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

February 9, 2016

Dear Ms. Honeycutt,

The InfraGard Maryland Members Alliance (IMMA) is a not-for-profit 501(c)(3) organization partnered with the Federal Bureau of Investigation (FBI). Through this public/private partnership IMMA is committed to increasing the security of the state of Maryland and national critical infrastructure through facilitate cross-sector information sharing to increase awareness of security threats. Our 1,100 members represent businesses, academic institutions, and law enforcement agencies dedicated to sharing intelligence to prevent hostile acts. The concepts and initiatives supporting the creation of the *Framework for Securing Critical Infrastructure Cybersecurity* are important to the same goals and ideals as the InfraGard core mission. For that reason we convey our support for ongoing efforts to maintain and continually improve upon the Framework.

In 2015 we surveyed our membership inquiring as to several aspects about the Framework. Nearly 25% of respondents conveyed that they would like to know more about the Framework. To enable cybersecurity awareness across sectors we coordinated outreach through the DHS Critical Infrastructure Cyber Community (C^3) program to speak to the Chapter and discuss the utility of the Framework. In support of the RFI, this year we surveyed a random focus group from our membership who provided their opinions concerning the Framework.

In our Framework focus group we observed the following trends:

- Most people stated that their organization had a mature cybersecurity program.
- Although most people stated that the Framework has affected their organization, there was only a moderate value realized when asked about the Framework's ability to reduce risk.
- The majority of participants conveyed that their organization is still very interested in learning more about the Framework.
- Many participants commented that NIST guidance, including special publications beyond the Framework, is valuable to their organization. They further added that standards such as ISO 27001/2, CMMI, and NERC CIP also provide benefit to their organizations' cybersecurity.
- Overwhelmingly, each member stated that the private sector should be involved in future governance of the Framework.

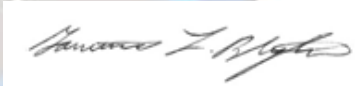
Our members have used the Framework successfully in identifying security gaps and addressing vulnerability findings. Members have also realized benefits toward developing IT infrastructure architecture, technology roadmap, system design, application development, and system security plans. Members have even commented that the Framework contributed to their individual and organizational contributions in shaping industry-wide security controls and the strategy development for creating a new Information Sharing and Analysis Center (ISAC).

Through our collective experience with the Framework, the following summarizes our recommendations for the Framework beyond the notable trends listed:

- Within the structure of the Framework, the Core was clearly the most helpful to private sector organizations. Profiles were recognized as the least helpful within the document. An emphasis on the Core should be the primary focus of Framework revisions. Any revision to the Tier and Profile sections should specifically relate to operational implementation of the Core and provide a detailed and quantifiable method for evaluating risk.
- Our members would like to see more outreach opportunities for industry to learn more about the Framework and specifically how to use it.
- Our membership would like to better understand how the Framework cohesively fits with the Risk Management Framework so that they can leverage that guidance explicitly or create an improved procedure to use the Framework within their organizational risk approach. Similarly, there needs to be a separate detailed guidance document for small business approaches to Framework use and risk reduction which accounts for budget constraints.

IMMA is very supportive of the Cybersecurity Framework and would like to make our chapter available to hold focus groups, industry pilot activities, or workshops to help NIST evaluate Framework improvements. We will continue to provide feedback from our industry members as well as incorporate new security guidance as it becomes available.

Sincerely,



Garrettson L. Blight
President
IMMA Board of Directors