BRIEFING BOOK FOR THE CALIFORNIA ROAD CHARGE TECHNICAL ADVISORY COMMITTEE

Pre-Meeting Background Reading for TAC Meeting #7

Prepared by D'Artagnan Consulting

July 24, 2015

D'ARTAGNAN CONSULTING

Contents

Section 1: TAC Decision Summary and Schedule 1

Section 2: Policy Decisions Overview 14

Section 3: Data Security in California's Road Charge Pilot Program 16

Section 4: California Road Charge Pilot Program Privacy Protections 48

Appendix 1: California Road Charge Privacy Protection Provisions 55

Section 1:
TAC Decision Summary and Schedule

Summary of TAC Decisions and Preview of Schedule

This section summarizes the TAC's decisions made to date, and previews issues the TAC will consider and address during the remaining meetings for 2015.

- The Decisions Summary page displays:
  - Decision points that the TAC has addressed in prior meetings
  - Any actions taken
  - A brief summary of the TAC's proposal reflecting more detailed direction on pilot design
- Next is the Decisions Schedule at-a-glance, which provides an overview of all remaining questions the TAC will address, organized chronologically and indicating which work streams will inform the TAC's discussion.
- Finally, a Detailed Monthly Decision Schedule can be found after the Schedule at-a-glance. This provides a more detailed look at each of the remaining TAC meetings through December. These pages include topic areas that each meeting will cover; statutory language associated with each topic area; and any corresponding TAC decision points to address in the meeting.

The Decisions Summary has been and will continue to be updated each month. Although the project team recommends that the TAC achieve consensus and direction on the questions in the timeframes presented, the Decision Schedule remains a living document. Any changes, such as moving questions up or down on the schedule or adding new questions will be reflected in the briefing materials each month and discussed at each meeting.

June TAC Meeting Decision Summary

PRIOR MONTH	TAC DECISION POINTS	ACTION
June	What evaluation criteria do the TAC recommend for the pilot?	The TAC recommended evaluation criteria as revised and presented in Appendix 2 of the June briefing book addendum.
	How many participants should be involved in the pilot?	The TAC recommended using the sub-group framework (“matrix”) and directed the project team to analyze the sub-groups and present recommendations at the July meeting.
	How should participation be distributed throughout the state?	
	What non-mileage based accommodations does the TAC recommend testing in the pilot?	The TAC recommended studying and reporting on issues and recommendations for non-mileage based accommodations and policies after the pilot concludes, as part of the final pilot report to the Legislature.

Based on TAC Decisions Made to Date, the Road Charge Pilot Has the Following Parameters:

The pilot will offer drivers a choice in account managers	
	More than one non-state account manager will be available for pilot participants to choose from.
The pilot will offer drivers a choice in mileage recording methods	
	Methods under consideration for the pilot include time permits, mileage permits, odometer charges (prepay and postpay), automated distance charging without location information, and automated distance charging with location information.
Out-of-state vehicles will be included in the pilot and simulate payment for driving on California roads	
	Drivers from neighboring states who drive regularly in California will be recruited to participate in the pilot.
The pilot will test an open system design	
	Security standards and privacy protections will be required, and data content messaging formats between service providers and the state may be defined. However, the system will otherwise be designed in a way that is technology neutral and allows entry of multiple operational concepts, technologies, and service providers.
The pilot will test the interoperability of California's system with that of other states	
	In the event another state does not have a pilot operational concurrent with California's, interoperability will be simulated using account managers.

Based on TAC Decisions Made To Date, the Road Charge Pilot Has the Following Parameters (continued):

The pilot will include individuals, households, businesses, and at least one government agency	
	This represents the diversity of vehicle ownership types most common in California.
The pilot will include a cross-section of vehicles that are reflective of the fleet currently using California's public road network	
	The pilot will recruit a variety of vehicles with the goal of forming a vehicle pool that reflects the diversity of the fleet currently using California roads.
The pilot will offer methods to exempt miles driven on private roads or out of state	
	Both manual and automated options for claiming mileage exemptions will be tested.
The pilot will feature three approaches for protecting privacy: governance, accountability, and legal protection	
	The TAC will adopt privacy principles (governance), evaluation criteria (accountability), and recommended privacy protection provisions (legal protection).
The pilot will be evaluated according to criteria recommended by the TAC	
	The 50 evaluation criteria adopted by the TAC in June span 8 categories.

Decisions Schedule-at-a-glance

MONTH	TOPICS	TAC DECISION POINTS TO BE RAISED
July	Technical Design	How many participants should be involved in the pilot?
		How should participation be distributed throughout the state?
		What system data security features should be used in the pilot?
	Policy	Comprehensive review of TAC Decisions made to date
		What privacy principles and privacy protection provisions does the TAC recommend?
	Report to CalSTA	Feedback on report outline
August	Technical Design	What type of enforcement and compliance activities should be demonstrated during the pilot?
September	Policy	Address additional questions raised during the course of TAC meetings.
	Communications	Has the TAC adequately gathered, considered, and addressed public comment on pilot issues?
October	Policy	Address additional questions raised during the course of TAC meetings.
	Report to CalSTA	Feedback on draft report.
November	Report to CalSTA	Feedback on draft report.
December	Report to CalSTA	Adopt final report on recommendations to CalSTA.

Detailed Monthly Decision Schedule

July: Meeting #7

FOCUS TOPICS	RELATED SB 1077 STATUTE	TAC DECISION POINTS
Technical Design: Inputs to Technical Design	3090(e): The TAC shall study road charge alternatives to the gas tax…and shall make recommendations on the design of a pilot program… 3090(f) 8: In studying the road charge alternatives… the TAC shall take the following into consideration: and public and private agency access… to data collected and stored for purposes of road charging.	• How many participants should be involved in the pilot? • How should participants be distributed throughout the state? • What system data security features should be used in the pilot?
Business Case Analysis: Initial cost estimates for operational concepts	3090(f) 3-4: In studying the road charge alternatives… the TAC shall take the following into consideration: the cost of administering the collection of taxes and fees as an alternative to the current system of… fuel taxes.	Informational item
Policy: Review	Comprehensive review of TAC decisions to date	Informational item
Policy: Privacy principles and model privacy protection provisions	3090(f) 2, 6, 7, and 8: In studying the road charge alternatives… the TAC shall take the following into consideration: the necessity of protecting all personally identifiable information used in reporting highway use… the ease of re-identifying location data… increased privacy concerns when location data are used in conjunction with other technologies	• What privacy principles and privacy protection provisions does the TAC recommend?
Communications: Focus groups and comment matrix update	3090(e): The TAC shall gather public comment on issues and concerns related to the pilot program…	Informational item
Report to CalSTA: Draft outline	3090(e): The TAC shall make recommendations on the design of a pilot program….	• Feedback on report outline

August: Meeting #8

FOCUS TOPICS	RELATED SB 1077 STATUTE	TAC ACTIONS
Technical Design: Inputs to Technical Design	3090(e): The TAC shall study road charge alternatives to the gas tax…and shall make recommendations on the design of a pilot program…	• What type of enforcement and compliance activities should be demonstrated during the pilot?
Organizational Design: Update from inter-agency work group	3090(f) 4: In studying the road charge alternatives… the TAC shall take the following into consideration: the ease… of administering the collection of taxes and fees as an alternative to the current system of taxing highway use through motor vehicle fuel taxes.	Informational item only
Communications: Telephone survey and comment matrix update	3090(e): The TAC shall gather public comment on issues and concerns related to the pilot program…	Informational item

September: Meeting #9

FOCUS TOPICS	RELATED SB 1077 STATUTE	TAC ACTIONS
Policy: Review of parking lot items	3090(e): The TAC shall study road charge alternatives to the gas tax…and shall make recommendations on the design of a pilot program…	• Address additional questions raised during course of TAC meetings
Communications: Review of TAC public engagement efforts	3090(e): The TAC shall gather public comment on issues and concerns related to the pilot program…	• Has the TAC adequately gathered and considered public comment on issues related to the pilot program and addressed them?

