NYCPS Quick Risk Evaluation Rubric - Version 1.5

Submitted by: Sentry Management Solutions

Date: [Current Date]

Project: NYCPS Office of Pupil Transportation - Transportation Management System (TMS) - RFP R1804

1. Introduction

This document provides a comprehensive risk evaluation of the proposed Transportation Management System (TMS) for NYCPS Office of Pupil Transportation (OPT). This assessment follows the NYCPS Quick Risk Evaluation Rubric Version 1.5 format and methodology to enable NYCPS to assess the risk profile of our solution and prepare appropriate security testing plans/approaches.

The rubric evaluates security risks across multiple domains, assigns risk ratings, and proposes mitigation strategies aligned with industry standards including NIST SP 800-53, NIST CSF, ISO 27001, and NYC-specific security requirements. This evaluation serves as input for NYCPS security testing teams to develop targeted testing procedures for our solution.

> *Additional detailed information about specific security controls, architecture, and implementation details can be found in supporting documentation referenced throughout this document, particularly the **Appendix P.1 - Security Strategy.pdf** and **Appendix M.1 - System Architecture.pdf** files.*

2. Risk Assessment Methodology

This assessment utilizes a systematic approach to evaluate security risks in accordance with NYCPS requirements:

2.1 Risk Evaluation Framework

- **Risk Identification:** Identification of potential threats, vulnerabilities, and security concerns across 12 key security domains
- **Risk Analysis:** Each risk is analyzed for potential impact and likelihood
- **Risk Rating:** A risk level (High, Medium, Low) is assigned based on the combination of impact and likelihood
- **Mitigation Strategy:** Controls and countermeasures are defined to reduce each identified risk

2.2 Risk Rating Criteria

Risk Level	Description
High	Critical vulnerabilities that could lead to significant data breaches, system compromise, unauthorized access to PII, or severe disruption of service. Requires immediate mitigation before system deployment.
Medium	Significant vulnerabilities that present moderate risk of data exposure, system compromise, or service disruption. Requires mitigation within defined timeframes according to security policies.
Low	Minor vulnerabilities with limited potential impact. Should be addressed as part of normal system hardening and ongoing security improvements.

Reference Documents:

- **Appendix O.2.2 - Project and Change - Risk Management Methodology.pdf** - Detailed risk management framework and processes
- **Appendix P.1 - Security Strategy.pdf** - Comprehensive security approach and controls

3. System Overview & Architecture

3.1 System Description

The proposed Transportation Management System (TMS) is a cloud-native application designed to modernize and streamline NYCPS's pupil transportation operations. The solution includes:

- GPS-based real-time vehicle tracking
- Dynamic routing engine
- Ridership tracking and student management
- Parent/student notification system
- Administrative dashboards and reporting
- Integration with existing NYCPS information systems
- Mobile applications for drivers, parents, and school staff

3.2 Architecture Summary

The system implements a cloud-native, microservices-based architecture deployed in AWS GovCloud (US). Key components include:

- Multi-tier architecture with proper network segmentation
- Serverless and container-based application components
- Secure API gateway for all external interfaces
- Encrypted data storage using AWS KMS and database encryption
- Web application firewall (WAF) for public-facing interfaces
- Comprehensive logging and monitoring infrastructure
- Role-based access control integrated with NYCPS identity providers

Reference Documents:

- **Appendix M.1 - System Architecture.pdf** - Detailed system architecture and AWS service specifications
- **Appendix P.1 - Security Strategy.pdf** - Security architecture and controls

- **Appendix O.2.1 - Change Management Framework.pdf** - Risk management approach

