Identify the standards, guidelines, practices, and processes that AV and smart city Stakeholders must adhere to
- Determine what cyber-related information is needed to build a common operating picture (COP)

To this end, the Cybersecurity and Cyber Resilience Requirements document has been created to account for **U^{2}C Program systemwide** and key U^{2}C Program components listed below.

- C/AVs
- Supervisory Systems
- Sensors
- Internet of Things (IoT) Devices and Networks

Again, these U^{2}C Program requirements are to define WHAT the components of the U^{2}C Program need to do—not how they do it.

As shown in **Figure 1.2.1**, cybersecurity encapsulates and is integrated into all aspects of the U²C Program. Connected (or connectable) technology can put the JTA and the public at risk if proper cybersecurity controls are not established and followed.

This project was performed by primary consultant RS&H with the specialized assistance of cybersecurity experts affiliated with the certified Disadvantaged Business Entity (DBE) Community Core Services, LLC (CCS, LLC).

CCS, LLC is a key part of the community of cybersecurity and community technology experts co-located at Kennedy Space Center. CCS, LLC helps public transportation agencies, city governments, and smart city programs navigate their complex technology, cybersecurity, and regulation needs to connect community transportation/AV, health, communications, and other critical services (CommunityCoreServices.com).

Development of this document was coordinated with the development of the U²C Program Safety and Security Requirements by RS&H with the specialized expertise of K & J.

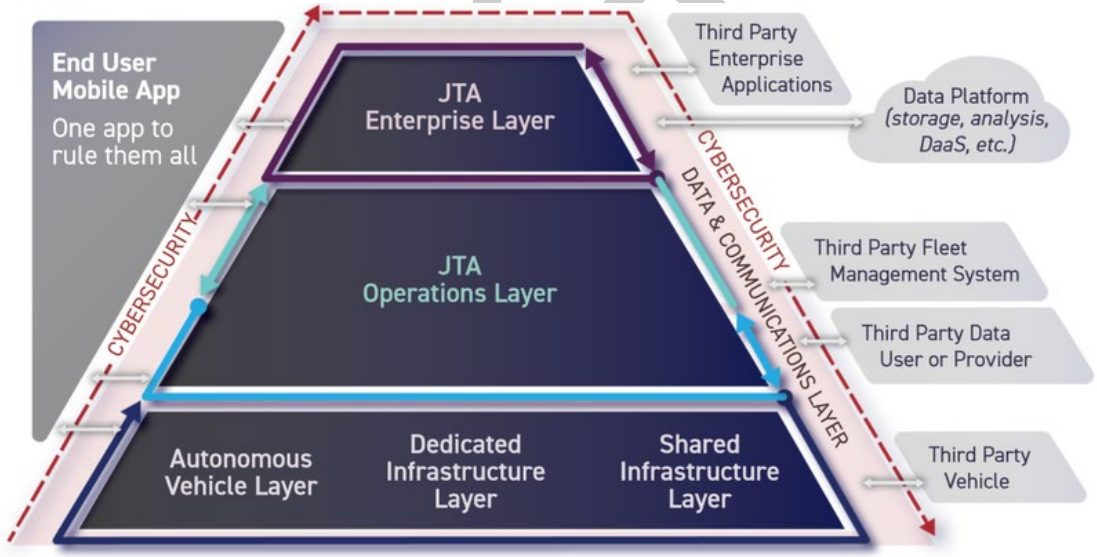

Figure 1.2.1: How cybersecurity fits in the U²C Program (RS&H diagram)

1.3 Key Considerations

The U^{2}C Program's cybersecurity and physical security (as it relates to cybersecurity) is to:

- Meet or exceed the U^{2}C Program security objectives
- Provide effective management and oversight of U^{2}C security risks
- Protect the JTA, its employees, partners, and clients from system disruption and misuse of assets
- Protect company data and the systems that collect, process, and maintain information
- Ensure every JTA user who interacts with data and systems understands their responsibility to know JTA security policies and how to conduct their activities accordingly
- Provide for the development, review, and maintenance of, and to ensure the effectiveness of, security controls over data and systems to support intended operational performance of all U^{2}C vehicles and functions

The U^{2}C Program is to protect JTA's data's and systems' CIAS. Each word that this acronym represents is defined below.

- **Confidentiality**: Addresses preserving restrictions on information access and disclosure so that access is restricted to only authorized users and services.
- **Integrity**: Addresses the concern that sensitive data have not been modified or deleted in an unauthorized and undetected manner.
- **Availability**: Addresses ensuring timely and reliable access to and use of information.
- **Safety:** Addresses reducing risk associated with embedded technologies that could fail or be manipulated by nefarious actors.

The U^{2}C Program is to uphold the JTA's Board-approved DSP. These requirements coordinate with and comply with the JTA Board-approved DSP. The DSP is based on the National Institute of Standards and Technology (NIST) Cybersecurity Framework. Specifically, the U^{2}C Program is to be in compliance with the DSP's Digital Security Policies, as all enterprise systems at the JTA:

- Policy Statement 1: Digital Security Governance (GOV) Policy
- Policy Statement 2: Asset Management (AST) Policy
- Policy Statement 3: Business Continuity & Disaster Recovery (BCD) Policy
- Policy Statement 4: Capacity & Performance Planning (CAP) Policy
- Policy Statement 5: Change Management (CHG) Policy
- Policy Statement 7: Compliance (CPL) Policy
- Policy Statement 8: Configuration Management (CFG) Policy
- Policy Statement 9: Continuous Monitoring (MON) Policy
- Policy Statement 10: Cryptographic Protections (CRY) Policy
- Policy Statement 11: Data Classification & Handling (DCH) Policy
- Policy Statement 12: Embedded Technology (EMB) Policy
- Policy Statement 13: Endpoint Security (END) Policy
- Policy Statement 14: Human Resources Security (HRS) Policy
- Policy Statement 15: Identification & Authentication (IAC) Policy
- Policy Statement 16: Incident Response (IRO) Policy
- Policy Statement 18: Maintenance (MNT) Policy
- Policy Statement 20: Network Security (NET) Policy
- Policy Statement 21: Physical & Environmental Security (PES) Policy
- Policy Statement 23: Project & Resource Management (PPM) Policy
- Policy Statement 24: Risk Management (RSK) Policy
- Policy Statement 25: Secure Engineering & Architecture (SEA) Policy
- Policy Statement 27: Security Awareness & Training (SAT) Policy
- Policy Statement 28: Technology Development & Acquisition (TDA) Policy

- Policy Statement 29: Third-Party Management (TPM) Policy
- Policy Statement 30: Threat Management (THR) Policy
- Policy Statement 31: Vulnerability & Patch Management (VPM) Policy

Finally, U^{2}C Program Stakeholders are to be in compliance with the JTA's Vendor Cybersecurity Compliance Program. JTA's Vendor Compliance Program is designed to enforce data protection controls, regardless of the location of the party responsible for those controls. The overarching policy and vendor responsibilities are listed below.

- **Vendor Compliance Policy:** All vendors are expected to meet the minimum controls that are identified in this policy that states: *"Vendors must protect the confidentiality, integrity and availability of JTA's data and systems, regardless of how the data is created, distributed or stored. Vendor's security controls must be tailored accordingly so that cost-effective controls can be applied commensurate with the risk and sensitivity of the data and system, in accordance with all legal obligations."*

- **Vendor Cybersecurity Compliance Program Vendor Responsibilities:**

  Cybersecurity Program Management (PM)
  Access Control (AC)
  Awareness and Training (AT
  Audit & Accountability (AU)
  Security Assessment & Authorization (CA)
  Configuration Management (CM)
  Contingency Planning (CP)
  Identification & Authentication (IA)
  Incident Response (IR)
  Maintenance (MA)
  Media Protection (MP)
  Physical & Environmental Protection (PE)

Planning (PL)
Personnel Security (PS)
Risk Assessment (RA)
System & Services Acquisition (SA)
System & Communication Protection (SC)
Systems & Information Integrity (SI)
Privacy – Authority & Purpose (AP)
Privacy – Accountability, Audit & Risk Management (AR)
Privacy – Data Quality & Integrity (DI)
Privacy – Data Minimization & Retention (DM)
Privacy – Individual Participation & Redress (IP)
Privacy – Security (SE)
Privacy – Transparency (TR)
Privacy – Use Limitation (UL)

1.4 Primer – How to Use This Document

The U²C Program Cybersecurity and Cyber Resilience Requirements are organized as shown below in **Figure 1.4.1**.

ID	U²C Cybersecurity Requirements	[INSERT ASPECT OF U²C TO WHICH THE REQUIRMENTS APPLY]								
		JTA DSP Control	CIS Control	CIS Sub-Control	Asset Type	Security Function	ST	MT-E	MT-A	LT

Figure 1.4.1. Template design of the U²C Program Cybersecurity and Cyber Resilience Requirements in Section 2.0.

As shown in Figure 1.4.1, the columns of the template are defined as follows:

Column 1: ID. This unique numerical identifier facilitates finding and identifying specific requirements in the document.

Column 2: U²C Cybersecurity Requirements. This column has the written requirement that applies to the aspect of the U²C Program as labelled at the top of the table on each page.

Column 3: JTA DSP Control. The entry in this column correlates to the relevant DSP (now on version 9) and its corresponding NIST Cybersecurity Framework practice.

Column 4: CIS Control. Published by the Center for Internet Security (CIS), Version 7.1 of the CIS Controls helps organizations better defend against known attacks by distilling key security concepts into actionable controls to achieve greater overall cybersecurity defense. CIS Controls are a prioritized set of actions that collectively form a defense-in-depth set of best practices that mitigate the most common attacks against systems and networks. This entry is a crosswalk to the CIS Control that corresponds to the Requirement. Some requirements do not have an applicable CIS Control, indicated by "NA."

Column 5: CIS Sub-Control. This column represents CIS Sub-Controls that correspond to the overarching CIS Control category (e.g., Inventory and Control of Hardware Assets, Inventory and Control of Software Assets, Continuous Vulnerability Management, Controlled Use of Administration Privileges, Secure Configuration for Network Devices). Some requirements do not have an applicable CIS Sub-Control, indicated by "NA."

Column 6: Asset Type. This column reflects if the requirement applies to Users, Devices, Applications, Network, or Data (also in CIS Controls Version 7.1). Some requirements do not have an applicable Asset Type, indicated by "NA."

Column 7: Security Functions. This column indicates if the Requirement "identifies, protects, detects, or responds." Some requirements do not have an applicable Security Function, indicated by "NA." The Security Functions are crosswalked from the CIS Controls in Version 7.1.

