Information Technology Industry Council

ITI Recommendations to the Department of Homeland Security Regarding its Work Developing a Voluntary Program Under Executive Order 13636, "Improving Critical Infrastructure Cybersecurity"

February 11, 2014

The Information Technology Industry Council (ITI) strongly supports the Administration's February 2013 Executive Order (EO) 13636, "Improving Critical Infrastructure Cybersecurity," as an effective and exemplary approach to cybersecurity policy. The approach in the EO, and specifically the resulting Cybersecurity Framework being led by the National Institute of Standards and Technology (NIST), 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.

Thus, ITI is pleased to present below four recommendations for the Department of Homeland Security (DHS) to consider as it develops and implements the Voluntary Program (the Program) intended to promote use of the Framework as called for under the EO.[1] We believe these recommendations can help DHS maximize the Program's positive impact on the cybersecurity posture of our nation and serve as a model as other countries grapple with these challenges.

1. DHS should prioritize outreach to raise awareness of the Framework and the Program as resources

The Administration, partnering with interested stakeholders, has made tremendous progress developing the NIST Cybersecurity Framework, and has gotten off to a solid start creating the DHS Voluntary Program. The Framework and the Program have the potential to be meaningful resources to help critical infrastructure (CI) owners and operators manage cyber risks to their systems, operations, and data. While many entities have been extensively involved in NIST's and DHS's work, significantly many more have not been involved, and may have only a cursory (if any) understanding of these efforts. A wide range of stakeholders need to know these resources exist and be comfortable in knowing how to use them to advance cybersecurity.

[1] Section 8 of the EO directs DHS to "... establish a voluntary program to support the adoption of the [National Institute of Standards and Technology (NIST)] Cybersecurity Framework by owners and operators of critical infrastructure [CI] and any other interested entities."

As such, outreach and awareness are essential to the Program's success, particularly in the first year. DHS should conduct an extensive campaign to communicate that the Framework and the Program exist (and are voluntary), and to promote 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. DHS should leverage its presence beyond Washington, DC to maximize outreach opportunities to all parts of the country and to all industries and players of all sizes.[2] Finally, while the Framework is relevant across the economy to businesses of all sizes, DHS must strategically define its target audience(s) (including different roles such as Chief Executive Officers (CEO), Chief Security Officers (CSO), and operational and technical staff) for such activities so outreach can be appropriately tailored to be most effective.

2. DHS should carefully determine how "success" is to be demonstrated

Given the focus on the Framework and the Program, many observers are carefully watching and wondering if a voluntary approach can "succeed." As such, defining success must be carefully considered and approached. Cybersecurity is a process of dynamically managing risks amidst ever-evolving threats, technologies, and business models. As noted in the Framework, it is important to create a "culture of security" where all stakeholders contribute to better managing their cyber risks. Attempting to quantify the number of cyber incidents is impossible and does not provide meaningful data, and counting the number of entities using the Framework or seeking support through the Program may be tempting, but will not ultimately demonstrate whether all stakeholders are managing cyber risks more effectively.

Therefore, we must focus on gauging the right things, in the right order, particularly as the Program unfolds. We should recognize that fostering use of the Framework is a multi-year process, and as such that "success" markers for the Program should be appropriate, realistic, and will by necessity change over time. Further, success will mean different things to the many and varied organizations that use the Framework and the Program. A meaningful demonstration of efficacy in the Program's first year would be the amount and nature of DHS's outreach and awareness campaign, and stakeholder participation from the defined target audience(s). As noted above, if stakeholders are unaware of the Framework and the Program, use will be limited. NIST's outreach efforts were successful, generating considerable involvement during the development of the Framework over the past year, and DHS should aim to build on NIST's model. DHS also should partner with industry over the coming years to determine the most effective ways to understand and demonstrate success in the nearer term, and to collectively identify and evolve realistic, objective, and comparable information over the longer term, as the Program becomes more well-known and utilized.

[2] Outreach to foreign governments and industry is also important as they are carefully watching the EO to assess its impact.

3. DHS should de-emphasize the current focus on incentives

We appreciate DHS's efforts to date analyzing incentives to promote participation in the Program,[3] but counsel the Administration against tying incentives development to the Program's "success" or "failure." Given limited fiscal resources and the complexity of incentives, including the necessary involvement of multiple stakeholders including Congress, it is highly unlikely any will be available at, or immediately following, the February 2014 launch of the NIST Cybersecurity Framework. Further, as DHS has stated, determining the feasibility of any incentives (much less putting any in place) could take a few years. Finally, we believe many entities will find parts of the Framework and the Program to be very useful to improving their cybersecurity, and managing risk, regardless of whether the government offers incentives.

While incentives might not be immediately available, they nonetheless warrant careful consideration and continued efforts by government and industry to be realized. DHS should work with stakeholders over the coming years on a nuanced, pragmatic, and phased exploration of incentives. Care must be taken to pinpoint options that are workable, that fill identified gaps, and that do not create unwieldy, compliance-based programs that undermine the "voluntary" nature of the Framework and the Program.

4. DHS should partner with industry on all aspects of the Program moving forward

Our three recommendations above share a common theme: they advocate multi-year, joint efforts by government and the private sector. Improving cybersecurity is a shared responsibility—neither government nor the private sector can act effectively alone. DHS must commit to a transparent, consultative process in which all interested stakeholders have a seat at the table and can contribute their ideas, expertise, and experience. We must develop "our" Program together.

DHS should leverage existing partnership structures such as the Critical Infrastructure Partnership Advisory Council (CIPAC) and Sector Coordinating Councils (SCCs). DHS should also utilize additional processes to involve a greater number and diversity of stakeholders, and work to encourage their participation in other cybersecurity and critical infrastructure activities. DHS should emulate many of the steps taken by NIST to maximize stakeholder input in developing the Framework, such as extensive public comment procedures, wide circulation of preliminary outlines and papers, meetings, and open workshops held around the United States.

[3] EO Section 8 (d) directs DHS to "coordinate establishment of a set of incentives designed to promote participation in the [Voluntary] Program."