ATS TECHNOLOGY ALLIANCE

February 20, 2016

VIA E-MAIL

Diane Honeycutt
National Institute of Standards and Technology
100 Bureau Drive, Stop 8930
Gaithersburg, MD 20899
cyberframework@nist.gov

Re: RFI - Framework for Reducing Cyber Risks to Critical Infrastructure

Dear Ms. Honeycutt:

American Technology Solutions Cyber Technology Alliance is pleased to submit the attached response to the RFI.

Thank you for the opportunity to do so.

Very truly yours,

Charles Steven Sedlacek IV
President
American Technology Solutions, Inc.
On Behalf of ATS Technology Alliance

Organizational Information	**Response**
Organization Name	ATS Technology Alliance
Organization Sector	Information Technology
Organization Size	Alliance of IT, ICS and cyber security companies and experts
Organization Website	
Organization Background	The ATS Technology Alliance is a group of IT, ICS and cyber security companies and experts sharing a belief that our Critical Infrastructure is woefully vulnerable. Our members are involved in providing defensive cyber solutions to government and industry. With respect to industry, we primarily serve large enterprises, including Fortune 500 companies, operating in the sixteen Critical Infrastructure Sectors.
Point of Contact Information	**Response**
POC Name	Chuck Sedlacek
POC E-mail	chuck@americantechIT.com
POC Phone	805-919-8504

#	Question Text	Response Text	References
1	Describe your organization and its interest in the Framework.	The ATS Technology Alliance is a group of IT, ICS and cyber security companies and experts sharing a belief that our Critical Infrastructure is woefully vulnerable. Our members are involved in providing defensive cyber solutions to government and industry. With respect to industry, we primarily serve large enterprises, including Fortune 500 companies, operating in the sixteen Critical Infrastructure Sectors. Although our public and private clients certainly consider the Framework in some context, the Framework is never considered or referenced in interactions with us. We believe this is because the Framework fails to provide guidance regarding technological concepts and options and accordingly fails to align business policy, business, and technological approaches regarding cyber risks.	
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.	We are responding as a group of Framework non-users and subject matter experts.	
3	If your organization uses the Framework, how do you use it? (e.g., internal management and communications, vendor management, C-suite communication).	Not applicable. The reasons we do not use the Framework are set forth below.	
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)?	As expressed in more detail in response to question 10, the absence of real guidance regarding technological concepts and options is preventing our use of the Framework.	

#	Question Text	Response Text	References
10	Should the Framework be updated? Why or why not?	The answer is a resounding yes. The Framework is an Architecture with great value in assessing cyber compliance. It should be updated to include a bridge to effective risk management. Specifically, our customers and security practitioners tell us that the Framework lacks specificity about technological concepts they should consider in order to implement effective cyber security defenses. They are hoping for more guidance. There are technological concepts, including concepts contemplated in the National Critical Infrastructure Security and Resilience Research and Development ("CISR R&D") Plan or discussed in the CISR R&D Plan Workshop, which might be recognized as options to consider. We need these concepts and options to be articulated so that Framework users can transition to functioning, real cyber security. We note Executive Order 13636 directed that, ""The Cybersecurity Framework shall include a set of standards, methodologies, procedures, and processes that align policy, business, and technological approaches to address cyber risks." We think far more can be done to marry technological approaches to policy and business approaches than has been done to date. This can be achieved while fully respecting principles of technology neutrality and a competitive marketplace for products and services.	
21	Should NIST consider transitioning some or even all of the Framework's coordination to another organization?	Yes. It should be transitioned to a group hosted by an entity which focuses on technology concepts on a more granular level—possibly the National Cybersecurity Center of Excellence (NCCoE) or the Critical Infrastructure Partnership Advisory Council (CIPAC). The group should include the CISR R&D participants, the Sector Information Sharing and Analysis Centers (ISACs), and others interested in technological pathways to real cyber security.	
22	If so, what might be transitioned (e.g., all, Core, Profile, Implementation Tiers, Informative References, methodologies)?	All further work regarding technological concepts and options should be transitioned.	