Security Functional Areas:

Identify – Assists in developing an organizational understanding to managing cybersecurity risk to systems, people, assets, data and capabilities. Understanding the business context, the resources that support critical functions, and the related cybersecurity risks enables an organization to focus and prioritize its efforts, consistent with its risk management strategy and business needs.

Protect – Outlines appropriate safeguards to ensure delivery of critical infrastructure services. The Protect Function supports the ability to limit or contain the impact of a potential cybersecurity event.

Detect – Defines the appropriate activities to identify the occurrence of a cybersecurity event. The Detect Function enables timely discovery of cybersecurity events.

Respond – Appropriate activities to take action regarding a detected cybersecurity incident. The Respond Function supports the ability to contain the impact of a potential cybersecurity incident.

Columns 8-11: Time horizon of the U^{2}C Program. The time horizon of each requirement in this document is to be defined by the JTA internally. Time horizons are to be categorized as:

- **ST**: Short-Term
- **MT-E**: Mid-Term, use of existing JTA Skyway elevated guideway
- **MT-A**: Mid-Term, use of shared at-grade environment
- **LT**: Long-Term (full build out)

2.0 Cybersecurity and Cyber Resilience Requirements

The U^{2}C Program Cybersecurity and Cyber Resilience Requirements are defined below in the following general categories:

- 2.1 U^{2}C Program: Systemwide Requirements
- 2.2 Supervisory System Requirements
- 2.3 C/AV Requirements
- 2.4 Sensor Requirements
- 2.5 IoT Network and Device Requirements

2.1 U²C Program: Systemwide Requirements

The U²C Program network of C/AVs will transport customers in and around the Jacksonville urban core on the elevated guideway (currently used by the Skyway) and at the street level**. The U²C Program will develop and implement a system-of-systems with Internet protocols and operational technologies that are to connect a variety of sensors across an IoT network that is managed by a supervisory system.**

Systemwide, the U²C Program will adhere to cybersecurity requirements in the DSP and the requirements listed below. Systemwide requirements will apply to all U²C systems and digital assets to assure confidentiality, integrity, availability, and safety. All U²C Stakeholders must comply with these requirements to foster safe and reliable services for the JTA's customers.

The following Systemwide Requirements are designed to address the needs described in the paragraphs above:

ID	Systemwide Requirements	JTA DSP Control	CIS Control	CIS Sub-Control	Asset Type	Security Function	ST	MT-E	MT-A	LT
2.1.1 Security Function: Protect										
2.1.1.1 CIS Control: 18 (Organizational) – Application Software Security										
2.1.1.1-01	All U²C Stakeholders shall demonstrate compliance with secure coding practices appropriate to the programming language and development environment being used.	AST-02 VPM-04	18	18.1	NA	Protect				
2.1.1.2 CIS Control: Not Applicable										
2.1.1.2-01	All U²C elements in C/AVs, devices, infrastructure, and applications shall be interoperable and communicate effectively and securely with other parts of the system as needed, regardless of where or when they are built and used.	NET-01 TPM-03	NA	NA	NA	Protect				

ID	Systemwide Requirements	JTA DSP Control	CIS Control	CIS Sub-Control	Asset Type	Security Function	ST	MT-E	MT-A	LT
2.1.1.2-02	All U^{2}C Stakeholders shall protect the Confidentiality, Integrity, Availability, and Safety (CIAS) of data and information systems, regardless of how data are created, distributed, or stored.	CRY-03 CRY-04 CRY-05 DCH-02	NA	NA	NA	Protect				
2.1.1.2-03	The U^{2}C shall use access control to prevent intrusion into networks in the maintenance work area from the elevated guideway.	PES-02 PED-03 PES-05	NA	NA	NA	Protect				
2.1.1.2-04	The U^{2}C shall meet or exceed the physical security requirements for existing JTA operations and those in the U^{2}C Program Security Requirements that affect cybersecurity, including: • Access Control • Gates, Fencing, and Lighting • Closed-Circuit Television (CCTV) Coverage • Installation of Physical Barriers to Reduce Unauthorized Access • Contractor Vetting and Credentialing • Program to Approve/Receive Access Badges • Require Escorts • Information Technology (IT) Components • Access to Sensitive Information	PES-02 PES-03 PES-05	NA	NA	NA	Protect				
2.1.1.2-05	The U^{2}C shall meet the applicable functional requirements of the Connected Vehicle Reference Implementation Architecture (CVRIA) "Center" Class and their "Physical Objects," including but not limited to: • Center Archived Data Center	CPL-01 CPL-02	NA	NA	NA	Protect				

ID	Systemwide Requirements	JTA DSP Control	CIS Control	CIS Sub-Control	Asset Type	Security Function	ST	MT-E	MT-A	LT
	• Authorizing Center • Commercial Vehicle Administration Center • Emergency Management Center • Fleet and Freight Management Center • Maintenance and Construction Management Center • Payment Administration Center • Transit Management Center • Transportation Information Center									
2.1.1.2-06	Any U^{2}C asset user must obtain authorization prior to relocation or transfer of hardware, software, or data offsite. Assets are prohibited from being removed from the JTA facilities without prior management authorization. Prior to the removal of the information system, the following applicable information must be captured: • Make / model / serial # of the asset • Owner of the asset • Reason the asset is being removed from the facility • Company and name of representative removing the asset • Estimated return date for the asset, if applicable	AST-02 AST-11 DCH-07	NA	NA	Device	Protect				
2.1.1.2-07	All U^{2}C Stakeholders shall comply with policies, procedures, and mechanisms that JTA has in place to support vulnerability, incident, and breach reporting and disclosure.	VPM-01 VPM-04 VPM-06 TPM-01	NA	NA	NA	Protect				

ID	Systemwide Requirements	JTA DSP Control	CIS Control	CIS Sub-Control	Asset Type	Security Function	ST	MT-E	MT-A	LT
2.1.1.2-08	All U²C Stakeholders shall comply with the JTA's a cybersecurity process that allows for JTA's auditing and accountability (e.g., risk assessments, penetration testing, organizational decisions).	GOV-02 GOV-04	NA	NA	NA	Protect				
2.1.1.2-09	All U²C Stakeholders shall undergo an Independent Verification and Validation (IV&V) process to ensure that all U²C requirements have been met.	GOV-02 GOV-04	NA	NA	NA	Protect				
2.1.1.2-10	All U²C Stakeholders' maintenance tools, techniques, or protocols used for maintenance or testing (e.g., analyzer) must be approved by the JTA and align with JTA's DSP.	GOV-02 GOV-04	NA	NA	NA	Protect				
2.1.2 Security Function: Identify										
2.1.2.1 CIS Control: 2 (Basic) – Inventory and Control of Software Assets										
2.1.2.1-01	All U²C Stakeholders shall provide adequate notice of the suspension of product updates, customer service, or technical support.	AST-02	2	2.2	Applications	Identify				
2.1.3 Security Function: Respond										
2.1.3.1 CIS Control: 19 (Organizational) – Incident Response and Management										
2.1.3.1-01	All U²C Stakeholders shall comply with the JTA's Incident Response Process that covers impact assessment, containment, recovery, remediation, and associated testing.	IRO-01 IRO-02 IRO-03 IRO-06 IRO-06(A) IRO-07 IRO-08	19	19.1 19.2 19.3	NA	Respond				

ID	Systemwide Requirements	JTA DSP Control	CIS Control	CIS Sub-Control	Asset Type	Security Function	ST	MT-E	MT-A	LT
		IRO-09 IRO-10 IRO-13 IRO-14 PRM-03 SAT-03 VPM-11								
2.1.4 Security Function: Not Applicable										
2.1.4-01	All U^{2}C Stakeholders shall meet or exceed applicable federal, state, and local regulations, codes, and standards.	CPL-01 SAT-01	NA	NA	NA	NA				
2.1.4-02	All U^{2}C connected or connectable technologies shall align with the NIST standards and guidelines.	GOV-02	NA	NA	NA	NA				
2.1.4-03	All U^{2}C Stakeholders shall comply with JTA's risk-based approach to cybersecurity.	RSK-01 RSK-03 RSK-04 RSK-06 RSK-08	NA	NA	NA	NA				

2.2 C/AV Requirements

The JTA is rapidly evolving its transportation network with new technologies that integrate C/AVs with other vehicles and roadside infrastructure. The security of these assets and conveyances creates a "cyber-physical" system (CPS). For this reason, securing the U²C C/AVs and their assets is paramount, as at-grade conveyances run on Jacksonville streets in a pedestrian environment. Additionally, the modernized system will be managed through communications networks comprised of sensors and control architectures connecting complex networks. This resulting transit system will have increased susceptibility to digital exploitation from cyber-attacks, for which the JTA can prepare.

The C/AVs will use functionality that allows mobile application connectivity for conveniences like cashless payments by customers and Wi-Fi access aboard vehicles. The physical hardening of vehicle controllers and electronic control units will be critical to maintaining the integrity of conveyances. Wireless communications will need to be encrypted and communications to and from the conveyance continuously validated.

