PRIORITIZING MISSION OBJECTIVES

Ranking System

- How important is each Mission Objective?
  - Scale: 1, 3, 5, 8, 13

1 3 5 8 13

SAMPLE CATEGORY PRIORITIZATION WORKSHEET

Mission Objectives	Categories (Please Label)														
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
IDENTIFY															
Asset Management (ID.AM)	2	1	1	1			1	H	1		H	1	H		
Business Environment (ID.BE)										1		2		3	3
Governance (ID.GV)															
Risk Assessment (ID.RA)														2	2
Risk Management Strategy (ID.RM)					H	H			3	3		3		1	1
PROTECT															
Access Control (PR.AC)										2		H	1		
Awareness and Training (PR.AT)															H
Data Security (PR.DS)	H		2	2		1	2	H					2		
Information Protection Processes & Procedures (PR.IP)		H		3	H				2		H			H	
Maintenance (PR.MA)						2									
Protective Technology (PR.PT)						3									
DETECT															
Anomalies and Events (DE.AE)		2		H							2	H		H	H
Security Continuous Monitoring (DE.CM)			3		1					H			H		
Detection Processes (DE.DP)	1					H	3	1	H		1				
RESPOND															
Response Planning (RS.RP)			H	H				2				H	H	H	H
Communications (RS.CO)											3				
Analysis (RS.AN)		3													
Mitigation (RS.MI)	3				2	H	H		H	H			3		
Improvements (RS.IM)															
RECOVER															
Recovery Planning (RC.RP)	H	H	H	H		H	H	3	H	H	H	H	H	H	H
Improvements (RC.IM)					3										
Communications (RC.CO)															

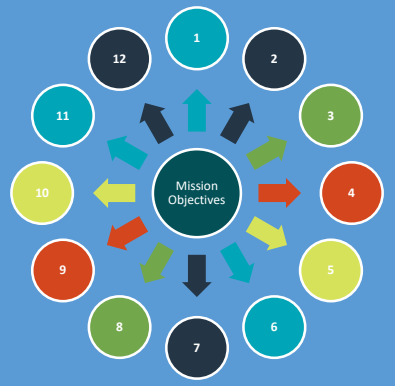
RANKING THE MISSION OBJECTIVES BY TRANSPOSING MISSION TO CYBER

1. Ensure Secure and Timely Communications
2. Plan, Deploy, and Operate Network
3. Manage Data Collection and Storage
4. Build Privacy into CV Program
5. Improve Mobility for Passenger Vehicles
6. Provide Transportation Efficiency for Commercial Vehicles and Fleets

7. Manage Users
8. Assure Asset Security and Operational Viability
9. Conduct Data Analyses
10. Minimize Driver Distraction and Workload
11. Measure and Evaluate Performance
12. Perform Strategic Communications to Facilitate Business and Driver Adoption

