Information Technology Industry Council

March 26, 2014

Information Technology Industry Council (ITI)
Response to Department of Homeland Security Request for Information:
Cyber Security Solutions for Small/Medium Sized Businesses
Solicitation # RFI20140220

ITI Point of Contact:

Danielle Kriz
Director, Global Cybersecurity Policy
Information Technology Industry Council
1101 K St. NW, Suite 610
Washington, DC 20005
dkriz@itic.org
p: 202-626-5731
m: 202-351-1661

The Information Technology Industry Council (ITI) appreciates the opportunity to respond to the Department of Homeland Security's Request for Information (RFI) on Cyber Security Solutions for Small/Medium Sized Businesses (SMBs). ITI strongly supports the National Institute of Standards and Technology (NIST) Cybersecurity Framework because it leverages public-private partnerships, is based on sound risk management principles, and will help preserve innovation because it is flexible and based on global standards. If implemented well, the Framework will help improve cybersecurity, and we are committed to helping it succeed. To that end, we also support appropriate DHS activities to promote use of the Framework.

Introductory Points: Need to Rethink Two Underlying Assumptions

On subsequent pages, ITI provides responses to the eight questions in this RFI. Before doing so, however, we must question two of the RFI's underlying assumptions. While we appreciate that DHS seeks SMBs to use the Framework, we are concerned with the assumptions that DHS has a role in shaping how industry provides and prices its cybersecurity solutions, and that the market does not already provide a range of solutions tailored to SMBs.

Firstly, and most importantly, the questions in the RFI presume a role for DHS that is neither accurate nor prudent. By asking what types of cybersecurity solutions industry provides, and whether they are affordable,[1] the RFI sends the signal that DHS believes it, not vendors (or the market generally), knows the appropriate pricing levels for cybersecurity solutions; that DHS doubts affordable solutions exist or will exist without government guidance; and that DHS has a role to play in private-sector pricing. In short, DHS risks inappropriately intervening in private-sector transactions, playing a role akin to industrial policy that the U.S. Government has traditionally largely and rightly avoided.

The second troubling underlying assumption in this RFI is that the market does not already meet SMBs' needs. In fact, industry provides a range of scalable product and service solutions with varying price points, designed to address the needs of entities of all sizes, sophistication, and threat/risk profiles—including SMBs. Further, we caution DHS not to attempt to force the provision of what it falsely believes need to be "cheaper" solutions. A one-dimensional perspective on appropriate cybersecurity solutions for SMBs—that they must be cheap above all else—could potentially result in solutions that are low-cost but incapable of addressing evolving, dynamic threats faced by entities with higher risk profiles.

ITI agrees that many SMBs might not be investing enough, or appropriately, in cybersecurity solutions. Rather than trying to steer the supply side (industry's provision of solutions), DHS should better use its resources to help in two ways.

First, DHS can play a valuable role in helping understand the unique challenges that SMBs face in terms of cybersecurity solution uptake, including knowing what cybersecurity solutions to buy. A more solid understanding of these challenges will help all stakeholders in their efforts to in turn help SMBs improve their cybersecurity risk management. We are not suggesting per se a subsequent RFI posing these questions. Rather, DHS should consult interagency among the range of peer government agencies and programs that work on a regular basis with SMBs on

[1] Five of the eight questions in the RFI touch on affordability or pricing: 3.1, 3.2, 3.3, 3.7, and 3.8.

cybersecurity issues, including those we list at the bottom of the next paragraph. There is likely a deep pool of knowledge within the federal government that has looked at this issue, and DHS could help by gathering this knowledge and helping us all to use it.

