CVISN Architecture Document
Proposed Scope Changes

- Move the brief description of Core CVISN capabilities into the CVISN Architecture document. See Figure A.
- Annotate the latest version of the sausage diagram (see CR 4758) to highlight CVO aspects and move it into the CVISN Architecture document. See Figure B.
- Add the table of standard identifiers to the CVISN Architecture document. This was last updated by the CVISN Working Groups in the summer of 2005. See Figure C.
- Add the brief descriptions of the 40 Expanded CVISN Capabilities to the CVISN Architecture document. These were documented in APL document SSD-PL-05-0202, *Expanded Commercial Vehicle Information Systems and Networks (CVISN) Summary Report*, June 2005.

Figure A

Definition of Core CVISN Deployment

- **An organizational framework for cooperative system development has been established among state agencies and motor carriers.**

- **A State CVISN System Design has been established that conforms to the CVISN Architecture and can evolve to include new technology and capabilities.**

- **All the elements of three capability areas (below) have been implemented using applicable architectural guidelines, operational concepts, and standards:**
  - Safety Information Exchange
    - **Inspection reporting using ASPEN (or equivalent) at all major inspection sites. ASPEN data sent to SAFER (Safety and Fitness Electronic Records) directly or indirectly.**
    - **Connection to the SAFER system to provide exchange of interstate carrier and vehicle data snapshots among states.**
    - **Implementation of CVIEW (or CVIEW equivalent) system for exchange of intrastate and interstate data within state and connection to SAFER for exchange of interstate data through snapshots.**

      -- OR --
    - **Utilization of SAFER option for exchange of inter- and intrastate data through snapshots.**
  - Credentials Administration
    - **Automated electronic processing via Web-based or computer-to-computer solutions from carrier to State (processing includes carrier application, state application processing, credential issuance, and tax filing) of at least IRP (International Registration Plan) and IFTA (International Fuel Tax Agreement) credentials; ready to extend to other credentials (intrastate, titling, OS/OW (Oversize/Overweight), carrier registration, HazMat). Note: Processing does not necessarily include e-payment.**
    - **Update SAFER with credential information for interstate operators as actions are taken.**
    - **Update CVIEW (or equivalent) with interstate and intrastate credential information as actions are taken.**
    - **Connection to IRP & IFTA Clearinghouses.**
    - **At least 10% of the transaction volume handled electronically; ready to bring on more carriers as carriers sign up; ready to extend to branch offices where applicable.**
  - Electronic Screening
    - **Use snapshots to support screening decisions.**
    - **Implemented at a minimum of one fixed or mobile inspection site.**
    - **Ready to replicate at other sites.**

Figure B

This Version of the National ITS Architecture Subsystems Interconnect Diagram Highlights the CVO Subsystems

