To: Diane Honeycutt, National Institute of Standards and Technology

From: Robert Arnold, Director, Office of Transportation Management –
U.S. Department of Transportation, Federal Highway Administration (FHWA)

Subj: Views on the Framework for Improving Critical Infrastructure Cybersecurity

Date: February 9, 2016

1. Describe your organization and its interest in the Framework.

In regard to the Framework, the role of FHWA is to coordinate, develop, and provide federal oversight and financial support for technology based highway transportation infrastructures administered by the State and local transportation agencies. We also provide technical assistance, promote the awareness of the Framework, and customize the Framework and its use for agencies to assess their transportation programs on cyber security risk.

2. Indicate whether you are responding as a Framework user/non-user, subject matter expert, or whether you represent multiple organizations that are or are not using the Framework.

In terms of the implementation of the Framework, the FHWA is a non-direct user and a subject matter expert. FHWA uses the Framework to develop guides and related policies, and to provide technical assistance and guidance to improve cyber resilience to the highway transportation sector.

3. If your organization uses the Framework, how do you use it? (*e.g.*, internal management and communications, vendor management, C-suite communication).

The FHWA is planning to recommend the use of the Framework as part of its outreach efforts to the transportation sector. The FHWA currently uses the Framework as a guide to develop guidelines and policies that can enhance the operations and safety for surface transportation at operating agencies.

4. What has been your organization's experience utilizing specific portions of the Framework (*e.g.*, Core, Profile, Implementation Tiers, Privacy Methodology)?

The use of the Framework and comprehensive understanding of cyber security is an emerging area for FHWA. Understanding of the principles also varies greatly for the States and local Department of Transportation's throughout the country. Current use of the Framework by States Department of Transportation and documenting the current

state of practice are not documented. Use of the Framework is not specified in Strategic Planning documents.

5. What portions of the Framework are most useful?

Collectively, the entire framework is useful to assess the agencies transportation management system program cyber security risk.

6. What portions of the Framework are least useful?

There are differences in terminologies and the use of the CS Framework requires a level of understanding of the concept behind control system resilience. The Framework can be challenging for organizations without such institutional knowledge to accept its utility as a tool. Functional and contextual description of terminologies and concepts can be helpful.

7. Has your organization's use of the Framework been limited in any way? If so, what is limiting your use of the Framework (*e.g.*, sector circumstance, organizational factors, Framework features, lack of awareness)?

There is not enough awareness from the transportation sector. For many transportation agencies, the development and implementation of the Framework is not yet on their priority list of things to do and is competing with the day-to-day operations (i.e. capital and safety projects, traffic operations programs, emergency maintenance operations etc.) activities of the State Department of Transportation agencies. Use of the Framework is not articulated within the State's Department of Transportation Strategic Planning documents and may not be one of the major strategic goals.

8. To what extent do you believe the Framework has helped reduce your cybersecurity risk? Please cite the metrics you use to track such reductions, if any.

N/A

9. What steps should be taken to "prevent duplication of regulatory processes and prevent conflict with or superseding of regulatory requirements, mandatory standards, and related processes" as required by the Cybersecurity Enhancement Act of 2014? [7]

Coordination and effective communications across the board would help. The lead federal agency for the Framework should have the main oversight and program administration in coordination with the federal sector agencies (USDOE, USDOT, USDOC etc.).

Possible Framework Updates.

10. Should the Framework be updated? Why or why not?

The Framework should be updated to include all the sector stakeholder needs including new emerging areas within their respective industries.

11. What portions of the Framework (if any) should be changed or removed? What elements (if any) should be added to the Framework? Please be as specific as possible.

n/a - no comment at this time

12. Are there additions, updates or changes to the Framework's references to cybersecurity standards, guidelines, and practices that should be considered for the update to the Framework?

n/a - no comment at this time

13. Are there approaches undertaken by organizations—including those documented in sector-wide implementation guides—that could help other sectors or organizations if they were incorporated into the Framework?

Yes, presently developing localization and tools to implement the framework for surface transportation specific to roadways.

14. Should developments made in the nine areas identified by NIST in its Framework-related "Roadmap" [8] be used to inform any updates to the Framework? If so, how?

n/a - no comment at this time

15. What is the best way to update the Framework while minimizing disruption for those currently using the Framework?

Implement a Configuration Management Plan to track and update the Framework which should include a specific timeframe to review, update, and complete the deliverables.

