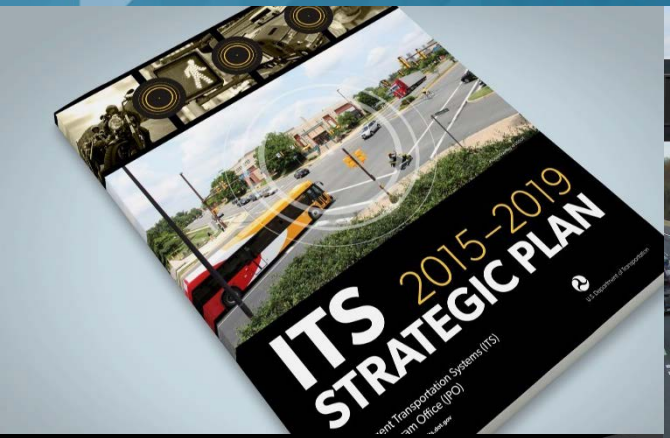
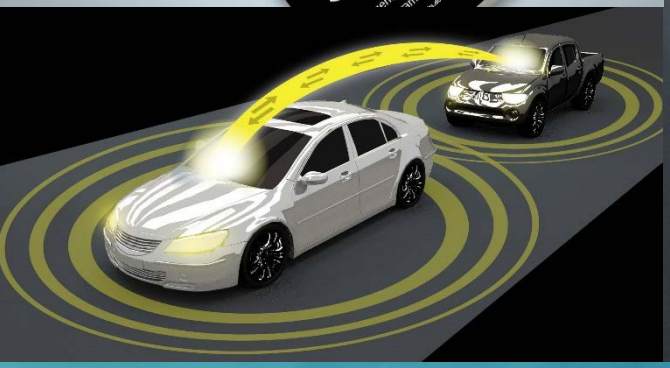
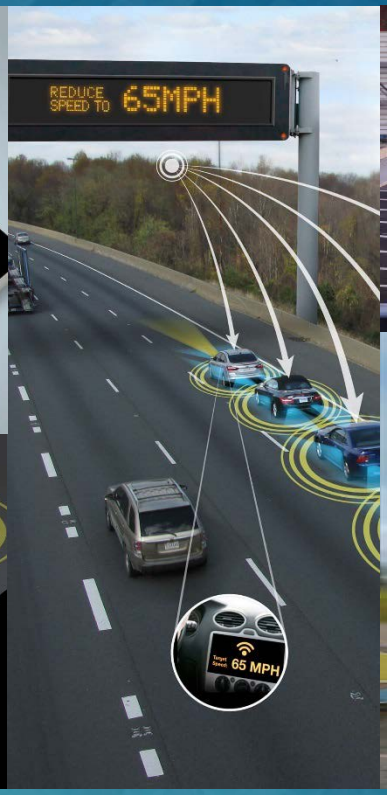
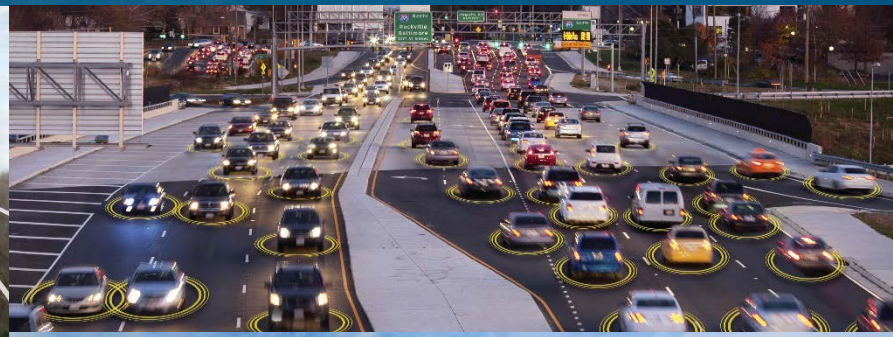
U.S. Department of Transportation









APPLYING NIST CSF TO A CV DEPLOYMENT

Transportation Research Board Annual Meeting 2018

January 9, 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.

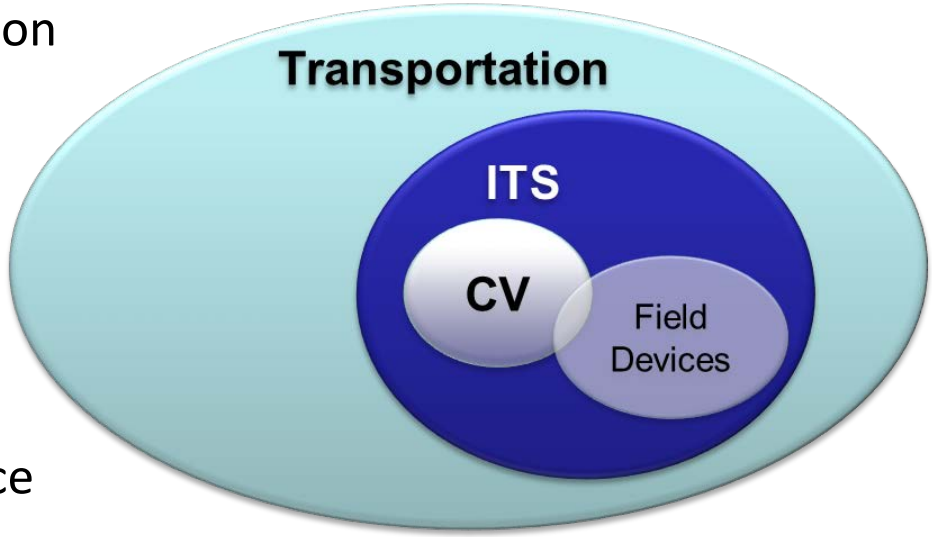
Strategic Direction: By applying cybersecurity and privacy guidance in a systematic manner to a connected vehicle environment, USDOT and stakeholders have the opportunity to create a set of detailed guidelines and tools that are specific to connected transportation and those organizations that deploy,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

