What we heard

The Cybersecurity Framework Workshop

Day 1 Working Sessions

May 17, 2017

cyberframework@nist.gov

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

Thank You!

Workshop Purpose

The purpose of this workshop is to provide attendees with the following:

- An opportunity to **provide comments** and discuss the Framework Draft V1.1
  - Working Sessions
- A forum for participants to **learn** from each other's **experiences** with the Framework
  - Presentations, Panels, Working Sessions
- An **update** on Framework-related **policy issues and the progress** of technical work that may **shape future enhancements**
  - Presentations, Panels

What we heard participants say: V1.1 (part 1)

- Measurement
  - Affirmed measurement is an important topic
  - Suggested the need to simplify the language in Section 4.0 and questioned how detailed measurement should be in the Framework
  - Suggested that further work needs to be done on different types of measurements, what makes good metrics and their specific value-add, why metrics are useful, and the limits of measurements
- Threat Intelligence
  - Affirmed that describing context is important in threat intelligence
  - Suggested modifying specific language in the core to specifically call out threat intelligence could be more clear

What we heard participants say: V1.1 (part 2)

- Identity
  - Affirmed that the current proposed language is appropriate
  - Suggested a new subcategory in PR.AC related to authentication
  - Suggested that more research be done into the incorporation of identity and the Framework
- Tiers
  - Affirmed that Tiers are useful
  - Suggested that more clarification is needed in the introductory section for the Tiers
  - Confirmed that Tiers and not maturity models

What we heard participants say: V1.1 (part 3)

- SCRM
  - Suggested adding clarifying language about SCRM to Section 3.3, including a definition and further explanation on its complexity
  - Affirmed that SCRM have its own category and subcategories under the Identify Function in v1.1, but consideration should be given to integrating SCRM throughout all of the Framework Functions, Categories and Subcategories in a v2.0
  - Affirmed that SCRM should be a separate aspect in the Framework Implementation Tiers
  - Confirmed that they are using Profiles in supplier management
  - Suggested that use cases be developed on how to apply SCRM to the whole Framework Core
  - Suggested that more research is needed on supplier prioritization (i.e. critical suppliers) and interdependency analysis.

What we heard participants say: Special Topics (part 1)

- Coordinated Vulnerability Disclosure
  - Affirmed that this topic is mature and ready for inclusion in the Framework
  - Suggested that more research be conducted in the intersection of Coordinated Vulnerability Disclosure and the Framework
- Policy and Law
  - Confirmed the notion that the voluntary nature of the Framework is beneficial
  - Suggested that more research and outreach be conducted into how regulators should view the Framework

What we heard participants say: Special Topics (part 2)

- Confidence Mechanisms
  - Affirmed that the concept of having industry led conformance testing models are beneficial
  - Suggested NIST publicize but not endorse these models
  - Suggested that more research and development be done in this area
- Future of Informative References
  - Affirmed that multiple types of mapping activities are useful
  - Suggested multiple options for achieving an evolving and modern process for updating informative references

What we heard participants say: Special Topics (part 3)

- Federal Use
  - Suggested that more clarity is needed on how to implement Executive Order and NISTIR 8170
  - Suggested that Section 4.0 and NISTIR 8170 become a worked example
- Innovations in the Framework
  - Suggested that more work be done in the governance space
  - Suggested that Profiles can be applied to anything and the need to highlight that fact in the Framework
  - Affirmed that there are natural dependencies between elements of the Framework that cannot be implemented interpedently
- Cybersecurity Insurance
  - Confirmed that Section 4.0 and linking metrics and measurement to business objectives may help both insurers and insured.
  - Confirmed that data is king – both for insurers for use in actuarial calculations and organizations for better risk management.

Next Steps

- Workshop report will be posted soon; please review it
  - Look for email survey on this workshop
- NIST will consider whether to revise and issue a second draft of V1.1
- Continue to work with us online
  - Send feedback to cyberframework@nist.gov
  - Comment on future posted materials
  - Submit additional candidates for Industry Resources on the Framework
- Encourage others to use the Framework
- Keep the momentum!