October: Meeting #10

FOCUS TOPICS	RELATED SB 1077 STATUTE	TAC ACTIONS
Policy: Review of parking lot items	3090(e): The TAC shall study road charge alternatives to the gas tax…and shall make recommendations on the design of a pilot program…	• Address additional questions raised during course of TAC meetings
Report to CalSTA: Review of draft recommendations report to CalSTA	3090(e): The TAC shall study road charge alternatives to the gas tax…and shall make recommendations on the design of a pilot program. The TAC may also make recommendations on the criteria to be used to evaluate the pilot program.	• Feedback on draft outline

November: Meeting #11

FOCUS TOPICS	RELATED SB 1077 STATUTE	TAC ACTIONS
Report to CalSTA: Draft final recommendations report to CalSTA	3090(e): The TAC shall study road charge alternatives to the gas tax…and shall make recommendations on the design of a pilot program. The TAC may also make recommendations on the criteria to be used to evaluate the pilot program.	• Feedback on updated draft report

December: Meeting #12

FOCUS TOPICS	RELATED SB 1077 STATUTE	TAC ACTIONS
Report to CalSTA: Final recommendations report to CalSTA	3090(e): The TAC shall study road charge alternatives to the gas tax…and shall make recommendations on the design of a pilot program. The TAC may also make recommendations on the criteria to be used to evaluate the pilot program. Section 3091: Based on the recommendations of the [TAC], [CalSTA] shall implement a pilot program to identify and evaluate issues related to the potential implementation of a [road charge] program.	• Adopt final report on recommendations to CalSTA

Summary of Topics & Decisions To Satisfy Statutory TAC Requirements

3090 SECTION	TOPICS THAT WILL INFORM TAC DISCUSSION AND DECISIONS
(e) Study road charge alternatives	Policy, Technical Design, Business Case Analysis, Organizational Design
(e) Recommend pilot design alternatives	Policy, Technical Design, Report to CalSTA
(e) Gather public comment on issues & concerns	Public Input and Involvement
(e) Recommend evaluation criteria	Evaluation Strategy, Report to CalSTA
(f) (1) Availability	Technical Design
(f) (1) Adaptability	Technical Design
(f) (1) Reliability	Technical Design
(f) (1) Security	Technical Design
(f) (2) Necessity of protecting PII	Policy, Technical Design
(f) (3) Ease of recording & reporting highway use	Technical Design
(f) (3) Cost of recording & reporting highway use	Business Case Analysis
(f) (4) Ease of administering collection of charges	Organizational Design, Technical Design
(f) (4) Cost of administering collection of charges	Business Case
(f) (5) Effective methods of maintaining compliance	Technical Design, Organizational Design
(f) (6) Ease of re-identifying location data	Technical Design, Policy
(f) (7) Privacy concerns when using location data with other technologies	Technical Design, Policy
(f) (8) Public & private agency access to data	Organizational Design, Technical Design, Policy

Section 2:
Policy Decisions Overview

To be discussed with Agenda Item #8

Policy Overview for Meeting #7

This month the TAC will continue deliberations of the design considerations to inform the business case for road charging, with an emphasis on providing background information to support discussions around data security and privacy.

As shown in the Decision Schedule, this month, we would like to reach consensus on two policy questions:

1. **What system data security features should be used in the pilot?**
2. **What privacy principles and privacy protection provisions does the TAC recommend?**

In addition, the TAC will re-visit two questions from June as follows:

3. **How many participants should be involved in the pilot?**
4. **How should participants be distributed throughout the state?**

The following sections of this Briefing Book provide more detailed information on question one listed above, while the appendix provides background on question two. Presentations at the July TAC meeting and accompanying handouts, to be distributed the week before the meeting, will provide more detailed information on questions three and four.

Section 3:
Data Security in California's Road Charge Pilot Program

To be discussed with Agenda Item #12

Terms Used in This Briefing Book

The following general terms in this list are used throughout this briefing book. Additional data security terms are defined as they are introduced in this briefing book.

Account Manager—the authority responsible for a given user's account, either a Commercial Account Manager or a state agency.

Authorized user—a user who has some rights to access specified privileged and personal information on a system, typically having a username/password for the system.

Customer Service Representative (CSR)—an individual responsible for providing services to customers of account managers, usually via telephone.

Data security—protecting data, such as a database, from destructive forces and from the unwanted actions of unauthorized users.[1]

Mileage Meter (MM)—a device installed in a participant's vehicle that reports miles driven to the Account Manager.

Information Technology (IT) Administrator—a member of an IT department with the rights and responsibility to manage the overall function of a given IT system.

[1] Summers, G. Data and databases. In: Koehne, H Developing Databases with Access: Nelson Australia Pty Limited, p. 4-5, 2004.

Terms Used in This Briefing Book (continued)

Participant—a volunteer motorist who will participate in California's Road Charge Pilot Program.

Personally Identifiable Information (PII)—information that can be used on its own or with other information to identify, contact, or locate a single person, or to identify an individual in context.

Usage-based Insurance (UBI)—car insurance with rates based on driving data.

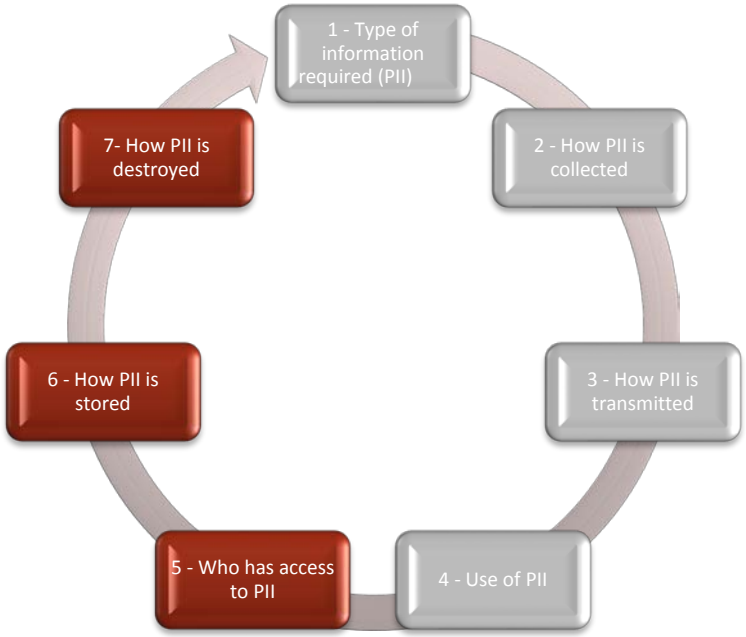
User—an individual that uses or attempts to use a given system.

Vehicle Identification Number (VIN)—a vehicle serial number, unique to every vehicle manufactured.

Introduction and Relationship to Privacy

As noted on the previous page, **data security** means protecting data, such as a database, from destructive forces and from the unwanted actions of unauthorized users.

Data security is also a more technical complement to privacy policy concepts introduced in May. On the figure below, privacy policy questions are grayed out, while data security questions, the focus of this month's briefing book, are shown in red below (items 5, 6, and 7).



Data Security Questions that Require TAC Recommendations

The highlighted terms in the following questions for the TAC's consideration will be defined in the coming pages. Specific recommendations for addressing each question are also provided.

- What user **Authentication** measures should be required in the pilot?
- What user **Authorization** measures should be required in the pilot?
- What **Data Modification Notification** measures should be required in the pilot?
- What **Data Masking** measures should be required in the pilot?
- What **Encryption** measures should be required in the pilot?
- What **Data Storage** security measures should be required in the pilot?
- What **Data Transmittal** security measures should be required in the pilot?
- What **Data Destruction** measures should be required in the pilot?
- What **General IT Network Security** measures should be required in the pilot?

Main Components of Data Security

The main components of data security are the following.[2] Representative examples are provided for some components to help explain how people commonly may hear about or experience these components in daily computer usage.

Authentication

- Authentication is the process used to verify that users (people or devices) are who they say they are.[3]
  - Representative example: Username/Password.

Authorization

- While authentication means verifying "you are who you say you are," authorization means verifying "you are permitted to do what you are trying to do". Authentication is thus a prerequisite for authorization.[4]
  - Representative example: strongly defined authorized user and administrator roles and permissions.

[2] Hiner, J. Security hinges on authentication, authorization, and encryption. TechRepublic: August 14, 2002. Available at: http://www.techrepublic.com/article/security-hinges-on-authentication-authorization-and-encryption/
[3] Op. cit. 2.
[4] Wikipedia. Authentication. Downloaded on June 27, 2015. Available at: https://en.wikipedia.org/wiki/Authentication.

Encryption

- In cryptography, encryption is the process of encoding messages or information in such a way that only authorized parties can read it. Encryption involves encoding a message with a special number called a key. Encryption does not prevent a message being intercepted, but denies the message content to the interceptor.[5]
  - Representative Example: the encryption protocol standard called Advanced Encryption Standard (AES). It is now commonly executed in using a 256-bit encryption key, and thus referred to as 256-bit AES.

[5] "Encryption Basics | EFF Surveillance Self-Defense Project." Encryption Basics | EFF Surveillance Self-Defense Project. Surveillance Self-Defense Project, n.d. Web. 06 Nov. 2013. <https://ssd.eff.org/tech/encryption>.

Additional Components of Data Security

There are several processes beyond encryption, authentication, and authorization that support data security. Below are the most important ones.

Data Modification Notification

- This involves notification of users that their file(s) (including all component data) has (have) changed.
  - Representative example: an email from a company saying that your account has changed.

