Data Security in California's Road Charge Pilot Program

Matthew Dorfman

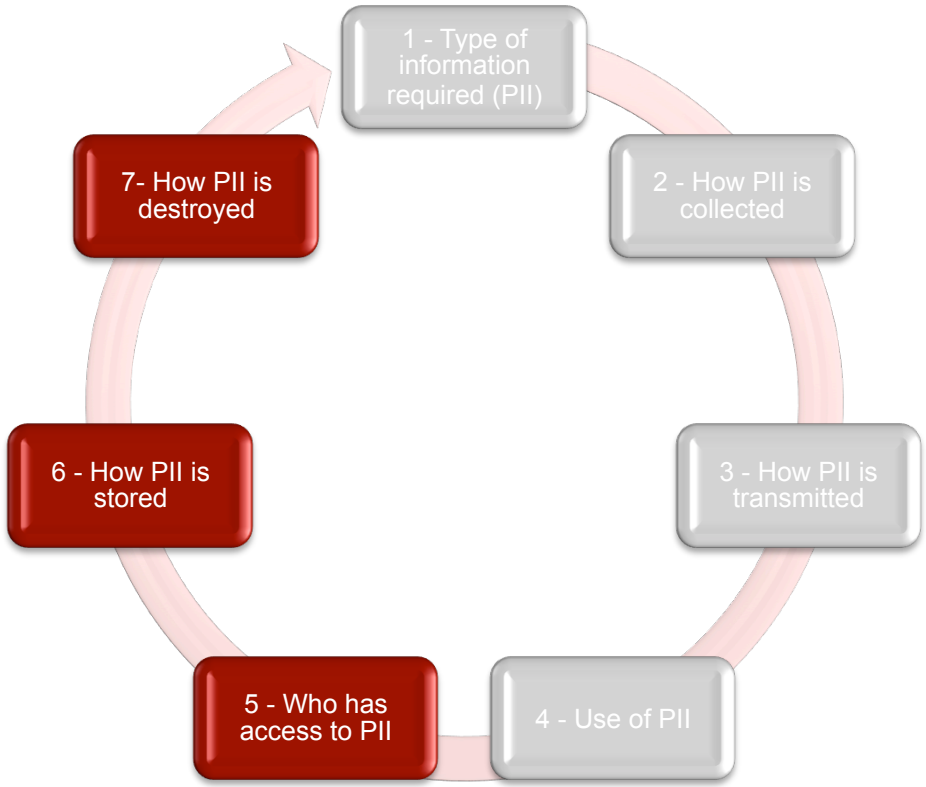
Agenda Item #12
TAC Meeting #7, July 24, 2015
South Lake Tahoe, CA

D'ARTAGNAN CONSULTING
The cutting edge of transport thinking

© D'Artagnan Consulting LLP

Introduction

- **Data security** means *protecting data from destructive forces and from the unwanted actions of unauthorized users.*
- It is the technical complement to privacy.

