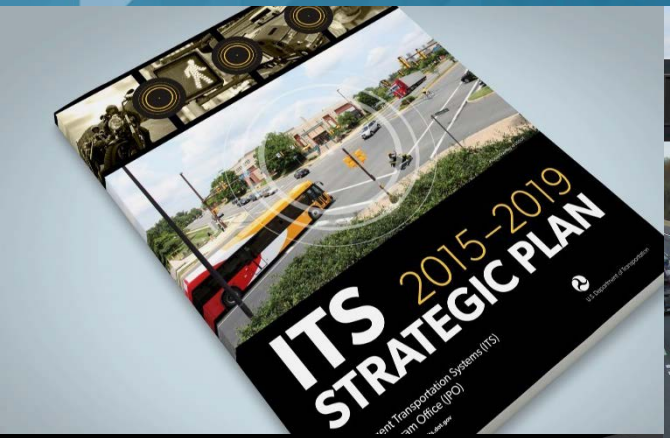
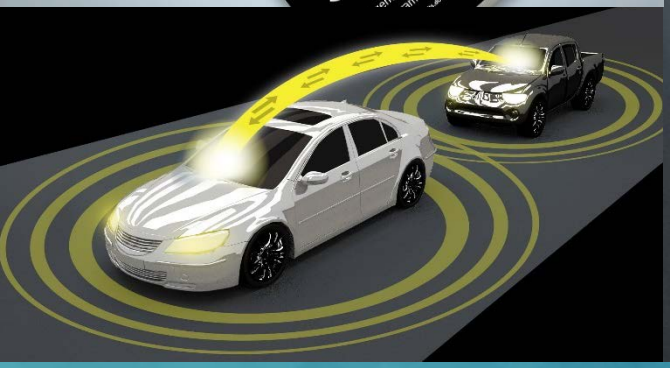
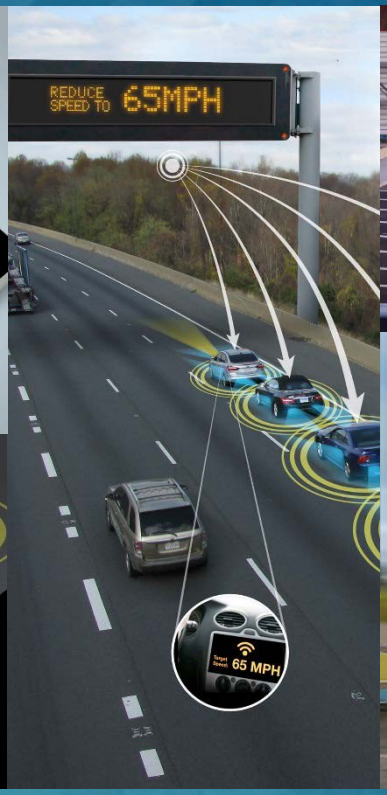
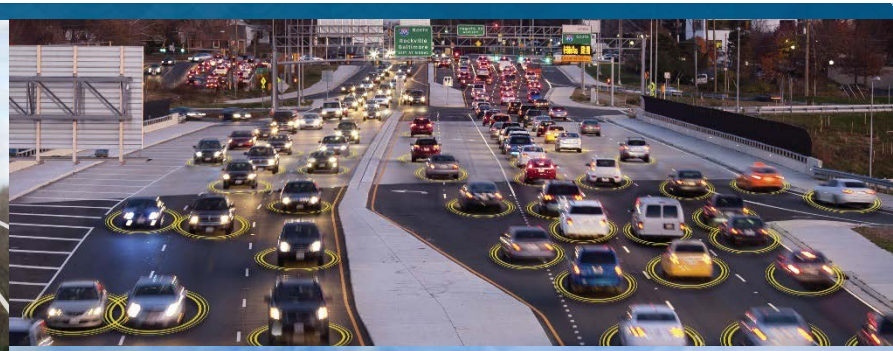
U.S. Department of Transportation