4. Security Risk Evaluation by Domain

4.1 Data Security & Privacy

ID	Risk	Risk Level	Mitigation Strategy
DS-01	Unauthorized access to student PII protected under FERPA and NY Ed Law 2-d	High	• Implement comprehensive data classification system with specific controls for PII • Encrypt all PII data at rest and in transit using AWS KMS with customer-managed keys • Apply strict role-based access control (RBAC) for all PII access • Implement automated access logging and audit for all PII data access • Data Loss Prevention (DLP) monitoring using AWS Macie
DS-02	Data leakage during integration with third-party systems	Medium	• Implement API Gateway with strict access controls for all integrations • Data minimization principles applied to all external interfaces • End-to-end encryption for all data transfers • Comprehensive API logging and monitoring

ID	Risk	Risk Level	Mitigation Strategy
DS-03	Insufficient data retention and secure disposal processes	Medium	• Automated data lifecycle management using AWS S3 lifecycle policies • Implementation of 7-year retention requirement with secure archiving • Secure deletion procedures with verification and documentation • Regular audit of retention policy implementation

Reference Documents:

- **Appendix P.1 - Security Strategy.pdf** (Section VI.C - Data Security & Privacy Controls)
- **Appendix S.1 - Data Governance and compliance controls.pdf**

4.2 Identity & Access Management

ID	Risk	Risk Level	Mitigation Strategy
IAM-01	Inadequate authentication mechanisms leading to account compromise	High	• Federation with NYCPS identity providers (SAML/OIDC) for staff accounts • AWS Cognito User Pools with MFA for SBC users without federation • Strong password policies compliant with NYC3 requirements • Automated account lockout after failed attempts

ID	Risk	Risk Level	Mitigation Strategy
			• Continuous monitoring of authentication attempts
IAM-02	Overprivileged service accounts and roles	Medium	• Implementation of least privilege principle across all IAM roles • Fine-grained AWS IAM policies with specific actions and resources • Regular access reviews and privilege recertification • Use of IAM Access Analyzer to identify unintended access
IAM-03	Inadequate secrets management for service credentials	Medium	• Centralized secrets management using AWS Secrets Manager • Automated secret rotation for all database credentials and API keys • No hard-coded secrets in application code or configuration files • Audit logging of all secrets access

Reference Documents:

- **Appendix P.1 - Security Strategy.pdf** (Section VI.A - Identity & Access Management)
- **Appendix M.1 - System Architecture.pdf** (Section 5 - Networking & Security)

4.3 Network Security

ID	Risk	Risk Level	Mitigation Strategy
NS-01	Inadequate network segmentation allowing lateral movement	High	• Implementation of multi-tier VPC architecture with proper subnet isolation • Granular security groups configured per application tier • Network ACLs as additional defense layer • Private subnets for all sensitive resources (databases, backend services) • VPC Flow Logs enabled for traffic analysis and incident response
NS-02	Exposure of sensitive services to public internet	Medium	• VPC Endpoints for private AWS service access • AWS PrivateLink for secure third-party service connectivity • Strict egress filtering via NAT Gateways • Use of AWS Systems Manager Session Manager for bastion-less secure administration
NS-03	DDoS attacks against public-facing applications	Medium	• Implementation of AWS Shield Advanced for DDoS protection • CloudFront for edge caching and traffic distribution • WAF rules for request rate limiting and filtering • Auto-scaling architecture to absorb traffic surges

Reference Documents:

- **Appendix P.1 - Security Strategy.pdf** (Section VI.B - Network Security)
- **Appendix M.1 - System Architecture.pdf** (Section 5 - Networking & Security)

4.4 Application Security

ID	Risk	Risk Level	Mitigation Strategy
AS-01	Web application vulnerabilities (OWASP Top 10)	High	• Secure SDLC with security requirements integrated from design phase • Regular SAST and DAST testing throughout development • AWS WAF implementation with OWASP rule sets • Input validation on both client and server side • Output encoding to prevent XSS • Parameterized queries to prevent SQL injection
AS-02	API security vulnerabilities	Medium	• API Gateway with request validation and throttling • OAuth 2.0/OIDC for API authentication • API schema validation against OpenAPI specifications • Regular API security testing
AS-03	Insecure mobile application implementations	Medium	• Secure coding standards for mobile applications