Data Masking

- Data masking is hiding sensitive original data with random characters or data.
  - Representative example: a credit card number appearing as XXXX XXXX XXXX 1234 on websites or apps.

Data Storage

- Data Storage security involves applying the above principles (authentication, authorization, encryption), and other measures to ensure that all data on a computer system are stored securely.

Additional Components of Data Security (continued)

Data Transmittal

- Applying the principles of secure data storage to data transmission: using authentication, authorization, and encryption to transmit PII / secure data from one system to another.

Data destruction

- Data destruction requires erasing all data (overwriting data, including associated files or database records, with meaningless information).
- This is more secure than simply “deleting” data, which typically means that only the beginning of a file is erased.

General IT network security

- General IT network security encompasses all means by which information and services are protected from unintended or unauthorized access, change, or destruction.[6]
  - Representative examples: firewalls, intrusion detection, anti-virus, anti-malware.

[6] "Reliance spells end of road for ICT amateurs", The Australian, May 07, 2013,

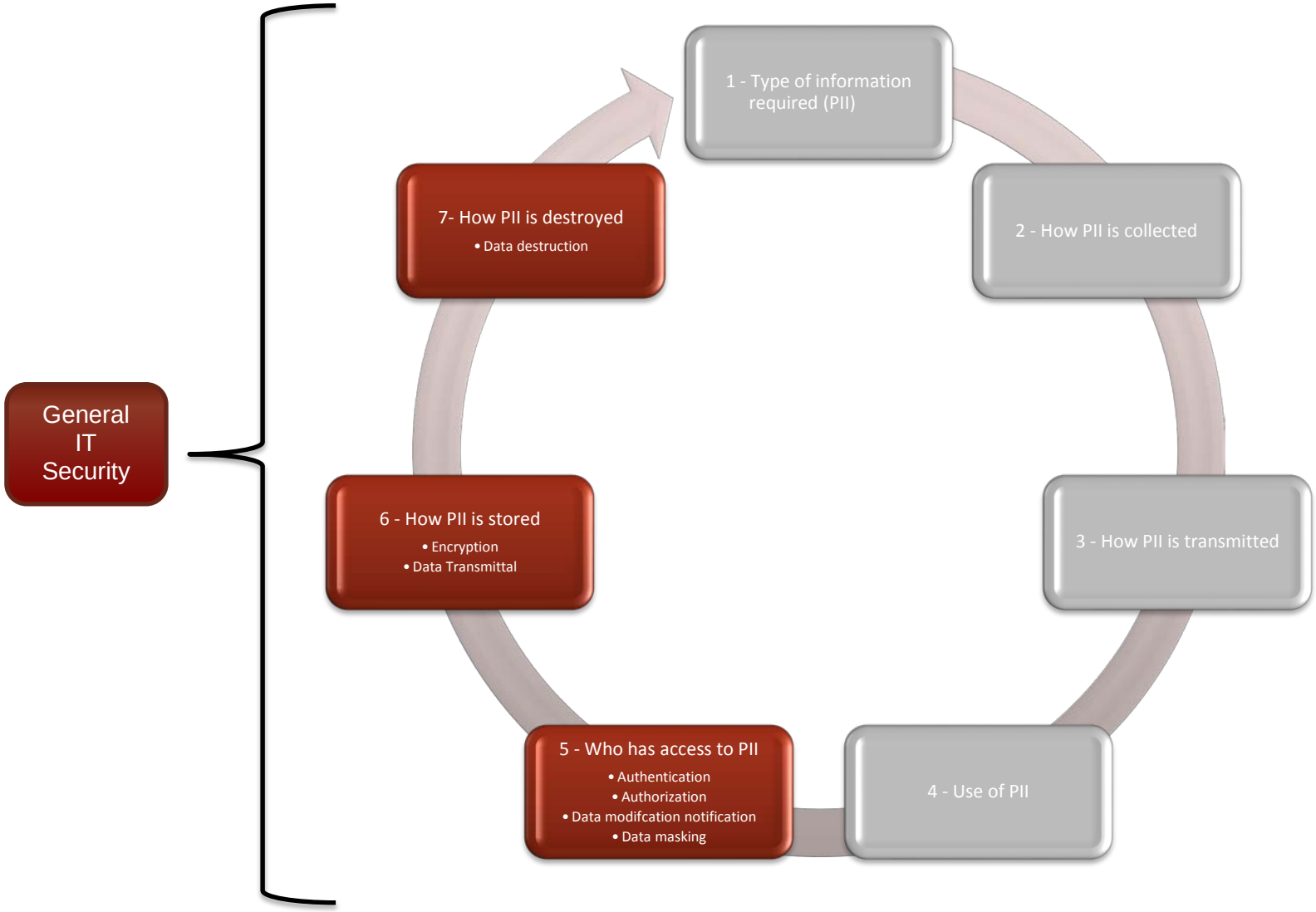
Data Security Needs in the Pilot

- During the pilot, **all PII**, including name, address, phone, payment, etc., need to be protected to guarantee privacy and security of all pilot participants.
- **Location data** may or may not be PII, depending on whether it can be associated with an individual or not. It should always be protected to guarantee privacy.
- **Data that is neither PII nor location data** should still be treated according to standard network security practices, but will not explicitly be addressed in this briefing book.

Data Security in the Road Charging System Architecture

- Security must be ensured in each block and in each link of the system architecture.
- Recall System Architecture from March Briefing Book:
  - Mileage Reporting: the subsystem that reports data from the vehicle to the account manager, including in-vehicle devices. The mileage reporting subsystem will not be used for manual methods such as the time permit or the odometer charge, as these do not require the use of vehicular data or in-vehicle electronics.
  - Account Management: the subsystem that takes in mileage data, updates participant accounts, sends invoices to customers, receives payment from customers, sends payments to the state, and reports road charge data to account management oversight. Account managers accept input from motorists choosing manual methods directly.
  - Account Management Oversight: the subsystem that takes road charge data from the account management subsystem and verifies that all account managers are paying appropriate sums of money to the state each month and that all account managers are abiding by the rules of the program.
- At the end of each subsection of this briefing book, a slide illustrates how the security elements discussed in that subsection relate to each block and link of the following architecture.

Where the Data Security Components Fit in the Cycle of Privacy



5 – Who Has Access to PII

The security of PII rests on restricting access to such information only to those authorized system users (such as customer service representatives) who have the rights to access it. Two components of data access control are authentication and authorization:

1. Authentication – verifying all authorized system users (participants, administrators, devices, or programs) are who they say they are.

- The key policy is requiring a username and password for all authorized users.
  - Strict password policies increase the likelihood of data protection from unauthorized access (password strength, maximum time of validity).

2. Authorization – verifying "you are permitted to do what you are trying to do."

- Every authorized user will be assigned a "user role."
  - A user role may correspond to a job function, like Customer Service Representative.
  - Each user role would be assigned different rights—rights to access certain data. Users of a role without rights to a given data set would be denied access to that data.
  - IT administrators may have many rights to work on the system that other user types not have (e.g., to install and delete software), but they may not have the right to view PII.
- To enforce, there should be a clearly documented data security policy describing user roles and their respective rights.
  - The data security policy describes who has what access to which PII.
  - There should be occasional auditing/checking to verify that these roles are enforced.

Authorization in Depth: User Roles and Related Policies

Example User Roles

- Enforcement
  - Enforcement Officers may only have rights to enter a license plate number to determine road charge registration status of vehicle, operational concept, and payment status.
- Account Management
  - CSRs may only have rights to create, view, and/or modify accounts. For accounts on Automated Distance Charge, CSRs may also have rights to view mileage data in order to support dispute resolution.
- Account Management Oversight
  - Accountant/Auditors may only have rights to view aggregate data from CAMs and individual data on anomalies. In addition, in cases of suspected noncompliance or fraud, accountants/auditors may be able to request detailed data of individuals.

Access control records

- Databases automatically record name of authorized user who accesses data and when.

Personnel policy

- A strong personnel policy is necessary to ensure data access controls are strictly obeyed.
- Criminal and possibly financial background checks for users in various roles.
- Retaining personnel records of infractions: one major infraction or several minor infractions leads to dismissal.

