IT Sector perspectives on the Cybersecurity Framework

Danielle Kriz
Director, Global Cybersecurity Policy

Briefing for NIST Internet Security and Privacy Advisory Board
October 23, 2014
ITI’s Work on Cybersecurity

- **ITI’s cybersecurity work and perspective is global**
  - ITI engages in DC and in capitals around the world (Beijing, Delhi, Brussels, Seoul, Tokyo…)

- **To be effective, any efforts to improve cybersecurity must:**
  - Leverage public-private partnerships and build upon existing initiatives and resource commitments;
  - Reflect the borderless, interconnected, and global nature of today’s cyber environment;
  - Be able to adapt rapidly to emerging threats, technologies, and business models;
  - Be based on effective risk management;
  - Focus on raising public awareness; and
  - More directly focus on bad actors and their threats.
Perspective on Framework - Generally

- Framework 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
  - Global, voluntary, consensus-based standards, guidelines, and best practices are essential tools to manage cybersecurity risk
  - Many organizations voluntarily use these standards and best practices – but others don’t… they likely may not know where to start or where to go next
  - The Framework aims to bridge this information gap
  - We hope to see much greater voluntary use of standards and best practices that can make a difference at the individual organization’s level, collectively raising all boats
- The Framework will help improve cybersecurity, and we are committed to helping it succeed
Perspective on Framework – Since Release

- NIST/administration have correctly focused on raising awareness of Framework and how it can be used to manage cyber risks
  - ITI and our companies are seeing growing awareness domestically and internationally
  - ITI companies getting inquiries from their customers
- We also are seeing different types of “use”
  - ITI companies are seeing important, valuable internal impacts
- Ancillary benefits - workshops and related events have fostered and/or augmented cross-sectoral discussions and collaborations
- Framework was released only eight months ago
  - We are just at the beginning of a tremendous multi-year effort
  - Goal is not use or adoption of Framework- goal is managing cyber risks and improving resilience
  - Answers from RFI helpful- to sharing initial lessons and prioritizing next steps
  - But answers likely will change as awareness and use of tools continues to grow
IT Sector Activities Around Framework

- ITI as an association
  - Outreach to international audiences: Korea, Japan, China, India, Israel, Germany, UK to date, more planned
  - October 1, ITI “Cybersecurity Summit” in Washington DC
- ITI member activities
  - Holding webinars, holding and speaking at events, arranging for NIST to speak at events
  - Speaking with the media
  - Directly engaging in policy outreach with foreign government policymakers
  - Developing or mapping ICT products and services to the Framework to help others use it
  - Issuing white papers, blogs, marketing materials and collaterals
- IT SCC chosen not to issue implementing guidance
What next?

- Gov’t and industry both need to double down on outreach and awareness
  - SMBs, internationally, even interagency
  - Promote industry-developed guidance
- Clarify key points
  - Voluntary, based on existing standards and best practices, cybersecurity as part of business risk management
- Manage narrative and expectations
- Roadmap – good topics, but some initial concerns RE supply chain, conformity assessment, technical privacy standards
- Don’t move yet to Framework v 2.0 – too early
  - Need time to understand v 1.0
- Other valuable NIST and DOC roles outside of CI (dust off 2011 Green Paper)