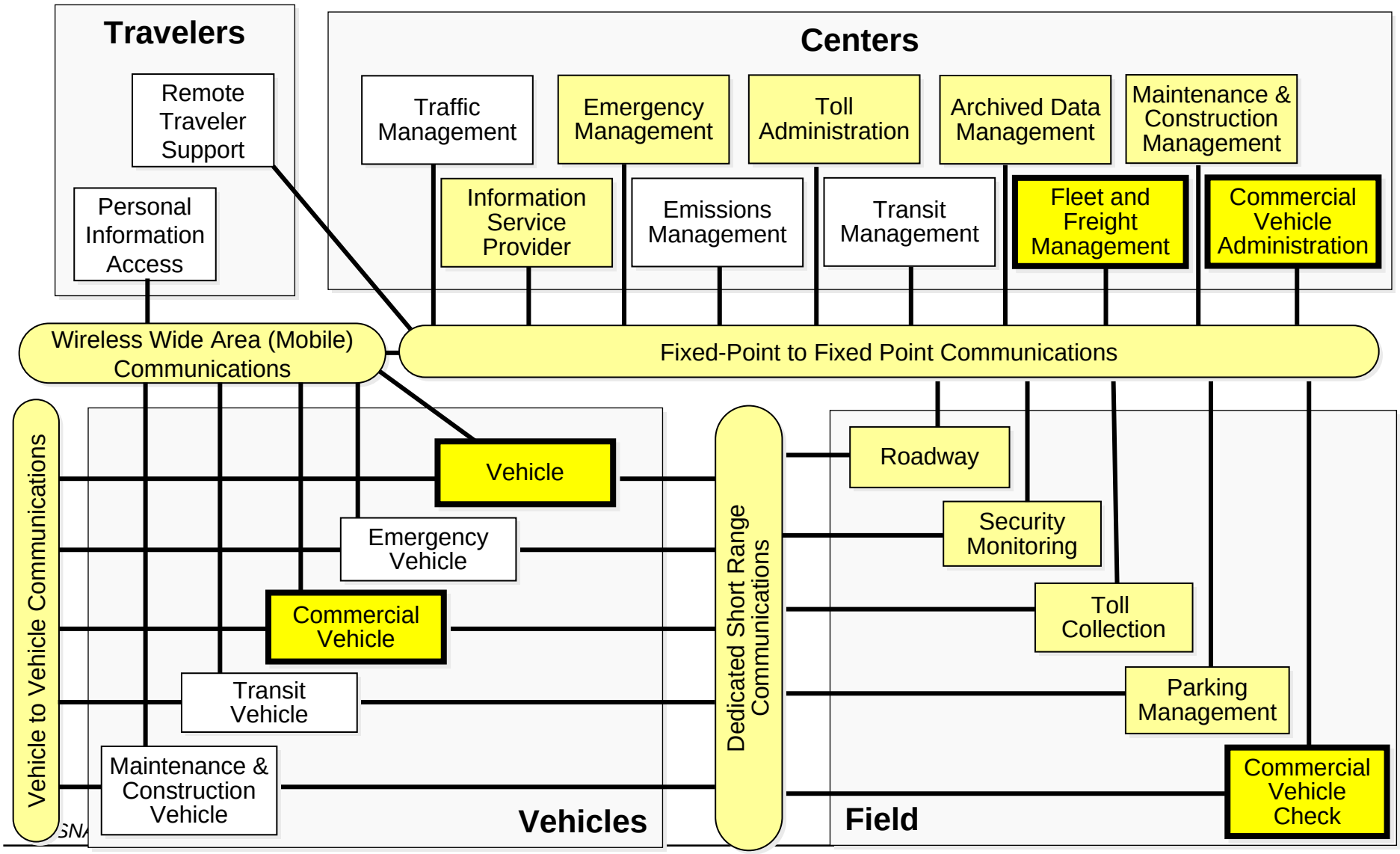

Figure C

To Enable Look-Up in Infrastructure Systems, Standard Identifiers Should Be Used

Carrier: USDOT number and EIN

- Vehicle:
  - Power unit: License plate ID, VIN, and transponder ID
  - Chassis: ??
  - Semi-trailer, trailer, tanker: License plate ID and equipment number (container ID?)
- Driver: License ID
  - Note: some concern that this is insufficient
- Cargo: Shipper DUNS number and bill of lading ID

Figure C

Carrier ID Details

Motor Carrier	Primary Carrier ID For ***interstate*** carrier: e.g., 12345 A001 (note that '12345' must be the carrier's USDOT # ; the terminal ID 'A001' is optional)	Carrier-Specific Identifier (alphanumeric); must be USDOT number + Carrier Terminal ID designated by carrier (alphanumeric) (optional) + CVO Company Type (optional)	12 (max) 4 (max) TBD
	For ***intrastate*** carrier: e.g., US CA 123A45689 1234 (note that the terminal ID '1234' is optional)	Country Code (alphanumeric); the allowable codes will be defined in the FHWA Code Directory + Jurisdiction (state or province) Code (alphanumeric); the allowable codes will be defined in the FHWA Code Directory + Carrier-Specific Identifier; if carrier is intrastate and has a USDOT number, must be USDOT number; for state-specific IDs, the Carrier-Specific Identifier may include a prefix to clarify the agency/source of the identifier) + Carrier Terminal ID designated by carrier (alphanumeric) (optional) CVO Company Type	2 2 12 (max) 4 (max) TBD
	For all carriers: Federal Taxpayer Identification Number e.g., E 123456789 Note: Open issue regarding Mexican and Canadian carriers. See section 8.1.	Type (alphanumeric); S for Social Security Number, E for Employer Identification number + Tax ID Number (alphanumeric)	1 9

Figure C

Vehicle and Container ID Details

Vehicle	Vehicle Identification Number e.g., 1FDKE30F8SHB33184 and	VIN assigned by manufacturer (alphanumeric)	30 (max)
	Vehicle Plate ID e.g., US CA 12345664820M	Country code (alphanumeric); allowable codes from ISO 3166-1, country codes (English) + Jurisdiction (state or province) code (alphanumeric); allowable codes from FHWA code directory + License plate ID (alphanumeric)	2 2 12 (max)

Container	Container Unique ID e.g., SUDU3070079	Suggested as a candidate: Container number marked on side (in accordance with ISO 6346) (alphanumeric)	11 (suggested)

Figure C

Transponder ID Details

Transponder	Transponder ID	segments shown below	10 (max)
		Transponder ID Definition Flag (0=current; 1=IEEE 1455-1999) +	1 (1 bit)
	e.g., 0 123456789	*If Transponder ID Definition Flag = current* , then the other segment is:	8
		Transponder Serial Number assigned by manufacturer	(32-bit hexadecimal value)
	or 1 9999 232323	*If Transponder ID Definition Flag = IEEE 1455-1999* , then the other segments are:	4
		Manufacturer Identifier +	(16 bits hexadecimal value)
		Transponder Serial Number assigned by manufacturer	5 (20 bits hexadecimal value)

