Transportation Systems Sector
Voluntary Web-Based Survey of NIST Version 1.1 Cybersecurity Framework Use

Overview
The National Institute of Standards and Technology (NIST) Framework for Improving Critical Infrastructure Cybersecurity Version 1.1 (Framework) is voluntary guidance—based on existing standards, guidelines, and practices—for organizations to better manage and reduce cybersecurity risk. NIST designed the Framework to help organizations manage and reduce risks. The Department of Transportation (DOT), Transportation Security Administration (TSA), and United States Coast Guard (USCG) need the information provided in this survey to provide operational awareness as to the readiness of the Transportation Systems Sector (TSS), and to better tailor education and outreach activities to help mitigate the risk associated with cyber-related threats to the TSS.

Q1. With which transportation sector is your organization associated? (Question 1)
With which transportation subsector is your organization associated? (Question 1a)
(Tree> Select one applicable sector then all subsectors that apply for second tier.)
(Next question for all answers it Q2.)

- ☐ Aviation
  - o Air Cargo
  - o Airports
  - o Commercial Airline
  - o General Aviation
- ☐ Freight Rail
  - o Class I
  - o Class II or Class III
- ☐ Highway and Motor Carrier
  - o Over-the-Road-Bus (Motorcoach)
  - o Pupil Transportation (School Bus)
  - o Trucking
  - o Infrastructure (Bridges and Tunnels)
- ☐ Maritime
  - o Maritime Transportation Security Act (MTSA) Regulated Facilities
  - o Non-regulated Facilities
  - o Passenger Vessels
  - o Maritime Bulk Liquid
  - o Offshore Operations
  - o Fishing Vessels
  - o Container Vessels
  - o Tankers
  - o Liquefied Natural Gas (LNG) Vessel
  - o Other MTSA regulated Vessel
- ☐ Mass Transit and Passenger Rail

OMB control number: 1652-0058

Exp. 9/30/2022

- Mass Transit (Heavy and Light rail, Transit Bus)
- Passenger Rail (Commuter Rail and Interstate Railroads)

- ☐ Pipeline Systems
  - Natural Gas (Transmission and Distribution)
  - Liquid (Upstream, Midstream or Downstream)
- ☐ Postal and Shipping

Q2. What is the size of your organization's workforce? Including contractors. (Select one)
(Go to Q3.)

- ☐ 1 to 500 employees
- ☐ 501 to 1,500 employees
- ☐ 1,501 to 5,000 employees
- ☐ 5,001+ employees

Q3. Is your organization aware of the Framework? (Select one)
(if Yes go to Q4. If no go to Q14)

- ☐ Yes
- ☐ No

Q4 How did your organization become aware of the Framework? (Select the most applicable) ***(Next Question Q5)***

- ☐ Federal Government
- ☐ Local and/or State Government
- ☐ Fusion Center
- ☐ Private Sector Risk Management Companies
- ☐ Trade Associations
- ☐ Information Sharing and Analysis Centers (ISACs)
- ☐ Online Media Outlets
- ☐ Other Critical Sector
- ☐ Other, please explain (do not include any PII): _____

Q5. Is your organization using the Framework? (Select one)
(If Yes go to Q6 If no go to Q11)

- ☐ Yes
- ☐ No.

Q6. How is your organization using the Framework? (Select all that apply)
(Go to Q7)

- ☐ To inform our approach to infrastructure cybersecurity
- ☐ To serve as a basis for an assessment of our infrastructure cybersecurity efforts
- ☐ To serve as the foundational methodology for our technical approach to infrastructure cybersecurity

- ☐ To serve as a foundational methodology for a company-wide, leadership-driven infrastructure cybersecurity risk management effort
- ☐ Our organization is not using the Framework
- ☐ Other: Please explain (do not include any PII): _____

Q7 To what extent has your organization implemented the Framework's five (5) core functions? (Select what applies)
(Go to Q8.)