The following C/AV Requirements are designed to address the needs described in the paragraphs above:

ID	C/AV Requirements	JTA DSP Control	CIS Control	CIS Sub-Control	Asset Type	Security Function	ST	MT-E	MT-A	LT
2.2.1 Security Function: Protect										
2.2.1.1 CIS Control: 12 (Foundational) – Boundary Defense										
2.2.1.1-01	The U²C C/AV interfaces for customers (e.g., USB port charging station) shall not interface with the SVS and shall be on segmented networks.	MON-01	12	12.7	Network	Protect				
2.2.1.2 CIS Control: 13 (Foundational) – Data Protection										
2.2.1.2-01	The U²C C/AV shall have encrypted communication across the network.	CRY-03	13	13.6	Data	Protect				

ID	C/AV Requirements	JTA DSP Control	CIS Control	CIS Sub-Control	Asset Type	Security Function	ST	MT-E	MT-A	LT
2.2.1.3 CIS Control: 17 (Organizational) – Implement a Security Awareness and Training Program										
2.2.1.3-01	The U²C C/AV Stakeholder shall train JTA staff to identify the most common indicators of a cybersecurity incident.	IRO-02	17	17.9	NA	Protect				
2.2.1.4 CIS Control: 18 (Organizational) – Application Software Security										
2.2.1.4-01	The U²C C/AV electronic architecture shall be hardened against potential attacks (e.g., EMP).	CFG-02 NET-01 NET-02 SEA-04 SEA-10	18	18.11	NA	Protect				
2.2.1.5 CIS Control: Not Applicable										
2.2.1.5-01	The U²C C/AV shall demonstrate proposed functionality on JTA's AV Test Track.	CPL-02	NA	NA	NA	Protect				
2.2.1.5-02	The U²C C/AV operating on the elevated guideway shall comply with the applicable security controls provided by the JTA.	CPL-02	NA	NA	NA	Protect				
2.2.1.5-03	The U²C C/AV operating on the at-grade roadway shall comply with the applicable security controls provided by the JTA.	CPL-02	NA	NA	NA	Protect				
2.2.1.5-04	The U²C C/AV shall be in compliance to the best practices that impact cybersecurity in the USDOT NHTSA Security Best Practices for Modern Vehicles (2016). Best practices include: • The U²C C/AV shall include Safety and Security Certification prior to being put into service.	CPL-01 CPL-02 GPV-02 IRO-02 IRO-03 IRO-06 IRO-06(A) IRO-07	NA	NA	NA	Protect				

ID	C/AV Requirements	JTA DSP Control	CIS Control	CIS Sub-Control	Asset Type	Security Function	ST	MT-E	MT-A	LT
	• The U²C C/AV shall require pre, post, and periodic physical and logical inspections. • The U²C C/AV shall provide for timely detection and rapid response to security incidents. • The U²C C/AV shall have a documented process to respond to incidents, vulnerabilities, and exploits.	IRO-08 IRO-09 IRO-10 IRO-13 MON-01 MON-05 MON-16 THR-01 THR-03								
2.2.1.5-05	The U²C C/AV equipment access panels shall be secured with tamper-proof hardware.	NA	NA	NA	NA	Protect				
2.2.1.5-06	The U²C C/AV shall be hardened to prohibit physical access to critical control, management, and maintenance components.	NA	NA	NA	NA	Protect				
2.2.1.5-07	The U²C C/AV shall provide secure access to Americans with Disabilities Act (ADA)-compliant pre-recorded or ad-hoc visual/audio systems.	EMB-02 EMB-03	NA	NA	NA	Protect				
2.2.1.5-08	The U²C C/AVs shall have the capability to securely upload pre-recorded visual and audible customer information.	CPL-01 CPL-02	NA	NA	NA	Protect				
2.2.1.5-09	The U²C C/AV shall enable JTA personnel to securely view on-board video cameras in real time to ensure proper operations.	EMB-01 EMB-02 EMB-03	NA	NA	NA	Protect				
2.2.1.5-10	The U²C C/AV shall be able to securely interact with customers'/end users' systems and mobile devices, using interoperable interface standards and best practices.	GOV-02 EMB-01 EMB-02 EMB-03	NA	NA	NA	Protect				

ID	C/AV Requirements	JTA DSP Control	CIS Control	CIS Sub-Control	Asset Type	Security Function	ST	MT-E	MT-A	LT
2.2.2 Security Function: Detect										
2.2.2.1 CIS Control: 12 (Foundational) – Boundary Defense										
2.2.2.1-01	The U²C C/AV shall monitor Engine Management Module (EMM) inputs and outputs for packet consistency, if applicable.	MON-01 CRY-04	12	12.5	Network	Detect				
2.2.3 Security Function: Respond										
2.2.3-01	Upon a successful attack of the U²C C/AV control unit, the U²C C/AV shall be capable of taking appropriate and safe action.	BCP-01 MON-18	NA	NA	NA	Respond				
2.2.3-02	The U²C C/AV shall provide the JTA the capability to automatically and remotely take the C/AV out of service due to security concerns.	EMB-02 EMB-03	NA	NA	NA	Respond				
2.2.3-03	The U²C C/AV shall provide customers with a secondary communication mechanism during emergencies when the primary system has been disabled.	EMB-01 EMB-02 EMB-03	NA	NA	NA	Respond				
2.2.4 Security Function: Not Applicable										
2.2.4-01	The U²C C/AV Onboard Equipment (OBE) shall be able to securely communicate with Roadside Equipment (RSE) via Vehicle to Infrastructure (V2I).	EMB-01 EMB-02 EMB-03	NA	NA	NA	NA				

2.3 Supervisory System Requirements

The U²C Program's supervisory system (SVS) must be capable of overseeing the digital health and secure management of the C/AV fleet, sensor network, communication assets, and network administration systems. The SVS must also be architected using security industry best practices and aligned with NIST guidelines. Failing to do so could negatively impact operations and endanger customers, as well as other JTA investments.

For the U²C Program to be high performing, the SVS' safety and security must be monitored. The SVS is particularly important because it can be used to remotely minimize cyber disruption or address a physical security issue. This is achieved by managing system vulnerabilities, threats, and consequences across the entire U²C program. SVS administrators must be able to manage each smart-node and understand the integrity of network devices. All communications across the SVS must be encrypted, and network changes must be detected through autonomous alerting.

The following SVS Requirements are designed to address the needs described in the paragraphs above:

ID	Supervisory System Requirements	JTA DSP Control	CIS Control	CIS Sub-Control	Asset Type	Security Function	ST	MT-E	MT-A	LT
2.3.1 Security Function: Protect										
2.3.1.1 CIS Control: 1 (Basic) – Inventory and Control of Hardware Assets										
2.3.1.1-01	The U²C SVS shall be limited to essential functionality only. Network servers and ports shall be protected to prevent unauthorized use.	IAC-07 IAC-10(A) IAC-15 IAC-21	1	1.7	Devices	Protect				
2.3.1.2 CIS Control: 2 (Basic) – Inventory and Control of Software Assets										
2.3.1.2-01	The U²C SVS Stakeholder shall use whitelisting technology on all assets to ensure that only authorized software run across the SVS.	AST-02	2	2.7	Applications	Protect				

ID	Supervisory System Requirements	JTA DSP Control	CIS Control	CIS Sub-Control	Asset Type	Security Function	ST	MT-E	MT-A	LT
2.3.1.2-02	The U²C SVS shall have whitelisting process and technology that ensures only authorized software libraries are allowed to load into an SVS process.	AST-02	2	2.8	Applications	Protect				
2.3.1.2-03	The U²C SVS shall use physically or logically segregated systems to isolate and run software that creates a higher risk to network security.	AST-02	2	2.10	Applications	Protect				
2.3.1.3 CIS Control: 3 (Basic) – Continuous Vulnerability Management										
2.3.1.3-01	The U²C SVS shall be capable of providing a dedicated account for authenticated vulnerability scans.	VPM-01	3	3.3	Users	Protect				
2.3.1.3-02	The U²C SVS shall be capable of deploying automated software update tools to ensure that the operating systems are running the most recent security updates.	VPM-04	3	3.4	Applications	Protect				
2.3.1.4 CIS Control: 4 (Basic) – Controlled Use of Administrative Privileges										
2.3.1.4-01	The U²C SVS shall, before deploying any new asset, change all default passwords to have values consistent with administrative level accounts.	AST-02 AST-04 AST-11 IAC-07 IAC-10(A) IAC-15 IAC-21	4	4.2	Users	Protect				
2.3.1.4-02	The U²C SVS shall ensure that all users with administrative account access use a dedicated or secondary account for elevated activities. Administrative accounts shall be used only for	IAC-07 IAC-10(A) IAC-15 IAC-21	4	4.3	Users	Protect				

ID	Supervisory System Requirements	JTA DSP Control	CIS Control	CIS Sub-Control	Asset Type	Security Function	ST	MT-E	MT-A	LT
	administrative activities and not Internet browsing, email, or similar activities.									
2.3.1.4-03	The U²C SVS shall use unique passwords, if multi-factor authentication is not supported.	IAC-07 IAC-10(A) IAC-15 IAC-21	4	4.4	Users	Protect				
2.3.1.4-04	The U²C SVS shall seek to use multi-factor authentication and encrypted channels for all administrative account access.	IAC-07 IAC-10(A) IAC-15 IAC-21	4	4.5	Users	Protect				
2.3.1.4-05	The U²C SVS shall ensure that administrators use a dedicated machine for all administrative tasks or tasks requiring administrative access. The machine shall be segmented from JTA's primary network and not allowed Internet access. The machine shall not be used for reading e-mail, composing documents, or browsing the Internet.	IAC-07 IAC-10(A) IAC-15 IAC-21	4	4.6	Users	Protect				
2.3.1.4-06	The U²C SVS shall limit scripting tool access to authorized administrative or development users.	IAC-07 IAC-10(A) IAC-15 IAC-21	4	4.7	Users	Protect				

ID	Supervisory System Requirements	JTA DSP Control	CIS Control	CIS Sub-Control	Asset Type	Security Function	ST	MT-E	MT-A	LT
2.3.1.5 CIS Control: 5 (Basic) – Secure Configuration for Hardware and Software on Mobile Devices, Laptops, Workstations and Servers										
2.3.1.5-01	The U²C SVS shall maintain documented security configuration standards for all authorized operating systems and software in line with NIST guidelines and standards.	CFG-02	5	5.1	Applications	Protect				
2.3.1.5-02	The U²C SVS Stakeholder shall document SVS security configurations for all authorized operating systems. Software configurations shall be in line with JTA's DSP.	CFG-02 CHG-02 CFG-02	5	5.1	Applications	Protect				
2.3.1.5-03	The U²C SVS shall be capable of automatically enforcing and redeploy configuration settings to systems at regularly scheduled intervals.	CFG-02	5	5.4	Applications	Protect				
2.3.1.6 CIS Control: 6 (Basic) – Maintenance, Monitoring and Analysis of Audit Logs										
2.3.1.6-01	The U²C SVS shall be capable of producing immutable logs of events that are sufficient to reveal the nature of a cybersecurity attack or breach.	CFG-02 THR-01 THR-03	6	6.3	Network	Protect				
2.3.1.7 CIS Control: 8 (Foundational) – Malware Defenses										
2.3.1.7-01	The U²C SVS shall use centrally managed anti-malware software to continuously monitor and defend each of the required workstations and servers.	END-04	8	8.1	Devices	Protect				
2.3.1.7-02	The U²C SVS shall ensure that anti-malware software updates scanning engine and signature databases on a regular basis.	END-04	8	8.2	Devices	Protect				
2.3.1.7-03	The U²C SVS shall not auto-run content from removable media.	END-04	8	8.5	Devices	Protect				