Additional Controls on Data Access

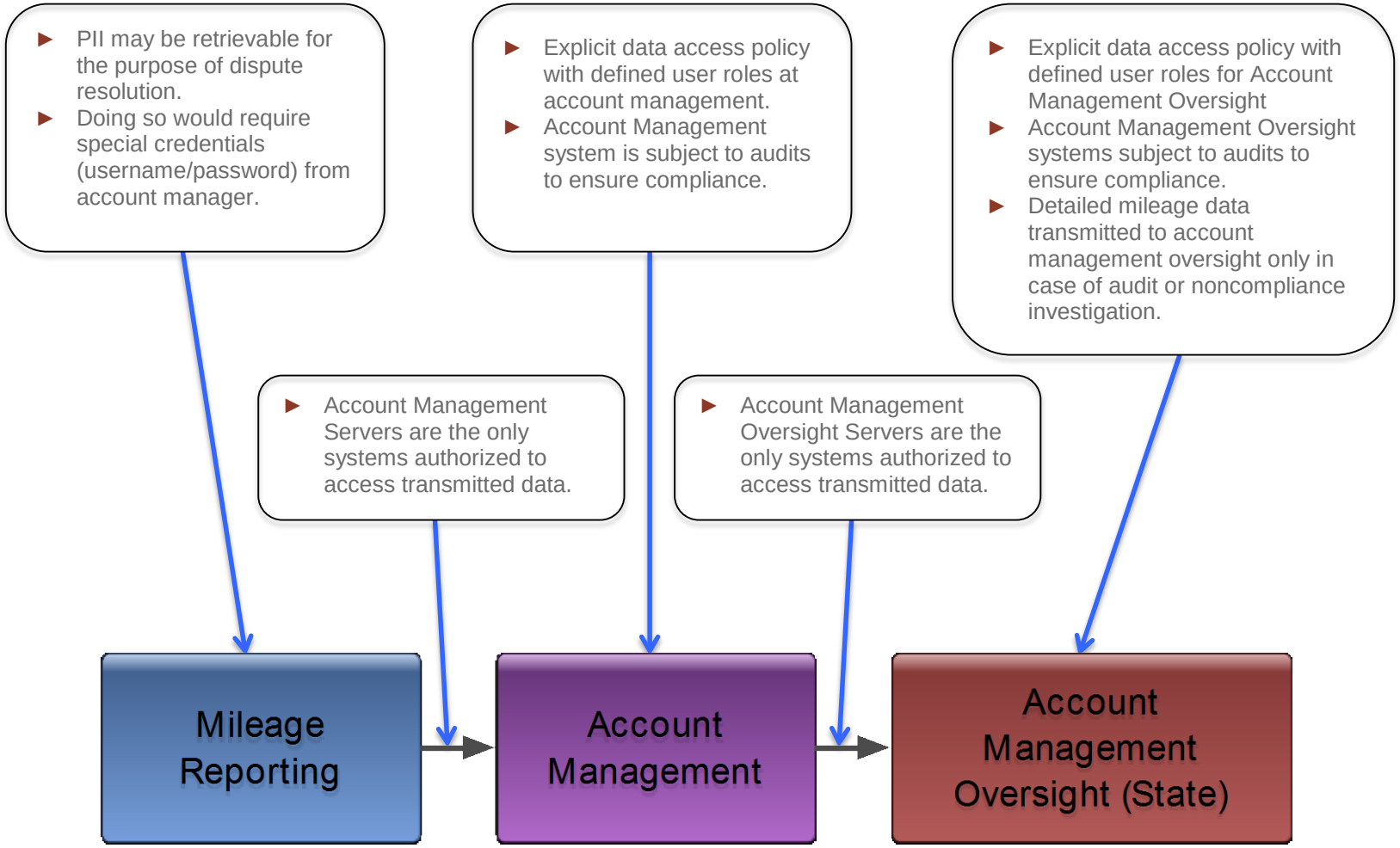
Data Modification Notification

- When significant information is changed on a participant account, the given participant should receive an automatic notification that their sensitive data (PII) has changed.
  - If the participant did not request the change, they can have the agency or Commercial Account Manager (CAM) investigate the change, and change the password or other security code on the account to prevent the unwanted access from recurring.
- Typical means of notification are e-mail, text message, and automated phone call.
  - Participants could be allowed to choose their preferred method of contact.

Data Masking

- Data Masking means hiding sensitive original data with random characters or data, such as when your credit card number appears XXXX XXXX XXXX 1234 on a payment website or smartphone app.
- For example, CSRs cannot view masked data.
- Typically, payment methods are masked, such as when your credit card number appears XXXX XXXX XXXX 1234.
- A CSR can view a payment card number when entering it, to verify that it has been entered correctly; once entered, it is permanently masked.

Who Has Access to PII in System Architecture Diagram



Recommendations: Data Access

- What user **Authentication** measures should be required in the pilot?
  - Minimum of 8-character passwords, letters and numbers, one capital.
- What user **Authorization** measures should be required in the pilot?
  - For pilot project, employ user roles with limited rights to PII access. Provide at least user roles of CSR, Enforcement, and Accountant/Auditor.
- What **Data Modification Notification** measures should be required in the pilot?
  - Require data modification notification to participant (primary account holder in the case of vehicle fleets) via e-mail or text message.
- What **Data Masking** measures should be required in the pilot?
  - At a minimum, mask all means of simulated payment and VINs.

6 – How PII Is Stored and Transmitted

This topic covers how PII is stored and transmitted. Data collected for the purposes of road charging may be stored on in-vehicle devices like smartphones and other Mileage Meters (MMs), as well as on servers that are maintained by CAMs and the state agency administering the road charge. In order to collect the road charge, those data must be transmitted between entities including the in-vehicle device, CAM/state servers, and various customer interfaces such as websites or mobile apps.

- Data must be securely stored and transmitted.
  - For the Automated Distance Measurement methods, we propose using UBI standards for the transmission from the vehicle to the Account Manager during the pilot, including strong encryption on all links, as well as secure storage of data.
  - For other internet-based interfaces, such as payments and reporting of odometer readings, we propose using HTTPS, a secure data exchange standard commonly used on the internet for exchange of secure information.
- The key to secure data storage is encryption.
  - Encryption is the process of encoding messages or information in such a way that only authorized users can read it. Encryption does not of itself prevent a message being intercepted, but denies the message content to the interceptor.[7]
  - 256-bit Advanced Encryption Standard (AES) is a common industry standard.

[7] Op. cit. 3.

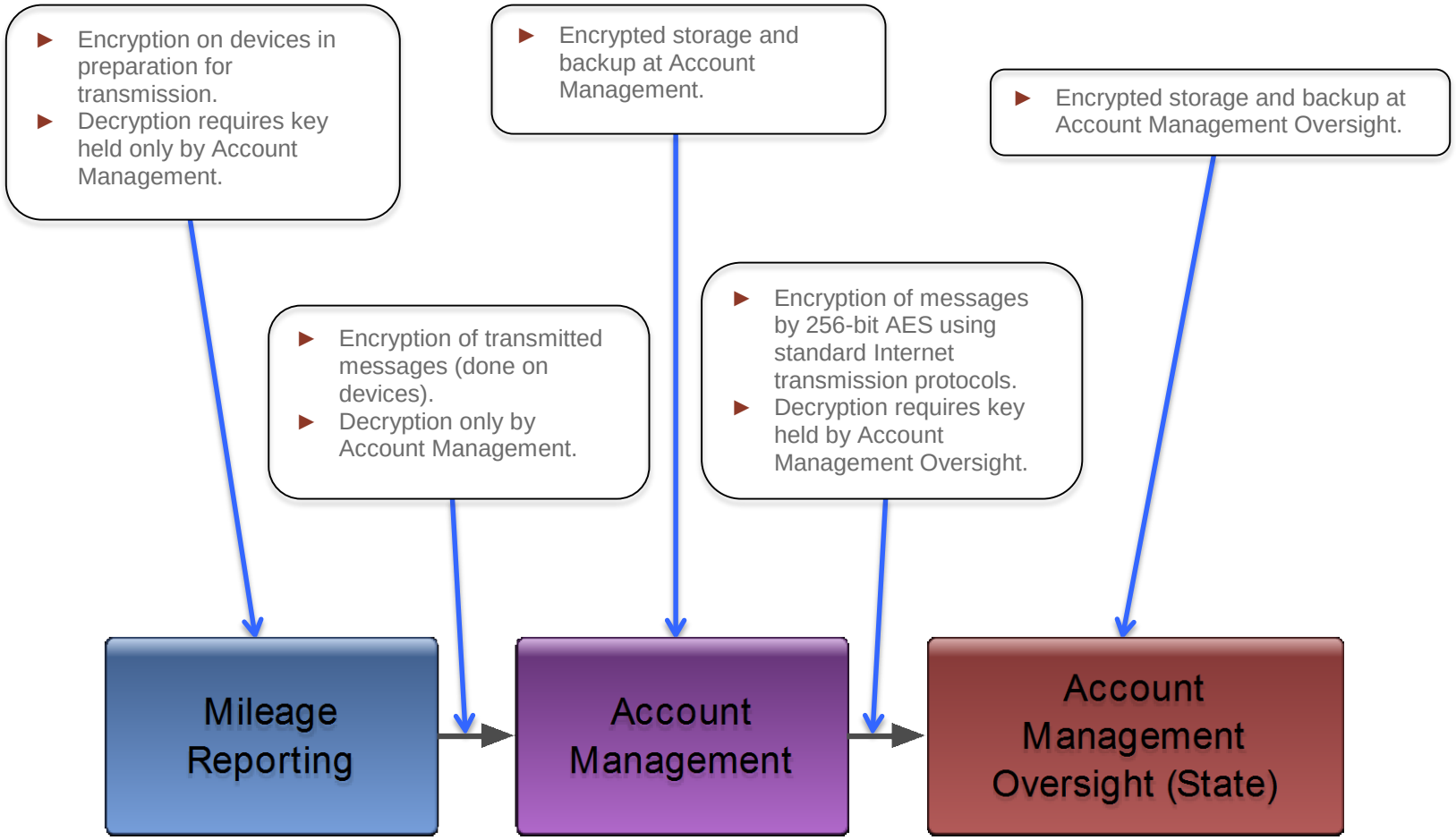
- Backup/archived data should also be encrypted.

