4th Cybersecurity Framework Workshop Outbrief and Discussion of Next Steps

September 13, 2013
University of Texas at Dallas

NIST
National Institute of
Standards and Technology
U.S. Department of Commerce

Questions for Reviewers to Consider

How can the Preliminary Framework:

- adequately define and address outcomes that strengthen cybersecurity and support business objectives?
- enable cost-effective implementation?
- appropriately integrate cybersecurity risk into business risk?
- provide the tools for senior executives and boards of directors to understand risks and mitigations at the appropriate level of detail?
- enable senior executive awareness of potential consequences of successful cyber attacks?
- provide sufficient guidance and resources to aid businesses of all sizes while maintaining flexibility?

Will the Discussion Draft, as presented:

- be inclusive of, and not disruptive to, effective cybersecurity practices in use today?
- enable organizations to incorporate threat information?

Is the Discussion Draft:

- presented at the right level of specificity?
- sufficiently addressing unique privacy and civil liberties needs for critical infrastructure?

What We Heard

- Additional clarification is needed on how the Framework Core, FITs, and Profiles integrate
    - Add more content to Profile section (how to use, when to use)
- Express Framework Core in terms of outcomes
- Additional sector-specific material is needed
- Depict the Functions as cyclic, not linear
- Augment Framework presentation
- Framework should account for organizations that are just getting started
- Clarify integration of threat and Framework implementation

Topic Specific Output

- DHS Voluntary Program – leverage SSAs/SCCs for implementation guidance
- Framework Governance – desire for the collaborative process to continue to further develop and refine the Framework
- Areas for Improvement – sector specific and cross-sector action plans, supply chain, interdependencies, training and workforce development
- Executive Engagement – make case for concept of cyber risk not Framework
- Framework Presentation and Tools – more usable examples
- Framework Implementation Guidance –application of subcategories needs to be clearer

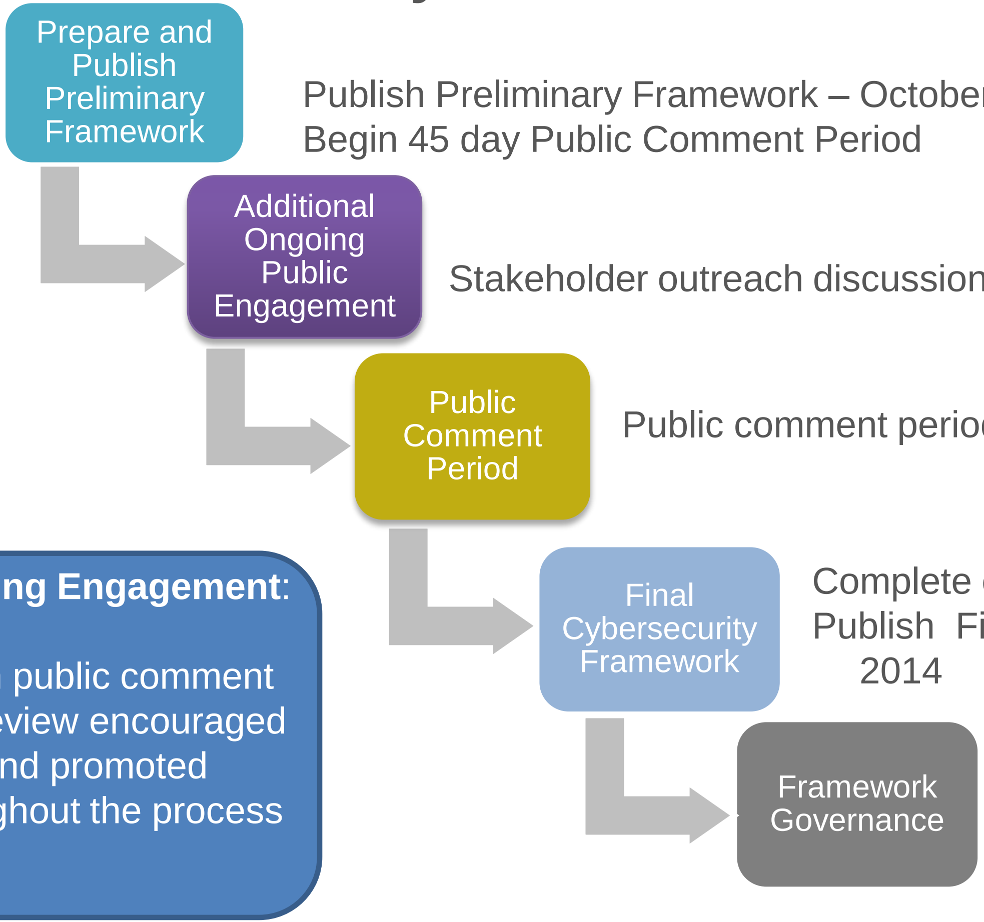
How to Adopt the Framework

EO 13636: *"The Cybersecurity Framework shall incorporate voluntary consensus standards and industry best practices to the fullest extent possible."*

The Framework builds on existing practices and can be leveraged by organizations in varying ways.

- Establish or Improve a Cybersecurity Program
- Communicate Cybersecurity Requirements with Stakeholders
- Identify Gaps

Getting from the Preliminary Framework to the Final Framework and Beyond



Prepare and Publish Preliminary Framework

Publish Preliminary Framework – October 10, 2013
Begin 45 day Public Comment Period

Additional Ongoing Public Engagement

Stakeholder outreach discussion continue

Public Comment Period

Public comment period closes – November 25, 2013

Final Cybersecurity Framework

Complete comment resolution and disposition
Publish Final Cybersecurity Framework – February 2014

Framework Governance

Framework maintenance and updates

Ongoing Engagement:

Open public comment and review encouraged and promoted throughout the process

Next Steps

- NIST is planning additional workshops
- Focus on implementing the Framework
  - What do sector-wide implementations look like?
  - What do organizational implementations look like?
- Publish Preliminary Framework for Formal Public Comment (October 10th, 2013)

Review material at http://www.nist.gov/itl/cyberframework.cfm

Please send us your continued observations and further suggestions at cyberframework@nist.gov

EO-PPD Deliverables

120 days – **June 12, 2013**

- Publish instructions: unclassified threat information
- Report on cybersecurity incentives
- Publish procedures: expand the Enhanced Cybersecurity Services

☑

150 Days - **July 12, 2013**

- Identify cybersecurity critical infrastructure
- Evaluate public-private partnership models
- Expedite security clearances for private sector

☑

240 Days – **October 10, 2013**

- Develop a situational awareness capability
- Update the National Infrastructure Protection Plan
- Publish draft voluntary Cybersecurity Framework

365 days – **February 12, 2014**

- Report on privacy and civil rights and civil liberties cybersecurity enhancement risks
- Stand up voluntary program based on finalized Cybersecurity Framework

Beyond 365 - **TBD**

- Critical Infrastructure Security and Resilience R&D Plan

For more info on Voluntary Program Development: EO-PPDTaskforce@hq.dhs.gov