ID	Supervisory System Requirements	JTA DSP Control	CIS Control	CIS Sub-Control	Asset Type	Security Function	ST	MT-E	MT-A	LT
2.3.1.8 CIS Control: 9 (Foundational) – Limitation and Control of Network Ports, Protocols and Services										
2.3.1.8-01	The U²C SVS shall ensure that only network ports, protocols, and services listening on a system has a valid business use.	EMB-03	9	9.2	Devices	Protect				
2.3.1.8-02	The U²C SVS shall apply host-based firewalls or port-filtering tools on end systems, with a default-deny rule that drops all traffic except those services and ports that are explicitly allowed.	EMB-03	9	9.4	Devices	Protect				
2.3.1.8-03	The U²C SVS shall place application firewalls in front of any critical servers to verify and validate the traffic going to the server.	EMB-03 MON-01 MON-06	9	9.5	Devices	Protect				
2.3.1.9 CIS Control: 12 (Foundational) – Boundary Defense										
2.3.1.9-01	The U²C SVS shall be capable of denying communications with known malicious or unused IP addresses and limit access only to trusted and necessary IP address ranges at each of the organization's network boundaries.	IAC-07 IAC-10(A) IAC-15 IAC-21	12	12.3	Network	Protect				
2.3.1.9-02	The U²C SVS shall be capable of denying communication over unauthorized Transmission Control Protocol (TCP) or User Datagram Protocol (UDP) ports or application traffic to ensure that only authorized protocols are allowed to cross in or out of the network at each of the organization's network boundaries.	IAC-07 IAC-10(A) IAC-15 IAC-21 MON-01	12	12.4	Network	Protect				

ID	Supervisory System Requirements	JTA DSP Control	CIS Control	CIS Sub-Control	Asset Type	Security Function	ST	MT-E	MT-A	LT
2.3.1.9-03	The U²C SVS Stakeholder shall use secure communication protocols and secure handshake when establishing connections with other systems and in a peer-to-peer architecture.	EMB-01 EMG-02 EMG-03	12	12.4	Network	Protect				
2.3.1.10 CIS Control: 14 (Foundational) – Controlled Access Based on the Need to Know										
2.3.1.10-01	The U²C SVS shall be capable of limiting or eliminating developer access in production devices.	IAC-07 IACI-10(A) IAC-15 IAC-21	14	14.1	Network	Protect				
2.3.1.10-02	The U²C SVS shall appropriately protect developer-level debugging interfaces, if developer access is necessary.	IAC-07 IACI-10(A) IAC-15 IAC-21	14	14.1	Network	Protect				
2.3.1.10-03	The U²C SVS shall be capable of securely segmenting single user or user groups, allowing flexible assignment of operating and maintenance control function on a granular access / permission level.	IAC-07 IACI-10 IAC-15 IAC-21	14	14.1	Network	Protect				
2.3.1.10-04	The U²C SVS shall apply segmentation and isolation techniques (boundary controls) to separate systems, networks, and external connections as appropriate to limit and control pathways from external threats (e.g., access through cyber-physical features, physical interfaces).	TPM-01 TPM-02 TPM-03 TPM-06 TPM-07 TPM-12	14	14.3	Network	Protect				

ID	Supervisory System Requirements	JTA DSP Control	CIS Control	CIS Sub-Control	Asset Type	Security Function	ST	MT-E	MT-A	LT
2.3.1.10-05	The U²C SVS shall be capable of disabling all workstation-to-workstation communication to limit an attacker's ability to move laterally and compromise neighboring systems, through technologies (e.g., private Virtual Local Area Network [VLAN], micro segmentation).	NET-01 NET-02 END-06 MON-01 MON-06 MON-16	14	14.3	Network	Protect				
2.3.1.10-06	The U²C SVS shall encrypt all sensitive information in transit and at rest.	CRY-03 CRY-04	14	14.4	Data	Protect				
2.3.1.10-07	The U²C SVS shall employ JTA-accepted encryption methods in any Internet Protocol (IP)-based operational communication.	CRY-03 CRY-04 CRY-05 NET-01 NET-02	14	14.4	Data	Protect				
2.3.1.10-08	Any U²C SVS key control (e.g., cryptographic interface) that can provide an unauthorized, elevated level of access shall be protected from disclosure.	IAC-07 IACI-10(A) IAC-15 IAC-21	14	14.4	Data	Protect				
2.3.1.10-09	The U²C SVS shall not provide a single key control for accessing multiple U²C technology platforms.	IAC-07 IACI-10(A) IAC-15 IAC-21	14	14.6	Data	Protect				
2.3.1.10-10	The U²C SVS shall reduce any opportunities for a third party to obtain unencrypted firmware during software updates.	IAC-07 IACI-10(A) IAC-15 IAC-21 TPM-01	14	14.7	Data	Protect				

ID	Supervisory System Requirements	JTA DSP Control	CIS Control	CIS Sub-Control	Asset Type	Security Function	ST	MT-E	MT-A	LT
2.3.1.11 CIS Control: 16 (Foundational) – Account Monitoring and Control										
2.3.1.11-01	During development, the U²C SVS Stakeholder shall implement a cooperative ITS credential management system (CCMS) to ensure that only authorized users receive credentials.	GOV-02 GOV-04 IAC-07 IAC-10(A) IAC-15 IAC-21	16	16.2	Users	Protect				
2.3.1.11-02	The U²C SVS shall encrypt the exchange of data between the SVS and any endpoint devices.	CRY-05 CRY-03	16	16.3	Users	Protect				
2.3.1.11-03	The U²C SVS shall interact securely with all U²C-approved mobile devices and other fixed station devices; the U²C SVS Stakeholder shall show that the security of this communication is tested and documented.	EMB-01 EMB-02 EMB-03 NET-01 NET-02 NET-14	16	16.2 16.3	User	Protect				
2.3.1.12 CIS Control: 18 (Organizational) – Application Software Security										
2.3.1.12-01	The U²C SVS shall use standard hardening configuration templates for applications that rely on a database.	CFG-02	18	18.11	NA	Protect				
2.3.1.13 CIS Control: 20 (Organizational) – Penetration Tests and Red Team Exercises										
2.3.1.13-01	The U²C SVS shall include cybersecurity penetration testing and documentation of the results.	TDA-11	20	20.1 20.2	NA	Protect				

ID	Supervisory System Requirements	JTA DSP Control	CIS Control	CIS Sub-Control	Asset Type	Security Function	ST	MT-E	MT-A	LT
2.3.1.13-02	The U²C SVS penetration testing shall include qualified testers who have not been a part of the development team.	TDA-11	20	20.1 20.2	NA	Protect				
2.3.1.13-03	The U²C SVS penetration testing documentation shall be maintained as part of the U²C IV&V documentation. Reports shall include identification of testers, their respective qualifications, and resulting recommendations.	TDA-11	20	20.1 20.2	NA	Protect				
2.3.1.13-04	The U²C SVS penetration testing reports shall include the disposition of detected cybersecurity vulnerabilities. If a vulnerability is fixed, the details of the fix shall be documented. If a vulnerability is not addressed, the reasoning behind the acceptability of the underlying risk shall be documented.	TDA-11 VPM-01 VPM-04 VPM-06	20	20.1 20.2	NA	Protect				
2.3.1.13-05	The U²C SVS Stakeholder shall maintain a test bed to simulate attacks against devices and systems.	TDA-11 TPM-03 CHG-03	20	20.6	NA	Protect				
2.3.1.14 CIS Control: Not Applicable										
2.3.1.14-01	The U²C SVS shall be able to interact securely with single C/AVs or platooned C/AVs (from the same or different manufacturers) using interoperable interface standards.	GOV-02 EMB-01 EMB-02 EMB-03	NA	NA	NA	Protect				
2.3.1.14-02	The U²C SVS shall use the CVRIA to support ongoing and future implementation of cybersecurity requirements for U²C interfaces and interoperability, as applicable.	GV-02	NA	NA	NA	Protect				

ID	Supervisory System Requirements	JTA DSP Control	CIS Control	CIS Sub-Control	Asset Type	Security Function	ST	MT-E	MT-A	LT
2.3.1.14-03	The U²C SVS shall employ control access to firmware to prevent unauthorized recovery and analysis.	IAC-07 IACI-10(A) IAC-15 IAC-21	NA	NA	NA	Protect				
2.3.1.14-04	The U²C SVS (OBE) shall be able to interact with other CVRIA "Physical Objects" via Dedicated Short Range Communication (DSRC), using interoperable interface standards.	GOV-02 EMB-01 EMB-02 EMB-03	NA	NA	NA	Protect				
2.3.1.14-05	The U²C SVS (OBE) shall be able to interact with other CVRIA "Physical Objects" via Wide Area Wireless Communication, including 4G and 5G, using interoperable interface standards.	GOV-02 EMB-01 EMB-02 EMB-03	NA	NA	NA	Protect				
2.3.2 Security Function: Identify										
2.3.2.1 CIS Control: 2 (Basic) – Inventory and Control of Software Assets										
2.3.2.1-01	The U²C SVS inventory system shall secure system data detailing name, version, publisher, and install date for all software.	AST-02	2	2.4	Applications	Identify				
2.3.2.1-02	The U²C SVS inventory system shall be capable of remotely identifying network assets.	AST-02 AST-11	2	2.4	Applications	Identify				
2.3.2.2 CIS Control: 9 (Foundational) – Limitation and Control of Network Ports, Protocols and Services										
2.3.2.2-01	The U²C SVS shall be capable of associating active ports, services, and protocols to the devices in the asset inventory.	AST-02	9	9.1	Devices	Identify				

ID	Supervisory System Requirements	JTA DSP Control	CIS Control	CIS Sub-Control	Asset Type	Security Function	ST	MT-E	MT-A	LT
2.3.2.3 CIS Control: 11 (Foundational) – Secure Configuration for Network Devices, such as Firewalls, Routers and Switches										
2.3.2.3-01	The U²C SVS Stakeholder shall provide as-built diagrams to describe the high-level design of the network. This includes information systems and implementation details of the security controls employed, with sufficient detail to permit analysis and testing.	AST-04	11	11.2	Network	Identify				
2.3.3 Security Function: Detect										
2.3.3.1 CIS Control: 3 (Basic) – Continuous Vulnerability Management										
2.3.3.1-01	The U²C SVS shall use recently updated Security Content Automation Protocol (SCAP)-compliant vulnerability scanning tool to automatically scan all systems on the network.	VPM-01 VPM-06	3	3.1	Applications	Detect				
2.3.3.2 CIS Control: 4 (Basic) – Controlled Use of Administrative Privileges										
2.3.3.2-01	The U²C SVS shall implement the principles of least privilege within logical access control mechanisms so that only authorized users can gain access to JTA's information system and data.	IAC-07 IAC-10(A) IAC-15 IAC-21	4	4.1	Users	Detect				
2.3.3.2-02	The U²C SVS shall use automated tools to inventory all administrative accounts, including domain and local accounts, to ensure that only authorized individuals have elevated privileges.	IAC-07 IAC-10(A) IAC-15 IAC-21	4	4.1	Users	Detect				