Sharing Information on using the Framework.

16. Has information that has been shared by NIST or others affected your use the Framework? If so, please describe briefly what those resources are and what the effect has been on your use of the Framework. What resources, if any, have been most useful?

The level of understanding (low, medium, high) of the Framework and its application varies among the State's Department of Transportation and local agencies. For many, it may be a learning curve because they lack the experience in risk management and conducting a process improvement review. There will also be inconsistencies among the transportation sector since there is no implementation guideline and policies to administer the Framework. Conducting a cyber security risk assessment is not a priority of day-to-day operations activities for the States Department of Transportation and local agencies. The use of the Framework may not be a priority if it is not articulated (not integrated) on the State's Department of Transportation and local agencies overall Strategic/Business Plans. Another potential weakness is educating the Framework to the non-cyber security transportation sector professionals and policy makers within their respective department. The administration of the Framework would be considered a collateral duty on top of a

transportation sector's professional day-to-day operations activity with competing priorities within their respective department. There is presently no professional capacity training on the use of the Framework for the transportation sector professionals. Providing funding and technical assistance to State DOTs and local agencies to implement the Framework would be extremely useful.

17. What, if anything, is inhibiting the sharing of best practices?

The current, limited, state of practice and lessons learned by the State's Department of Transportation have not been widely documented by the transportation sector. In addition, a single repository to search for available best practices reports for each of the respective sectors would help address this gap.

18. What steps could the U.S. government take to increase sharing of best practices?

Develop a marketing plan, utilizing social media; provide investment and financial incentives to "spark" interest and the sharing of best practices.

19. What kind of program would help increase the likelihood that organizations would share information about their experiences, or the depth and breadth of information sharing (*e.g.*, peer-recognition, trade association, consortia, federal agency)?

For the transportation sector at the Federal Highway Administration: this initiative as part of EDC – Every Day Counts, or SHRP II-Strategic Highway Research Program 2 --- tailored to each federal agency major initiatives.

Private Sector Involvement in the Future Governance of the Framework

20. What should be the private sector's involvement in the future governance of the Framework?

- **solicit the private sector input (will assist the federal agencies in planning);**
- **consider as an equal partner in the governance;**
- **help promote/engage innovation.**

21. Should NIST consider transitioning some or even all of the Framework's coordination to another organization?

Yes, coordination transition to industry/sector-specific (i.e. US DOT, DOE, etc.) should be considered. But NIST should retain the lead coordination role as the Framework matures and application experiences are available for feedback.

22. If so, what might be transitioned (*e.g.*, all, Core, Profile, Implementation Tiers, Informative References, methodologies)?

(All framework components would apply as noted in question 21)

23. If so, to what kind of organization (*e.g.*, not-for-profit, for-profit; U.S. organization, multinational organization) could it be transitioned, and could it be self-sustaining?

Continuity (self-sustaining) of the program administration and business operations for not-for-profit/for-profit agencies, U.S./multinational organization, universities (i.e. NIST Framework Resource Center for specific sector), etc., will depend on various factors which includes dedicated State/Federal funding from sponsor Federal/State agencies/private sector to sustain the operation of the organization, following applicable Federal/State grant administration requirements, developing a Strategic Plan to sustain the program, compliance with financial audits, etc.

24. How might any potential transition affect those currently using the Framework? In the event of a transition, what steps might be taken to minimize or prevent disruption for those currently using the Framework?

n/a - no comment at this time

25. What factors should be used to evaluate whether the transition partner (or partners) has the capacity to work closely and effectively with domestic and international organizations and governments, in light of the importance of aligning cybersecurity standards, guidelines, and practices within the United States and globally?

A Cybersecurity System Management Transition Plan (clearly defined organizational structure, board of trustees, MOU/MOA, By-laws, Strategic Plan, Annual Program/Budgeting, Annual financial auditing, etc.) should be developed for non-profit/profit companies if they're selected to address the transfer of roles/responsibilities, goals, and objectives. Qualification factors to verify their capacity may include technical understanding of the Framework, approach to domestic/international organizations collaboration, Strategic Planning which includes goals/objects, vision, etc. to sustain the program.