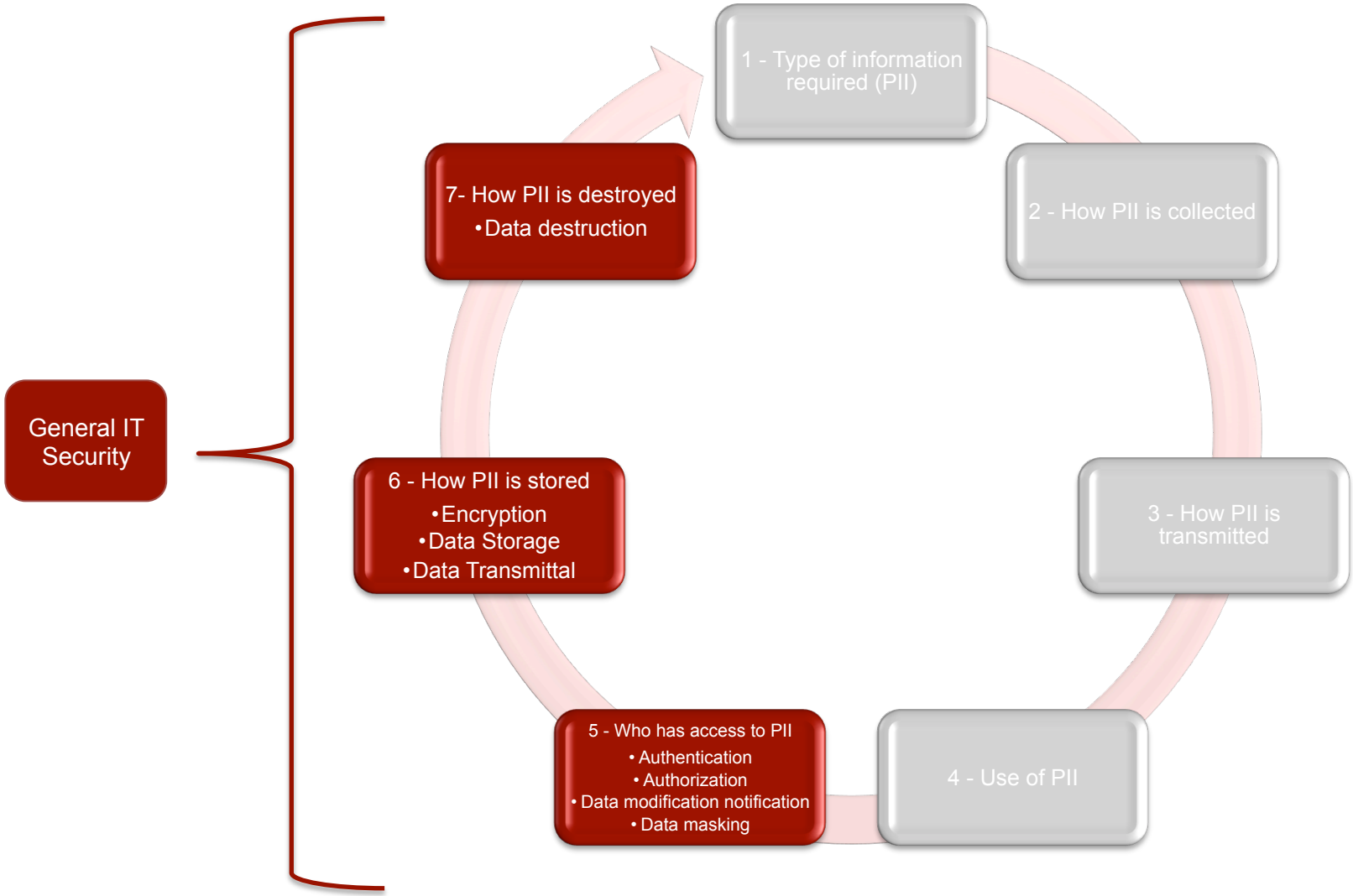


TAC Recommendations Needed on Data Security Questions in the Following Areas

- Authentication
- Authorization
- Data Modification Notification
- Data Masking
- Encryption
- Data Storage
- Data Transmittal
- Data Destruction
- General Information Technology (IT) Network Security

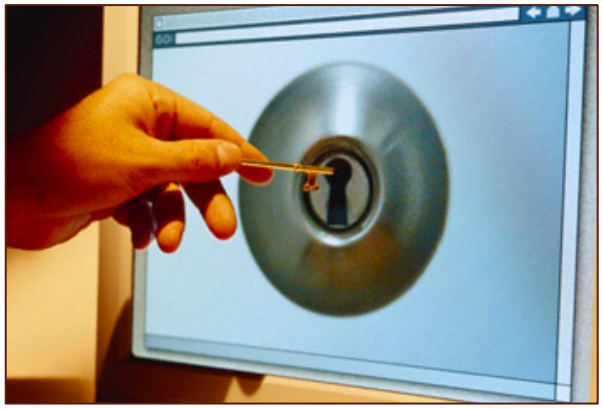
© D'Artagnan Consulting LLP

Data Security in the Cycle of Privacy



Who has Access to PII?