ID	Supervisory System Requirements	JTA DSP Control	CIS Control	CIS Sub-Control	Asset Type	Security Function	ST	MT-E	MT-A	LT
2.3.3.2-03	The U²C SVS shall configure systems to issue a log entry and alert when an account is added to or removed from any group assigned administrative privileges.	CFS-02 IAC-07 IAC-10(A) IAC-15 IAC-21	4	4.8	Users	Detect				
2.3.3.2-04	The U²C SVS shall configure systems to issue a log entry and alert on unsuccessful logins to an administrative account.	CFS-02 IAC-07 IAC-10(A) IAC-15 IAC-21	4	4.9	Users	Detect				
2.3.3.3 CIS Control: 5 (Basic) – Secure Configuration for Hardware and Software on Mobile Devices, Laptops, Workstations and Servers										
2.3.3.3-01	The U²C SVS shall use a SCAP-compliant configuration monitoring system to verify all security configuration elements, catalog approved exceptions, and transmit alerts when unauthorized changes occur.	CFG-02	5	5.5	Applications	Detect				
2.3.3.4 CIS Control: 6 (Basic) – Maintenance, Monitoring and Analysis of Audit Logs										
2.3.3.4-01	The U²C SVS shall use at least three synchronized time sources from which all servers and network devices retrieve time information on a regular basis so that timestamps in logs are consistent.	CFG-02 NT-02 MNT-05 MON-01 MON-06	6	6.1	Network	Detect				
2.3.3.4-02	The U²C SVS shall ensure that local logging has been enabled on all systems and networking devices.	NET-01 NET-02 NET-14 MNT-02 MNT-05	6	6.2	Network	Detect				

ID	Supervisory System Requirements	JTA DSP Control	CIS Control	CIS Sub-Control	Asset Type	Security Function	ST	MT-E	MT-A	LT
		MON-01 MON-06								
2.3.3.4-03	The U²C SVS shall enable system logging to include detailed information, such as event source, date, user, timestamp, source addresses, destination addresses, and other useful elements.	MON-01 MON-06 NET-01 NET-02 NET-14 MNT-02 MNT-05	6	6.3	Network	Detect				
2.3.3.4-04	The U²C SVS shall ensure that all systems that store logs have adequate storage space for the logs generated.	CFG-02 NET-01 NET-02 MNT-02 MNT-05 MON-01 MON-06	6	6.4	Network	Detect				
2.3.3.4-05	The U²C SVS shall ensure that appropriate logs are being aggregated to a central log management system for analysis and review.	MNT-02 MNT-05 MON-01 MON-06	6	6.5 6.6	Network	Detect				
2.3.3.4-06	The U²C SVS shall be able to receive, process, and present failure alarms.	SEA-10 PES-13	6	6.5 6.6	Network	Detect				
2.3.3.4-07	The U²C SVS shall be compatible with most Security Information and Event Management (SIEM) or log analytical tool for log correlation or analysis that identifies anomalies or abnormal events.	CFG-02 NET-01 NET-02 MNT-02 MNT-05 MON-01 MON-06	6	6.6	Network	Detect				

ID	Supervisory System Requirements	JTA DSP Control	CIS Control	CIS Sub-Control	Asset Type	Security Function	ST	MT-E	MT-A	LT
2.3.3.4-08	The U²C SVS shall maintain log events and periodically scrutinize events by qualified analysts to detect trends of a cyberattack.	MNT-02 MNT-05	6	6.6	Network	Detect				
2.3.3.4-09	The U²C SVS shall be able to collect, analyze, and report historical information.	GOV-02 GOV-05	6	6.7	Network	Detect				
2.3.3.5 CIS Control: 8 (Foundational) — Malware Defenses										
2.3.3.5-01	The U²C SVS shall enable anti-exploitation features that are available in an operating system or deploy appropriate toolkits that can be configured to apply protection.	END-04	8	8.3	Devices	Detect				
2.3.3.5-02	The U²C SVS shall configure devices so that they automatically conduct an anti-malware scan or detect removable media when inserted or connected.	END-04	8	8.4	Devices	Detect				
2.3.3.5-03	The U²C SVS shall be capable of sending all malware detection “events” to enterprise anti-malware administration tools and event log servers for analysis and alerting.	END-04	8	8.6	Devices	Detect				
2.3.3.5-04	The U²C SVS shall enable Domain Name System (DNS) query logging to detect hostname lookups for known malicious domains.	END-04	8	8.7	Network	Detect				
2.3.3.5-05	The U²C SVS shall enable command-line audit logging for command shells.	END-04	8	8.8	Devices	Detect				

ID	Supervisory System Requirements	JTA DSP Control	CIS Control	CIS Sub-Control	Asset Type	Security Function	ST	MT-E	MT-A	LT
2.3.3.6 CIS Control: 12 (Foundational) – Boundary Defense										
2.3.3.6-01	The U²C SVS shall take a layered approach to cybersecurity in order to reduce the probability of an attack's success and ability to mitigate the ramifications of potential unauthorized access.	NET-01 NET-02	12	12.2	Network	Detect				
2.3.3.7 CIS Control: 14 (Foundational) – Controlled Access Based on the Need to Know										
2.3.3.7-01	The U²C SVS shall be capable of capturing and reporting unauthenticated or unauthorized access attempts.	IAC-15	14	14.5	Data	Detect				
2.3.4 Security Function: Respond										
2.3.4-01	The U²C SVS shall have a redundant system for communications.	EMB-03	NA	NA	NA	Respond				
2.3.5 Security Function: Not Applicable										
2.3.5-01	The U²C SVS shall support C/AVs with automation level 4, as defined by the Society of Automotive Engineers International (SAE).	CPL-01 CPL-02	NA	NA	NA	NA				
2.3.5-02	The U²C SVS shall support C/AVs with automation level 5, as defined by the SAE.	CPL-01 CPL-02	NA	NA	NA	NA				

2.4 Sensor Requirements

The U²C sensor network stands alone, yet it is also a system-of-systems. The free-standing embedded computing and sensor technologies will allow complex and responsive information delivery and autonomous system decision-making. Depending on their purposes, sensor data can be an integral part of measuring the environment, identifying system health, or making changes in the environment.

The integrity of each sensor must be protected both physically and logically. This includes limiting access to the devices, continuously understanding each sensor's integrity, and mitigating potential disruption of information flow. Many of the potential vulnerabilities may be mitigated in the design of the sensor network. However, when required, sensors must be capable of immediate remote patching and supervisory management.

The following Sensor Requirements are designed to address the needs described in the paragraphs above:

ID	Sensor Requirements	JTA DSP Control	CIS Control	CIS Sub-Control	Asset Type	Security Function	ST	MT-E	MT-A	LT
2.4.1 Security Function: Protect										
2.4.1.1 CIS Control: 3 (Basic) – Continuous Vulnerability Management										
2.4.1.1-01	The U²C sensors shall allow secure software upgrades, upgradable firmware, patching, and dynamic testing.	VPM-01	3	3.4 3.5	Applications	Protect				
2.4.1.2 CIS Control: 11 (Foundational) – Secure Configuration for Network Devices, such as Firewalls, Routers and Switches										
2.4.1.2-01	The U²C sensor shall allow secure two-way communication amongst system operations, C/AV, and OCC.	EMB-01 EMB-02 EMG-03	11	11.5	Network	Protect				
2.4.1.3 CIS Control: 18 (Organizational) – Application Software Security										
2.4.1.3-01	The U²C sensors shall use strong encryption and not static non-unique keys.	CRY-03	18	18.5	NA	Protect				

ID	Sensor Requirements	JTA DSP Control	CIS Control	CIS Sub-Control	Asset Type	Security Function	ST	MT-E	MT-A	LT
2.4.1.3-02	The U^{2}C sensors shall assure tools (e.g., CarShark) can be used to observe traffic on existing networks (e.g., Controller Area Network [CAN]).	EMB-01	18	18.5	NA	Protect				
2.4.1.3-03	The U^{2}C sensors shall be maintained in separate environments for production and non-production systems. Developers should not have unmonitored access to production environments.	TDA-11	18	18.9	NA	Protect				
2.4.1.4 CIS Control: 20 (Organizational) – Penetration Tests and Red Team Exercises										
2.4.1.4-01	The U^{2}C sensors must be penetration tested to confirm secure interfaces for reception of sensor data, transmission of sensor data, and over-the-air management.	VPM-11	20	20.2 20.3	NA	Protect				
2.4.1.5 CIS Control: Not Applicable										
2.4.1.5-01	The U^{2}C sensors placement shall be managed to minimize the threat of physically manipulation, spoofing, jamming, or signal interception.	RSK-04 RSK-06	NA	NA	NA	Protect				
2.4.1.5-02	The U^{2}C should provide hazard/risk analysis for station placement (e.g., center island versus roadside).	PES-02 PED-03 PES-05	NA	NA	Infra-structure	Protect				
2.4.1.5-03	Before inserting a U^{2}C sensor into a legacy network, the U^{2}C sensor shall be assessed to assure no expansion of the attack surface. If the attack surface is expanded, a remediation plan must be put in place and documented.	RSK-02 RSK-04 RSK-08	NA	NA	NA	Protect				

ID	Sensor Requirements	JTA DSP Control	CIS Control	CIS Sub-Control	Asset Type	Security Function	ST	MT-E	MT-A	LT
2.4.2 Security Function: Detect										
2.4.2.1 CIS Control: 6 (Basic) – Maintenance, Monitoring and Analysis of Audit Logs										
2.4.2.1-01	The U²C sensor Stakeholder shall ensure that the sensor's behavior can be rigorously monitoring to detect if it is operating normally.	VPM-06 NET-01	6	6.3	Network	Detect				
2.4.2.1-02	The U²C sensor network shall be capable of monitoring and reporting unauthenticated or unauthorized access attempts.	IAC-07 IAC-10(A) IAC-15 IAC-21 MON-01 MON-05 MON-16	6	6.3	Network	Detect				
2.4.2.1-03	The U²C sensors shall have the computing power to manage security requirements such as advanced encryption.	PRM-01 PRM-07	6	6.4	Network	Detect				
2.4.2.2 CIS Control: 12 (Foundational) – Boundary Defense										
2.4.2.2-01	The U²C sensors shall be capable of detecting modification of data algorithms used by the aggregator to combine and weigh data received from the sensors of the base station firmware.	RSK-06 CRY-04 CRY-05	12	12.5 12.8	Network	Detect				
2.4.2.2-02	The U²C sensors shall be capable of detecting the transmission of malicious command and control information to the sensors and base station / aggregator.	CRY-04 CRY-05	12	12.5 12.8	Network	Detect				
2.4.2.2-03	The U²C sensor network must be able to verify the integrity of sensor data, firmware, and configuration.	RSK-06 CRY-04 CRY-05	12	12.5 12.8	Network	Detect				

