Cybersecurity Framework Workshop 2017 Summary

What we heard and next steps

July 21, 2017

1 Background

Cybersecurity risk management is more important than ever to organizations of all sizes and across all sectors – whether or not they are formally considered to be part of the Nation's critical infrastructure. The Framework for Improving Critical Infrastructure Cybersecurity provides a voluntary, flexible approach to help an organization better understand, manage, and reduce its cybersecurity risks. Based on existing standards, guidelines, and practices, the Framework can aid in prioritizing investments and maximizing the impact of each dollar spent on cybersecurity. By providing a common language, it is especially helpful in communicating about cybersecurity inside and outside the organization. That includes improving cybersecurity communications, awareness, and understanding between and among information technology, planning, and operating units, as well as senior executives and between a buyer and supplier.

The National Institute of Standards and Technology (NIST) utilized a year-long consultative process with stakeholders to create the Framework in response to Executive Order 13636 issued in February of 2013. Released February 12, 2014, the Framework is an approach to cybersecurity risk management that aligns policy requirements, business needs, and technological approaches.

NIST has continued to engage with stakeholders through multiple avenues of communication: hosting workshops, receiving feedback from individuals and groups in response to several requests for public input, as well as unsolicited observations and recommendations. These communications focused on how the Framework is being used and identified opportunities for improvement. NIST has shared widely a set of resources based on organizations' use of the Framework with the goal of encouraging and assisting others to put the Framework to use in improving their management of risk.

Most recently, NIST:

- Published a proposed draft version 1.1 of the Cybersecurity Framework[1] on January 10, 2017. This update sought to clarify, refine, and enhance the Framework, while minimizing change for current and potential users,
- Issued a Request for Comments (RFC), through the Federal Register[2], on the Framework draft proposed updates. NIST received and analyzed over 120 responses to the RFC[3], and
- Published an initial RFC analysis[4] on May 15, 2017.

NIST held a workshop at NIST headquarters in Gaithersburg, Maryland on May 16-17, 2017 to discuss the initial RFC comments and analysis and to continue processing the proposed

[1] https://www.nist.gov/cyberframework/draft-version-11
[2] https://www.federalregister.gov/documents/2017/01/25/2017-01599/proposed-update-to-the-framework-for-improving-critical-infrastructure-cybersecurity
[3] https://www.nist.gov/cyberframework/rfc-cybersecurity-framework-draft-version-11
[4] https://www.nist.gov/sites/default/files/documents/2017/05/16/rfc2-response-initial-analysis-20170515.pdf

updates. Discussion topics included Framework Implementation Tiers, supply chain risk management (SCRM), and metrics and measurement using the Framework. Approximately 1,200 individuals from across the country and around the world participated in the workshop either in person or via webcast.

This document highlights the most prevalent themes and findings from the May 2017 workshop. It summarizes areas of agreement as well as issues in which there is a lack of consensus and describes NIST's plans to continue facilitating use of the Framework.

2 Cybersecurity Framework Use

Workshop participants and panelists provided their experiences and observations on their use of the Framework. These included the use and customization of the Framework across all organization sizes and various sectors such as: healthcare, finance, maritime transportation, and communications. The workshop also identified International users of the Framework which includes organizations in the United Kingdom, Canada, Israel, and Malaysia.

Consistent with past input, participants overwhelmingly and consistently said that the Framework is a useful tool for discussing and coordinating cybersecurity needs at all levels within an organization. The Framework was described as very helpful in identifying and communicating cybersecurity needs and requirements with 3rd party vendors and service providers. Participants described the Framework's value in creating cybersecurity policies and expressing sector specific requirements.

3 Evolution

Future evolution of the Framework was a key topic at the workshop, with participants discussing the amount of change that should be incorporated into Version 1.1 of the Framework versus what would be a more appropriate fit for Version 2.0. Based on earlier stakeholder input, NIST's stated goal is for Version 1.1 to incorporate improvements based on lessons learned while remaining fully interoperable with the original version of the Framework, Version 1.0. NIST reiterated at the workshop that updates adversely affecting interoperability with Version 1.0 will be deferred until draft Framework Version 2.0 is produced.

Workshop participants said that adjusting the Framework title could have a positive impact in encouraging greater use by conveying its broad use outside of critical infrastructure sectors, consistent with input from RFC respondents. Participants also discussed the effects a title change could have on reducing the perception that the Framework is U.S. focused, expanding its usage internationally. Many participants recommended that the title be changed to simply "The Cybersecurity Framework," rather than the extended "Framework for Improving Critical Infrastructure Cybersecurity."