- Authentication
  - Verifying that users are who they say they are
  - Example: Username/Password
  - Strict password policies improve data security (password strength, maximum time of validity)



- Authorization
  - Verifying users are permitted to do what they are trying to do
  - Implemented via user roles with limited access to sensitive data
  - Example User Roles: Enforcement Officer, Customer Service Representative, Accountant/Auditor

© D'Artagnan Consulting LLP

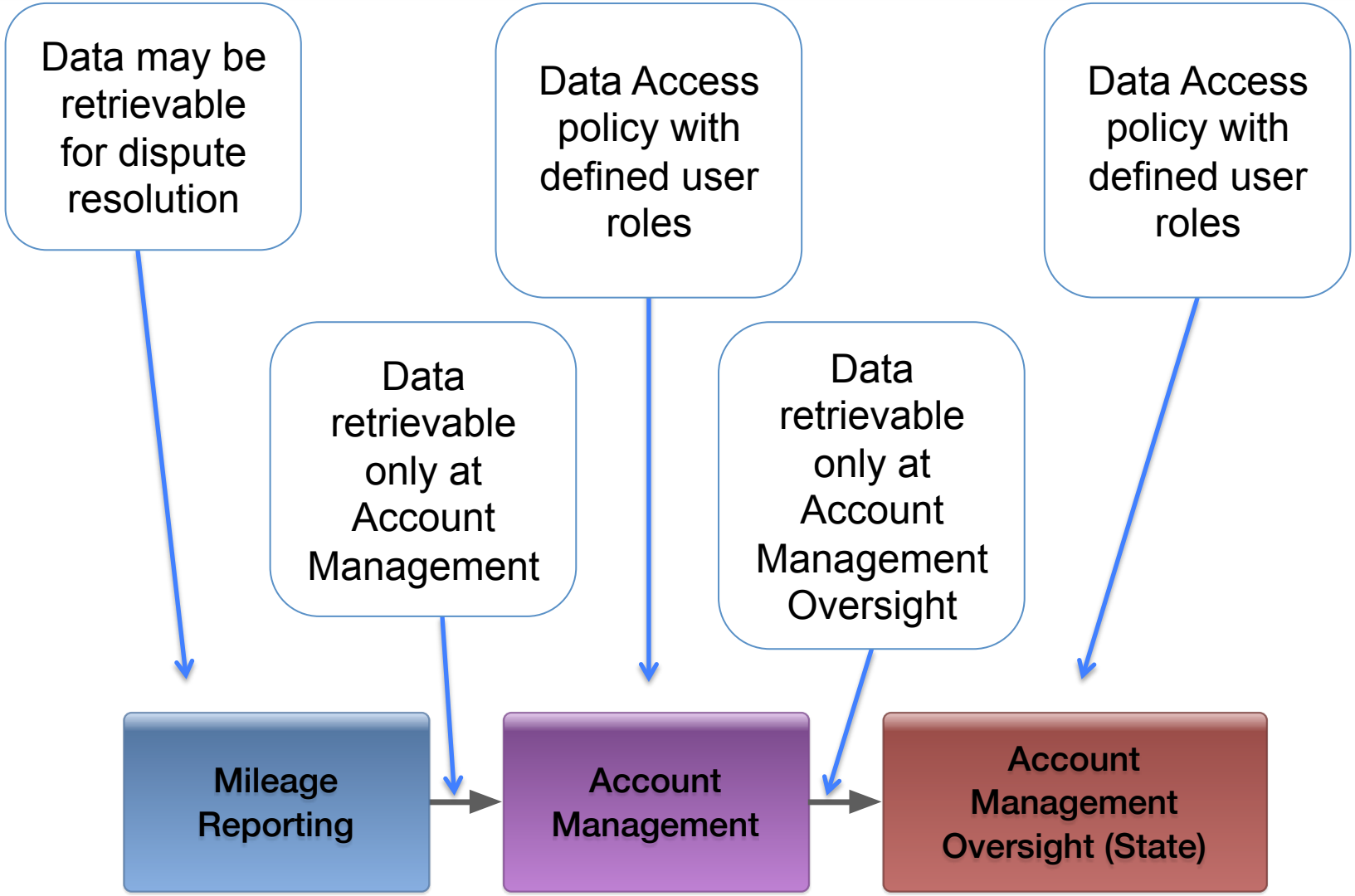
Who has Access to PII? (continued)

- Data Modification Notification
  - Notifying users that their data has changed
- Data Masking
  - Hiding sensitive original data with random characters or data.