ID	Sensor Requirements	JTA DSP Control	CIS Control	CIS Sub-Control	Asset Type	Security Function	ST	MT-E	MT-A	LT
2.4.2.2-04	The U^{2}C sensors shall use hashing algorithms to ensure the integrity of sensor data and algorithms.	IAC-10 IAC-15	12	12.5 12.8	Network	Detect				
2.4.2.2-05	The U^{2}C sensors shall us a root of trust to ensure the integrity of the sensor's firmware and configuration.	END-04 END-06 EMB-01 EMB-03	12	12.5 12.8	Network	Detect				
2.4.3 Security Function: Not Applicable										
2.4.3-01	The U^{2}C sensors shall be capable of securely exchanging data with other "Physical Objects," as defined by the CVRIA, using the specified: • Data Flows • Information Flows	CPL-02 NET-01 NET-14	NA	NA	NA	NA				
2.4.3-02	The U^{2}C C/AV sensors shall have tamper-proof hardware.	EMB-01 EMB-03	NA	NA	NA	NA				

2.5 IoT Network and Device Requirements

IoT networks and their components allow the connectivity of smart nodes and IP-based systems that interact autonomously and deliver information and services to the JTA. The wide-area placement of these smart devices and the autonomy of nodes—combined with the wide distribution, openness, and relatively high processing power of IoT objects—make these networks an ideal target for impactful cyber-attacks.

Due to IoT network confidentiality, integrity, and availability, the use of IoT sensor data for decision-making, process control, and other functions within organizations has increased. However, the increased dependence on IoT data also increases the potential ramifications of a successful IoT-directed cyber-attack. Networking a legacy operational technology that was not originally designed for remote management with IoT also increases the impact of a cyber-attack. Consequently, IoT components must be individually identifiable, secured by cryptographic schemes, and provisioned, as described in the DSP. Additionally, IoT components must be monitored, capable of remote patching, and capable of detecting physical and logical tampering.

The following IoT Network and Device Requirements are designed to address the needs described in the paragraphs above:

ID	IoT Network and Device Requirements	JTA DSP Control	CIS Control	CIS Sub-Control	Asset Type	Security Function	ST	MT-E	MT-A	LT
2.5.1 Security Function: Protect										
2.5.1.1 CIS Control: 1 (Basic) – Inventory and Control of Hardware Assets										
2.5.1.1-01	The U²C IoT networks and devices shall use port level access control following IEEE 802.X standards to control which devices can authenticate to networks or other devices.	AST-02	1	1.7	Devices	Protect				
2.5.1.2 CIS Control: 3 (Basic) – Continuous Vulnerability Management										
2.5.1.2-01	The U²C IoT networks should provide a means of updating devices and software either over network connections or through automation.	END-04 IAC-07	3	3.4	Applications	Protect				

ID	IoT Network and Device Requirements	JTA DSP Control	CIS Control	CIS Sub-Control	Asset Type	Security Function	ST	MT-E	MT-A	LT
2.5.1.3 CIS Control: 4 (Basic) – Controlled Use of Administrative Privileges										
2.5.1.3-01	The U^{2}C IoT network shall meet the DSP-required password strength. It shall not use hardcode at design or default passwords.	IAC-10	4	4.2	Users	Protect				
2.5.1.4 CIS Control: 8 (Foundational) – Malware Defenses										
2.5.1.4-01	The U^{2}C IoT network shall be configured to allow software patching to kept up to date, mitigate malware, allow auditing, and protect handshaking credentials.	EMB-02 EMB-03	8	8.1 8.2	Devices	Protect				
2.5.1.5 CIS Control: 11 (Foundational) – Secure Configuration for Network Devices, such as Firewalls, Routers and Switches										
2.5.1.5-01	All U^{2}C IoT data exchange shall be encrypted at every interface.	CRY-03 CRY-04	11	11.5	Network	Protect				
2.5.1.6 CIS Control: 13 (Foundational) – Data Protection										
2.5.1.6-01	All U^{2}C IoT networks shall be monitored to identify anomalous traffic and emergent threats.	MON-01 MON-16	13	13.3	Data	Protect				
2.5.1.6-02	All U^{2}C IoT devices shall be connected to the smallest controlled network segment feasible, rather than having access to the full IP network.	EMB-01 EMB-02 EMB-03	13	13.4	Data	Protect				
2.5.1.6-03	The U^{2}C IoT network devices shall use cryptographic mechanisms to protect enterprise data stored on all mobile devices.	CRY-03 CRY-05	13	13.6	Data	Protect				
2.5.1.7 CIS Control: 14 (Foundational) – Controlled Access Based on the Need to Know										
2.5.1.7-01	The U^{2}C IoT network shall be segmented based on the label or classification level of the information stored on the servers.	TDA-11	14	14.1	Network	Protect				

ID	IoT Network and Device Requirements	JTA DSP Control	CIS Control	CIS Sub-Control	Asset Type	Security Function	ST	MT-E	MT-A	LT
2.5.1.7-02	The U²C IoT network shall be capable of enabling firewall filtering between VLANs to ensure that only authorized systems are able to communicate with other systems necessary to fulfill their specific responsibilities.	NET-01 NET-02	14	14.2	Network	Protect				
2.5.1.7-03	The U²C IoT network's back-end systems shall ensure only authorized devices, developers, and apps communicate with hardware embedded and software APIs.	MON-16 IAC-07 PES-05	14	14.2	Network	Protect				
2.5.1.7-04	The U²C IoT network shall encrypt all sensitive information in transit and at rest.	CRY-03 CRY-04	14	14.4	Data	Protect				
2.5.1.7-05	The U²C IoT network shall use an active discovery tool to identify all sensitive information stored, processed, or transmitted by the organization's technology systems, including those located on-site or at a remote service provider, and update the organization's sensitive information inventory.	AST-02 CRY-03 CRY-04 CRY-05	14	14.4	Data	Protect				
2.5.1.7-06	The U²C IoT network shall assure devices are not resource-constrained and lack the compute resources necessary to implement strong security.	CAP-01	14	14.4	Data	Protect				
2.5.1.8 CIS Control: 15 (Foundational) – Wireless Access Control										
2.5.1.8-01	The U²C IoT network shall use encryption strategies that allow the trust and controls needed to distribute and identify public encryption keys, secure data exchanges over networks, and verify identity (user and device).	CRY-03 CRY-04	15	15.7	Network	Protect				

ID	IoT Network and Device Requirements	JTA DSP Control	CIS Control	CIS Sub-Control	Asset Type	Security Function	ST	MT-E	MT-A	LT
2.5.1.8-02	The U²C IoT network Stakeholder shall disable wireless peripheral access of devices (e.g., Bluetooth, Near Field Communication [NFC]), unless such access is required for a business purpose.	GOV-02 NET-01	15	15.9	Devices	Protect				
2.5.1.9 CIS Control: 18 (Organizational) – Application Software Security										
2.5.1.9-01	The U²C IoT network and device Stakeholders shall coordinate and agree to disclosure vulnerabilities to the JTA as soon as they are identified with an action plan for remediation.	CRY-03 RSK-04 VPM-04 VPM-11	18	18.8	NA	Protect				
2.5.1.9-02	The U²C IoT network shall protect web applications by deploying web application firewalls (WAFs) that inspect all traffic flowing to the web application for common web application attacks. For applications that are not web-based, specific application firewalls shall be deployed if such tools are available for the given application type. If the traffic is encrypted, the device shall either sit behind the encryption or be capable of decrypting the traffic prior to analysis. If neither option is appropriate, a host-based web application firewall shall be deployed.	VPL-02 SEA-04 VPM-04	18	18.10	NA	Protect				
2.5.1.10 CIS Control: 19 (Organizational) – Incident Response and Management										
2.5.1.10-01	The U²C IoT network shall enable authorized JTA personnel to securely contact Stakeholders.	EMB-03	19	19.5	NA	Protect				

ID	IoT Network and Device Requirements	JTA DSP Control	CIS Control	CIS Sub-Control	Asset Type	Security Function	ST	MT-E	MT-A	LT
2.5.1.11 CIS Control: 20 (Organizational) – Penetration Tests and Red Team Exercises										
2.5.1.11-01	The U²C IoT network shall be pen tested. Tests shall include a full scope of blended attacks, such as wireless, client-based, and web application attacks.	VPM-04 VPM-11	20	20.1	NA	Protect				
2.5.1.11-02	The U²C IoT network shall maintain a test bed to simulate attacks against elements, such as attacks against supervisory control and data acquisition and other control systems.	VPM-04	20	20.6	NA	Protect				
2.5.1.12 CIS Control: Not Applicable										
2.5.1.12-01	U²C IoT Stakeholders shall assess safety-related risk associated with embedded technologies, remediate vulnerabilities, and apply compensating controls when vulnerabilities cannot be remediated.	EMB-01 EMB-02 EMB-03	NA	NA	NA	Protect				
2.5.1.12-02	The U²C IoT network shall securely enable customers to buy tickets with their mobile devices/applications.	EMB-01 EMB-02 EMB-03	NA	NA	NA	Protect				
2.5.1.12-03	The U²C IoT network shall meet the applicable functional requirements of the CVRIA "Center" Class and their "Physical Objects," including but not limited to: • Center Archived Data Center • Authorizing Center • Commercial Vehicle Administration Center • Emergency Management Center • Fleet and Freight Management Center	CPL-01 CPL-02 MNT -02 MNT-05	NA	NA	NA	Protect				