How Location Data Are Stored and Transmitted

This section applies only to the Automated Distance Reporting (general location) operational concept.

- The most private way to store location data is to retain the data only in mileage "buckets." Mileage buckets are aggregate values of mileage driven, such as the following:
  - Miles driven in state on public roads
  - Miles driven out of state
  - Total miles driven
- In order to assign mileage to the correct bucket, specific location data will need to be transmitted from Mileage Meters (MMs) to Account Managers. Transforming specific location data (which may include latitude/longitude points) into mileage buckets requires "map matching," which means comparing the data points with boundaries on a digital map. Typical MMs do not have the memory or computing power to perform map matching, which is why the Account Manager handles this computation in the back office.
- The lifecycle of detailed location data is as follows:
  - Detailed location data are generated by the MM (Mileage Reporting).
  - The MM encrypts detailed location data and transmits it to the Account Manager.
  - The Account Manager destroys detailed location data as soon as the map matching process takes place and miles are assigned to buckets (see next subsection).
- Optionally, account managers could allow users to opt out of the destruction of detailed location data, so they could view their own usage, or so that data could be anonymized (de-identified) and used for research purposes.
  - Any information transmitted back to the MM should be encrypted as well, even though it will not contain PII.

How PII Is Stored and Transmitted in System Architecture Diagram



Recommendations: Data Storage and Data Transmittal

- What **Encryption** measures should be required in the pilot?
  - Use 256-bit AES encryption.

- What **Data Storage** security measures should be required in the pilot?
  - Use 256-bit AES to encrypt primary and backup data.
  - At Account Manager and Account Management Oversight, store location data only in Mileage buckets.

- What **Data Transmittal** security measures should be required in the pilot?
  - Use mileage buckets to transmit mileage data to CAMs.
  - Use 256-bit AES for encryption.
  - Use HTTPS for internet-based secure data exchange.

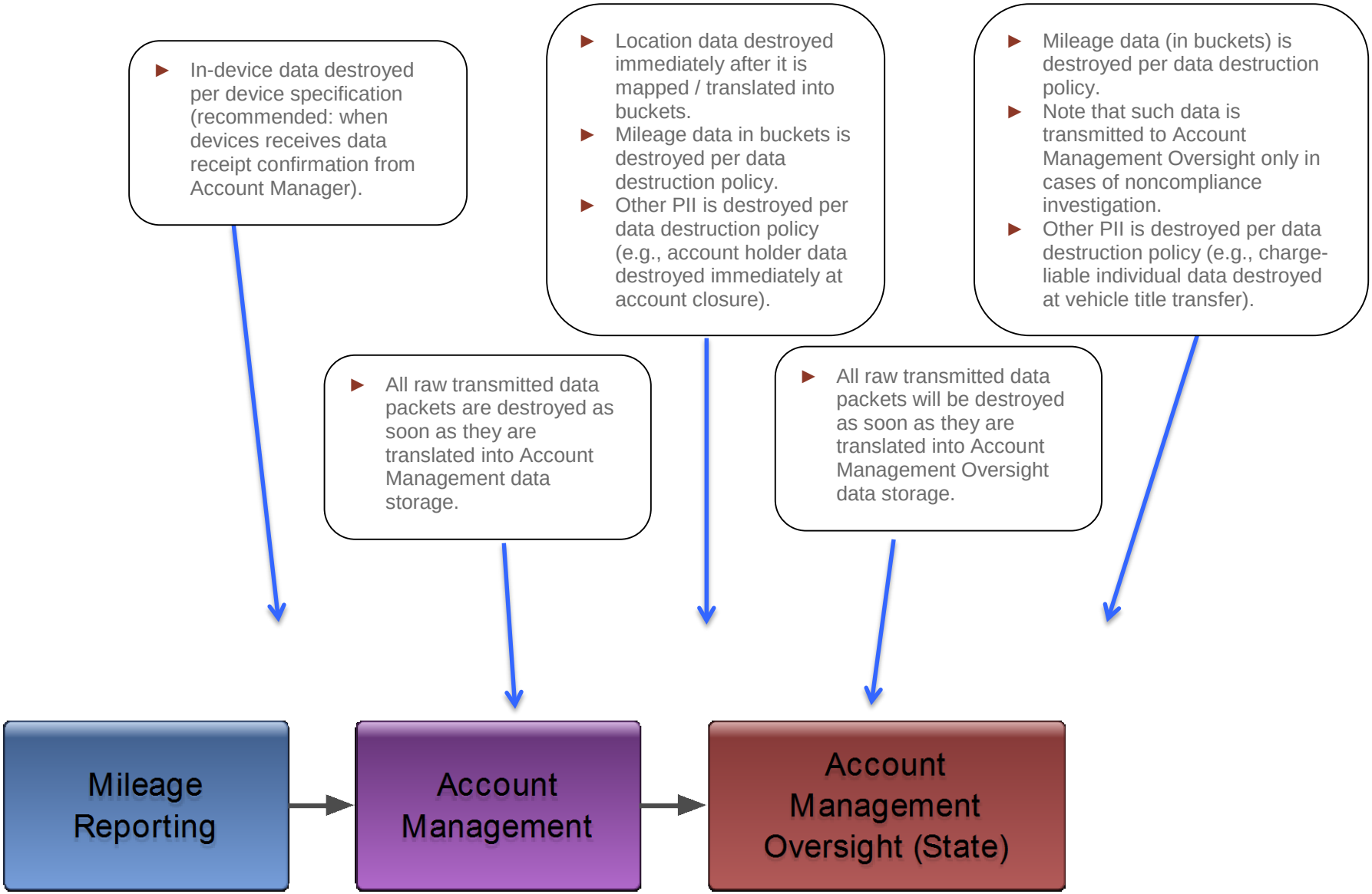
7 – How PII Is Destroyed

- PII data needs to be erased, not just deleted.
  - When data or files are “deleted” they are removed from a computer’s active memory, but the data are usually still retrievable, even by relatively unskilled individuals.
  - To make data inaccessible in the future, they must be overwritten or erased.
  - To be destroyed, data must also be erased from backups / archives.
- Mileage data – miles by user by day – and by zone for Automated Distance Measurement (general location) – are among the most sensitive data.
  - The law that created the Oregon Road Usage Charging Program includes provisions for mileage data destruction that were developed in collaboration with the Oregon chapter of the American Civil Liberties Union (ACLU).
  - These provisions require that mileage data be destroyed within 30 days after latest of the following:
    - Payment processing
    - Dispute resolution
    - Noncompliance investigation
- Most data destruction will occur at Account Management:
  - Account Management Oversight will only get detailed mileage data in case of a noncompliance investigation.
  - General/aggregate information may be retained longer for accounting and auditing purposes.

Data Destruction in the Pilot

- The TAC may want to allow private vendors to offer longer data retention based on user preference (opt-in) to support optional value-added services.
- For the purposes of the pilot only, the TAC may wish to support opt-in for a longer period to support evaluation and research activities related to the project.
- Data destruction on devices may differ from data destruction on computer systems.
  - The most secure standard is to destroy data on devices immediately when data receipt is acknowledged by the Account Manager (when the device is certain that the Account Manager has successfully received the data). This approach is recommended for the pilot.
  - In an operational road charging system, data logs on devices could be retained longer so users can access these logs in case of a dispute.

How PII Is Destroyed in System Architecture Diagram



Recommendations: Data Destruction

- What **Data Destruction** measures should be required in the pilot?
  - Opt-in option for all participants to preserve data for purposes of pilot data analysis.
  - For those who do not opt in, destroy mileage data stored on servers within 30 days after latest of:
    - Simulated payment processing,
    - Simulated dispute resolution, or
    - Simulated noncompliance investigation.
  - For those who do not opt in, destroy mileage data stored on Mileage Meters (MMs) immediately upon successful receipt by account management servers.