- Strong access control records, personnel policy required

© D'Artagnan Consulting LLP

Who Has Access to PII in System Architecture Diagram



Recommendations: Data Access

- **Authentication:**
  - Have minimum of 8-character passwords, letters and numbers, one capital
- **Authorization:**
  - Have 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 participant via e-mail or text message
- **Data Masking:**
  - Mask all means of simulated payment and VINs

© D'Artagnan Consulting LLP

How PII Is Stored and Transmitted

- Data must be securely stored and transmitted.
  - For Automated Distance Measurement, use UBI standards
  - For other internet-based interfaces, use HTTPS

- The key to secure data storage is encryption.
  - Encoding information so that only authorized parties can read it
  - Example: 256-bit Advanced Encryption Standard (AES)
  - Backup/archived data should also be encrypted

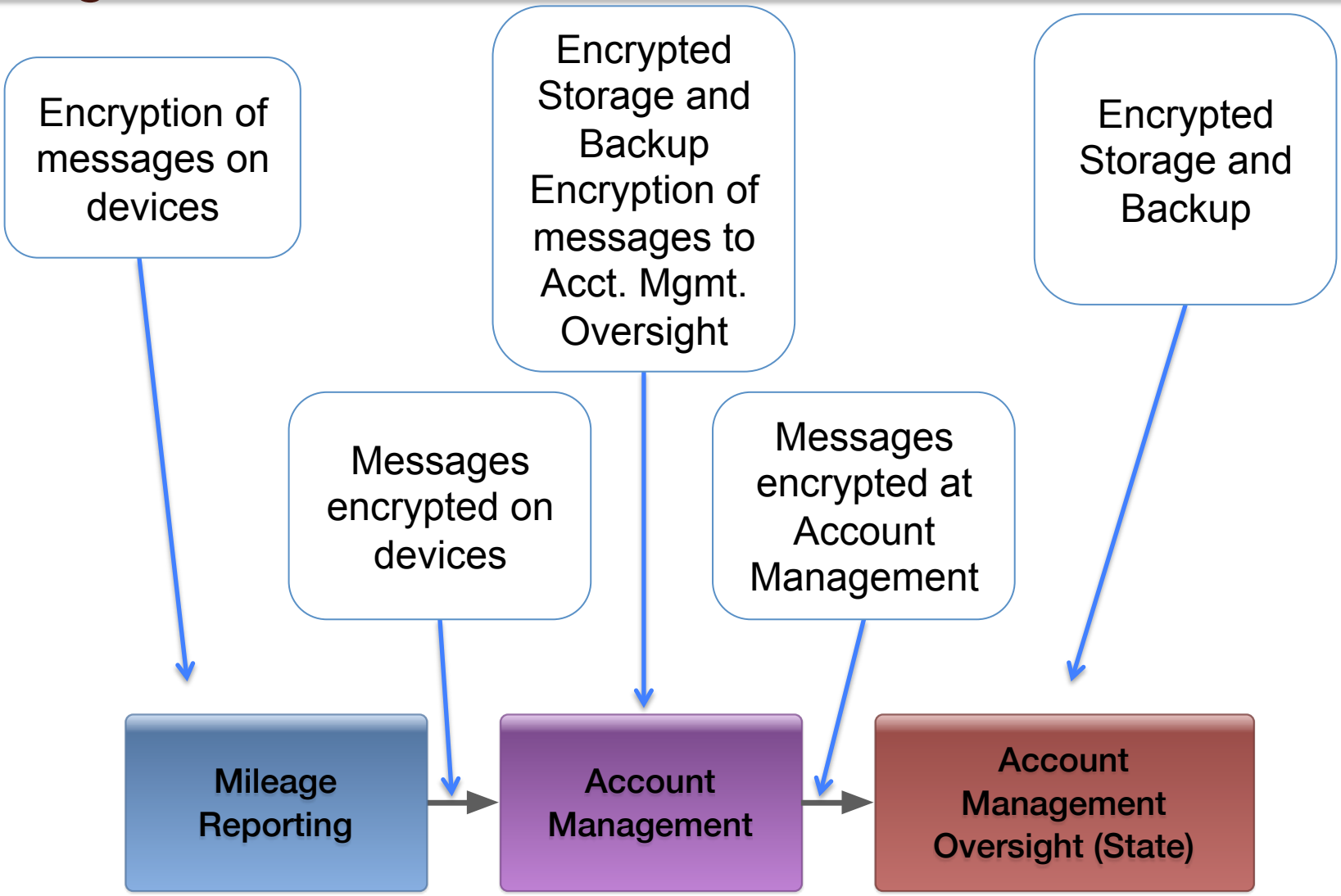
How Location Data Are Stored and Transmitted