ID	IoT Network and Device Requirements	JTA DSP Control	CIS Control	CIS Sub-Control	Asset Type	Security Function	ST	MT-E	MT-A	LT
	• Maintenance and Construction Management Center • Payment Administration Center • Transit Management Center • Transportation Information Center									
2.5.1.12-04	The U²C shall apply a message authentication scheme to control communications and limit the possibility of spoofing.	NET-01 CPL-02	NA	NA	NA	Protect				
2.5.1.12-05	All U²C IoT acquisitions shall be supported by a business case.	TPM-03	NA	NA	NA	Protect				
2.5.1.12-06	All U²C IoT devices shall only be acquired through approved procurement processes.	TPM-03	NA	NA	NA	Protect				
2.5.1.12-07	Each U²C IoT implementation and associated data streams shall be supported by a security and privacy risk analysis.	RSK-01 RSK-03 RSK-04	NA	NA	NA	Protect				
2.5.1.12-08	The U²C IoT network shall be based upon a Modular Open Systems Approach (MOSA) employing a modular design, and use widely supported, open (publicly available) and consensus-based standards for its key interfaces.	GOV-02	NA	NA	NA	Protect				
2.5.1.12-09	The U²C IoT network shall be able to interact securely with JTA enterprise systems, using interoperable interface standards.	GOV-02 EMB-01 EMB-02 EMB-03	NA	NA	NA	Protect				

ID	IoT Network and Device Requirements	JTA DSP Control	CIS Control	CIS Sub-Control	Asset Type	Security Function	ST	MT-E	MT-A	LT
2.5.1.12-10	The U²C IoT network shall be able to interact securely with the U²C SVS, using interoperable interface standards.	GOV-02 EMB-01 EMB-02 EMB-03	NA	NA	NA	Protect				
2.5.1.12-11	The U²C IoT network shall be able to interact securely with other CVRIA "Enterprise Objects," using interoperable interface standards.	GOV-02 EMB-01 EMB-02 EMB-03	NA	NA	NA	Protect				
2.5.2 Security Function: Identify										
2.5.2.1 CIS Control: 1 (Basic) – Inventory and Control of Hardware Assets										
2.5.2.1-01	The U²C IoT devices shall connect securely to the network and update (manually or automatically) the hardware asset inventory (e.g., use of active discovery tool).	AST-02	1	1.1	Devices	Identify				
2.5.2.1-02	The U²C IoT network or device shall be capable of verifying the network identity of IoT devices and track the provenance of the information they provide.	AST-02	1	1.2	Devices	Identify				
2.5.2.1-03	The U²C IoT network shall use a passive discovery tool to identify devices connected to the network or other devices and automatically update the IoT asset inventory.	AST-02	1	1.2	Devices	Identify				
2.5.2.1-04	The U²C SVS shall use Dynamic Host Configuration Protocol (DHCP) logging on all DHCP servers or IP address management tools to update the IoT asset inventory.	AST-02	1	1.3	Devices	Identify				

ID	IoT Network and Device Requirements	JTA DSP Control	CIS Control	CIS Sub-Control	Asset Type	Security Function	ST	MT-E	MT-A	LT
2.5.2.1-05	The U²C SVS shall maintain an accurate and up-to-date inventory of all IoT assets with the potential to store or process information including all assets whether connected to the network, other device, or not connected.	AST-02	1	1.4	Devices	Identify				
2.5.2.1-06	The U²C shall ensure that IoT asset inventory records include the network (or other device) address, hardware address, machine name, data asset owner, and department for each asset, and whether the hardware asset has been approved to connect to the network or other devices.	AST-02	1	1.5	Devices	Identify				
2.5.3 Security Function: Detect										
2.5.3.1 CIS Control: 12 (Foundational) – Boundary Defense										
2.5.3.1-01	The U²C IoT net-flow connection capabilities should be deployed on network boundary devices.	MON-01 MON-06 ZPM-04	12	12.8	Network	Detect				
2.5.4 Security Function: Respond										
2.5.4.1 CIS Control: 1 (Basic) – Inventory and Control of Hardware Assets										
2.5.4.1-01	The U²C IoT network shall be capable of detecting, isolating, and removing unauthorized IoT devices.	NA	1	1.6	Devices	Respond				
2.5.4.1-02	The U²C shall ensure that unauthorized IoT assets are either removed from the network, quarantined, or the inventory is updated in a timely manner.	AST-02 AST-11	1	1.6	Devices	Respond				

ID	IoT Network and Device Requirements	JTA DSP Control	CIS Control	CIS Sub-Control	Asset Type	Security Function	ST	MT-E	MT-A	LT
2.5.5 Security Function: Not Applicable										
2.5.5.1 CIS Control: 18 (Organizational) – Application Software Security										
2.5.5.1-01	All U²C enterprise mobile devices shall pass through the five-step U²C Device Security Life Cycle: 1. **Un-provisioned** – The device does not have any of the crypto material or certificates necessary to interact with any parts of the SVS CCMS, other than provisioning components. The device cannot interact in a trustworthy manner with other end entities. 2. **Provisioned and Unenrolled** – The device has the crypto material and root certificates necessary to communicate with the JTA's enrollment process. The end entity is still not part of the SVS CCMS and cannot in a trustworthy manner interact with other end entities. 3. **Enrolled and Unauthorized** – The device has all the material it needs to communicate with the JTA's authorization process. 4. **Operational** – The device has all the material it needs to communicate with the misbehavior components, revocation components, and other U²C operational end entities. 5. **End-of-Life** – The device does/should not communicate with any CCMS component or other end entities.	EMB-01 EMB-02 EMB-03 NET-01 NET-02 NET-14	18	18.3	NA	NA				

ID	IoT Network and Device Requirements	JTA DSP Control	CIS Control	CIS Sub-Control	Asset Type	Security Function	ST	MT-E	MT-A	LT
2.5.5.1-02	All U²C enterprise mobile devices that are designated to be in an End-of-Life stage shall not be able to communicate with any component of the SVS CCMS or other end entity (or remotely reachable).	RSK-04	18	18.3	NA	NA				
2.5.5.1-03	The U²C IoT network or device Stakeholder shall actively manage the supply chain from factory to installation.	TPM-03	18	18.4	NA	NA				

3.0 Acronyms and Definitions

The below section describes acronyms, abbreviations, and definitions critical to this document. The table are as follows:

- **Table 3.1.1**: Acronyms
- **Table 3.2.1:** General Definitions
- **Table 3.2.2**: IT and Cybersecurity Definitions

3.1 Acronyms

TABLE 3.1.1	
Acronyms	
ADA	Americans with Disabilities Act
APTA	American Public Transportation Association
AV	Automated Vehicle
C/AV	Connected and Automated Vehicle
CAN	Controller Area Network
CCMS	Cooperative ITS Credential Management System
CCTV	Closed-Circuit Television
CIAS	Confidentiality, Integrity, Availability and Safety
COP	Common Operating Picture
CPS	Cyber-Physical System
CVRIA	Connected Vehicle Reference Implementation Architecture
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name System

TABLE 3.1.1	
Acronyms	
DoD	Department of Defense
DOT	Department of Transportation
DSP	Digital Security Program
DSRC	Dedicated Short-Range Communication
EMM	Engine Management Module
EMP	Electromagnetic Pulse
FTA	Federal Transit Administration
INCOSE	International Council on Systems Engineering
IoT	Internet of Things
IP	Internet Protocol
IT	Information Technology
ITS	Intelligence Transportation System
ITS-JPO	Intelligence Transportation System-Joint Program Office
IV&V	Independent Verification and Validation
LPANS	Logical Processing Area Networks
LT	Long-Term
MOSA	Modular Open Systems Approach
MT-A	Mid-Term, At-Grade (Roadway)
MT-E	Mid-Term, Elevated (Guideway)
NFC	Near Field Communication
NHTSA	National Highway Traffic Safety Administration
NIST	National Institute of Standards and Technology

TABLE 3.1.1	
Acronyms	
OBE	Onboard Equipment
OCC	Operations Control Center
RSE	Roadside Equipment
SAE	Society of Automotive Engineers
SCADA	Supervisory Control and Data Acquisition
SCAP	Security Content Automation Protocol
SIEM	Security Information and Event Management
ST	Short-Term
SVS	Supervisory System
TCP	Transmission Control Protocol
U^2C	Ultimate Urban Circulator Program
CCMS	Cooperative ITS Credential Management System
USB	Universal Serial Bus
UDP	User Datagram Protocol
USDOT	United States Department of Transportation
VLAN	Virtual Local Area Network
V2I	Vehicle to Infrastructure (Communication)
V2V	Vehicle to Vehicle (Communication)
V2X	Vehicle to Everything (Communication)
WAFs	Web Application Firewalls

3.2 Definitions

TABLE 3.2.1	
General Definitions	
Automated Vehicle Test Track	Roadway separated from traffic used specifically to evaluate automated vehicles before use for transit service.
Business Requirement	INCOSE: Definition of the business framework within which Stakeholders define their requirements. Business requirements govern the project, including agreement constraints, quality standards, cost, and schedule constraints.
Connected and Automated Vehicle	Vehicle that does not require full driver input and uses technologies (e.g., wireless communications, on-board computer processing, sensors, navigation, smart infrastructure) to identify threats and hazards on the roadway and communicate that information over networks.
Connected Vehicle Reference Implementation Architecture (CVRIA)	Basis for identifying the key interfaces across the connected vehicle environment. CVRIA supports policy considerations for certification, standards, core system implementation, and other elements of the connected vehicle environment.
Dedicated Short Range Communication	A wireless communications channel used for close-proximity communications between vehicles and the immediate infrastructure.
Mid-Term	JTA: Time horizon for implementation of the desired requirements. To be demonstrated on either the conversion of the JTA elevated guideway or in a shared at-grade environment (public roadways).
Long-Term	JTA: Time horizon for implementation of the desired requirements. Full U^2C build out, including the conversion of the JTA elevated guideway or in a shared at-grade environment (public roadways).
Near Field Communication	Short-range wireless connectivity standard (Ecma-340, ISO/IEC 18092) that uses magnetic field induction to enable communication between devices when they're touched together or brought within a few centimeters of each other.
Onboard Equipment	Equipment associated with the vehicle that communicates with roadside equipment.
Operations Control Center	APTA: Main location from which all aspects of the system are controlled, and operational decisions are made regarding normal and non-normal operations.

