MORGANFRANKLIN® CONSULTING

ACCOUNTING & TRANSACTION SERVICES
STRATEGY, FINANCE & OPERATIONS
RISK & COMPLIANCE
INFORMATION MANAGEMENT & TECHNOLOGY

MORGANFRANKLIN® CONSULTING

February 9, 2016

Diane Honeycutt
National Institute of Standards and Technology
100 Bureau Drive, Stop 8930
Gaithersburg, MD 20899

Dear Ms. Honeycutt,

On behalf of MorganFranklin Consulting, thank you for affording us the opportunity to respond to your request for information regarding Views on the Framework for Improving Critical Infrastructure Cybersecurity. We currently enjoy working closely with a number of commercial, civilian, and defense agencies and provide direct support to them in various capacities. We understand the challenges that NIST faces in developing and updating a framework for improving critical infrastructure cybersecurity. MorganFranklin's engagements across the commercial and public sectors provide us with a comprehensive understanding of organizations, processes, and cultures impacted by the requirements for cybersecurity.

As a result, we are uniquely qualified to provide comments to assist NIST with understanding:

- the variety of ways in which the Framework is being used to improve cybersecurity risk management,
- how best practices for using the Framework are being shared,
- the relative value of different parts of the Framework,
- the possible need for an update of the Framework, and
- options for the long-term governance of the Framework.

If you have questions regarding this response, please contact Scott Binder, Director, at (202) 770-2865, scott.binder@morganfranklin.com.

Sincerely,

Scott Binder
Director

MorganFranklin Consulting, LLC

Views on the Framework for Improving Critical Infrastructure Cybersecurity		
#	**Question**	**Response**
1	Describe your organization and its interest in the Framework	MorganFranklin Consulting is a strategy and execution-focused business consulting firm and professional advisor. We provide strategic thinking and hands-on support to help clients manage growth and maximize performance. Our solutions always consider the key connections between business, operations, technology, risk and compliance—connections that are critical to success. We work with clients to clearly define risks, establish controls to mitigate them, and utilize a framework for demonstrating compliance with internal and external standards. We help companies maintain the availability, confidentiality and integrity of critical data and infrastructure including networks, operating systems, databases, and applications. We also ensure consistency of process execution for administration of system users, configuration changes, and data center operations. At MorganFranklin, we understand that each organization faces unique risks and security requirements.
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.	Non-User
3	If your organization uses the Framework, how do you use it? (e.g., internal management and communications, vendor management, C-suite communication).	N/A
4	What has been your organization's experience utilizing specific portions of the Framework (e.g., Core, Profile, Implementation Tiers, Privacy Methodology)?	N/A
5	What portions of the Framework are most useful?	The following portions of the framework are most useful: a) The framework is based on the collaboration between government and the private sector, uses a common language to address and manage cybersecurity risks in a cost-effective way based on business needs without placing additional regulatory requirements on businesses. b) It enables organizations to determine their current cybersecurity capabilities, set individual goals, and establish a plan for improving and maintaining cybersecurity programs. c) The framework provides a common lexicon for risks and cybersecurity, which in turn would bring uniformity and also help in effectively communicating with various stakeholders,

		specifically third-party partners, service providers and regulators. d) Organizations may avoid legal and regulatory implications that they were negligent on cybersecurity best practices in the event of an incident. e) The framework defines standardized cybersecurity activities, desired outcomes, existing frameworks and is organized by five continuous functions.
6	What portions of the Framework are least useful?	The following portions of the framework are least useful: a) Framework Implementation Tiers ("Tiers") b) "Tiers do not represent maturity levels" c) "Successful implementation of the Framework is based upon achievement of the outcomes described in the organization's Target Profile(s) and not upon Tier determination". d) Tiers may be reduced to a theoretical exercise. It may also lead to a situation where identification may be just a redundant step.
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)?	N/A
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?	Policy makers should collaborate with federal agencies and the private sector to review and prevent duplication of regulatory processes and prevent conflict with superseding of regulatory requirements, mandatory standards, and related processes.
10	Should the Framework be updated? Why or why not?	The framework should be updated on periodic basis. This would allow new or outdated information to be incorporated (e.g. regulatory changes and leading practices).
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.	NIST may want to incorporate the following into the framework: a) Increasing communications and notices around the framework could enhance use of the framework. b) Issues relating to data privacy and civil liberties, which are important to both the private and public sectors should be included in the framework.

		c) Numerous companies and organizations continue to use legacy or outdated systems. Specific language could be incorporated into the framework to help address environments that might not be able to implement portions of the framework. d) Additional emphasis and details could be incorporated into the framework for incident response steps.
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?	No comments.
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?	This is organizational specific, no additional comments.
14	Should developments made in the nine areas identified by NIST in its Framework-related "Roadmap" be used to inform any updates to the Framework? If so, how?	NIST may want to incorporate methodologies used by software companies for patching and implementing system upgrades.
15	What is the best way to update the Framework while minimizing disruption for those currently using the Framework?	Provide periodic updates and incorporate timeframes for implementation.
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?	N/A
17	What, if anything, is inhibiting the sharing of best practices?	Lack of training, collaboration, and methods to share best practices.
18	What steps could the U.S. government take to increase sharing of best practices?	Periodic workshops, training material and communication notices.
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)?	Workshops, training material and collaboration between professional information security/cybersecurity associations.
20	What should be the private sector's involvement in the future governance of the Framework?	Private sector should play a critical role including have a voice in decision making and be involved in all stages of governance.

21	Should NIST consider transitioning some or even all of the Framework's coordination to another organization?	NIST should continue to provide direction and updates for the framework and should continue to collaborate with private corporations and public sector agencies.
22	If so, what might be transitioned (e.g., all, Core, Profile, Implementation Tiers, Informative References, methodologies)?	No comments.
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?	No comments.
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?	No comments.
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?	No comments.