CYBERSECURITY TRANSPORTATION PROJECTS COORDINATION: 3 KEY PROJECTS

- Establishing a Roadway Transportation System Cybersecurity Framework and Tools
  - FHWA and ITS Joint Program Office
  - ITE
- Cybersecurity of Traffic Management Systems
  - NCHRP
  - Southwest Research Institute
- Application of the NIST Cybersecurity Framework
  - ITS Joint Program Office
  - NIST/MITRE

CRITICAL INFRASTRUCTURE

- Improve cybersecurity of 3 related but distinct parts of critical transportation infrastructure
- All implement NIST Framework Process
- All seek to develop tailored guidance
- NCHRP & ITE projects considering organizing ongoing response and recovery operations

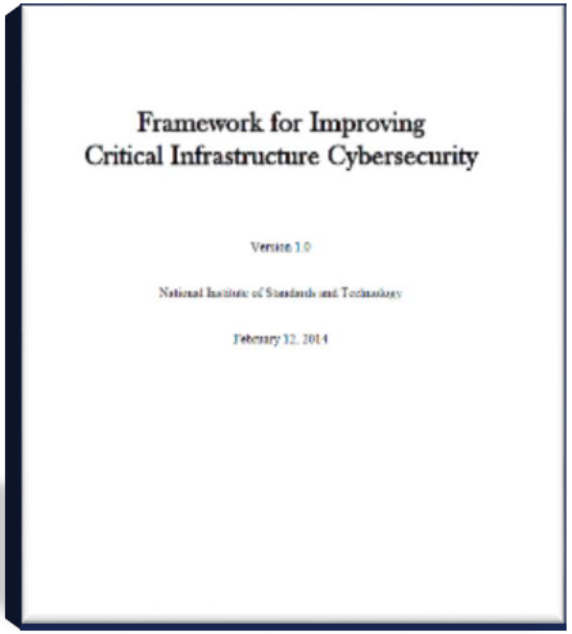


NIST CYBERSECURITY FRAMEWORK

NIST CSF

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
- Uses common terminology to discuss cybersecurity risk
- Ensures business drivers guide cybersecurity activities
- Considers cybersecurity risks as part of organization's overall risk management process

