

# APPLYING NIST CSF TO A CV DEPLOYMENT

*ITS World Congress 2018*  
TS50 : SECURITY

September 20, 2018

Ray Resendes  
Volpe National Transportation Center  
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.

---

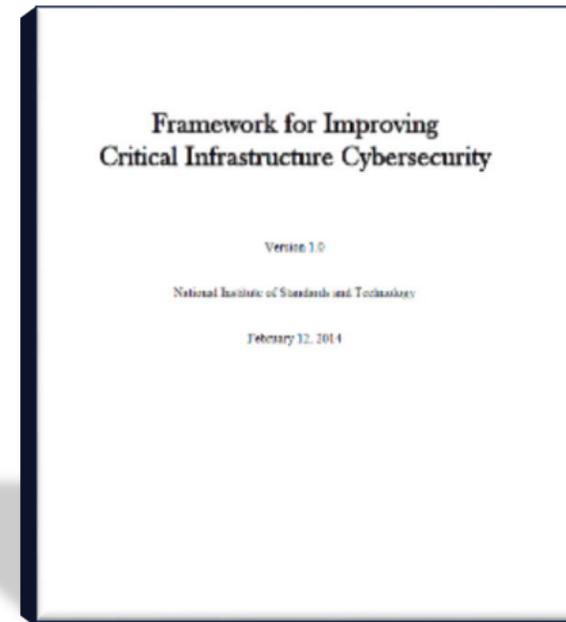
# NIST CYBERSECURITY FRAMEWORK

---

## NIST CSF

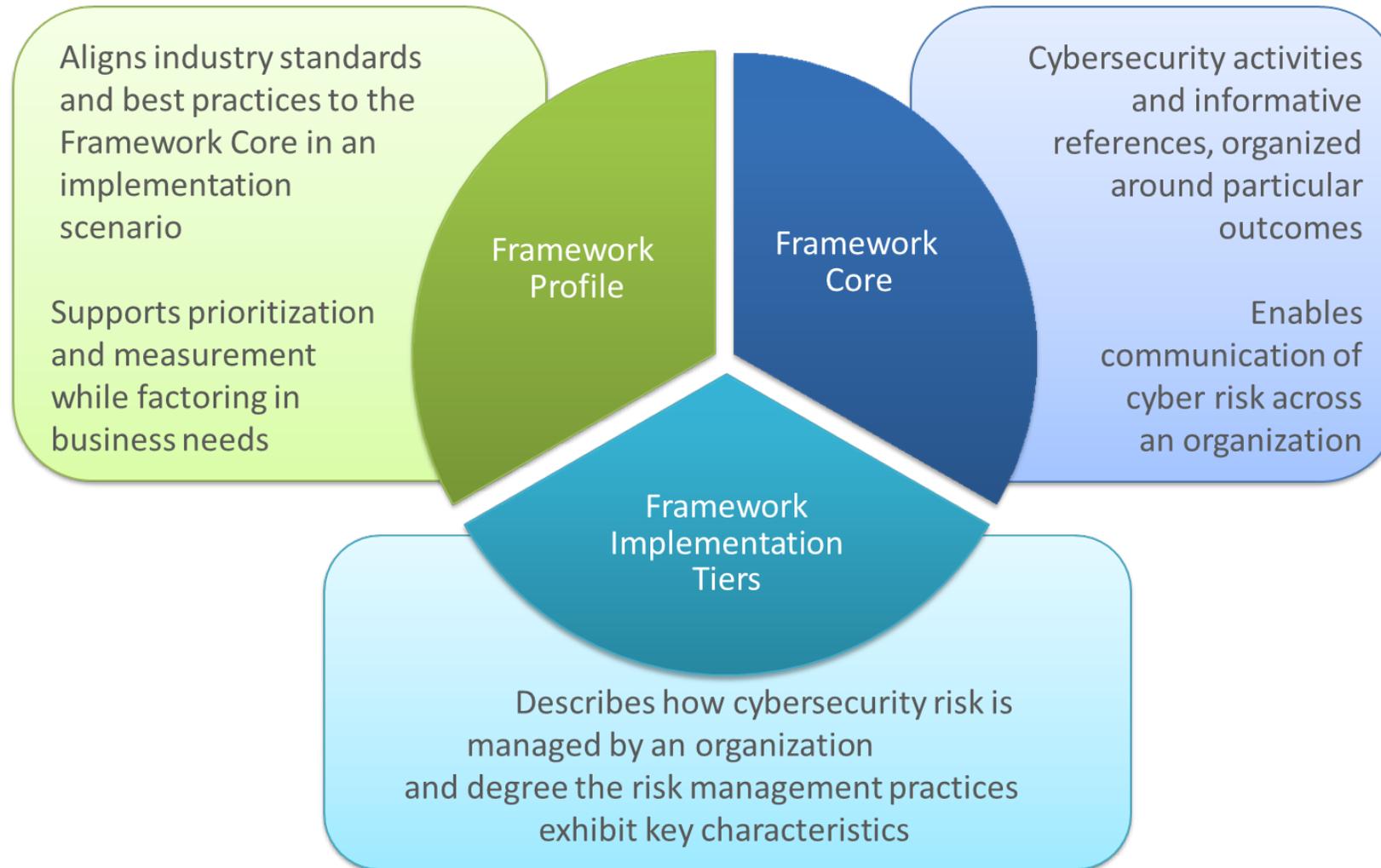
Outcome of Executive Order 13636, and result of collaboration between public and private sectors