General IT Network Security

The overall computer system must be secure for the data policies to be effective. Otherwise, a hacker could potentially gain access to the system and violate the data security policies in place.

The following list includes some of the most important IT network security elements, but this list is not comprehensive:

- **Firewall** is a software system that controls the incoming and outgoing network traffic based on an applied rule set. A firewall typically establishes a barrier between a trusted, secure internal network and another network (e.g., the Internet) that is assumed not to be secure and trusted.[8]
- **Intrusion detection** – detects unauthorized access to a system.
- **Policies to protect against "Social engineering" attacks such as phishing** – in IT security, the term "social engineering" refers to psychological manipulation of people to share their username/password or other secure information, or install software that opens the system to intruders, so these are policies to train employees not to fall for phishing or similar attacks.
- **Antivirus** – programs frequent scans for self-replicating malicious software such as viruses and Trojans.

[8] Oppliger, Rolf (May 1997). "Internet Security: FIREWALLS and BEYOND". *Communications of the ACM* **40** (5): 94.

- **Anti-malware** – program to defend against other malicious software.

International Standards Organization (ISO) 27000

- ISO 27000 is a worldwide family of standards, which, taken together, constitute a significant benchmark for measuring a computer system as secure. The most important are ISO 27001 and ISO 27002.
  - ISO 27001 covers organizational aspects of security, including:
    - Information security leadership and high-level support for policy;
    - Planning an information security management system; risk assessment; risk treatment; and
    - Making an information security management system operational.
  - ISO 27002 covers overall best practices for information security management, such as:
    - Human Resource Security,
    - Asset Management,
    - Access Control,
    - Cryptography, and
    - Physical and environmental security.
  - There are now over 20 standards in the ISO 27000 family.
- To be certified ISO 27000 compliant requires a rigorous certification process that can be quite lengthy. Due to time and budget constraints, such a certification will not be possible before the pilot, but it will be possible for vendors to leverage existing ISO 27000 compliant systems.

Recommendations: General IT Network Security

- What **General IT Network Security** measures should be required in the pilot?
  - Use ISO 27000 best practices:
    - ISO 27000 system certification and audits will not be possible during the pilot.
    - Vendors may be asked to self-report any significant deviations from ISO 27000 best practices, so the pilot team may review and determine if they are acceptable.

Data Security Recommendations Summary

- **Authentication**: minimum of 8-character passwords, letters and numbers, one capital, require periodic password change.
- **Authorization**: for pilot project, employ user roles with limited rights to PII access. Provide at least user roles of CSR, Enforcement, and Accountant/Auditor.
- **Data Modification Notification**: require data modification notification to motorist or primary account holder (in the event of vehicle fleets) via e-mail or text message.
- **Data Masking**: at a minimum, mask all means of simulated payment and VINs.
- **Encryption**: use 256-bit AES encryption.
- **Data Storage**: Use 256-bit AES to encrypt primary and backup data; at Account Manager and Account Management Oversight, store location data only in Mileage buckets.
- **Data Transmittal**: use mileage buckets to transmit mileage data to CAMs; use 256-bit AES for encryption.
- **Data Destruction**:
  - Opt-in option for all participants to preserve data for purposes of pilot data analysis.
  - For those who do not opt in, destroy mileage data within 30 days after latest of:
    - Simulated payment processing,
    - Simulated dispute resolution, or
    - Simulated noncompliance investigation.
  - Data on devices destroyed when data receipt confirmation received from acct. manager.

- **General IT Network Security**: use ISO 27000 best practices (although full system certification and audits will not be possible during the pilot).

Section 4: California Road Charge Pilot Program Privacy Protections

To be discussed during Agenda Item #13

Review of Earlier TAC Decisions

At the May TAC meeting, the Committee was briefed on personal privacy protections related to transportation and vehicle technologies, then considered the question: what specific personal privacy protections should be used for the pilot?

The May 2015 TAC decisions and direction included:

1. Draft California Road Charge Privacy Principles, to be presented for final adoption at the July TAC meeting.
2. Direct the Independent Evaluator to measure the pilot program's performance against the privacy evaluation criteria presented in at the May 2015 TAC meeting; and against Privacy Principles to be adopted by the TAC.
3. Develop and recommend Road Charge Privacy Legal Protection Provisions for review and comment by the TAC prior to proposed adoptions at the July 2015 TAC meeting.

Additional privacy protection measures may be considered after the TAC is briefed on Enforcement Measures at their August 2015 meeting.

Road Charge Privacy Protection Principles

If adopted by the TAC, these proposed Privacy Protection Principles will govern all decisions throughout the full road charge program lifecycle: design, implementation, operations, independent evaluation and wind down of pilot program activities).

PROPOSED California Road Charge Privacy Protection Guiding Principles:

1. The Road Charge pilot must at all times recognize and respect an individual's interests in privacy and information use pursuant to Section 1 of Article I of the California Constitution.
2. The Road Charge must offer motorists a time-based system of paying for road use, as an alternative payment method for individuals concerned about disclosing their mileage driven.
3. The Road Charge must allow motorists choice in how mileage will be reported.
4. The Road Charge system must be designed, implemented and administered in a manner transparent to the public and to individual motorists.
5. The Road Charge system must comply with applicable federal and state laws governing privacy and information security.
6. Personal information required for the Road Charge system must not be disclosed to any persons or entities without motorists' consent, specific statutory authority authorizing disclosure, appropriate legal process, or emergency circumstances as defined in law.

Road Charge Privacy Protection Principles (continued)

7. The Road Charge system must not collect information beyond what is needed to properly calculate, report and collect the road charge, unless the motorist provides his or her consent.
8. Road Charge system data retained beyond the period of time necessary to ensure proper mileage account payment must have all personal information removed, and may only be used for public purposes (i.e., improve the safety and efficiency of the traveling public).
9. Motorists who choose to release personal information must provide their consent in a clear, unambiguous and written manner.
10. The Road Charge system must not require use of specific locational information, including specific origins or destinations, travel patterns or times of travel.
11. The Road Charge system must allow motorists an opportunity to view all personal data being collected and stored to ensure only data required for proper accounting and payment of road charges is being collected and retained.
12. The Road Charge system must investigate all potential errors identified by motorists and make all corrections to ensure road charge records remain accurate.

Privacy Accountability Measures: Privacy Evaluation Criteria

These criteria will be used to evaluate the pilot program's performance against the adopted set of specific privacy protection criteria. **The TAC previously adopted these criteria at their June 2015 meeting**.

Goals	Source	Evaluation Criteria
Honor personal privacy	CTIP	User perception of privacy protections
Protect personally-identifiable information (PII)	SB 1077 (f)(2)	Sufficiency of PII protection measures
Ensure identity protection using location data even after removal of PII	SB 1077 (f)(6)	Sufficiency of identify protection using location data after PII removal
Ensure privacy protection when using location data with other technologies	SB 1077 (f)(7)	Sufficiency of privacy protection measures when using location data with other technologies
Protect privacy pursuant to Article I Section 1 of the California Constitution with respect to data access by public agencies (including law enforcement) and private firms	California Constitution and SB 1077(f)(8)	Sufficiency of privacy protection measures re: California Constitution
		Appropriateness of data retention
		Compliance of data retention
Respect user privacy trade-offs		User valuation of privacy

Privacy Accountability Measures: Data Security Evaluation Criteria (continued)

Goals	Source	Evaluation Criteria
Honor personal privacy (data security)	CTIP	User perception of data security
▸ Ensure data are secure from external breaches ▸ Ensure data are secure from internal breaches ▸ Ensure data are secure from abuse based on internal process exposure		Ability of system to withstand breaches of attacks
		Protection of data
		Availability of data for appropriate and necessary uses
		Conformity with relevant ISO 9000 data security standards
		Conformity with relevant ISO 27001 data security standards

Road Charge Privacy Protection Provisions

The TAC directed development of model legal provisions to specifically protect privacy in California's Road Charge program, consistent with Section 1(i) of SB 1077. Since the TAC cannot unilaterally enact these privacy protections in law, and since these are not proposed for legislative or agency enactment prior to commencing the pilot project, the TAC intends to simulate these model privacy protection provisions and test their effectiveness during the pilot. If successful, these provisions could serve as a useful reference point for action by the California legislature, adoption by a state agency via rulemaking, or incorporation into contractual terms with future road charge private vendors.