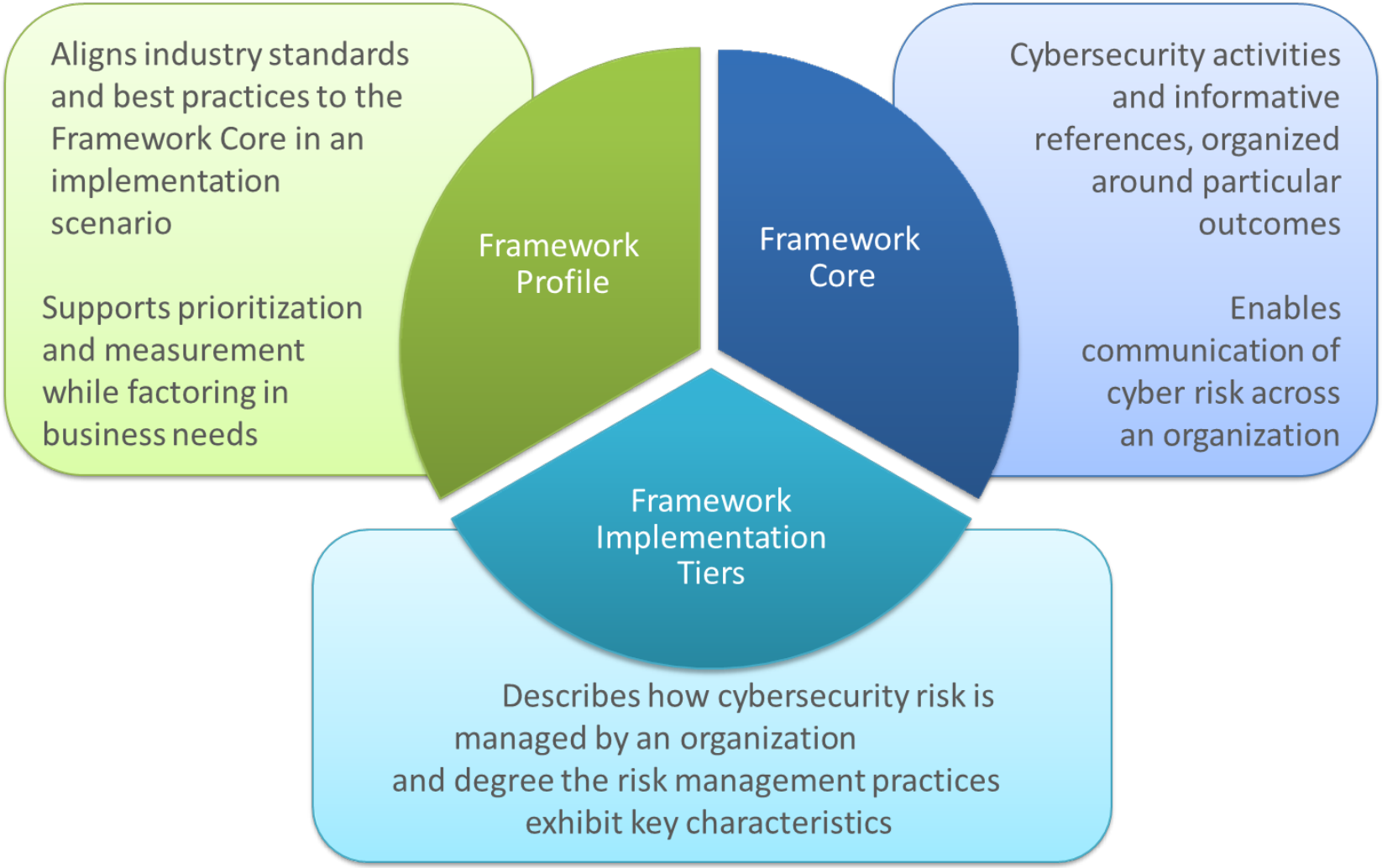

Framework for Improving
Critical Infrastructure Cybersecurity

Version 1.0

National Institute of Standards and Technology

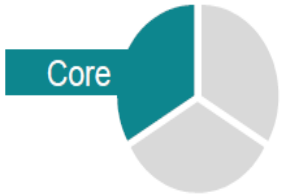
February 12, 2014

CYBERSECURITY FRAMEWORK COMPONENTS



CSF – FUNCTIONS

Functions



Functions		
ID	Identify	Develop the organizational understanding to manage cybersecurity risk to systems, assets, data, and capabilities
PR	Protect	Develop and implement the appropriate safeguards to ensure delivery of critical infrastructure services
DE	Detect	Develop and implement the appropriate activities to identify the occurrence of a cybersecurity event
RS	Respond	Develop and implement the appropriate activities to take action regarding a detected cybersecurity event
RC	Recover	Develop and implement the appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity event

CSF – PROFILES

Profiles

The alignment of the Framework core with an organizations business requirements, risk tolerance, and resources

- Describes the current state and desired future state
- Reveals gaps that can flow into action plan development
- Facilities a roadmap for reducing cybersecurity risk

CSF – TIERS

Tiers

Reflect how an organization views cybersecurity risk and the processes in place to manage that risk

- Tier 4 › **Adaptive**: Practices fully established and continuously improved
- Tier 3 › **Repeatable**: Practices approved and established by organizational policy
- Tier 2 › **Risk Informed**: Practices approved but not completely established by policy
- Tier 1 › **Partial**: Informal, ad hoc, reactive responses

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.***

PROJECT STATUS

- A technical meeting was held in November to develop the cybersecurity profile and conduct a privacy risk assessment.

- Step One: Define the AACVTE Mission

  - *Using communications between vehicles and the infrastructure to enable applications that improve safety, mobility and sustainability*.

PROJECT STATUS

- Step Two: Define the AACVTE Mission Objectives
  - 16 Objectives identified
  - Grouped into 4 categories

- The Core Functions were then transposed to the categories and subcategories of the Cyber Framework. The group then prioritized the functions.

Mission Objectives
Develop Requirements
a. Develop application requirements
Design and Build
a. Install devices
b. Specify components
c. Plan network architecture
d. Define Security architecture
e. Develop installation & verification procedures
f. Procure components and select suppliers
Verification and validation
a. Test devices/certification
b. Evaluate performance and complia
Operations and maintenance
a. Support data analysis
b. Maintain data
c. Manage assets
d. Operate and maintain system
e. Perform communications and mark
f. Conduct education and outreach
g. Recruit subjects/users

Functions	
ID	Identify
PR	Protect
DE	Detect
RS	Respond
RC	Recover

PROJECT STATUS

- Developed the Privacy Risk Assessment Methodology (PRAM)
  - PRAM is a process to assess the risk to personally identifiable information (PII) in a system/organization.
  - Evaluated the data flows in the system to understand the use of PII.

LOOKING AHEAD

- The NIST team will use the information from the workshop to:
  - Develop the implementation tiers.
  - Develop guidance on handling PII in a connected vehicle environment.

- Coordinate with the CV Pilot sites

- Develop guidance adapted specifically for the connected vehicle environment.

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**