- 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



# CYBERSECURITY FRAMEWORK COMPONENTS

---



# CYBERSECURITY FRAMEWORK PROFILE DEVELOPMENT STEPS

---

<b>Define the Scope of the Profile</b>	<b>Completed</b>
<b>Determine Initial Scope of the Profile</b>	<b>Completed</b>
<b>Conduct stakeholder workshops</b> <ul style="list-style-type: none"><li>• <b>Conduct Mission Objective Development</b></li><li>• <b>Conduct Mission Objective Scoring</b></li></ul>	<b>Completed</b>
<b>CSF Profile Post-Workshop Analysis</b> <ul style="list-style-type: none"><li>• <b>Analyze Category Scoring</b></li><li>• <b>Develop &amp; Share Draft Mission Objectives &amp; Category Scoring</b></li><li>• <b>Develop Subcategory selection</b></li><li>• <b>Develop Summary Subcategory-Level Matrix</b></li><li>• <b>Develop Detailed Matrix</b></li></ul>	<b>Completed</b>
<b>Develop Profile and Guidance Document</b>	<b>In-Progress</b>

---

# DEVELOP MISSION OBJECTIVES

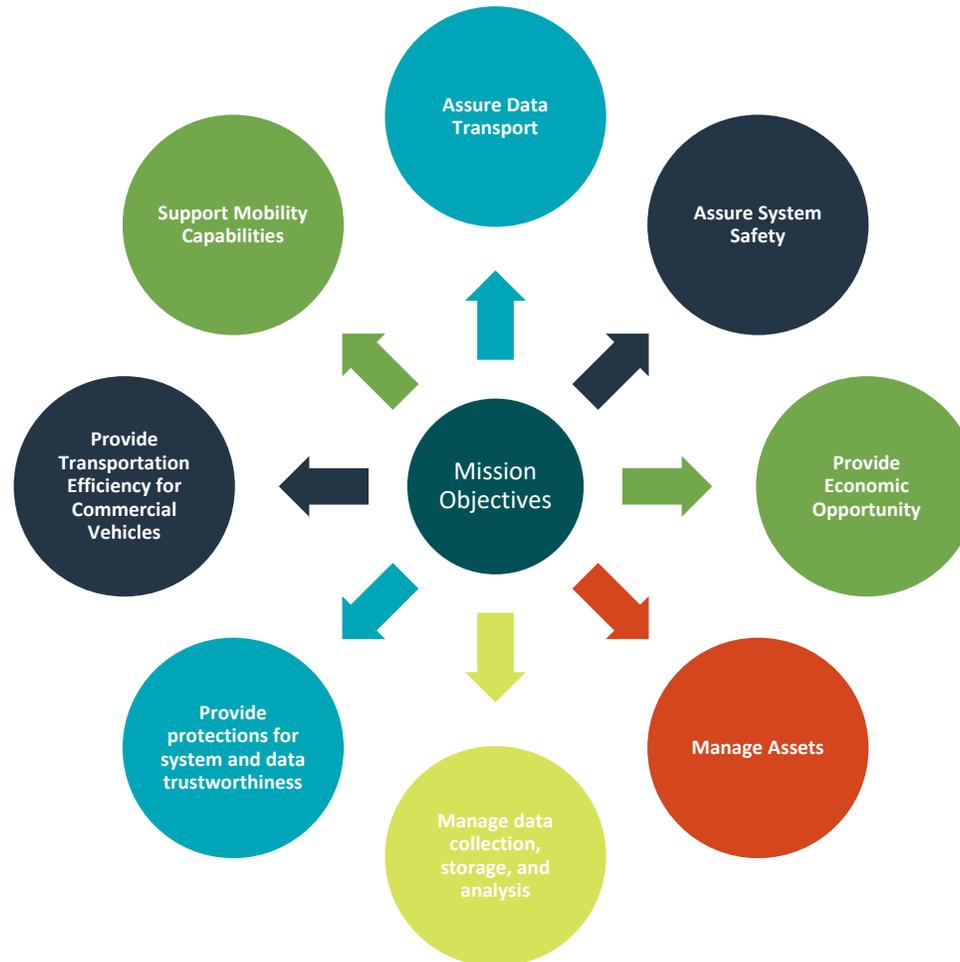


KEY:

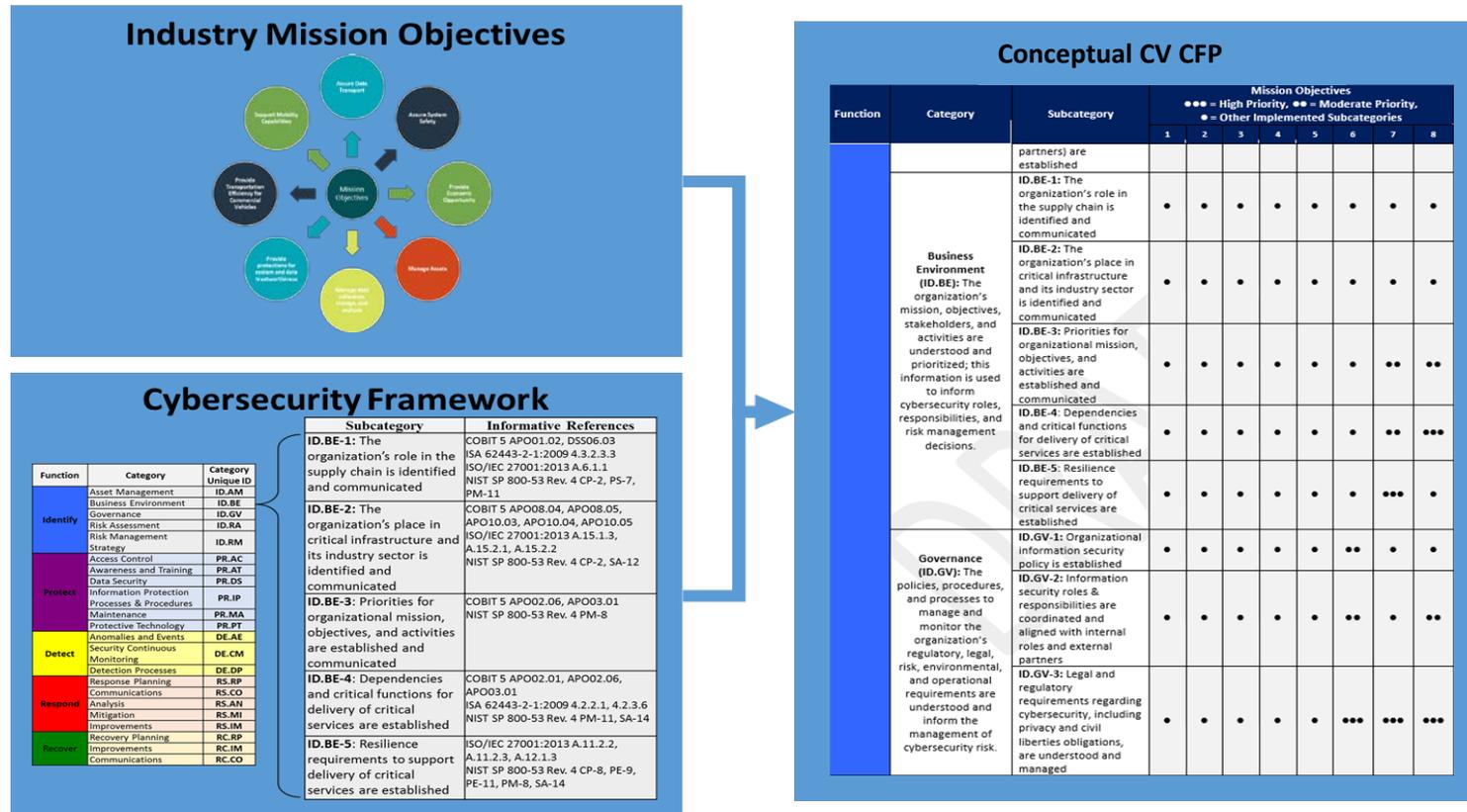
All Consensus

AACVTE

# RANKING THE MISSION OBJECTIVES BY TRANSPOSING MISSION TO CYBER

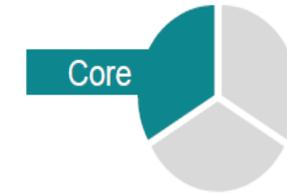


# CYBERSECURITY FRAMEWORK PROFILE POST-WORKSHOP ANALYSIS



# CSF – FUNCTIONS

## Functions



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

# SUMMARY OF SUBCATEGORY PRIORITIES BY MISSION OBJECTIVE

Function	Category	Subcategory	Mission Objectives											
			1	2	3	4	5	6	7	8	9	10	11	12
IDENTIFY (ID)	Asset Management (ID.AM): The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to business objectives and the organization's risk strategy.	ID.AM-1: Physical devices and systems within the organization are inventoried	•	•••	•	•	••	•••	•	•••	•	•	•	
		ID.AM-2: Software platforms and applications within the organization are inventoried	•	•••	•	•	••	••	•	•••	•	•	•	
		ID.AM-3: Organizational communication and data flows are mapped	•	•••	•••	•	•••	•••	•	••	•	•	•	
		ID.AM-4: External information systems are catalogued	•	••	••	•	••	••	•	•••	•	•	•	
		ID.AM-5: Resources (e.g., hardware, devices, data, time, personnel, and software) are prioritized based on their classification,	•	•••	••	•	••	•••	•	•••	•	•	•	

# FRAMEWORK SUBCATEGORIES

Function	Category	Subcategory	Informative References
<b>IDENTIFY (ID)</b>	<b>Asset Management (ID.AM):</b> The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to organizational objectives and the organization's risk strategy.	<b>ID.AM-1:</b> Physical devices and systems within the organization are inventoried	CIS CSC 1 COBIT 5 BAI09.01, BAI09.02 ISA 62443-2-1:2009 4.2.3.4 ISA 62443-3-3:2013 SR 7.8 ISO/IEC 27001:2013 A.8.1.1, A.8.1.2 NIST SP 800-53 Rev. 4 CM-8, PM-5