CYBERSECURITY FRAMEWORK PROFILE DEVELOPMENT

CV Pilot Mission Objectives



Cybersecurity Framework

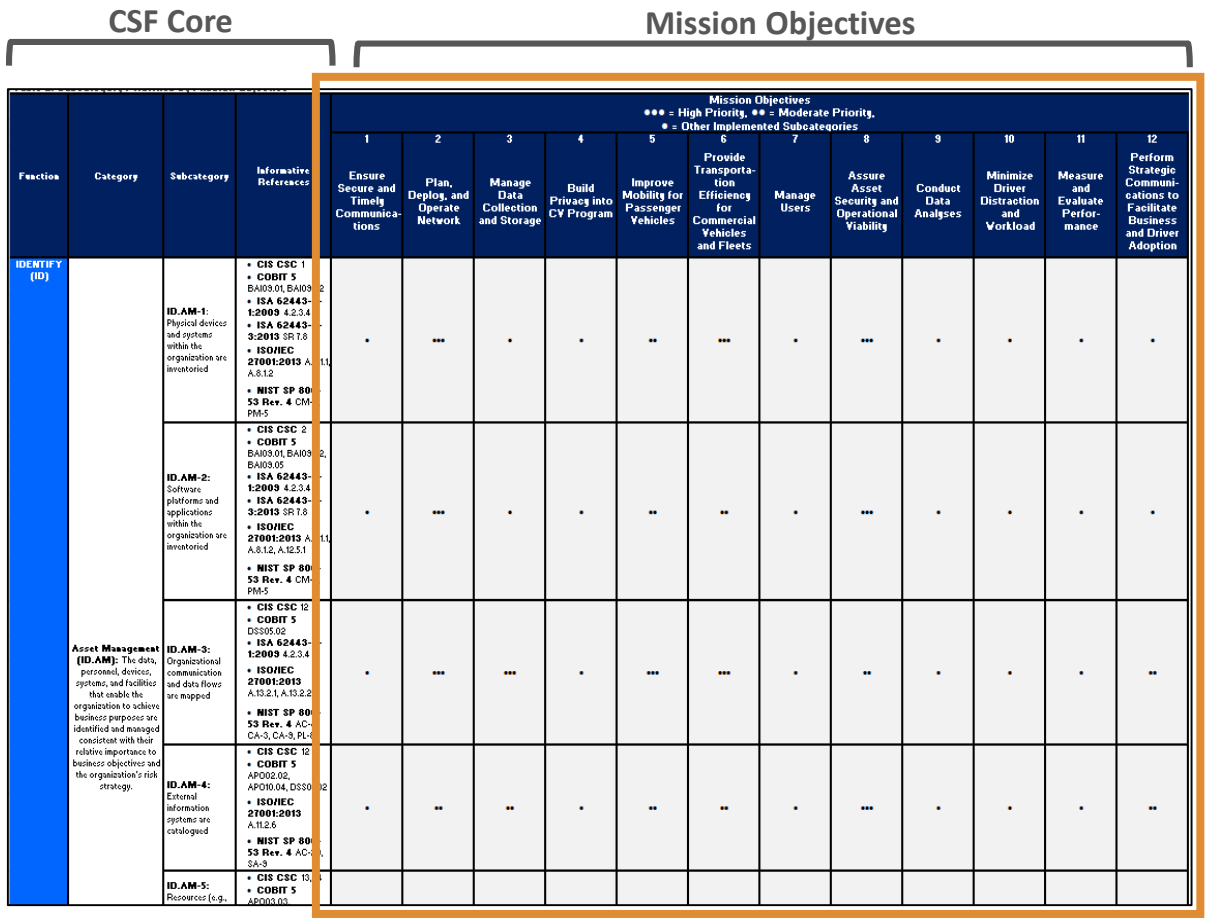
Function	Category
IDENTIFY (ID)	Asset Management (ID.AM)
	Business Environment (ID.BE)
	Governance (ID.GV)
	Risk Assessment (ID.RA)
	Risk Management Strategy (ID.RM)
	Supply Chain Risk Management (ID.SC)
PROTECT (PR)	Identity Management, Authentication and Access Control (PR.AC)
	Awareness and Training (PR.AT)
	Data Security (PR.DS)
	Information Protection Processes and Procedures (PR.IP)
	Maintenance (PR.MA)
	Protective Technology (PR.PT)
DETECT (DE)	Anomalies and Events (DE.AE)
	Security Continuous Monitoring (DE.CM)
	Detection Processes (DE.DP)
RESPOND (RS)	Response Planning (RS.RP)
	Communications (RS.CO)
	Analysis (RS.AN)
	Mitigation (RS.MI)
	Improvements (RS.IM)
RECOVER (RC)	Recovery Planning (RC.RP)
	Improvements (RC.IM)
	Communications (RC.CO)

Category	Subcategory
ID.BE-1: The organization's role in the supply chain is identified and communicated	• **COBIT 5** APO08.01, APO08.04, APO08.05, APO10.03, APO10.04, APO10.05 • **ISO/IEC 27001:2013** A.15.1.1, A.15.1.2, A.15.1.3, A.15.2.1, A.15.2.2 • **NIST SP 800-53 Rev. 4** CP-2, SA-12
ID.BE-2: The organization's place in critical infrastructure and its industry sector is identified and communicated	• **COBIT 5** APO02.06, APO03.01 • **ISO/IEC 27001:2013** Clause 4.1 • **NIST SP 800-53 Rev. 4** PM-8
ID.BE-3: Priorities for organizational mission, objectives, and activities are established and communicated	• **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-4: Dependencies and critical functions for delivery of critical services are established	• **COBIT 5** APO10.01, BAI04.02, BAI09.02 • **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
ID.BE-5: Resilience requirements to support delivery of critical services are established for all operating states (e.g. under duress/attack, during recovery, normal operations)	• **COBIT 5** BAI03.02, DSS04.02 • **ISO/IEC 27001:2013** A.11.1.4, A.17.1.1, A.17.1.2, A.17.2.1 • **NIST SP 800-53 Rev. 4** CP-2, CP-11, SA-13, SA-14

Draft CV Pilot CSF Profile (Representative Excerpt)

