Original Message-----
From: Larry Marks
Sent: Saturday, December 12, 2015 5:24 PM
To: cyberframework <cyberframework@nist.gov>
Subject: Private user Comments on the Cyber framework

Attached are my comments as a private user of the NIST Cyber framework.

1 Describe your organization and its interest in the Framework. We are a privately held financial services firm with offices worldwide. We employ more than 6000 employees. We wanted to use the Framework to perform a Risk Assessment of the cyber controls. This assessment was intended to help develop a strategic plan to enhance existing cyber security controls and identify the gaps in processes, controls and technology.
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. User
3 If your organization uses the Framework, how do you use it? (e.g., internal management and communications, vendor management, C-suite communication).
4 What has been your organization's experience utilizing specific portions of the Framework (e.g., Core, Profile, Implementation Tiers, Privacy Methodology)?
5 What portions of the Framework are most useful? Implementation Tiers
6 What portions of the Framework are least useful? Privacy Methodology
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)? No
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. We track metrics based on #incidents/response time
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?
Question Text Response Text
10 Should the Framework be updated? Why or why not? The Framework should be updated to:

1. provide more detail how to evaluate data governance and privacy,

2. reflect the overlap with the recently issued FFIEC assessment.

3. mention should be made about the other regulatory controls related to geo such as Luxembourg or India, since they have different standards and frameworks

4. Network segmentation best practices

5. reflect different sizes of firm - large, medium and small. Based on their budgets, the framework should be segragated into categories for implementation and assessment by size of

firm, since smaller firms do not have the means such as large firms to implement the tiers of controls and will have different risk appetites.
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.
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? The Framework should be updated to:

1. provide more detail how to evaluate data governance and privacy,

2. reflect the overlap with the recently issued FFIEC assessment.
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?
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?
15 What is the best way to update the Framework while minimizing disruption for those currently using the Framework? Since the framework is not regulatory, updates to the framework should be evaluated by their impact and implemented on a scheduled basis.
Question Text Response Text
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? Have reviewed other related NIST frameworks more in depth related to network security
17 What, if anything, is inhibiting the sharing of best practices?
18 What steps could the U.S. government take to increase 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)?
Question Text Response Text
20 What should be the private sector's involvement in the future governance of the Framework? The private sector and organizations such as FS-ISAC should be involved in helping draft and vet the updates to the framework.
21 Should NIST consider transitioning some or even all of the Framework's coordination to another organization? No
22 If so, what might be transitioned (e.g., all, Core, Profile, Implementation Tiers, Informative References, methodologies)? NA
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? NA
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?
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??