Figure C

Driver and Shipment ID Details

Driver	Driver Unique ID e.g., US MD B99999999999A	Country code (alphanumeric); the allowable country codes will be defined in the FHWA Code Directory + Jurisdiction (state or province) code (alphanumeric); the allowable subdivision codes will be defined in the FHWA Code Directory + Driver specific identifier (driver license number) assigned by jurisdiction (alphanumeric)	2 2 16 (max)

Shipment	Shipment Unique ID e.g., 123456789776655443322	Shipper ID. DUNS number suggested as a candidate (alphanumeric) + Bill of Lading number assigned by the shipper identified above (numeric)	9 (suggested) 12 (max)

Figure D

Expanded CVISN Capabilities: Driver Information Sharing

D1. Establish, maintain and provide controlled access to driver snapshots/Use and maintain driver snapshots for all processes.

D2. Improve access to driver information for enforcement and carrier personnel to target driver safety risk.

D3. Provide roadside tools to evaluate compliance with hours-of-service regulations.

D4. Improve identity checks in all driver-licensing processes.

D5. Link driver performance data to related carrier ID to identify high-risk carriers.

D6. Determine security rating for drivers.

D7. Provide on-line tools to help carriers assess potential drivers and monitor current drivers' performance.

D8. Ensure that systems control access to driver records.

D9. Allow the driver to review, challenge and correct information in their driving record.

D10. Expand the use of standards for commercial drivers' licenses (CDLs) and information systems that store driver data; include standards for identification security.

D11. Improve the standardization of citation data collection and information sharing among enforcement agencies.

Figure D

Expanded CVISN Capabilities: Enhanced Safety Information Sharing

S1. Establish data timeliness, data accuracy and integrity measures.

S2. Regularly check data used in CVISN processes for timeliness, accuracy and integrity; purge stale data and repair errors.

S3. Expand core safety systems to include standard information storage and exchange for intrastate and foreign carriers, in addition to interstate carriers.

S4. Establish or expand “data stores” for cargo, carrier, vehicle and driver credential, safety and enforcement data.

S5. Provide on-line tools to enable appropriate users to provide timely information about corrections of deficiencies detected during inspections.

S6. Improve the carrier’s ability to review safety data associated with its record. Consider proactively delivering safety data to carrier.

S7. Provide on-line tools for law enforcement to submit crash and citation reports.

S8. Enable jurisdictions to maintain up-to-the-minute inspection history data.

Figure D

Expanded CVISN Capabilities: Smart Roadside

R1. Expand access to data collected by on-board systems to improve roadside operations.

R2. Provide integrated and improved access for roadside personnel to data stored in core infrastructure systems [e.g., Safety and Fitness Electronic Records (SAFER), Motor Carrier Management Information System (MCMIS), CDL data systems].

R3. Provide carriers with streamlined and timely access to citation, crash, and inspection information so they are better informed about safety problems.

R4. Associate high-risk cargo with the container, manifest, chassis, vehicle/transponder, carrier(s), vehicle and driver transporting it.

R5. Expand the use of standard electronic security devices (ESDs) to improve container and trailer security and reduce theft.

R6. Monitor status of the ESDs throughout the trip by collecting “event data” at toll booths, ports of entry, inspection/weigh stations and freight yard entries/exits.

R7. Expand the use of technologies and processes to verify authorized drivers and personnel are able to access the vehicle, trailer and container.

R8. Provide access to the event data and related information to authorized private and public sector users – based on legitimate needs for information to improve productivity, streamline operations and improve security.

R9. Expand the use of mobile data entry devices [e.g., laptop, personal data assistant (PDA), cell phone] and applications to improve data quality and streamline data collection.

R10. Expand the use and capabilities of virtual/remote sites to increase the effectiveness of enforcement.

R11. Expand the use of technology to generate real-time safety and security alerts.

Figure D

Expanded CVISN Capabilities: Expanded Electronic Credentialing

C1. Reduce complexity and redundancy for users by offering access to multiple credentials from a single source.

C2. Increase the number of e-credentials that are available [e.g., oversize/overweight (OS/OW) permitting, Hazardous Materials (HazMat)].

C3. Offer a variety of standard e-payment options.

C4. Improve the process for enrolling in multi-jurisdiction programs (e.g., e-screening programs, e-toll) through provision of links.

C5. Provide for automated queries to cross-check supporting requirements across agencies, states and federal systems through use of unique carrier, vehicle, driver and load identifiers.

C6. Legacy credentialing systems update Commercial Vehicle Information Exchange Window (CVIEW) with changes in credentials data for real-time access.

C7. Enhance interfaces and systems for information sharing to provide improved access to more current and accurate credentials information for authorized stakeholders.

C8. Designate one authoritative source for each credential-related data element and provide date/time stamp; manage changes; auditable.

C9. Use secure electronic identification, notification, documentation and screening for vehicles, carriers, drivers and cargo.

C10. Expand the set of standard data elements for information exchange related to credentials.