NHTSA
NATIONAL HIGHWAY TRAFFIC SAFETY ADMINISTRATION

Achieving V2X Interoperability & Security

Results from USDOT's Security Credential Management System (SCMS) Deployment Workshops

March 2019

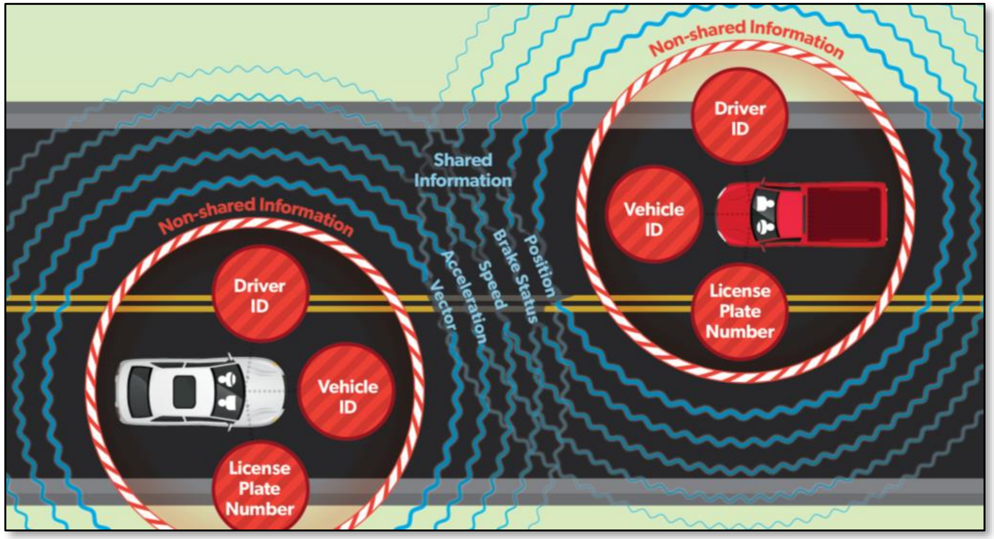
Why do we want V2X communications ?

Light Vehicle crash avoidance safety benefits are the tip of the iceberg for V2X!

- Vehicle to Pedestrian (V2P)
- Vehicle to Motorcycle (V2M)
- Commercial Vehicles
- Mobility Applications
  - Platooning
  - Coordinated movements at:
    - Intersections
    - entrance ramps and merging
- Automated Driving System Applications that will leverage sensor sharing and pathway communications to further advance safety and mobility of ADS equipped vehicles.

But security and trust in messaging is key!

- Integrity – the message was not modified between sender and receiver
- Authenticity – the message originates from a trustworthy and legitimate device
- Privacy – the message must appropriately protect the privacy of the sender