APPLYING NIST CSF TO A CV DEPLOYMENT

ITS America Annual Meeting 2018

SS24: CYBERSECURITY CHALLENGES FOR CAVS

June 6, 2018

Kevin Gay
ITS Joint Program Office
U.S. Department of Transportation

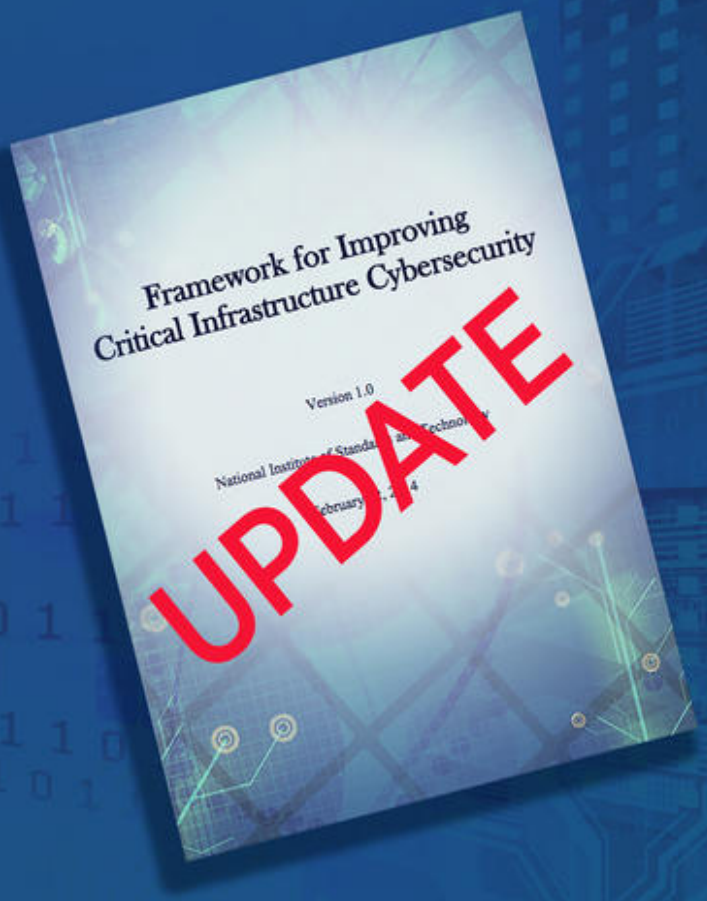
PROGRAM STRATEGY

Purpose: The program's objective is to:

- Help organizations apply the principles and best practice of risk management to improving the cybersecurity and resilience of critical transportation infrastructure.
- The Privacy Research Analysis achieving freedom from conditions that can create problems for individuals with unacceptable consequences that arise from transportation systems that process PII.

Strategic Direction: By applying cybersecurity and privacy guidance in a systematic manner to a connected vehicle environment, USDOT and stakeholders have the opportunity to create a set of detailed guidelines and tools that are specific to connected transportation and those organizations that deploy, operate, and maintain the network and systems.

NIST CYBERSECURITY FRAMEWORK



- Outcome of Executive Order 13636, and result of collaboration between public and private sectors
  - Manages cybersecurity risks in a cost-effective way, while protecting privacy and civil liberties
  - References the globally accepted standards (COBIT, ISO/IEC, ISA, NIST, CCS) that are working well today
  - Intended for worldwide adoption – not US only
  - Use common terminology to discuss cybersecurity risk
  - Ensures business drivers guide cybersecurity activities
  - Considers cybersecurity risks as part of organization's overall risk management process

Credit: N. Hanacek/NIST and ©bluebay/Shutterstock

FRAMEWORK COMPONENTS

- Voluntary framework developed through a collaborative process by industry, academia, and government stakeholders
- Provides an approach to prioritize cybersecurity resources, make risk decisions, and take action to reduce risk.
- The Cybersecurity Framework consists of 3 components:
  1. **The Core:** provides an easy-to-understand set of desired cybersecurity outcomes.
  2. **Profiles:** portrays organizations' unique requirements, objectives, risk appetite, and resources.
  3. **Implementation Tiers:** indicates how an organization manages cybersecurity risks.