With the TAC's acquiescence, these Privacy Protection Provisions were influenced by these sources:

- Key provisions found in **SB 1077, authorizing the Road Charge pilot program**.
- **TAC committee discussions** and direct TAC member input.
- Key provisions found in California's **Electronic Toll Collections law**.
- Key provisions found in California **SB 34 (2014)** by Sen. Hill, related to **use of locational data**.
- Key provisions found in California's **Online Privacy Protection Act**.
- All of the TAC-recommended **Road Charge Privacy Principles**.
- **Best practices from other jurisdictions** that have specific privacy protections in a road charge program.
- **Data Security provisions** recommended for TAC adoption at the July 2015 meeting.

** Due to its length, the draft of the model Privacy Protection Provisions are found in Appendix 1.

Appendix 1: California Road Charge Privacy Protection Provisions

California Road Charge Privacy Protection Provisions

Section Index:

Section 1. Findings and Intent
Section 2. Definitions
Section 3. Motorist choice of road charge reporting methods
Section 4. Non-mileage based road charge methods must be provided
Section 5. Disclosure of data to be collected by road charge software and devices
Section 6. Limitations on the collection and reporting of personal information
Section 7. Express written permission required to collect location information and share other personal information
Section 8. Road charge information and data to be de-identified wherever possible
Section 9. Duty to protect personal information
Section 10. Limitation on the disclosure and transmission of personal information
Section 11. Road charge data is confidential, not subject to disclosure
Section 12. Record of access to motorists' account information
Section 13. Data security requirements
Section 14. Disclosure and notice of security breach
Section 15. Limitation on the retention of data and requirement for data destruction
Section 16. Motorists' right to inspect records
Section 17. Establishment of privacy policy required
Section 18. Penalties for willful breach
Section 19. Internal audit and certification of compliance

SECTION 1. Findings and intent

The privacy protection provisions in this Act are based on the following findings and declarations:

(a) The road charge pilot must at all times recognize and respect an individual's interests in privacy, information use, and civil liberties pursuant to Section 1 of Article I of the California Constitution. {Privacy Principle 1}; {SB 34 (2014), 1798.90.51 (b)(1).}

(b) Experience to date in other states across the nation demonstrates that mileage-based charges can be implemented in a way that ensures data security and maximum privacy protection for drivers. {SB 1077}

(c) Any exploration of alternative revenue sources shall take privacy implications into account, especially with regard to location data. Trip origins, destinations, times of travel and routes shall not be reported, and legal and technical safeguards shall protect personal information. {SB 1077}

(d) The practice of bundling user fees for roads and highways into the gas tax makes it difficult for motorists to understand the amount they are paying for roads and highways. {SB 1077}

(e) The road charge system must be designed, implemented and administered in a manner transparent to the public and to individual motorists. {Privacy Principle 4}

SECTION 2. Definitions

The following terms and definitions shall apply to this Act:

(a) "Breach of the security of the system" means unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of personal information maintained by the department or a road charge account manager. Good faith acquisition of personal information by an employee or agent of the department or road charge account manager for the purposes of administering road charges is not a breach of the security of the system, provided that the personal information is not used or subject to further unauthorized disclosure. {CA Online Privacy Protection Act}

(b) "Department" means the department of transportation, the department of motor vehicles and any other state department designated by the legislature or the California state transportation agency to participate in the administration of a road charge program.

(c) "General location data" means information about whether a vehicle has traveled on taxable roadways within the state of California.

(d) "Mileage recording" means the act or process of measuring and storage vehicle mileage driven.

(e) "Mileage reporting" means the act or process of transmitting vehicle mileage driven data.

(f) "Motorist" means a person who drives a vehicle and is subject to road charge payment, recording or reporting, whether or not that person is the registered owner.

(g) "Personal information" means any information about an individual which, on its own or when combined with other information, is reasonably capable of revealing the identity or activities of a specific person. Personal information includes, but is not limited to: trip making details, address, telephone number, email address, license plate number, driver's license number, California identification card number, account number, social security number, photograph, bank account information, or credit card number.

For purposes of this Act, "personal information" does not include publicly available information that is lawfully made available to the general public from federal, state, or local government records.

(h) “Public purposes” means research, testing and information gathering that advances the safety of the motoring public and the adequate preservation, maintenance and upkeep of public roadways.

(i) “Registered owner of a vehicle” has the same meaning as [cite to CA law that defines owners to include lessees].

(j) “Road charge” means a fee collected from the registered owner of a vehicle that is paid in lieu of the per-gallon retail price of motor fuel attributable to state motor fuel taxes.

(k) “Road charge account manager” means a public agency or private vendor that has been certified by the state of California to administer the collection of road charge payments from registered vehicle owners.

(l) “Specific location data” means information about the origin, destination, waypoint, or specific route of travel of a motor vehicle.

SECTION 3. Motorist choice of road charge mileage reporting methods

(a) The road charge system must allow motorists to choose from at least two methods for how vehicle mileage will be reported for road charge tax accounting purposes. {Privacy Principle 3}

(b) In providing mileage-reporting options, the road charge system must provide at least one method that does not require use of general or specific locational information, including specific origins or destinations, trip frequencies or times of travel. {Privacy Principle 10}

SECTION 4. Non-mileage based road charge methods must be provided

(a) In addition to the methods provided under section 3 of this Act, the road charge system must offer motorists a time-based method of paying for road use, as an alternative payment method for motorists concerned about disclosing their vehicle mileage driven. {Privacy Principle 2}

(b) The time-based road charge method must not require any personal information beyond that required to legally register a motor vehicle under [cite to state motor vehicle registration requirements]. {TAC Meeting Discussions}

SECTION 5. Disclosure of data to be collected by road charge software and devices

(a) Any third-party provider of software, devices or mechanisms offered for motorists' use in recording or reporting vehicle mileage traveled for purposes of calculating road charges must clearly and fully disclose all known information and data that such software, devices or mechanisms are intended to record or report. This disclosure must be given to motorists:

(1) at the time of motorists' initial selection of road charge reporting methods;

(2) when software, devices or mechanisms are provided to the motorist for use; and

(3) at least annually, as part of the transmittal of an account manager's road charge privacy policy, required under section 17 of this Act. {Privacy Principle 4}

(b) In lieu of subsection (a) of this section, automotive manufacturers that offer their customers with optional road charge reporting services that utilize in-vehicle telematics technologies may provide disclosure of data recording and reporting capabilities in the owners' manual that is provided with the original purchase of the vehicle; or upon the motorist's activation or subscription to the optional road charge reporting services.

(c) In providing motorists the choice of road charge reporting methods as required in section 3(a) of this Act, the department and any road charge account manager authorized by the state to

administer or collect road charges must provide a clear description of the type of personal information and data that is required for each reporting method, and must provide a comparison of the benefits and personal privacy-related tradeoffs for each of the available reporting methods. This information must be provided prior to a motorist's selection of a road charge payment method. {TAC Meeting Discussions}

SECTION 6. Limitations on the collection and reporting of personal information

(a) The Road Charge system shall not collect any personal information beyond what is necessary to properly calculate, report and collect the road charge, unless the motorist provides his or her express written consent for the collection of additional information in a manner consistent with section 7 of this Act. {Privacy Principle 7} {CA Information Practices Act, Civil Code section 1798} {SB 1077}

(b) Road charge reporting methods shall not record or report specific location data, including origins, destinations, waypoint locations, trip frequencies or times of travel unless a motorist specifically consents to the recording or reporting of such location data in a manner consistent with section 7 of this Act. {SB 1077} {Privacy Principle 10}

(c) Road charge reporting methods may record or report general location data as that term is defined in section 1 of this Act, provided:

(1) the motorist chooses that specific reporting method;

(2) proper disclosure of the reporting method was made pursuant to section 5 of this Act; and

(3) the motorist specifically consents to the reporting of general location in a manner consistent with section 7 of this Act.