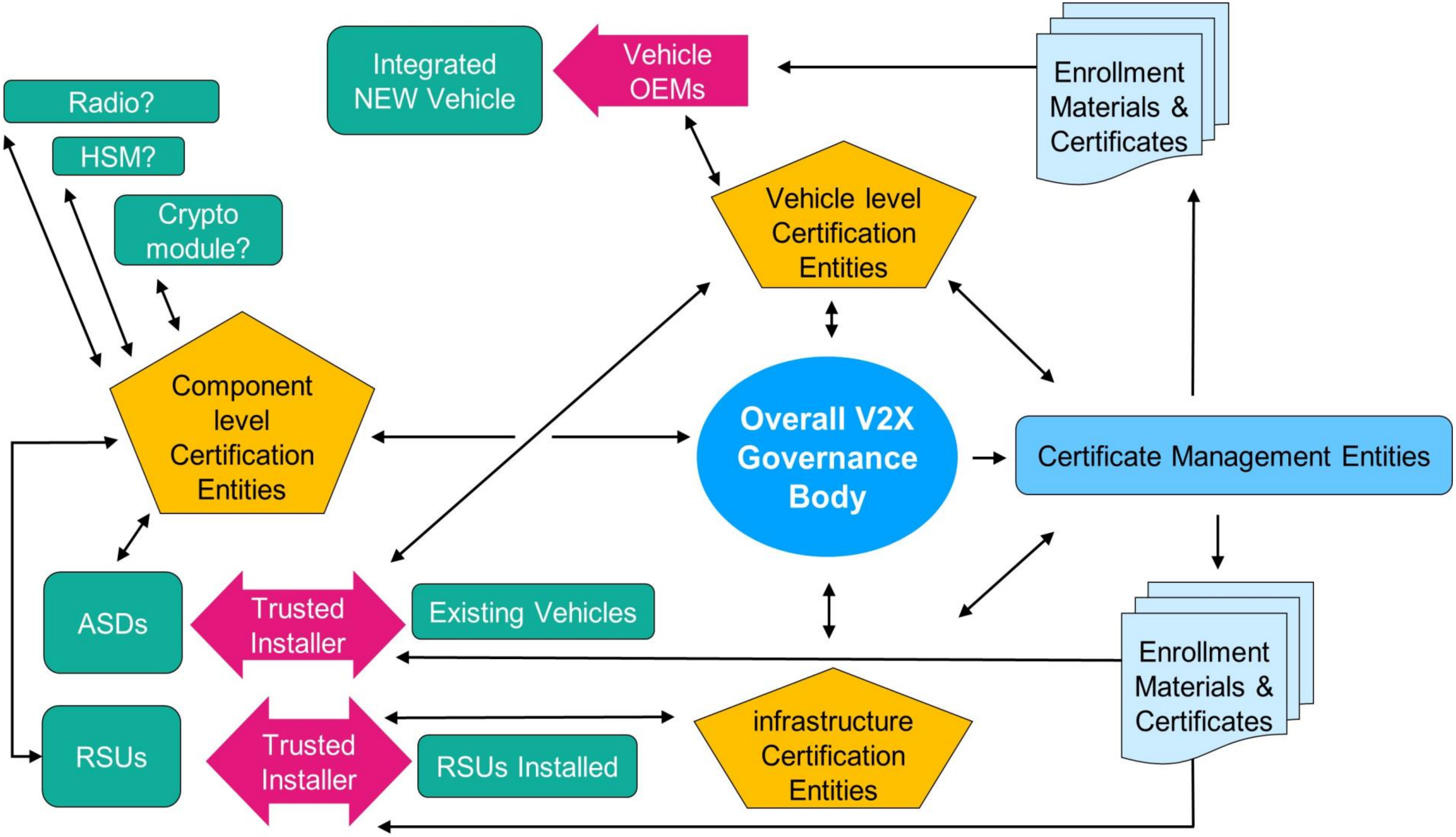


Implementing V2X security requires some functions to be centralized

- Device Certification Eco-system
- Misbehavior Detection and Revocation
- Root certificate(s) management

......and associated decision making and enforcement actions (if/when something goes wrong) must be implanted in a consensus fashion

Authority needs to start somewhere…example, certification eco-system


Integrated NEW Vehicle
Vehicle OEMs
Enrollment Materials & Certificates
Radio?
HSM?
Crypto module?
Vehicle level Certification Entities
Component level Certification Entities
Overall V2X Governance Body
Certificate Management Entities
ASDs
Trusted Installer
Existing Vehicles
Enrollment Materials & Certificates
RSUs
Trusted Installer
RSUs Installed
infrastructure Certification Entities

If there is not a centralized authority and management entity …what could happen?

