Appendix-11

Data Security Report

SECURITY REVIEW FINAL REPORT

California Road Charge Pilot Program

June 15, 2016

Cambria Solutions

(This page intentionally left blank.)

TABLE OF CONTENTS

Prepared by:

Document Owner(s)	Project/Organization Role
Rich Cefola	Security Analyst

Project Charter Version Control

Version	Date	Author	Change Description
0.1	06/02/2016	Rich Cefola	Document Created
0.2	06/15/2016	Rich Cefola	Updates from draft

1. INTRODUCTION

1.1 PURPOSE OF REPORT

The purpose of this summary report is to provide an executive compilation of the data acquired and analyzed through the security assessment phase of the project.

1.2 OBJECTIVES OF SURVEY

The California Transportation Commission (CTC) Technical Advisory Committee (TAC) determined that Data Security is an important area of the pilot program. With the importance of security in mind, the security survey had the following objectives.

- Identify the data security measures each partner company will employ
- Collect details about how each applies the system security requirements recommended by the TAC
- Determine compliance with security requirements and features
- Ensure that all pilot program participants' data are properly handled, and protected from unnecessary disclosure

1.3 EXECUTIVE SUMMARY

As a participant in the Road Charge Pilot Program, firms are required to meet certain security requirements to ensure that all pilot program participants' data is properly handled, and protected from unnecessary disclosure. All vendors demonstrated that they had sufficient security measures in place in order to start the pilot. Issues noted or raised are aspirational for those firms that are noted and not so significant as to hinder the start of the pilot. The details of those issues can be found in Section 3.2 of areas not in compliance.

2. SECURITY SURVEY APPROACH

In order to assess each partner's current security readiness, we asked that each vendor to provide system documentation describing their security measures including but not limited to, security policy, description of technology platform, published data policies and privacy statements, and current security certifications. This included system architectural drawings, published policies and process material detailing how the organization collects and uses private customer data.

This was followed by a security review survey. The goal of this survey was to collect an overview of current capabilities, security protocols, and a variety of other technical capabilities to analyze its alignment with the Road Charge Pilot Program requirements. The partner company survey contained questions related to 17 areas of the ISO/IEC 27002 information security standard. In general vendors that had applicable processes that utilized personal data, it was proven that processes were in place and appropriate controls were installed to protect this data.

Subsequent to the survey, our team conducted interviews to collect additional information related to the implemented systems used to manage Road Charge data. Our interview team focused mainly in the areas of the security survey where either a negative or no response to the survey section was presented. The team also assessed background information on the vendor such as company size, number of employees, number of offices and general maturity of the business. The data gathered in the survey and follow up interviews were analyzed and are presented in this final report.

3. FINDINGS

Cambria collected and analyzed data from each vendor against the D'Artagnan defined security requirements as defined by the nomenclature SYS.SSD.X. These requirements were then aligned to the ISO/IEC 27002 information security standard for the purpose of the survey and interview:

- SYS.SSD.3 Develop an Information Classification Scheme
- SYS.SSD.4 Identify and Respond to Information Security Incidents
- SYS.SSD.5 Information Security Policies
- SYS.SSD.6 Address Your Technical Vulnerabilities
- SYS.SSD.7 Respect Business Requirements
- SYS.SSD.8 Control Access to Systems
- SYS.SSD.9 Manage All User Access Rights
- SYS.SSD.10 Protect Your Organization from Malware
- SYS.SSD.11 Control How Physical Media are Handled
- SYS.SSD.12 Protect Information Transfers
- SYS.SSD.14 Protect Networks and Facilities
- SYS.SSD.15 Use Logs to Record Security Events
- SYS.SSD.16 Control the Use of Cryptographic Controls and Keys
- SYS.SSD.18 Establish a Teleworking Security Management Policy
- SYS.SSD.19 Establish a Mobile Device Security Risk Management Policy
- SYS.SSD.21 Protect Information and Facilities from External Threats
- SYS.SSD.22 Establish Information Security Continuity Controls

The vendors surveyed were compliant with the majority of the security standards; however, some vendors had areas with less than full compliance. The specifics of the security surveys is presented in the following subsections.

3.1 AREAS IN COMPLIANCE

The following vendors were compliant with the security standards in all 17 areas surveyed. Their overall maturity and process varied from passing to fully mature including the documentation of policies, the application standards and adherence to process:

- Azuga
- Driveway
- Vehcon
- Arvato
- IMS

3.2 Areas Not In Compliance

The following tables outlines compliance areas where the vendors should look to improve their current compliance with the standards and requirements. Although these vendors showed a deficiency, it was deemed as minor and would not affect the performance in a pilot environment. The following table provides details where the remaining vendors were not fully compliant.

Table 1:

Security Standard Area	Deficiency
SYS.SSD.3 Develop an Information Classification Scheme	**PRR** PRR has not developed or adopted a security classification scheme. This scheme has not been developed as the organization does not handle PII information in its current business process. It is recommended that going forward, PRR document an information classification scheme for the data that it collects.
SYS.SSD.4 Identify and Respond to Information Security Incidents	**SmartCar** SmartCar does not have established and documented information security incident procedures due to the small number of employees. We recommend that SmartCar consider developing a classification of security incidents at a minimum as informational, medium, and critical in an effort implement the proper response to security incidents. **EROAD** EROAD established and has documented their information security incident procedures. Overall, their incident management procedures and processes are adequate, but they do not have a schema to classify security incidents and events. The recommendation would be that EROAD consider developing a classification of at a minimum informational, medium, critical to implement the proper response to security incidents.
SYS.SSD.5 Information Security Policies	**PRR** The organization defined information security policies and management approved those policies. PRR communicated the policies to all levels within the organization but they are not published. It is recommended that PRR publish a public version of their policies. **SmartCar** The organization defined, and management approved terms of use policies. The organization does not currently have documented security policies. It is recommended that SmartCar develop a privacy policy and internal security policies.

SECURITY STANDARD AREA	DEFICIENCY
SYS.SSD.7 Respect Business Requirements	**SmartCar** The organization has not established policies to control access to information because of the current scope of services and limited number of users in the organization. It is recommended that SmartCar consider in the development of a security policy that these policies are addresses within that document.
SYS.SSD.11 Control How Physical Media are Handled	**SmartCar** SmartCar delivers all IT services through cloud implementations. There is currently no physical media used for the transfer of the data. There is no specific process defined for the transfer or transport of media but it is recommended that this be added to their security policy in the future.
SYS.SSD.22 Establish Information Security Continuity Controls	**PRR** The organization has not established disaster recovery plan and procedures. It is recommended that the organization consider the establishment of a DR plan to ensure business continuity of its business services.

4. RECOMMENDATIONS

In summary, all of the vendors interviewed understood and respected the need for security privacy and protection in their implementations. As provided in the table above, there are pointed recommendations for some vendors to increase their documented compliance with some of the standards.

As an overall observation, several of the vendors are using third party hosting services such as Amazon AWS, Azure or Digital Ocean for their technologies. These services have significant benefits to the flexibility and scalability of rapidly developed applications. They provide extracted stability and elastic flexibility to support varying workloads. All vendors surveyed using these technologies have cloud level encryption and have taken appropriate steps to protect personally identifiable information.

As a contractual caution, it is recommended that when moving from pilot to production phase that the contract flow downs are appropriate for each of these third party hosts and that adequate protection and procedures are in place in the case of breach of these public services.

From the perspective of the currently documented requirements, they are well aligned with the ISO/IEC 27001 standards and cover the pertinent areas of operations in the scope of the pilot.