	NIST Core Functions				
Implementation Level	Identify	Protect	Detect	Respond	Recover
Fully implemented what is applicable to our organization					
Have mostly implemented what is applicable to our organization					
Have implanted some items					
Have not implemented anything in the core function					
Not aware of any implementation					

Q8: Has your organization leveraged the Framework to develop a cybersecurity profile specific to your organization? (select one) ***(Go to Q9.)***

- ☐ Yes
- ☐ No
- ☐ Not sure

Please explain (do not include any PII):
_____

Q9: Did a contract or other agreement required implementation of the Framework?) ***(Go to Q10.)***

- ☐ Yes
- ☐ No _____

Q10: To the best of your ability please determine the general value the Framework has provided to these aspects of your organization. (select what applies) ***(Go to Q11.)***

	Effect			
Possible Value of Framework Regarding:	**Positive**	**Neutral**	**Negative**	**Non-Applicable**
Understanding or managing cybersecurity risk				
Managing or fulfilling cybersecurity requirements				
Prioritizing the relative importance of cybersecurity requirements or activities				

Determining areas for improvement and developing plans to achieve improvements				
Reducing risk				

Q11. What are the challenges to using the Framework? (Select all that apply) ***(go to Q12)***

- ☐ Lack of specific implementation guidance or technical information sources
- ☐ The Framework is complex and difficult to understand
- ☐ Our organization lacks technical expertise to support implementation
- ☐ We have insufficient information on the cost burden of Framework implementation
- ☐ Insufficient budget
- ☐ Cost-effectiveness considerations
- ☐ Our organization uses some other standard(s)/framework(s) instead
- ☐ Regulatory requirements or mandatory standards that may conflict with the Framework
- ☐ Other
- ☐ Please explain your selections (do not include any PII): _____

Q12. Are there any perceived gaps within the Framework? ***(Next Question is Q13)***

- ☐ Yes, Please Explain (do not include any PII): -
  _____
- ☐ No.

Q13. What topics would like to see addressed or expanded upon in future versions of the Framework? (Select all that Apply)
(Go to Q14.)

- ☐ Access Control
- ☐ Analysis
- ☐ Anomalies and Events
- ☐ Asset Management
- ☐ Awareness and Training
- ☐ Business Environment
- ☐ Communications
- ☐ Data Security
- ☐ Detection Processes
- ☐ Governance
- ☐ Improvements
- ☐ Information Protection and Procedures
- ☐ Maintenance
- ☐ Mitigation
- ☐ Protective Technology
- ☐ Recovery Planning
- ☐ Response Planning
- ☐ Risk Assessment

- ☐ Risk Management Strategy
- ☐ Security Continuous Monitoring
- ☐ Other
  Please explain (do not include any PII): _____

Q14. Is your organization using a cybersecurity risk management methodology in addition to or other than the Framework? (For example: API 1164, CIS Critical Security Controls, ISO/IEC Standards (ISO 27000 and/or 31000 Series))

(If yes go to Q15, if No go to Q16)

- ☐ Yes.
- ☐ No.

Q15. Which industry recognized cybersecurity standards does your organization use to support the Framework or other cybersecurity risk methodology? (Select all that Apply)
(Go to Question 16.)

- ☐ API 1164
- ☐ CIS Critical Security Controls
- ☐ Control Objectives for Information and Related Technologies (COBIT)
- ☐ Committee of Sponsoring Organizations of the Treadway Commission (COSO)
- ☐ ISO/IEC Standards (ISO 27000 and/or 31000 Series)
- ☐ North American Electric Reliability Corporation (NERC CIP)
- ☐ Payment Card Industry Data Security Standard (PCI DSS)
- ☐ Technical Committee on CyberSecurity (TY CYBER)
- ☐ NIST SP800-53
- ☐ Other: Please Explain/List (do not include any PII)
  _____

Q16. Are you aware of the Transportation Systems Sector's (TSS) NIST Cybersecurity Framework Implementation Guidance? (Select one)
(If yes go to Q17; If no, go to Q18)

- ☐ Yes
- ☐ No

Q17. Was the TSS Framework Implementation Guidance helpful in your organization's efforts to implement the Framework? (Select one)
(Go to Q18)

- ☐ Yes
- ☐ No
- ☐ To some extent
  Please explain (do not include any PII): _____

Q18. Has your organization used any other Framework implementation guidance other than the TSS Cybersecurity Framework Implementation Guidance? ***(Select One)***
(If yes go to Q19, if no or not aware go to 20.)