IDENTIFY
- Asset management
- Business environment
- Governance
- Risk assessment
- Risk management strategy

PROTECT
- Access control
- Awareness and training
- Data security
- Information protection and procedures
- Maintenance
- Protective technology

DETECT
- Anomalies and events
- Security continuous monitoring
- Detection process

RESPOND
- Response planning
- Communications
- Analysis
- Mitigation
- Improvements

RECOVER
- Recover planning
- Improvements
- Communications

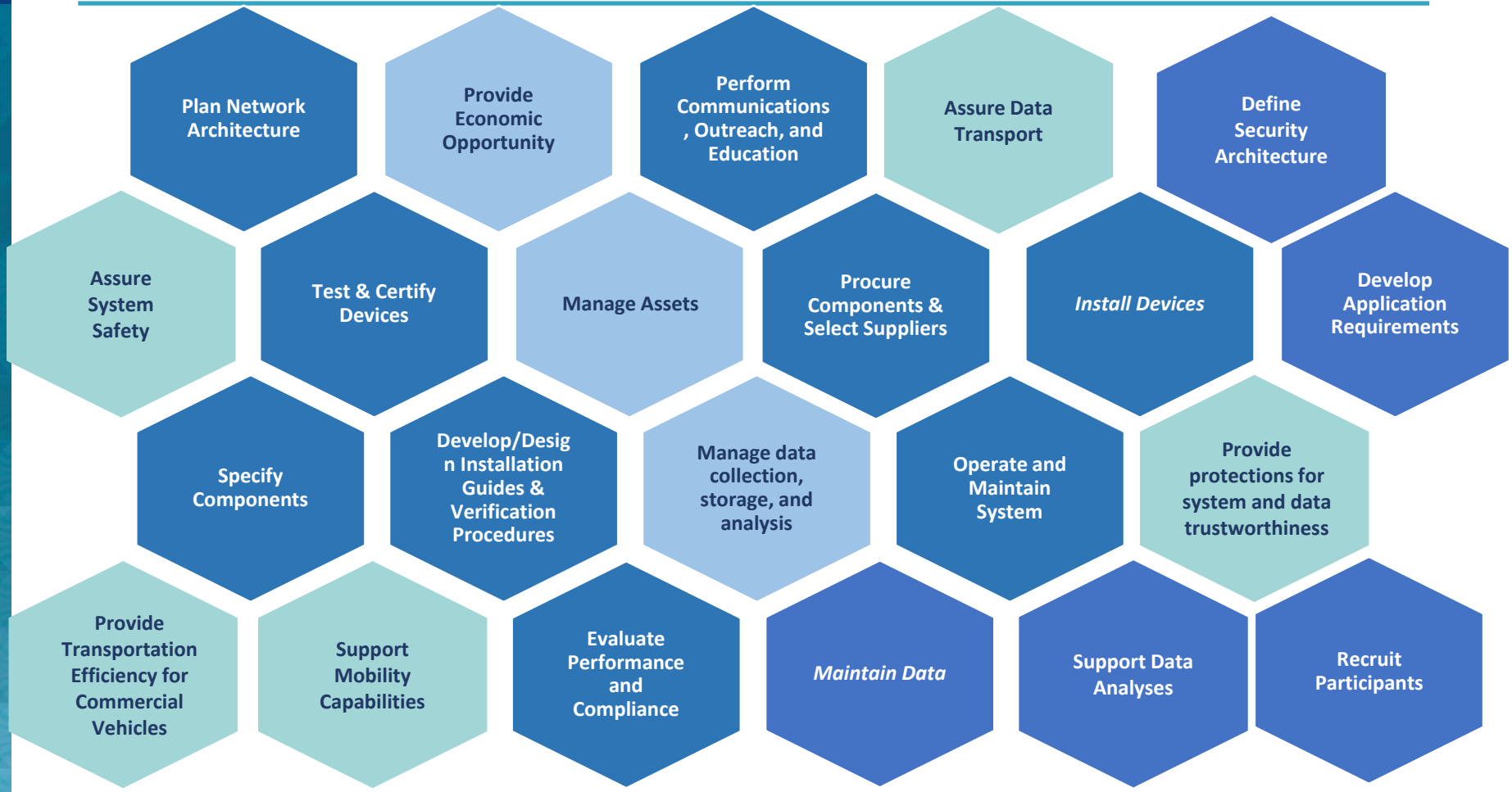
CYBERSECURITY FRAMEWORK PROFILE DEVELOPMENT STEPS

ANN ARBOR CONNECTED VEHICLE TEST ENVIRONMENT

- Largest existing deployment of connected vehicles and connected infrastructure
- Expanding on Safety Pilot Model Deployment
- Covers 27 square miles
- Adding 1500 vehicles per year

- ***The Ann Arbor Connected Vehicle Test Environment was used as the initial test case for implementing the NIST Framework because it is the most extensive and mature environment available.***