Non-interoperable systems with differing policies and requirements

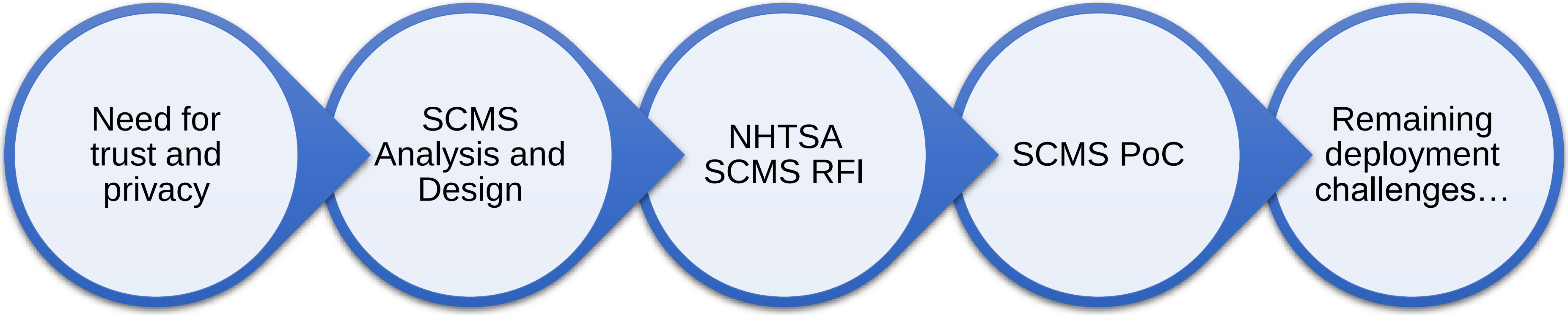
Lack of effective enforcement mechanisms, reducing security, trust and/or privacy

Non-sustainable system with inconsistent funding streams

A Security Credential Management System (SCMS), and associated governing structure, is therefore vital to securing the V2X ecosystem

USDOT SCMS Research and Development

- Conducted SCMS analysis and outreach efforts on how to deploy at scale
- Built and demonstrated the SCMS Proof-of-Concept (PoC)
- **Conducted outreach activities and workshops with industry stakeholders to assess pathways (or models) for how a large-scale (National) SCMS eco-system could be established.**



Stakeholder Groupings

SCMS IMPLEMENTERS INCLUDE:

- PKI Security Services
- Certification Services
- OEMs
- USDOT
- Communications Service Providers

SCMS USERS INCLUDE:

- Vehicle Owner/ Operators
- Dealers and Installers
- Service and Parts Facilities
- CV Equipment and Application Suppliers
- OEMs
- State and Local DOTs
- Public Infrastructure System Integrators

SCMS OTHER INTERESTED PARTIES INCLUDE:

- USDOT
- Academia
- Standards Organizations
- Advocacy Groups

SCMS Model Ownership and Governance Attributes

SCMS Structure Attributes

- Initial Ownership
- Initial Funding
- SCMS Manager Sustainment Funding
- Technical Component Sustainment Funding
- Competition
- Legislation/Regulation

SCMS Manager Roles and Responsibilities Attributes

- Initial Policy Development
- Recurring Policy Development and Approval
- Oversight and Auditing
- Misbehavior Authority Management
- End Entity Certification
- Trust Anchor Management

Range of Ownership and Governance Models

Public Model
Government controls by establishing new office to serve as SCMS Manager