Function	Category	Subcategory	Informative References	Mission Objectives ●●● = High Priority, ●● = Moderate Priority, ● = Other Implemented Subcategories											
				1 Ensure Secure and Timely Communications	2 Plan, Deploy, and Operate Network	3 Manage Data Collection and Storage	4 Build Privacy into CV Program	5 Improve Mobility for Passenger Vehicles	6 Provide Transportation Efficiency for Commercial Vehicles and Fleets	7 Manage Users	8 Assure Asset Security and Operational Viability	9 Conduct Data Analyses	10 Minimize Driver Distraction and Workload	11 Measure and Evaluate Performance	12 Perform Strategic Communications to Facilitate Business and Driver Adoption
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	• **CIS CSC** 1 • **COBIT 5** BAI03.01, BAI03.02 • **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	●	●●●	●	●	●●	●●●	●	●●●	●	●	●	●
		ID.AM-2: Software platforms and applications within the organization are inventoried	• **CIS CSC** 2 • **COBIT 5** BAI03.01, BAI03.02, BAI03.05 • **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	●	●●●	●	●	●●	●●	●	●●●	●	●	●	●
		ID.AM-3: 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	●	●●●	●●●	●	●●●	●●●	●	●●	●	●	●	●●
		ID.AM-4: 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	●	●●	●●	●	●●	●●	●	●●●	●	●	●	●●
		ID.AM-5: Resources (e.g.,	• **CIS CSC** 13, 14 • **COBIT 5** APO03.03,												

CYBERSECURITY FRAMEWORK PROFILE CONTENTS AND USE



Function	Category	Subcategory	Informative References	Mission Objectives ●●● = High Priority, ●● = Moderate Priority, ● = Other Implemented Subcategories											
				1 Ensure Secure and Timely Communications	2 Plan, Deploy, and Operate Network	3 Manage Data Collection and Storage	4 Build Privacy into CV Program	5 Improve Mobility for Passenger Vehicles	6 Provide Transportation Efficiency for Commercial Vehicles and Fleets	7 Manage Users	8 Assure Asset Security and Operational Viability	9 Conduct Data Analyses	10 Minimize Driver Distraction and Workload	11 Measure and Evaluate Performance	12 Perform Strategic Communications to Facilitate Business and Driver Adoption
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	• CIS CSC 1 • COBIT 5 BAI03.01, BAI09.[illegible] • ISA 62443-[illegible]:2009 4.2.3.4 • ISA 62443-[illegible]:2013 SR 7.8 • ISO/IEC 27001:2013 A.[illegible].1.1, A.8.1.2 • NIST SP 800-53 Rev. 4 CM-8, PM-5	●	●●●	●	●	●●	●●●	●	●●●	●	●	●	●
		ID.AM-2: Software platforms and applications within the organization are inventoried	• CIS CSC 2 • COBIT 5 BAI03.01, BAI03.[illegible], BAI03.05 • ISA 62443-[illegible]:2009 4.2.3.4 • ISA 62443-[illegible]:2013 SR 7.8 • ISO/IEC 27001:2013 A.[illegible].1.1, A.8.1.2, A.12.5.1 • NIST SP 800-53 Rev. 4 CM-8, PM-5	●	●●●	●	●	●●	●●	●	●●●	●	●	●	●
		ID.AM-3: Organizational communication and data flows are mapped	• CIS CSC 12 • COBIT 5 DSS05.02 • ISA 62443-[illegible]: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-[illegible]	●	●●●	●●●	●	●●●	●●●	●	●●	●	●	●	●●
		ID.AM-4: External information systems are catalogued	• CIS CSC 12 • COBIT 5 APO02.02, APO10.04, DSS01.[illegible] • ISO/IEC 27001:2013 A.11.2.6 • NIST SP 800-53 Rev. 4 AC-[illegible], SA-9	●	●●	●●	●	●●	●●	●	●●●	●	●	●	●●
		ID.AM-5: Resources (e.g.,	• CIS CSC 13, [illegible] • COBIT 5 APO03.03												

Prioritized Subcategories for Each Mission Objective

- Industry and mission/business contexts inform priority Subcategories
  - Suggests areas of focus for newer cybersecurity programs
  - Provides a crosswalk for established programs demonstrate their capabilities
- Three levels:
  - ●●● = High Priority
  - ●● = Moderate Priority
  - ● = Other Implemented Subcategories
- Organizations should strive to conduct activities in support of all relevant Subcategories
- Organizations have the flexibility to determine how and in what order they address High and Moderate Priority Subcategories
- Implementation details may facilitate use

SUMMARY OF SUBCATEGORY PRIORITIES BY MISSION OBJECTIVE

Function	Category	Subcategory	Mission Objectives ●●● = High Priority, ●● = Moderate Priority, ● = Other Implemented Subcategories ✕ = Subcategories to NOT Implement											
			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
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 organizational objectives and the organization's risk strategy.	**ID.AM-1:** 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
		ID.AM-2: 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
		ID.AM-3: 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
		ID.AM-4: 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
		ID.AM-5: Resources (e.g., hardware	**CIS CSC** 13, 14