ID	Risk	Risk Level	Mitigation Strategy
			• Certificate pinning to prevent MITM attacks • Secure local storage with encryption • Regular mobile application security testing • Compliance with OWASP Mobile Top 10

Reference Documents:

- **Appendix P.1 - Security Strategy.pdf** (Section VI.D - Application Security)
- **Appendix N.1.1 - SDLC Methodology.pdf**
- **Appendix N.2.1 - DevOps Strategic Framework.pdf**

4.5 Infrastructure & Cloud Security

ID	Risk	Risk Level	Mitigation Strategy
CS-01	Insecure cloud infrastructure configurations	High	• Infrastructure as Code (IaC) using Terraform with security guardrails • AWS Config rules aligned with security best practices • Security Hub implementation for continuous compliance monitoring • Regular infrastructure security assessments
CS-02	Container security vulnerabilities	Medium	• Image scanning in ECR for vulnerabilities

ID	Risk	Risk Level	Mitigation Strategy
			• Use of minimal base images (e.g., distroless) • No elevated privileges in containers • Strict container resource limits
CS-03	Inadequate infrastructure patching	Medium	• AWS Systems Manager Patch Manager for EC2 instances • Regular container image rebuilds with updated dependencies • Automated vulnerability scanning with AWS Inspector • Defined patching SLAs based on vulnerability severity

Reference Documents:

- **Appendix P.1 - Security Strategy.pdf** (Section VI.E - Infrastructure Security)
- **Appendix N.2.2 - DevOps Technical Implementation.pdf**
- **Appendix M.1 - System Architecture.pdf**

4.6 Incident Management & Resilience

ID	Risk	Risk Level	Mitigation Strategy
IR-01	Inadequate security incident detection capabilities	High	• Comprehensive security monitoring using AWS GuardDuty, CloudTrail, Security Hub • Centralized log collection and analysis • Real-time alerts for suspicious activities

ID	Risk	Risk Level	Mitigation Strategy
			• 24/7 security operations monitoring
IR-02	Ineffective incident response procedures	Medium	• Formal Security Incident Response Plan (SIRP) with defined roles and responsibilities • Regular incident response simulations and tabletop exercises • Integration with NYCPS incident management processes • Post-incident review (PIR) process for continuous improvement
IR-03	Single points of failure in critical components	Medium	• Multi-AZ deployments for all critical components • Auto-scaling groups for application tiers • RDS Multi-AZ for database resilience • Disaster recovery capabilities with RPO/RTO aligned to requirements

Reference Documents:

- **Appendix P.1 - Security Strategy.pdf** (Section VII - Security Operations & Incident Response)
- **Appendix Q.3 - Incident Management SOP and SLAs.pdf**
- **Appendix Q.1 - Business Continuity Plan And Operational Excellence.pdf**

4.7 Compliance & Governance

ID	Risk	Risk Level	Mitigation Strategy
CG-01	Non-compliance with regulatory requirements (FERPA, NY Ed Law 2-d)	High	• Comprehensive Compliance Requirements Traceability Matrix (CRTM) • Specific controls implemented for each compliance requirement • Regular compliance assessments and gap analysis • Staff training on regulatory requirements
CG-02	Inadequate security policy framework	Medium	• Development of comprehensive security policies aligned with NIST and NYC3 requirements • Regular policy reviews and updates • Policy awareness training for all staff • Automated policy compliance monitoring where possible
CG-03	Insufficient audit trails for compliance demonstration	Medium	• Comprehensive logging of all security-relevant events • Immutable audit logs stored in dedicated, access-controlled S3 buckets • Regular review of audit log completeness • Automated audit reporting capabilities

Reference Documents:

- **Appendix P.1 - Security Strategy.pdf** (Section IV - Compliance Framework Implementation)
- **Appendix P.3 - Audit Framework.pdf**
- **Appendix S.1 - Data Governance and compliance controls.pdf**