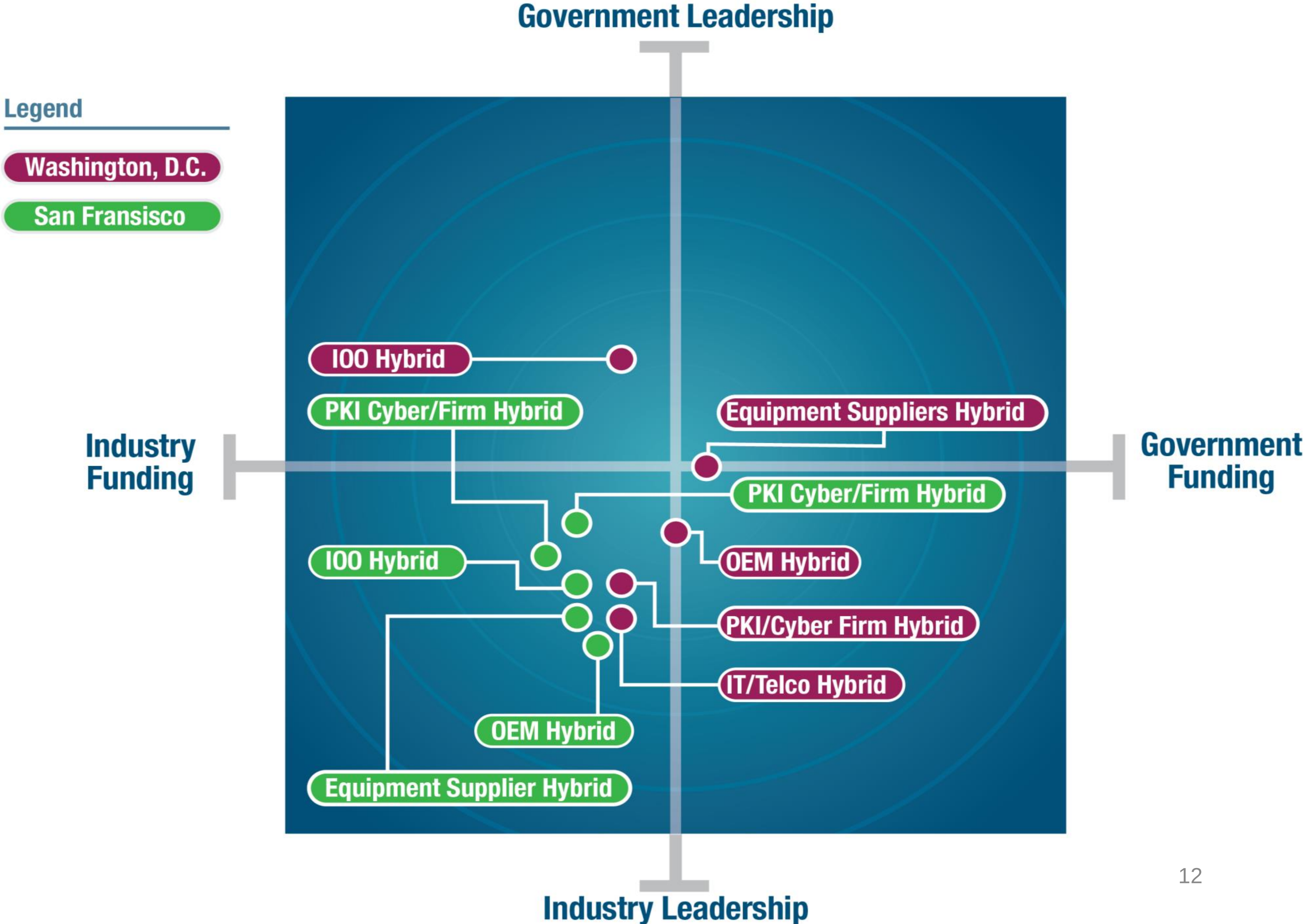
Government-led Public Private Partnership (P3)
Government office leads creation of public-private team

P3 Concession
Government facilitates and governs. SCMS Manager is run as a concession.

Industry-led P3
Government is on the board for facilitation and oversight, and financially assists only with initiation

Private Model
Government is only a stakeholder. Industry forms a consortium and funds development.

Day 2 Models: Both Workshops

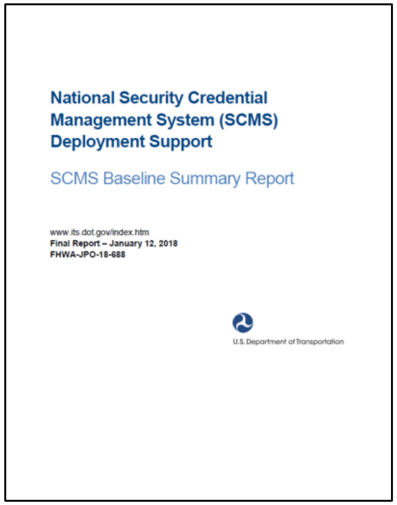


Key Stakeholder Recommendations

1. Stakeholders must continue to meet and drive the establishment of a largely self-regulated SCMS Governance entity—but Government has a facilitation role
   a. Security and technical policies are needed to initiate PKI operations
   b. High level business (funding) model must be establish
2. Agreements are needed to memorialize relationships among stakeholder groups
3. Additional research is needed around misbehavior detection and certificate revocation
4. Additional research is needed around device certification and initial enrollment and provisioning