- ☐ Yes
- ☐ No
- ☐ Not aware of such guidance

Q19. What was the source(s) of the Framework Guidance your organization uses? (Check all that apply)
(go to Q20)

- ☐ Local and/or State Government
- ☐ Fusion Center
- ☐ Private Sector Risk Management Companies
- ☐ Trade Associations
- ☐ Information Sharing and Analysis Centers (ISACs)
- ☐ Online Tutorials
- ☐ Other Sector Specific Agency

Q20. From where does your organization receive cybersecurity threat information and alerts? (Select all that apply)
(Go to Q21.)

- ☐ Aviation Cyber Initiative
- ☐ Aviation Domain Intelligence Integration and Analysis Cell
- ☐ Cybersecurity and Infrastructure Security Agency
- ☐ Department of Defense
- ☐ Department of Energy,
- ☐ Department of Transportation
- ☐ Federal Aviation Administration
- ☐ Federal Bureau of Investigation
- ☐ Fusion Centers
- ☐ Information Sharing and Analysis Centers (ISACs) For example: Auto-ISAC, Aviation-ISAC, ST-ISAC, MT-ISAC
- ☐ Local and/or State Government
- ☐ Pipeline Cybersecurity Initiative
- ☐ Private Sector Information Security Providers
- ☐ Surface Information Sharing Cell (SISC)
- ☐ Trade Associations
- ☐ Transportation Security Administration
- ☐ United States Coast Guard
- ☐ Other
  Please explain (do not include any PII):
  _____

Q21. From where does your organization get cybersecurity recommended practices? (Select all that apply)
(Go to Q22.)

- ☐ Aviation Cyber Initiative
- ☐ Cybersecurity and Infrastructure Security Agency
- ☐ Department of Defense
- ☐ Department of Energy,
- ☐ Department of Transportation
- ☐ Federal Aviation Administration
- ☐ Federal Bureau of Investigation
- ☐ Fusion Centers
- ☐ Information Sharing and Analysis Centers (ISACs) For example: Auto-ISAC, Aviation-ISAC, ST-ISAC, MT-ISAC
- ☐ Local and/or State Government
- ☐ Pipeline Cybersecurity Initiative
- ☐ Private Sector Information Security Providers
- ☐ Trade Associations
- ☐ Transportation Security Administration
- ☐ United States Coast Guard
- ☐ Other
  Please explain (do not include any PII):
  _____

Q22. To what extent does your organization apply the Framework or cybersecurity guidance to your supply chain? (Select all that apply)
(Go to Q23.)

- ☐ Please explain (do not include any PII): _____

Q23. What is the best method for your organization to receive information and/or learn more about the Framework? (Select all that apply)
(Go to Q24.)

- ☐ Email
- ☐ Homeland Security Information Network (HSIN)
- ☐ Websites
- ☐ Webinars
- ☐ In-person Training
- ☐ Online Training
- ☐ Other: Please explain (do not include any PII): _____

Q24. Are there any additional comments, concerns, or questions that you would like to share with the Transportation Systems Sector co-SSA regarding voluntary adoption of the NIST Cybersecurity Framework and its implementation?

(End of Survey)

- Please explain (do not include any PII): _____

Thank you for participating in this survey. We will use your feedback to help us better support Transportation Systems Sector partners in improving critical infrastructure cybersecurity.

PAPERWORK REDUCTION ACT STATEMENT: TSA is collecting this information to gather input from Transportation Systems Sector stakeholders on the adoption of the NIST Version 1.1 Cybersecurity Framework. The public burden for collecting this information is estimated to be approximately 10 minutes. This is a voluntary collection of information. Send comments regarding this burden estimate or collection to: TSA-11, Attention: PRA 1652-0058, Transportation Systems Sector Voluntary Web-Based Survey of NIST Version 1.1 Cybersecurity Framework Use, 6595 Springfield Center Drive, Springfield, VA 20598. An agency may not conduct or sponsor, and persons are not required to respond to a collection of information, unless it displays a valid OMB control number. The OMB control number assigned to this collection is 1652-0058, which expires 09/30/2022.