Submitted by:

Angela McKay, Chair
Information Technology Sector Coordinating Council (IT SCC)
901 K Street NW, 11TH Floor
Washington, DC 20001

angela.mckay@microsoft.com

April 8, 2014

Introduction

The Information Technology Sector Coordinating Council (IT SCC) is pleased to submit our response to the Department of Homeland Security's (DHS) Request for Information (RFI) seeking information from industry on its capacity to provide broadly scalable cybersecurity solutions at an affordable cost to Small and Medium Businesses (SMBs) in support of adoption of the National Institutes for Standards and Technology (NIST) Framework for Improving Critical Infrastructure (CI) Cybersecurity.

The IT Sector is central to the Nation's security, economy, public health, and safety, and the sector's products and services are relied on by all critical infrastructure sectors. The recent release of the *NIST Framework for Improving Critical Infrastructure Cybersecurity*, created through public-private collaboration, reflects the efforts of a broad range of industries and is a recent example of the results of government and industry working together collaboratively. As DHS takes the lead in implementing the Critical Infrastructure Cyber Community C³ Voluntary Program, the IT SCC looks forward to continuing this type of public-private collaboration. We welcome the interest that DHS is showing in seeking to better understand SMBs' needs related to cybersecurity risk management and look forward to leveraging our partnership model to continue to assist DHS in this regard.

The IT SCC appreciates that DHS has pursued an open and inclusive process, enabling a broad range of stakeholders to be involved in development of efforts to enhance cybersecurity of SMBs. The process used to solicit input for this RFI, however, raises a few questions. First, why was www.FedBizOps.gov, the point-of-entry for Federal government procurement opportunities over $25,000, chosen as the means for soliciting input? Why was the Federal Register not used? Does DHS anticipate a future procurement related to this RFI? We are inquiring because the RFI lacked context about the purpose, which would have been helpful for all public commenters to provide more meaningful input. Despite this constraint, the IT SCC is confident that our response can help guide DHS's efforts to advance cybersecurity of SMBs.

The IT SCC recommends that DHS's primary focus should be on educating SMBs about cybersecurity risks, and how the Framework can assist SMBs strengthen their overall cybersecurity posture. While the RFI focuses heavily on providers and solutions, it lacked questions to understand issues that are important to other affected stakeholders, most notably SMBs. We suggest that DHS's engagement have much greater focus on the target beneficiaries of any SMB initiative.

As this process continues to evolve, we encourage DHS to engage with industry early and often through open and transparent communications so industry can help DHS and all relevant stakeholders achieve key cybersecurity objectives, including one of DHS's key goals, which is for business interests to be served for providers and consumers through stronger cybersecurity.

The following responses are informed by input from our IT SCC members who represent a broad base of owners, operators, associations, and other entities—both large and small. The IT SCC response focuses on questions 3.3, 3.5, 3.6 and 3.7.

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

DHS' current efforts for outreach and education to GCCs, SCCs and other relevant stakeholders through the C^3 voluntary program are a positive and necessary first step in raising the awareness and need for strengthening the cybersecurity of our nation's critical infrastructure. The C^3 Voluntary program can also serve as an effective vehicle to extend the government's efforts for outreach and education to SMBs. DHS should leverage existing government programs through agencies such as the Small Business Administration (SBA), General Services Administration (GSA) or the Department of Commerce's Minority Business Development Agency (MBDA) to reach SMBs and help them understand the risks to their businesses. One area DHS could help SMBs is by leveraging and customizing existing resources, such as the cyber resilience reviews, to help SMBs implement the Cybersecurity Framework.

These outreach and awareness activities will help foster a culture of cybersecurity, and stimulate the marketplace where free market principles based on a various conditions and factors will ultimately drive prices. The IT SCC believes reinforcing the value or affordability of cybersecurity solutions is not an area in which the government should play a role. Value and affordability will be determined by the SMB community.

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

The IT SCC readily recognizes that SMBs make up a substantial share of the national economy, are an important part of the critical infrastructure community, and offer products and services to CI. Despite this RFI, it is unclear how SMBs fit within DHS' intended audience for implementation of the NIST Cybersecurity Framework. Arguably, implementation of the Framework could be beneficial to businesses of all types and sizes regardless of whether they are considered critical infrastructure or not. For the purposes of identifying applicable CI services for SMBs, DHS could more clearly define its intended audience for voluntary implementation of the Cybersecurity Framework.

The IT SCC does not believe there is a need for DHS to create new or different size characterizations of SMBs for the purposes of implementing the Cybersecurity Framework. DHS should rely on existing size parameters that have been defined and long used by agencies such as the SBA.

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/government should not have any role in defining or establishing guidelines for providers. The IT SCC appreciates that the Framework is intended as flexible guidance to be adapted for the specific risk considerations unique to an individual organization. Organizations will make their own decisions on what their Target Profiles should be and how they will achieve those results in accordance on the organization's risk tolerance. As a result, the concept of setting guidelines for providers to determine adoption is inconsistent with the voluntary nature of the Framework and the C^3 Voluntary Program. It also raises concerns about having government determine for providers what "adoption" should look like for customers.

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

The IT SCC does not believe there are technical or policy impediments in place that inhibit the marketplace from providing affordable cybersecurity solutions for SMBs. Our member companies do see value, however, in DHS focusing on educating SMBs on the importance of adopting a culture of cybersecurity risk management.

Summary

The IT SCC supports efforts to promote the use of the NIST Cybersecurity Framework and applauds DHS' interest in understanding its role in helping SMBs determine the appropriate investments they need in cybersecurity solutions. DHS's objectives can best be achieved by focusing on 1) Outreach and education to SMBs to raise awareness of the existence of the Cybersecurity Framework 2) Leveraging government resources through existing programs or federal agencies such as the SBA to help SMBs improve their cybersecurity postures and 3) Using the partnership model to work more closely with industry to identify the needs of SMBs so that industry can best meet those needs.