FINDINGS SUMMARY

eFare Security, Technical Design & Integration Assessment

PREPARED FOR:

Tri-County Metropolitan Transportation District of Oregon

Report Date: February 22, 2016

Contact: Adam Gaydosh, adam.gaydosh@anitian.com

ANITIAN

TABLE OF CONTENTS

1. PROJECT OVERVIEW

The Tri-County Metropolitan Transportation District of Oregon ("TriMet") engaged Anitian to perform a technical security, design and integration assessment of their eFare environment. This document summarizes the high-level findings of the assessment.

The goal of this project was to review the current state of Tri-Met's eFare system in an effort to ensure the safety of payment and personal data stored in eFare's collection systems. Specific tasks related to this project are as follows:

Technical Design and Integration Assessment Project Tasks

- Task 1: Design
  - Assess system design for quality of architecture and scalability; evaluate openness of design to ensure future upgrades and API backward compatibility
  - Perform a holistic review of the integration points between applications
  - Ensure that a system of record is identified and properly managed for each master data and transactional data subject area
  - Validate that APIs are structured to transmit key record fields to properly integrate with the databases in the receiving applications
- Task 2: Volume
  - Evaluate capacity to process anticipated transaction volumes through a 5-year projection, including expected peak traffic and delayed load (traffic generated after an offline system returns online)
- Task 3: Data Security
  - Review test plan for efficiency, clarity, inclusivity, feasibility, and compliance including negative test strategy of the application designs
- Task 4: Disaster Recovery
  - Ensure ability to recover to a fully redundant state in both a total disaster recovery (all is lost) scenario as well as a single site lost scenario
  - Assess design for appropriate fault tolerance and redundancy, ensuring no single points of failure even with loss of one site
  - Review disaster recovery plan to assess:
    - Mitigation strategies for the backup and storage of data
    - Alternative communication channels
    - Offsite operations of critical business functions
    - Remote staffing plans
  - Ensure that the sequences within the plan align with business priorities
- Task 5: Design Documentation
  - Perform documentation review to ensure inclusivity of all critical design elements, employment of robust version and change control management practices, and proper documentation of all modifications
- Task 6: Hosting

- Review selected hosted solution and approach to ensure it meets the business requirements for application up-time and quality

System Security Assessment Project Tasks

- Task 1: Compliance Review
  - Payment Card Industry (PCI): Review PCI compliance approach to ensure data flow and control points around open payments and bank card information are secure and PCI-compliant with payment card industry data security standards (PCI – DSS 3.0 or more recent); *NOTE: A separate PCI Compliance contract is already in place; TriMet is not seeking a PCI Compliance certification in this scope of work, but rather seeks a related review and recommendations.*
- Task 2: Network Security
  - Authorization schemas
  - Firewall rules
  - Network accessibility, such as use of dial-up lines; website and custom app security; monitoring vendor/third-party access lines to the system; network security breach detection and response
  - Server security, flow/packet/volume traces, and advanced network traffic monitoring and analysis
  - Network traffic monitoring and Network behavioral analysis tools in use or to be implemented by TriMet
- Task 3: Data Security
  - Assess location of protected information assets (PCI, PII, sensitive, etc.), along with methods of access (as part of the network security analysis) for vulnerabilities
  - Evaluate data security and integrity, including but not limited to:
    - Compliance with PCI
    - Access control standards
    - Logon/password controls
    - Transaction-level and data-level authorization schemas
    - Distribution or introduction of data
    - Data and program backup protection
    - Malware prevention/detection/removal
- Task 4: Physical Security
  - Review & assess the level of physical and logical security in TriMet's server data centers
  - Evaluate physical security to ensure servers/network equipment are located in a secure facility
  - Recommend physical security improvements, such as access control, internal installation/maintenance procedures, and data policy to prevent data center equipment damage, theft, and security incidents
- Task 5: Application Security
  - Evaluate applications, such as but not limited to TriMet's CRM, eFare website, payment card solutions, onboard card readers, and mobile applications, for authentication and security of PII, sensitive information, and payment card access
  - Assess authorization schemas and ensure consistency and penetration risks

  - Confirm that application customizations and modifications are versioned, logged, and do not introduce security loopholes
- Task 6: IT Policies
  - Review system design to ensure compliance with internal IT security policies
- Task 7: Test Plans
  - Review integration test plans to ensure that sufficient positive/negative tests are planned to protect sensitive data

1.1. Risk Summary

TriMet has demonstrated thorough due diligence in defining the business, IT and security requirements for eFare and in coordinating with their vendors. Not all aspects of the design have been finalized, but the most critical components have been designed and in some cases now exceed industry best practices. While there are gaps with best practices in other areas, they are relatively minor and are easily addressable at this early stage of the system development lifecycle.

Strengths	Opportunities
• Very effective use of security technologies at point of sale to encrypt payment data and minimize impact on compliance • Robust coordination between vendors and design components • The existing PCI security control framework can be easily extended to apply to eFare systems	• Components of the architecture are not yet designed or finalized; most notably, the details concerning encryption and key management • Vendor development processes do not include consistently formal, robust security reviews • System and network security controls are not currently deployed on pre-production systems

2. FINDINGS SUMMARY

1.1.1. Project Task List – Technical Design and Integration Assessment

Task / Project	Description
Task 1: Design	• Finalized components demonstrate robust design, open or incomplete design areas should be addressed before final acceptance.
Task 2: Volume	• Potential bottlenecks exist between validator cellular network usage and calls to back-office components
Task 3: Data Security	• The GlobeSherpa-hosted environment is not fully dedicated to Tri-Met production eFare system
Task 4: Disaster Recovery	• The Data Warehouse implementation used for report generation is not fully redundant. • Existing continuity of operations plan (COOP) is robust but needs to be updated for eFare • Data backup process not efficiently integrated with virtual server system. • Restoration of certain components currently dependent on vendor assistance
Task 5: Design Documentation	• System designs are very well documented in most cases • Open and recently designed components require additional documentation before final acceptance.
Task 6: Hosting	• Some vendor-hosted environments need to be formally aligned with industry or regulatory security standards

1.1.2. Project Task List – System Security Assessment

Task / Project	Description
Task 1: Compliance Review	• Validator encryption scheme aligns with payment card industry guidelines. Obtain formal approval of the scheme from TriMet's merchant bank • Some vendor products are currently undergoing industry standard security validation. Deploy validated software versions to EFare environment.
Task 2: Network Security	• Approach for remote vendor access to production environment should be finalized prior to commissioning of this environment. eFare network is not currently segmented by trust level of systems. Additional network segmentation should be implemented prior to commissioning of production system.
Task 3: Data Security	• Formal system security standards should be developed and deployed to eFare servers • Encryption key management process should be formalized for all databases and vendors.
Task 4: Physical Security	• Inconsistent level of formality in physical system access control across different groups. A consistent approach should be defined and enforced. Fare media handling procedures should be updated and enforced for EFare.
Task 5: Application Security	• Enforce patch management to all systems regardless of vendor support • Customized version of commercial software (IVR) introduces risk that application updates are not propagated to the custom deployment. Work with vendors to ensure that important application updates are implemented in the EFare software branch. • Formalize secure software development and change management practices for all application development
Task 6: IT Policies	• A responsibilities matrix should be created to define specific management responsibilities for each vendor
Task 7: Test Plans	• Complete all test plans and include security testing

.

APPENDIX A. DOCUMENT HISTORY

All revisions to this document are logged below on the date they began.

Date	Revision	Author	Description of Changes
02/09/2016	0.1	Adam Gaydosh	First draft
02/17/2016	0.2	Greg Ragland	Editorial Review