Another effective and appropriate role DHS should play regarding SMBs' uptake of cybersecurity solutions generally and the NIST Framework specifically is to conduct outreach and raise awareness along three key dimensions: 1) helping SMBs understand cybersecurity threats so they can make informed decisions based on their unique risk profiles; 2) communicating to all entities, including SMBs, that the Framework and the Program exist (and are voluntary), and the existence and availability of both DHS and private sector capabilities of which companies can avail themselves to learn how to use the Framework to assist with their cybersecurity risk management; and 3) helping SMBs understand the range of existing federal agencies and programs available to help small entities manage their cyber risks and invest in the appropriate products and services, people, and processes to address these risks. These agencies/programs include, but certainly are not limited to, the Small Business Administration (SBA)'s *Cybersecurity for Small Businesses* program,[2] NIST Manufacturing Extension Program (MEP), NIST National Cybersecurity Center of Excellence (NCCoE), and DHS's own *Stop.Think.Connect.* Campaign.

Responses to Specific RFI Questions

3.1 Is there a viable marketplace for providing cyber security services at a low, affordable price for SMBs in support of the NIST Cybersecurity Framework?

Yes. As described above, industry provides a wide range of solutions that are scalable to customers of all sizes and risk profiles.

3.2 Would NIST Cybersecurity Framework adoption by an SMB make them a more attractive customer and potentially eligible for more advantageous pricing?

Companies' decisions on pricing are based on a multitude of factors and are tied to their proprietary business strategies. It is impossible to make a blanket statement regarding what factor a given SMB's adoption of the Framework will have.

Further, and equally importantly, there is no agreed-upon definition of what is meant by "adoption" or "use" of the NIST Framework. Per NIST, and the Administration generally, the Framework is designed to be flexible so that different entities can use it in different ways. Thus, we strongly caution DHS from asking questions about "adoption" of the Framework, as this could inappropriately convey that the Administration itself now believes the word has a set definition.

3.3 How can the government help reinforce the value of affordable cyber security solutions to SMBs?

We believe SMBs, if they are knowledgeable about their own cybersecurity risk profiles, will be able to determine which solutions are valuable to them—from both feature and price perspectives—and how much they should spend.

[2] http://www.sba.gov/tools/sba-learning-center/training/cybersecurity-small-businesses

3.4 What security products and/ or services would you envision being able to offer and how might those be communicated in terms of the NIST Cybersecurity Framework's core functions (Identify, Protect, Detect, Respond, Recover)?

This question assumes that both customers and industry solutions are one-size-fits-all. In reality, no two companies (customers) are alike, and the solutions a vendor might offer to one SMB customer might not be the same as solutions the same vendor offers to another SMB customer.

3.5 How would you characterize SMBs for the purpose of identifying applicable services, eligible customers, etc.?

The purpose of this question is not apparent, nor is it clear what DHS would do with this information.

3.6 Does DHS/government have a role in helping establish the guidelines for capability providers to determine what adoption of the NIST Cybersecurity Framework is?

No. DHS/the government does not have a role to play in establishing a conformity assessment program to verify "adoption" of the Framework, largely because (per our response to question 3.2), NIST and the Administration generally have stated there is no agreed-upon definition of what is meant by "adoption" or "use" of the NIST Framework and adoption (or use) of the framework will by necessity vary by entity.

3.7 Are there technical or policy impediments that inhibit the marketplace from providing cyber security solutions at a low, affordable price for SMBs?

As explained in our introductory narrative, we do not believe DHS has a role in questioning how industry decides to price its products and services for private-sector customers.

3.8 Are there ways in which economies of scale could be used to make a market for SMBs cyber security solutions more attractive and financially viable for both buyers and sellers? If so, how could these economies of scale best be fostered?

Per our response to question 3.2, companies' decisions on pricing are based on a multitude of factors and are tied to their proprietary business strategies. It is impossible to make a blanket statement regarding what factor a given SMB's adoption of the Framework will have.

Conclusion

ITI and its member companies strongly support DHS's efforts to promote use of the Cybersecurity Framework. We understand DHS seeks to determine if and how it might help SMBs make appropriate investments they need in cybersecurity solutions. The objectives of these efforts can be best achieved by DHS using its expertise and resources to 1) help all stakeholders better understand the unique challenges that SMBs face in terms of cybersecurity solution uptake and 2) conduct outreach and raise awareness to help SMBs understand cybersecurity threats, the existence of the Framework and available resources to learn how to use it, and the range of other existing federal agencies and programs available to help SMBs improve their cybersecurity postures.