For Automated Distance Reporting (general location) only

- Most private way to store location data: mileage "buckets"
  - Miles driven in state on public roads
  - Miles driven out of state
  - Total miles driven
- Specific location data will be transmitted from Mileage Meters (MMs) to Account Managers.
- Optionally, participants may opt out of specific location data destruction.

© D'Artagnan Consulting LLP

How PII Is Stored and Transmitted in System Architecture Diagram



© D'Artagnan Consulting LLP

Recommendations: Data Storage and Data Transmittal

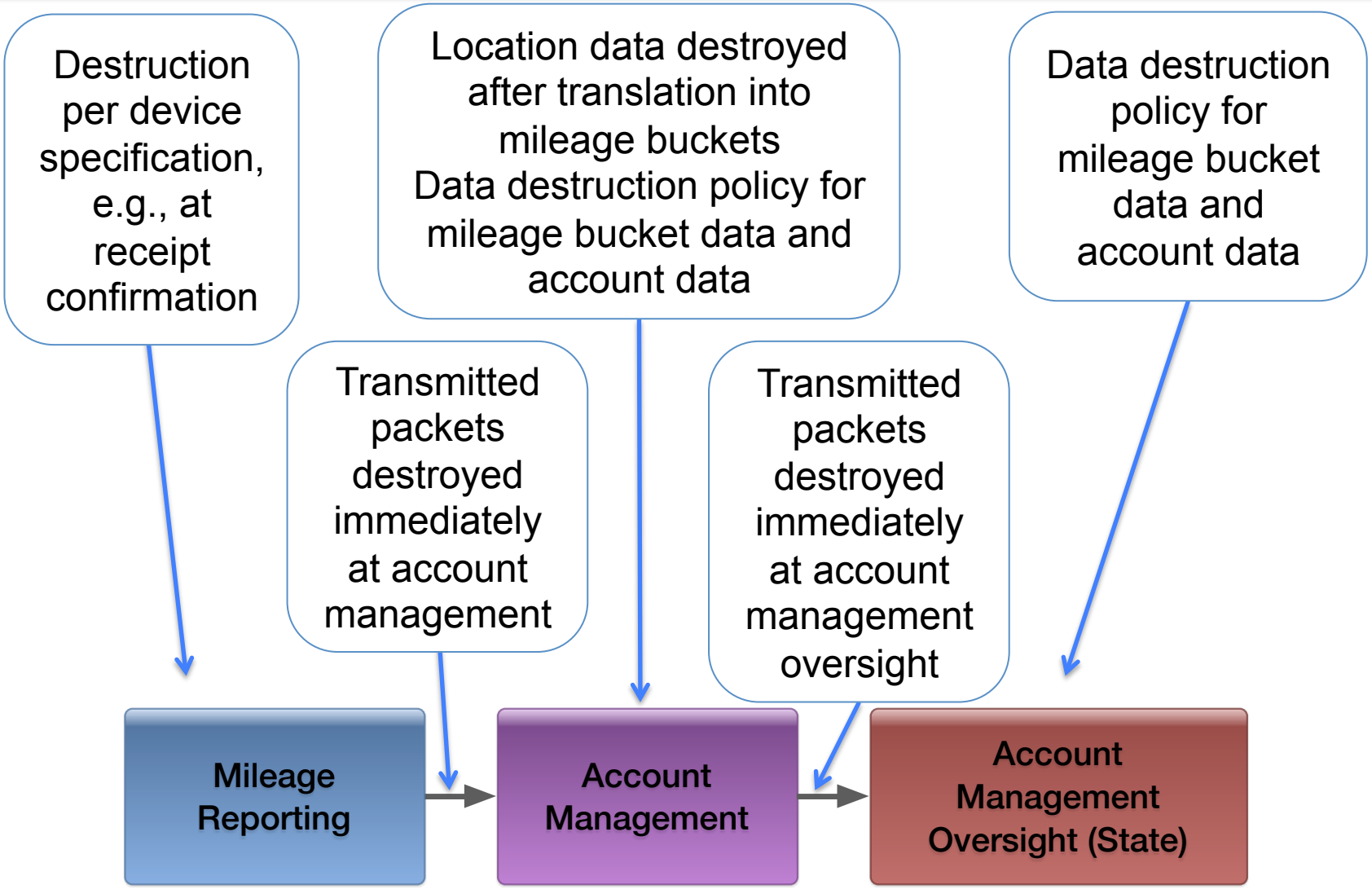
- Encryption:
  - Use 256-bit AES encryption
- Data Storage:
  - Use 256-bit AES to encrypt primary and backup data
  - Store location data only in mileage buckets after map matching
- Data Transmittal
  - Use mileage buckets to transmit mileage data to CAMs
  - Use 256-bit AES for encryption
  - Use HTTPS for internet-based secure data exchange

