Question Text

Describe your organization and its interest in the Framework.

The National Cyber Security Alliance is the nation's leading cybersecurity education and awareness organization**.** We engage diverse groups, including businesses, in adopting better cybersecurity practices. Our key initiatives are National Cyber Security Awareness Month, STOP. THINK. CONNECT., and Data Privacy Day. We are a 501 c 3 public private partnership working with government, industry and civil society. (www.staysafeonline.org).

Submitted by Michael Kaiser, Executive Director

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 in a variety of ways as SME that uses the framework for education, awareness and training.

If your organization uses the Framework, how do you use it? (e.g., internal management and communications, vendor management, C-suite communication).
We use the framework in a variety of ways.

- Communications: the framework comprises the key way we message to businesses through media and programmatic activities, such as national Cyber Security Awareness Month (See infographic with framework elements https://staysafeonline.org/stay-safe-online/resources/creating-a-culture-of-cybersecurity-in-your-business-infographic). We find the framework an excellent way to respond to media and other inquires around how do businesses begin to address cybersecurity. It provides and easy way to give businesses a starting point and trajectory for better cybersecurity. The message, start by protecting the crown jewels of your business, seems to have resonance and provides a gateway to the rest of the framework. One of the greatest benefits as a communication tool is that helps SMBs focus back on what's critical to them and away from protecting against every risk that's out there. Also see how we have worked with others to communicate a 5 steps approach. This example the BBB (https://www.bbb.org/globalassets/local-bbbs/council-113/media/cybersecurity-microsite/resources/bbbcybersecurity_5stepsguide_revised-9.pdf)
- Training: with the Council of BBB's we have created a version of the Framework in a basic training for small and medium-sized businesses that will be rolled out spring of 2016. The idea for the training is is to instill in SMBs the idea of the framework as way to think about cyber and their business and begin the process of tailoring the framework to their specific needs. The training is deigned to be interactive and takes SMBs through the framework by

using a couple of scenarios of how it might apply to an SMB. For example, one scenario takes an SMB through a ransomware incident on system used for inventory. Our goal is to get business to view cybersecurity through the framework so it becomes the guiding principal of how they approach cyber going forward and make the framework a guide as their business grows or they implement new technology. We recognize the SMBs will not likely do a full blown implementation of the framework but if we can get them started even being able to identify key assets, be better at protecting them and having the start of ways to detect a problem and respond and recover, we will have major advances in the SMB community on cybersecurity. The training is supplemented with information about specific technologies (Wi-Fi, Mobile, etc) so business can create plans based on the tech they use. We are looking at a couple of different roll out models, including training BBB staff around the country to deliver the training and/or holding some training with BBB staff. The partnership allows for the NCSA to bring cybersecurity legitimacy and the BBB has the relationships (at over 100 local chapters across the country) to fill a room.

- National Cyber Security Awareness Month (October): One week each October is devoted to creating a culture of cybersecurity at work. The framework is always featured by us and of course by our partner DHS in their messaging that week.

synch that with framework in some way as well have consistent messaging across the Federal Government on how businesses address cybersecurity.

Should the Framework be updated? Why or why not?

Cybersecurity is ever evolving some thought should be given to how IoT might impact the framework. While in many cases, IoT is an extension of a network and an asset, we should be keeping a close eye on if the framework is flexible enough to include the many manifestations of IoT.

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. **N/A**

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?

Good case examples of smaller businesses that have adopted the framework would be helpful.

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? **N/A**

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? **N/A**

What is the best way to update the Framework while minimizing disruption for those currently using the Framework?

Don't change the core principals and steps. Build out the knowledge base with case studies and examples of success (For example, how did following the framework help an organization after an attack took place?).

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**

What, if anything, is inhibiting the sharing of best practices? N/A

What steps could the U.S. government take to increase sharing of best practices?
Might consider funding an organization to take on the work of developing an understanding, through surveys and case studies, to explore how the framework is being used in different sectors, lessons learned and feedback from companies of various sizes. Also develop case examples across sectors of success stories that will resonate with businesses of all sizes.

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)?

Cybersecurity remains a hot topic for the business community. There is a great interest in learning how implement cost effective, meaningful cybersecurity practices. Creating a place where there could be sharing of implementation stories as well as possibly peer-to-peer support for those implementing the framework is an idea to consider. Harder but worth considering is finding ways to share how the framework was helpful in thwarting or responding to an attack. Showing how following the framework allowed a business to bounce back, return to normal operations and mitigate losses after an attack would be good motivation for others to adopt the framework.

What should be the private sector's involvement in the future governance of the Framework?

The private sector engagement in the creation of the framework is a significant source of its legitimacy. Finding away to maintain the private sectors involvement overtime is essential to future adoption.

Should NIST consider transitioning some or even all of the Framework's coordination to another organization?

If it is in the best interest of continuity and increased broad based implementation, yes.

If so, what might be transitioned (e.g., all, Core, Profile, Implementation Tiers, Informative References, methodologies)?

Should consider a broad more business friendly messaging campaign and easy implementation guide for smaller businesses.

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?

Probably nonprofit.

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?

N/A

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?

Transition partner would have to have the respect of those in industry and government.