		<b>ID.AM-2:</b> Software platforms and applications within the organization are inventoried	CIS CSC 2 COBIT 5 BAI09.01, BAI09.02, BAI09.05 ISA 62443-2-1:2009 4.2.3.4 ISA 62443-3-3:2013 SR 7.8 ISO/IEC 27001:2013 A.8.1.1, A.8.1.2, A.12.5.1 NIST SP 800-53 Rev. 4 CM-8, PM-5
		<b>ID.AM-3:</b> Organizational communication and data flows are mapped	CIS CSC 12 COBIT 5 DSS05.02 ISA 62443-2-1:2009 4.2.3.4 ISO/IEC 27001:2013 A.13.2.1, A.13.2.2 NIST SP 800-53 Rev. 4 AC-4, CA-3, CA-9, PL-8
		<b>ID.AM-4:</b> External information systems are catalogued	CIS CSC 12 COBIT 5 APO02.02, APO10.04, DSS01.02 ISO/IEC 27001:2013 A.11.2.6 NIST SP 800-53 Rev. 4 AC-20, SA-9
		<b>ID.AM-5:</b> Resources (e.g., hardware)	CIS CSC 13, 14

# NEXT STEPS

---

- Draft under review September 2018
- Webinar November 2018
- Public Release January 2019
- Public Workshop February 2019
  
- *Initiate development for an ITS-wide Profile* January 2019



# STAY CONNECTED

---

For more information, contact...

## **Ray Resendes**

Volpe National Transportation Center  
U.S. Department of Transportation  
[Raymond.Resendes@dot.gov](mailto:Raymond.Resendes@dot.gov)

## **Kevin Gay**

ITS Joint Program Office  
U.S. Department of Transportation  
[Kevin.Gay@dot.gov](mailto:Kevin.Gay@dot.gov)



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