© D'Artagnan Consulting LLP

How PII Is Destroyed

- PII data needs must be erased (overwritten) not just deleted.
- Provisions for mileage data destruction developed in collaboration with the Oregon chapter of American Civil Liberties Union (ACLU):
  - Mileage data must be destroyed within 30 days after latest:
    - Payment processing
    - Dispute resolution
    - Noncompliance investigation
- Data destruction on MMs may differ from data destruction on computer systems.

How PII Is Destroyed in System Architecture Diagram



© D'Artagnan Consulting LLP

Recommendations: Data Destruction

- Provide opt-in option to all participants and 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
  - 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

© D'Artagnan Consulting LLP

General IT Network Security

- The overall computer system must be secure for the data policies to be effective.
- *Some* of the most important elements of IT network security:
  - **Firewall**
  - **Antivirus**
  - **Anti-malware**
  - **Intrusion detection** – detects unauthorized access to a system.
  - **Policies to protect against "Social engineering" attacks**

International Standards Organization (ISO) 27000

- ISO 27000 is a worldwide family of standards for measuring a computer system secure.
- ISO 27001 covers organizational aspects of security.
- ISO 27002 covers overall best practices for information security management.
- There are now over 20 standards in the ISO 27000 family.
- Due to time and budget constraints, ISO 27000 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

- Use ISO 27000 best practices:
  - ISO 27000 system certification and audits not possible during the pilot
  - Vendors can be asked to self-report any significant deviations from ISO 27000 best practices

Data Security Recommendations Summary

Data Access

1. **Authentication**: minimum of 8-character passwords, letters and numbers, one capital, require periodic password change
2. **Authorization**: for pilot project, employ user roles with limited rights to PII access. Provide at least user roles of CSR, Enforcement, and Accountant/Auditor
3. **Data Modification Notification**: require notification to motorist via e-mail or text message
4. **Data Masking**: at a minimum, mask all means of simulated payment and VINs

Data Storage

5. **Encryption**: use 256-bit AES encryption

© D'Artagnan Consulting LLP

Data Security Recommendations Summary (continued)

Data Storage (continued)

6. **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
7. **Data Transmittal**: use mileage buckets to transmit mileage data to CAMs; use 256-bit AES

Data Destruction

8. **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
     - Simulated noncompliance investigation
   - Data on devices destroyed when data receipt confirmation received from account manager

© D'Artagnan Consulting LLP

Data Security Recommendations Summary (continued)

General IT Network Security

9. **General IT Network Security**: use ISO 27000 best practices

© D'Artagnan Consulting LLP

Policy Questions and Staff Recommendation

What system data security features should be used in the pilot?

Staff recommends adoption of the nine Data Security provisions related to: Authentication; Authorization; Data Modification Notification; Data Masking; Encryption; Data Storage; Data Transmittal; Data Destruction; and General IT Network Security as fully described on pages 46-47 of the TAC Briefing Book #7.

© D'Artagnan Consulting LLP