TABLE 3.2.1	
General Definitions	
Platooning	Linking of two or more vehicles in convoy, using connectivity technology and automated driving support systems.
Risk Management	Coordinated activities to direct and control an organization with regard to risk.
Roadside Equipment	Connected vehicle roadside devices that are used to send and receive messages.
Supervisory System	JTA: Control system that oversees a variety of systems, including proprietary devices and networks (e.g., vehicle, infrastructure, telecom).
Short-Term	JTA: Time horizon for implementation of the requirements. To be demonstrated on the JTA AV Test Track.
Standard	Formally established requirements in regard to processes, actions, and configurations.
Vehicle to Infrastructure	JTA: Signal communication of standardized data (e.g., signal timing) to and from vehicles from roadside units.
Vehicle to Vehicle	JTA: Vehicle to Vehicle communication through wireless, ad hoc network (e.g., DSRC).

TABLE 3.2.2	
IT and Cybersecurity Definitions	
Asset	Any data, devices, applications, services or other components of the environment that supports information-related activities. An asset is a resource with economic value that JTA owns or controls.
Attack Surface	Set of interfaces (the "attack vectors") where an unauthorized user can try to enter data to or extract data from a system or modify a system's behavior.
Attack Vector	The interfaces or paths an attacker uses to exploit a vulnerability. For instance, an exploit may use an open IP port vulnerability on a variety of different attack vectors such as Wi-Fi, cellular networks, IP over Bluetooth, etc. Attack vectors enable attackers to exploit system vulnerabilities, including the human element.
Control	Any management, operational, or technical method that is used to manage risk. Controls are designed to monitor and measure specific aspects of standards to help JTA accomplish stated goals or objectives. All controls map to standards, but not all standards map to controls.
Controller Area Network	Dominant serial communication network protocol used for intra-vehicle communication.

TABLE 3.2.2	
IT and Cybersecurity Definitions	
Cooperative ITS Credential Management System	Based upon the CVRIA, a Cooperative ITS Credential Management System (CCMS) is a representation of the interconnected systems that enable trusted communications between mobile devices and other mobile devices, roadside devices, and centers and protect data they handle from unauthorized access. The U^{2}C-CCMS Operating Period is the time during which the U^{2}C functionality and interfaces are active.
Credentialing	Attestation of qualification, competence, or authority issued to an individual by a third party.
Cybersecurity Requirements	Constraints arising from security concerns. Cybersecurity requirements do not specify how the constraints are satisfied, but only what the constraint is.
Data	Information resource that is maintained in electronic or digital format. Data may be accessed, searched or retrieved via electronic networks, or other electronic data processing technologies.
Data Flow	ITS-JPO: Unaggregated types of communication that are aggregated into information flows, which are the subject of standardization efforts.
Debug	Activity of discovering errors or undesirable actions within computer code.
Device Security Life Cycle	Five security states that categorize the stage of an end entity: 1) Unprovisioned, 2) Provisioned and Unenrolled, 3) Enrolled and Unauthorized, 4) Operational, or 5) End-of-Life.
Domain Name System Query Logging	Detects hostname lookups for known malicious domains.
Dynamic Host Configuration Protocol	Automatically provides a host with IP address that expires (dynamic).
Electronic Control Unit	An embedded system that provides a control function to a vehicle's electrical system or subsystems through digital computing hardware and associated software.
Encryption	Conversion of data from its original form to a form that can only be read by someone that can reverse the encryption process. The purpose of encryption is to prevent unauthorized disclosure of data.
Enterprise System	JTA: Large-scale applications software that integrates processes for the agency, not the end users.

TABLE 3.2.2	
IT and Cybersecurity Definitions	
Exploit	An action that takes advantage of a vulnerability in order to cause unintended or unanticipated behavior to occur on computer software or hardware. An example of an exploit would be using a diagnostic port vulnerability to take advantage of a buffer overflow that allows access over IP networks.
Firmware	The software code and data that reside on an embedded system, such as an automotive electronic control system, that implements dedicated functions and manage system resources (e.g., system input/outputs) to execute those functions. Firmware may take a variety of different forms. For example, in some cases "firmware" may refer to source code while in some cases it may take the form of a binary image consisting of a file system and compiled code.
Guidelines	Recommended practices that are based on industry-recognized leading practices. Unlike standards, guidelines allow users to apply discretion in their interpretation, implementation, or use.
Incident	An occurrence that actually or potentially jeopardizes the confidentiality, integrity, or availability of an information system on a vehicle computing platform through the use of an exploit.
Incident Response Process	Covers impact assessment, containment, recovery, remediation, and associated testing.
Information Flow	ITS-JPO: Information that is exchanged between physical objects. The primary tool used to define the Regional ITS Architecture interfaces that form the basis of the ongoing standards work in the national ITS program.
Information Security	Covers the protection of information against unauthorized disclosure, transfer, modification or destruction, whether accidental or intention. The focus is on Confidentiality, Integrity, Availability and Safety of data.
Information Technology	Computers, ancillary equipment including (imaging peripherals, input, output and storage devices necessary for security and surveillance), peripheral equipment designed to be controlled by the central processing unit of a computer, software, firmware and similar procedures, services (including support services), and related resources.
Internet of Things	Network of Internet connected objects able to collect and exchange data.
Internet Protocol	Set of rules for sending and receiving data over the Internet.
Interoperability	Ability to exchange information and services with minimal effort. Facilitated by common standards or interfaces.

TABLE 3.2.2	
IT and Cybersecurity Definitions	
Key Control	Methods to ensure that those who are authorized are the only ones who have access to encryption keys.
Least Privilege	Theory of restricting access by only allowing users or processed the least set of privileges necessary to complete a specific job or function.
Modular Open Systems Approach	System design approach that prioritizes highly cohesive, loosely coupled, and severable modules that can be competed separately and acquired from independent Stakeholders.
Multi-factor Authentication	Security enhancement that allows the user to present two credentials when logging in to an account.
Network	Information system(s) implemented with a collection of interconnected components. Such components may include routers, hubs, cabling, telecommunications controllers, key distribution centers, and technical control devices.
Penetration Testing	Testing of a system, network, or web application to identify vulnerabilities that could be exploited.
Supervisory Control and Data Acquisition	System of software and hardware elements that allows organizations to: 1) Control processes locally or remotely, 2) Monitor, gather, and process data, 3) Interact with devices, and 4) Log events.
Security Content Automation Protocol	Multi-purpose framework of specifications that supports automated configuration, vulnerability and patch checking, technical control compliance activities, and security measurement.
Security Information and Event Management	Enterprise security technology that incorporates threat intelligence, alert correlation, analytics, and automation to report on potential threats.
Sensitive Personal Data / Sensitive Personally Identifiable Information	Personal data, revealing the first name or first initial and last name, in combination with any one or more of the following data elements: - Social Security Number / Taxpayer Identification Number / National Identification Number - Driver License or another government-issued identification number (e.g., passport, permanent resident card) - Financial account number or Payment card number (e.g., credit card, debit card) - Racial or ethnic origin - Political opinions

TABLE 3.2.2	
IT and Cybersecurity Definitions	
	- Religious or philosophical beliefs - Trade-union membership - Physical or mental health - Sex life and sexual orientation - Genetic data - Biometric data
System	An asset, an information system or network that can be defined, scoped and managed. This includes, but is not limited to, computers, workstations, laptops, servers, routers, switches, firewalls, and mobile devices.
Threat	Any intentional circumstance or event with the potential to cause loss of or damage to an asset or death or injury to transit personnel and the public.
User Datagram Protocol	Alternative communications protocol to Transmission Control Protocol.
Vulnerability	Weakness in a system or its associated networks, system security procedures, internal controls, or implementation that could be exploited to obtain unauthorized access to system resources. For instance, an open diagnostic port on an Electronic Control Unit is a vulnerability.

4.0 Appendix

4.1 Connected Vehicle Reference Implementation Architecture (CVRIA) Resources

CVRIA Category	Webpage
General	https://local.iteris.com/cvria/index.html
Roadside Equipment	http://local.iteris.com/cvria/html/physobjects/physobj11.ht ml#tab-0
Data Flow	http://local.iteris.com/cvria/html/dataflows/dataflows.html
Information Flow	http://local.iteris.com/cvria/html/infoflows/infoflows.html
Enterprise Objects	https://local.iteris.com/cvria/html/applications/app37.html#tab-3
Physical Objects	http://local.iteris.com/cvria/html/physobjects/physobjects.html#tab-2
Security and Credentials Management	https://local.iteris.com/cvria/html/applications/app63.html#tab-3

4.2 Center for Internet Security (CIS) Controls

CIS Controls can be downloaded at: https://www.cisecurity.org/controls/.

4.3 National Institute of Standards and Technology (NIST) Resources

NIST Category	Webpage
Cybersecurity Framework	https://www.nist.gov/cyberframework/framework
Risk Management Resources	https://www.nist.gov/cyberframework/framework-resources/risk-management-resources
Informative References	https://www.nist.gov/cyberframework/informative-references/informative-reference-catalog
Computer Security Glossary	https://csrc.nist.gov/glossary?index=C

4.4 U.S. Department of Transportation (USDOT) Resources

USDOT Preparing for the Future of Transportation: Automated Vehicles 3.0 can be downloaded at: https://www.transportation.gov/av/3/preparing-future-transportation-automated-vehicles-3.

The above USDOT document built upon the USDOT National Highway Safety Administration Automated Driving Systems: A Vision for Safety 2.0 that can be downloaded at: https://www.nhtsa.gov/sites/nhtsa.dot.gov/files/documents/13069a-ads2.0_090617_v9a_tag.pdf.

4.5 Department of Defense (DoD) and United States Government Accountability Office (GAO) Resources

DoD CIO Policy Recommendations for the Internet of Things can be found at: https://dodcio.defense.gov/Portals/0/Documents/Announcement/DoD%20Policy%20Recommendations%20for%20Internet%20of%20Things%20-%20White%20Paper.pdf?ver=2017-01-26-152811-440.

GAO Report "Internet of Things Enhanced Assessments and Guidance Are Needed to Address Security Risks in DoD" can be found at: https://www.gao.gov/assets/690/686203.pdf.

4.6 Society of Automotive Engineers International Resources

The SAE recommended practice "Taxonomy and Definitions for Terms Related to Driving Automation Systems for On-Road Motor Vehicles J3016_201806," which defines the six levels of automation, can be previewed and downloaded at: https://www.sae.org/standards/content/j3016_201806/.

An updated graphic of the evolving J3016 "Levels of Driving Automation" standard can be found at: https://www.sae.org/news/2019/01/sae-updates-j3016-automated-driving-graphic.

4.7 Jacksonville Transportation Authority U²C Program Resources

Skyway and U²C Research reports are provided by the JTA at: https://www.jtafla.com/blueprint/ultimate-urban-circulator/skyway-u2c-researchreports/.