March 3, 2023

Alicia Chambers
Executive Secretariat
National Institute of Standards and Technology
100 Bureau Drive
Gaithersburg, MD 20899

RE: NIST Cybersecurity Framework 2.0 Concept Paper: Potential Significant Updates to the Cybersecurity Framework

Dear Executive Secretariat Chambers,

As the nation's leading advocate for the technological modernization of our transportation system by focusing on advancing research and deployment of intelligent transportation technology, the Intelligent Transportation Society of America (ITS America) is grateful for the opportunity to comment on the National Institute of Standards and Technology's (NIST) Cybersecurity Framework 2.0 Concept Paper: Potential Significant Updates to the Cybersecurity Framework.

ITS America was founded in 1991 as an advisory council to the U.S. Department of Transportation (USDOT) on technology innovation and emerging transportation technologies. ITS America is the only organization in the country that represents all sectors – public, private, academic, and nonprofit – to advance transportation technology. Our membership includes state and city departments of transportation, transit agencies, metropolitan planning organizations, automotive manufacturers, technology companies, engineering firms, automotive suppliers, insurance companies, and research and academic universities. Our vision is a better future transformed by intelligent mobility: one that is safer, greener, and smarter for all.

Our focus is policy that accelerates the deployment of seamless mobility technology, connected and automated vehicle technologies, and smart infrastructure; policy that breathes new life into our transportation system by expanding investments in technologies that support smart communities; policy that encourages new models and modes of transportation, including micro-transit, ride-sourcing, carshare, bikeshare, micro-mobility, and unmanned systems; and policy that does all of this while making our transportation system safer, greener, and smarter for all. Investments in these technologies should address issues of transportation equity, so everyone gains access to mobility and opportunity, and should address the valid concerns of the transportation workforce. However, our first and foremost priority has always been, and continues to be, safety.

Given the ability to cause loss of life and inflict significant economic damage in a highly visible manner, cybersecurity attacks directed at those producing or operating technologies traveling over or connected to U.S. roadways will intensify. Infrastructure with Intelligent Transportation Systems (ITS) leverages modern communications systems to support transportation management and operations. As a result, intelligent transportation technologies no longer function as closed systems, thus exposing transportation facilities and infrastructure to cyber threats due to their connectivity.

As such, ITS America and our members are fully cognizant of the importance of cybersecurity throughout all aspects of implementation of transportation innovations. We believe we must manage the vulnerabilities that come with a more complex and connected transportation system and stop thinking of cybersecurity as something to add to our infrastructure. We support the full integration of cybersecurity as part of our infrastructure and support making intelligent transportation systems secure by design. Specifically, we intend to help our members contextualize cyber risks, implement appropriate mitigation strategies for the risks they have identified as relevant to them, and help them prepare for cyber incursions.

To that end, ITS America is grateful for NIST's continued leadership in the cybersecurity space, including but not limited to the guidance provided through NIST's Cybersecurity Framework (referred to hereinafter as Framework). The Framework's voluntary cybersecurity risk management standards, guidelines, and best practices provide a critical structure from which to approach cyber threat mitigation, both within the transportation sector and across the broader connected world. ITS America's members consistently rely on the guidance provided by this Framework to help inform their approach to cybersecurity practices. Thus, we appreciate the opportunity to share four specific perspectives on cybersecurity as it relates to the transportation sector, in anticipation of NIST's development and release of the Framework 2.0.

Cybersecurity before Deployment

> The Framework 2.0 concept paper emphasizes the importance of supply chain risk management, which ITS America believes is prudent. However, particularly with ITS, there should be an emphasis on cybersecurity through the procurement cycle. A post-deployment assessment of cybersecurity for a particular project can be insufficient, both in terms of risk mitigation as well as the additional costs associated with reconfiguration after cybersecurity risks are identified. Many local municipalities lack the sophisticated discovery tools to even identify areas of cyber risk, let alone solve for those risks through tools such as a Configuration Management Database. Therefore, we believe that the Framework 2.0 should recognize the importance of consideration of cybersecurity components as a precondition of projects, rather than as an aspect to consider after the project has been delivered.

Misalignment between the Hardware Lifecycle and Technology

> ITS America believes that the Framework 2.0 should address the too-often undefined middle ground between the responsibilities of the vendor and the infrastructure owner-operator as relates to cybersecurity compliance. If you are in the public sector, you want what you paid for to be compliant and secure. If you are in the private sector, you want to be sure you are paid to provide that compliance and security. Too often, software maintenance agreements are missing from contracts, and there is no requirement to keep software up to date. NIST's Framework has the opportunity to establish firm expectations on both sides of this issue – ensuring that existing infrastructure is secure so as to not compromise new features being installed, and ensuring that cybersecurity requirements are present at the outset of new projects so vendors have a target to aim for.

Profile Samples

ITS America applauds NIST's work to further develop profile samples, which we believe can be leveraged to create specific conditions for certain transportation asset types, such as connected vehicles, automated vehicles, traffic operations, and others through sector-specific guidelines. ITS America's Cybersecurity Working Group looks forward to working with NIST to help develop guidelines specific to transportation conditions.

Establishment of Trust

In the ITS world, we are often dealing with multi-vendor environments. A traffic light needs to be able to trust a car, and that car needs to be able to trust a roadside unit. Communication is just one aspect of that, as is policy. We need some level of discussion of interoperability and trust between and across vendors that goes beyond a Security Credential Management System (SCMS). An SCMS just tells you that a device is who it says it is, but not that you can trust what it is saying. ITS America believes a cybersecure relationship goes far beyond identification, and looks forward to NIST's suggestions as to how to improve the trust dynamic in Framework 2.0.

These are just a few aspects of ITS America's priorities as they pertain to a new Framework, and we look forward to NIST identifying further amendments to the Framework via this comment process and additional processes that will appropriately capture the challenges of our industry and the connected ecosystem more broadly. We look forward to supporting NIST's Framework 2.0, and appreciate the opportunity to provide these comments during the drafting process. If you have any questions about the comments we have provided, please contact Bobby McCurdy at bmccurdy@itsa.org. ITS America and our members remain grateful for NIST's continued leadership in this space, evidenced by the impacts that the original Framework has had on cybersecurity practices across all sectors.

Sincerely,

Laura D. Chace
President and CEO