4.8 Vendor & Third-Party Risk

ID	Risk	Risk Level	Mitigation Strategy
VR-01	Inadequate security controls in third-party integrations	High	• Formal vendor security assessment process • Contractual security requirements for all vendors • Secure integration architecture with strict access controls • Regular security reviews of vendor components
VR-02	Supply chain vulnerabilities in software dependencies	Medium	• Software Composition Analysis (SCA) in CI/CD pipeline • Verified vendor sources for all dependencies • Maintenance of Software Bill of Materials (SBOM) • Regular dependency updates and vulnerability remediation
VR-03	Excessive third-party access to system components	Medium	• Just-in-time access provisioning for vendor support • Comprehensive monitoring of all third-party access

ID	Risk	Risk Level	Mitigation Strategy
			• Granular access controls limited to required components • Regular review and revocation of vendor access

Reference Documents:

- **Appendix P.1 - Security Strategy.pdf** (Section VIII - Vendor & Third-Party Security Management)
- **Appendix U.1 - Vendor and Third Party Management.pdf**

4.9 Device & Endpoint Security

ID	Risk	Risk Level	Mitigation Strategy
DS-01	Insecure GPS hardware devices in vehicles	High	• Secure device provisioning and authentication • Encrypted communication channels for all device data • Regular firmware updates and security patches • Physical security controls for device access
DS-02	Compromised mobile devices accessing the system	Medium	• Device posture checking before authentication • Mobile application security features (certificate pinning, app hardening) • Secure local storage with encryption

ID	Risk	Risk Level	Mitigation Strategy
			• Ability to remotely wipe sensitive data
DS-03	Lost or stolen endpoint devices containing sensitive data	Medium	• Data minimization on endpoint devices • Encryption of all locally stored data • Automatic session timeouts and secure logout • Remote device management capabilities

Reference Documents:

- **Appendix U.2 - Hardware Lifecycle and Logistics Management.pdf**
- **Appendix M.2 - Solution Design Functional and Non Functional Requirements.pdf**

4.10 DevSecOps & Secure SDLC

ID	Risk	Risk Level	Mitigation Strategy
SD-01	Security vulnerabilities introduced during development	High	• "Shift Left" security approach with security integrated throughout SDLC • Threat modeling during design phase • Secure coding standards and training • Automated SAST, DAST, and SCA in CI/CD pipeline • Security-focused code reviews

ID	Risk	Risk Level	Mitigation Strategy
SD-02	Insecure deployment processes	Medium	• Infrastructure as Code (IaC) with security validation • Immutable infrastructure approach • Separation of duties in deployment pipeline • Automated security testing in staging environments
SD-03	Lack of security regression testing	Medium	• Automated security test suites maintained alongside functional tests • Regular security regression testing • Penetration testing before major releases • Continuous security validation in production

Reference Documents:

- **Appendix P.1 - Security Strategy.pdf** (Section V - Embedding Security Throughout the DevSecOps Lifecycle)
- **Appendix N.1.1 - SDLC Methodology.pdf**
- **Appendix N.2.1 - DevOps Strategic Framework.pdf**

4.11 Business Continuity & Disaster Recovery

ID	Risk	Risk Level	Mitigation Strategy
BC-01	Extended system downtime affecting transportation operations	High	• Multi-AZ architecture with high availability design • Comprehensive disaster recovery plan with defined RPO/RTO • Regular DR testing and validation • Backup and restoration procedures
BC-02	Data loss during disaster scenarios	Medium	• Multi-region data replication for critical components • Point-in-time recovery capabilities for databases • Regular backup testing and validation • Secure data restoration procedures
BC-03	Inadequate emergency response procedures	Medium	• Documented emergency response procedures • Regular tabletop exercises and simulations • 24/7 on-call support with escalation procedures • Integration with NYCPS emergency management

Reference Documents:

- **Appendix Q.1 - Business Continuity Plan And Operational Excellence.pdf**

- **Appendix M.1 - System Architecture.pdf** (Section 8 - High Availability & Disaster Recovery)

4.12 Security Awareness & Training

ID	Risk	Risk Level	Mitigation Strategy
SA-01	Inadequate security awareness among system users	Medium	• Comprehensive security awareness program for all user types • Role-based security training for staff, administrators, drivers • Regular security communications and updates • Simulated phishing exercises
SA-02	Social engineering vulnerabilities	Medium	• Specific training on social engineering techniques • Clear reporting procedures for suspicious activities • Regular awareness campaigns • Verification procedures for sensitive operations

ID	Risk	Risk Level	Mitigation Strategy
SA-03	Insufficient security documentation for system administrators	Low	• Comprehensive security administration documentation • Secure configuration baseline documentation • Regular training for system administrators • Knowledge base for security best practices

Reference Documents:

- **Appendix T.1 - User Onboarding and Training Strategy.pdf**
- **Appendix X.1 - Team Structure and Processes.pdf**

5. Recommended Security Testing Approach

Based on the risk assessment above, we recommend the following security testing approach for the TMS solution:

5.1 Pre-Deployment Testing

- **Architecture Review:** Comprehensive security architecture review against NYC3 requirements and NIST frameworks
- **Threat Modeling:** In-depth threat modeling of critical components and data flows
- **Static Application Security Testing (SAST):** Code analysis to identify security vulnerabilities
- **Dynamic Application Security Testing (DAST):** Testing of running applications to find runtime vulnerabilities

- **API Security Testing:** Specialized testing of API endpoints for security issues
- **Mobile Application Security Testing:** Testing of iOS and Android applications
- **Infrastructure Security Testing:** Assessment of AWS GovCloud configuration security
- **Penetration Testing:** Simulated attacks against the system to identify exploitable vulnerabilities

5.2 Continuous Security Testing

- **Automated Security Scanning:** Integration of security testing into CI/CD pipeline
- **Vulnerability Management:** Regular vulnerability scanning and remediation
- **Configuration Compliance Checking:** Ongoing verification of security configurations
- **Continuous Monitoring:** Real-time security monitoring and anomaly detection

5.3 Priority Testing Areas

Based on the risk assessment, the following areas should be prioritized for security testing:

- Student PII data handling and access controls
- Authentication and authorization mechanisms
- API security and integration points
- Mobile application security
- GPS device communication security
- Cloud infrastructure security configuration

Reference Documents:

- **Appendix R - Testing Strategy.pdf**
- **Appendix P.1 - Security Strategy.pdf**
- **Appendix N.2.1 - DevOps Strategic Framework.pdf**

6. Conclusion & Risk Summary

This risk evaluation identified 36 specific security risks across 12 domains, categorized as follows:

Risk Level	Count	Description
High	9	Critical risks requiring robust mitigation before system deployment
Medium	26	Significant risks requiring mitigation according to defined timeframes
Low	1	Minor risks to be addressed as part of normal system hardening

The proposed TMS solution incorporates comprehensive security controls and mitigation strategies to address all identified risks. Our security-by-design approach integrates security throughout the development lifecycle, infrastructure, and operational processes.

We welcome NYCPS's security testing team to validate the effectiveness of our security controls and are committed to addressing any additional findings during the security assessment process. The detailed security architecture and controls outlined in the referenced documents provide a solid foundation for secure implementation of the Transportation Management System.

Primary Reference Documents:

- **Appendix P.1 - Security Strategy.pdf** - Comprehensive security approach
- **Appendix M.1 - System Architecture.pdf** - System architecture with security controls
- **Appendix O.2.2 - Project and Change - Risk Management Methodology.pdf** - Risk management approach
- **Appendix Q.3 - Incident Management SOP and SLAs.pdf** - Incident response capabilities
- **Appendix Q.1 - Business Continuity Plan And Operational Excellence.pdf** - Business continuity measures