DEVELOP MISSION OBJECTIVES



KEY: All Consensus | AACVTE

RANKING THE MISSION OBJECTIVES

NEXT STEPS

Industry Mission Objectives

Cybersecurity Framework

Function	Category	Category Unique ID
Identify	Asset Management	ID.AM
	Business Environment	ID.BE
	Governance	ID.GV
	Risk Assessment	ID.RA
	Risk Management Strategy	ID.RM
Protect	Access Control	PR.AC
	Awareness and Training	PR.AT
	Data Security	PR.DS
	Information Protection Processes & Procedures	PR.IP
	Maintenance	PR.MA
	Protective Technology	PR.PT
Detect	Anomalies and Events	DE.AE
	Security Continuous Monitoring	DE.CM
	Detection Processes	DE.DP
Respond	Response Planning	RS.RP
	Communications	RS.CO
	Analysis	RS.AN
	Mitigation	RS.MI
	Improvements	RS.IM
Recover	Recovery Planning	RC.RP
	Improvements	RC.IM
	Communications	RC.CO

Subcategory	Informative References
ID.BE-1: The organization's role in the supply chain is identified and communicated	COBIT 5 APO01.02, DSS06.03 ISA 62443-2-1:2009 4.3.2.3.3 ISO/IEC 27001:2013 A.6.1.1 NIST SP 800-53 Rev. 4 CP-2, PS-7, PM-11
ID.BE-2: The organization's place in critical infrastructure and its industry sector is identified and communicated	COBIT 5 APO08.04, APO08.05, APO10.03, APO10.04, APO10.05 ISO/IEC 27001:2013 A.15.1.3, A.15.2.1, A.15.2.2 NIST SP 800-53 Rev. 4 CP-2, SA-12
ID.BE-3: Priorities for organizational mission, objectives, and activities are established and communicated	COBIT 5 APO02.06, APO03.01 NIST SP 800-53 Rev. 4 PM-8
ID.BE-4: Dependencies and critical functions for delivery of critical services are established	COBIT 5 APO02.01, APO02.06, APO03.01 ISA 62443-2-1:2009 4.2.2.1, 4.2.3.6 NIST SP 800-53 Rev. 4 PM-11, SA-14
ID.BE-5: Resilience requirements to support delivery of critical services are established	ISO/IEC 27001:2013 A.11.2.2, A.11.2.3, A.12.1.3 NIST SP 800-53 Rev. 4 CP-8, PE-9, PE-11, PM-8, SA-14

Conceptual CV CFP

Function	Category	Subcategory	Mission Objectives ●●● = High Priority, ●● = Moderate Priority, ● = Other Implemented Subcategories							
			1	2	3	4	5	6	7	8
		partners) are established								
	Business Environment (ID.BE): The organization's mission, objectives, stakeholders, and activities are understood and prioritized; this information is used to inform cybersecurity roles, responsibilities, and risk management decisions.	**ID.BE-1:** The organization's role in the supply chain is identified and communicated	●	●	●	●	●	●	●	●
		ID.BE-2: The organization's place in critical infrastructure and its industry sector is identified and communicated	●	●	●	●	●	●	●	●
		ID.BE-3: Priorities for organizational mission, objectives, and activities are established and communicated	●	●	●	●	●	●	●●	●●
		ID.BE-4: Dependencies and critical functions for delivery of critical services are established	●	●	●	●	●	●	●●	●●●
		ID.BE-5: Resilience requirements to support delivery of critical services are established	●	●	●	●	●	●	●●●	●
	Governance (ID.GV): The policies, procedures, and processes to manage and monitor the organization's regulatory, legal, risk, environmental, and operational requirements are understood and inform the management of cybersecurity risk.	**ID.GV-1:** Organizational information security policy is established	●	●	●	●	●	●●	●	●
		ID.GV-2: Information security roles & responsibilities are coordinated and aligned with internal roles and external partners	●	●	●	●	●	●●	●	●●
		ID.GV-3: Legal and regulatory requirements regarding cybersecurity, including privacy and civil liberties obligations, are understood and managed	●	●	●	●	●	●●●	●●●	●●●

STAY CONNECTED

For more information, contact…

Kevin W. Gay, PMP

Chief – Policy, Architecture, & Knowledge Transfer
Intelligent Transportation Systems Joint Program Office
U.S. Department of Transportation
Kevin.Gay@dot.gov

Twitter: @ITSJPODirector

Facebook: www.facebook.com/DOTRITA

Website: http://www.its.dot.gov