Public Reports from Project

- SCMS Baseline Summary Report: https://rosap.ntl.bts.gov/view/dot/36397
- Literature Search Report: https://rosap.ntl.bts.gov/view/dot/36395
- Potential SCMS Ownership and Governance Models: https://rosap.ntl.bts.gov/view/dot/36393
- Full-Scale Security Credential Management System (SCMS) Deployment Workshop Read Ahead: https://rosap.ntl.bts.gov/view/dot/36651
- Workshop Findings: TBD

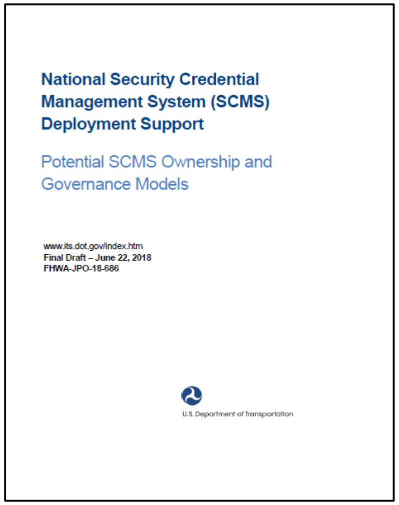


National Security Credential Management System (SCMS) Deployment Support

SCMS Baseline Summary Report

www.its.dot.gov/index.htm
Final Report – January 12, 2018
FHWA-JPO-18-688

U.S. Department of Transportation

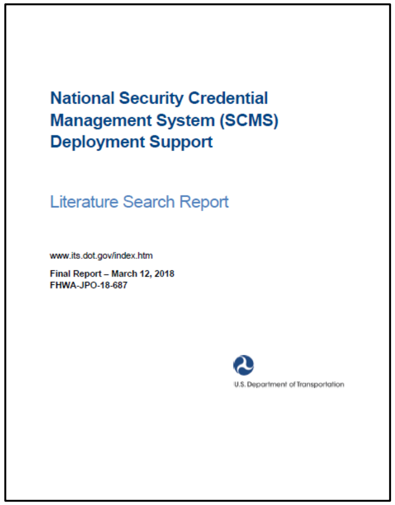


National Security Credential Management System (SCMS) Deployment Support

Potential SCMS Ownership and Governance Models

www.its.dot.gov/index.htm
Final Draft – June 22, 2018
FHWA-JPO-18-686

U.S. Department of Transportation



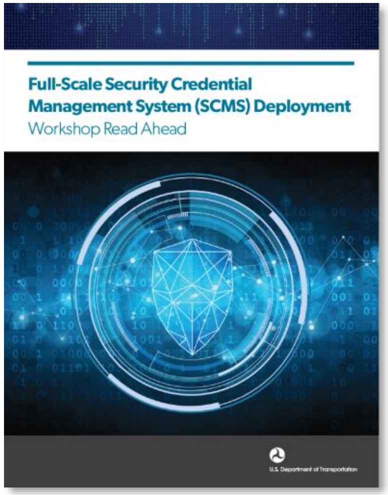
National Security Credential Management System (SCMS) Deployment Support

Literature Search Report

www.its.dot.gov/index.htm

Final Report – March 12, 2018
FHWA-JPO-18-687

U.S. Department of Transportation



Full-Scale Security Credential Management System (SCMS) Deployment

Workshop Read Ahead

U.S. Department of Transportation

Questions for U.S. DOT?

Points of Contact

Kevin Gay
Senior Advisor for Technology Policy

Office of the Administrator

U.S. DOT National Highway Traffic Safety Administration

Robert Kreeb
Division Chief, Intelligent Technologies Division

U.S. DOT National Highway Traffic Safety Administration