SECTION 7. Express written permission required to collect location information and to share other personal information

Motorists who consent to the release of personal information, or who consent to the recording or reporting of general or specific location data must provide their consent in a clear, unambiguous and written manner. {Privacy Principle 9}

SECTION 8. Road charge information and data to be de-identified wherever possible

(a) Road charge system data retained beyond the period of time necessary to ensure proper mileage account payment must have all personal information removed, and may only be used for public purposes as defined in section 2(h). {Privacy Principle 8}

(b) This section does not prohibit the department or a road charge account manager from providing aggregated traveler information derived from collective data that relates to a group or category of persons from which personal information has been removed. {CA ETC law, Streets and Highway Code section 31490}

(c) If the department or a road charge account manager provides aggregated or de-identified data for public purposes, the department or road charge account manager must first consider the ease of re-identifying location data, even when personal information has been removed from the data, before authorizing release of that data for public purposes. {SB 1077}; {TAC discussions}

SECTION 9. Duty to protect personal information

The chief information technology officer for each department with responsibility to administer the road charge system in whole or part, and any road charge account manager, has an affirmative public duty to:

(a) Ensure that road charge information is protected with reasonable operational, administrative, technical, and physical safeguards to ensure its confidentiality and integrity;

(b) Implement and maintain reasonable security procedures and practices in order to protect road charge information from unauthorized access, destruction, use, modification, or disclosure; and

(c) Implement and maintain a usage and privacy policy as specified in section 17 of this Act in order to ensure that the collection of road charge information is consistent with respect for individuals' privacy and civil liberties. {SB 34 (2014) relating to locational privacy}

SECTION 10. Limitation on the disclosure and transmission of personal information

(a) Personal information required for the road charge system shall not be disclosed to any persons or entities without (1) motorists' consent, (2) specific statutory authority authorizing disclosure, (3) appropriate legal due process, or (4) emergency circumstances as defined in law. {Privacy Principle 6}

(b) Personal information may be provided for the following purposes:

(1) The department and a road charge account manager may exchange personal information for the purpose of facilitating the motorist's choice in method of road charge payment, setup of the motorist's road charge account, and managing the accounting and collection of charges. {Oregon SB 810}

(2) (A) The department or a road charge account manager may make personal information of a person available to a law enforcement agency only pursuant to a search warrant. Absent a provision in the search warrant to the contrary, the law enforcement agency shall immediately, but in any event within no more than five days, notify the person that his or her

records have been obtained and shall provide the person with a copy of the search warrant and the identity of the law enforcement agency or peace officer to whom the records were provided. {CA ETC law, Streets and Highways Code section 31490 (e)(1)} {SB 1077}

(B) This section does not prohibit a peace officer, [as defined in Section 830.1 or 830.2 of the Penal Code], when conducting a criminal or traffic collision investigation, from obtaining personal information of a person if the officer has good cause to believe that a delay in obtaining this information by seeking a search warrant would cause an adverse result, as defined in [subparagraphs (A) to (E), inclusive, of paragraph (2) of subdivision (a) of Section 1524.2 of the Penal Code.] {CA ETC law, Streets and Highways Code section 31490 (e)(2)}

(3) This section does not prohibit the department or a road charge account manager from performing financial and accounting functions such as billing, account settlement, enforcement, or other financial activities required to operate and manage the road charge system. This section does not prohibit the sharing of data between state agencies, road charge public agencies in other states, and their road charge account managers for the purpose of properly accounting for mileage or allocation of road charge revenue between those state agencies or account managers. {CA ETC law, Streets and Highways Code section 31490 (i)}

(4) This section does not prohibit the department or a road charge account manager from communicating, either directly or through a contracted third-party vendor, to motorists enrolled in the road charge system about products and services offered by the agency, a business partner, or the entity with which it contracts for the system, using personal information limited to the subscriber's name, address, and electronic mail address, provided that the department or road charge account manager has received the motorist’s express written consent to receive the communications. {CA ETC law, Streets and Highways Code section 31490 (j)}

SECTION 11. Road charge data is confidential, not subject to disclosure

Personal information acquired for testing, development or operation of a road charge system is specifically exempt from California's public disclosure law, [cite to code]. {Privacy Principle 6}

SECTION 12. Record of access to motorists' account information

If the department or a road charge account manager accesses, or provides access to a motorist's account information, the department or a road charge account manager shall maintain a record of that access. At a minimum, the access control log shall include all of the following:

(a) The date and time the information is accessed;

(b) The license plate number, VIN number or other data elements used to query the road charge database or system;

(c) The person who accesses the information; and

(d) The purpose for accessing the information.

{CA SB 34 of 2014, relating to locational privacy, section 1798.90.52}

SECTION 13. Data security requirements

Road charge system data must be secured to ensure the protection of privacy and the integrity of road charge data collected. The department or a road charge account manager must establish information and data security standards and practices that represent best information technology industry practices, including data encryption and conformity with applicable ISO data security standards. {SB 1077}

SECTION 14. Disclosure and notice of security breach

(a) Any agency or road charge account manager that owns, manages, receives or transmits personal information obtained from motorists enrolled in the road charge system must disclose any breach of the security of the system following discovery or notification of the breach in the security of the data to any resident of [California] whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person. The disclosure shall be made in the most expedient time and manner possible and without unreasonable delay, consistent with the legitimate needs of law enforcement, as provided in [section 1798.29 of the California Civil Code], or any measures necessary to determine the scope of the breach and restore the reasonable integrity of the data system.

(b) Requirements for disclosure of data security breaches must conform to the provisions of [California Civil Code Section 1798.29 and 1798.82.] {CA SB 34 (2014) relating to locational privacy}

SECTION 15. Limitation on the retention of data and requirement for data destruction

(a) Road charge system data retained beyond the period of time necessary to ensure proper mileage account payment must have all personal information removed, and may only be used for public purposes as defined in section 2(h) of this Act. {Privacy Principle 8}

(b) The department or a road charge account manager, within practical business and cost constraints, may store only personal information of a person such as, to the extent applicable, the account name, credit card number, billing address, vehicle information, and other basic account information required to perform account functions such as billing, account settlement, or enforcement activities. All other information shall be discarded no more than 30 days after payment processing, dispute resolution for a single reporting period or a non-compliance investigation, whichever period is latest. The department and road charge account managers

shall destroy data related to the location and daily mileage use of any subject vehicle after the billing cycle has concluded, the bill has been paid, and all road charge disputes or violations, if applicable, have been resolved. {CA ETC law, Streets and Highways code section 31490}; {*Oregon SB 810, Section (4)(b)*}

(c) The department or a road charge account manager shall make every effort, within practical business and cost constraints, to purge the personal account information of an account that is closed or terminated. In no case shall the department or a road charge account manager maintain personal information more than 30 days after the date an account is closed or terminated. {CA ETC law, Streets and Highways code section 31490}

SECTION 16. Motorists' right to inspect records

(a) The road charge system must be designed, implemented and administered in a manner transparent to the public and to individual motorists. {Privacy Principle 4}

(b) The road charge system must allow motorists an opportunity to view all personal data being collected and stored to ensure only data required for proper accounting and payment of road charges is being collected and retained. {Privacy Principle 11}

(c) The department or a road charge account manager must publish the process by which a motorist may review and request changes to any of his or her personal information. {CA ETC law, Streets and Highways code section 31490 (b)(5)}

SECTION 17. Establishment of privacy policy required

(a) The department and all road charge account managers providing services to the state must establish, publish and adhere to a usage and privacy policy. The usage and privacy policy shall be available in writing, and shall be posted conspicuously on the department and road charge account managers' Internet website.

(b) The usage and privacy policy shall, at a minimum, include all of the following:

(1) The authorized purposes for collecting road charge information.

(2) A description of the employees and independent contractors who are authorized to access road charge system data and to collect personal information. The policy shall identify the training requirements necessary for those authorized employees and independent contractors.

(3) A description of how the use of road charge data collection will be monitored to ensure compliance with all applicable privacy laws and a process for periodic system audits, including any audits of the system access log required to be maintained under section 12 of this Act.

(4) A description of reasonable measures that will be used to ensure the accuracy road charge information and a process to correct data errors.

(5) A description of how the department and road charge account managers will comply with the security procedures and practices implemented and maintained pursuant to section 13 of this Act.

(6) The length of time road charge data and account information will be stored or retained.

(7) The official custodian of road charge system data and information, and which employees and independent contractors have the responsibility and accountability for implementing this section.

(8) The purpose of, and process for, sharing or disseminating road charge system information with other persons, whether by the department or road charge account managers in accordance with this Act, or by motorists through their express written consent pursuant to section 7 of this Act. {CA SB 34 (2014) relating to locational privacy, section 1798.90.51(b)(1).}

SECTION 18. Penalties for willful breach of duty

(a) In addition to any other sanctions, penalties, or remedies provided by law, an individual who has been harmed by a violation of this Act may bring a civil action in any court of competent jurisdiction against a person who knowingly caused that violation.

(b) The court may award a combination of any one or more of the following:

(1) Actual damages, but not less than liquidated damages in the amount of two thousand five hundred dollars ($2,500).

(2) Punitive damages upon proof of willful or reckless disregard of the law.

(3) Reasonable attorney's fees and other litigation costs reasonably incurred.

(4) Other preliminary and equitable relief as the court determines to be appropriate. {CA SB 34 (2014) relating to locational privacy, section 1798.90.54}

SECTION 19. Internal Audit and Certification of Compliance

The department and any road charge account manager shall adopt a comprehensive compliance program that is designed to ensure compliance with all provisions of this Act. The department’s internal auditor, and a road charge account manager’s internal or external auditor as the case may be, must include in their annual audit report a certification of compliance with the provisions of this

Act. The certification of compliance must be made annually, and must be made available to the public on the department or road charge account manager's internet web site.