4 Working Session Summaries

NIST built an agenda for the 2017 workshop to reflect topics of interest based on the responses received in the 2015 RFI, 2016 workshop, and 2017 RFC. Generally, those topics addressed the

evolution of Framework, select Roadmap areas, and customization of Framework by specific groups of users. Frequent themes identified from the stakeholder feedback included the use of and relationship between Implementation Tiers and Profiles, application of the Framework to support supply chain risk management, intent and use of Section 4.0 - *Measuring and Demonstrating Cybersecurity*, and small business use of the Framework. Breakout sessions at the workshop were structured to address specific topics, with applicable themes as a subset of the discussion. The following sections summarize the working session discussions.

4.1 Communications Sector Use

Within the Communications Sector, a number of organizations have developed their own methods to measure the effectiveness of NIST Cybersecurity Framework adoption. While this may be beneficial for individual organizations, it does not provide a sector-level approach to measuring Framework effectiveness. This session discussed potential approaches to measurement across the sector, including recent studies by sector working groups on issues related to cybersecurity, risk management, and best practices.

Participants affirmed the importance of metrics to risk-based application of the Framework and that cybersecurity measurement is important to making business decisions and ensuring users are measuring the intended objective. There was a general desire to see the metrics used in a simple, flexible, and easy to understand manner. Participants confirmed that metrics should be flexible, both to address emergence of new technologies and threats, and to ensure that organizations of all sizes can effectively use metrics, since the best use of metrics for a large organization might be quite different from those that would benefit smaller organizations. The cost of measurement and measurement systems was also discussed—namely the significant cost to larger organizations, the lack of resources available to smaller organizations, and the possible assistance that would better serve small companies.

Session participants generally agreed that the new measurement section of the Framework was important, but wanted some aspects clarified. Specifically, participants wanted more detail on what organizations should measure. Smaller businesses would benefit from more education and use cases, to improve their understanding and application of the Framework. Finally, some suggested that the discussion of metrics belonged in another document.

4.2 Confidence Mechanisms

This session explored topics related to the development, use, and adoption of different types of mechanisms to increase confidence in an organization's ability to manage cybersecurity risk. Topics included: the depth/breadth of the approach; the use of measures and scale (quantitative or qualitative); translational value of the approach; and the approach's organizational focus.

One of the session's key themes was how to gain confidence in the sufficiency and efficacy of an implementation of the Framework, and how to determine the comparative confidence across multiple Framework implementations. Flexibility is a key benefit of the Framework, yet

participants reported that same flexibility makes it difficult to compare outcomes consistently, and presents challenges to those who need to review Profiles (e.g., internal auditors). Participants considered both internal and external audits, and identified the Framework as a useful tool for guidance when conducting audits and identifying threats and gaps in an organization's cybersecurity program.

Several organizations presented examples of confidence mechanisms that they have developed. British Standards Institute (BSI) Group described its work building a third-party review of Framework outcomes as part of an existing Certification to International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC) 27001. Information Systems Audit and Control Association (ISACA) described a Framework-based audit program that provides confidence in the effectiveness of an organization's cyber security governance, processes, and controls. The Capability Maturity Model Integration (CMMI) Institute described a new risk-based offering that aims to apply the established CMMI understanding of maturity to evaluation of cybersecurity capability and practices. It is important to note that NIST does not endorse any one commercial approach and is supportive of private sector efforts to determine and express confidence.

Session participants debated information security certification, expressing concerns that using the Framework itself as a standard might increase the tendency to use Framework as an object of compliance, ultimately inhibiting Framework implementation. There was general agreement that accountability should come from within an organization's industry in the form of developing and communicating minimum practices. Participants suggested NIST not set minimum practices but rather continue in its traditional role of defining measurement science. Attendees noted variations in how companies gained confidence in Framework implementation and suggested that as the Framework becomes more widely used—including in the evaluation of supply chain risk—better methods for calibration might be needed.

4.3 Coordinated Vulnerability Disclosure

Vulnerabilities have always been a concern for cybersecurity risk managers. The Framework offers some guidance to organizations in handling vulnerabilities in a cybersecurity program. However, industry has provided comments suggesting more could be done within the Framework to address vulnerabilities. This breakout session centered around the topic of Coordinated Vulnerability Disclosure (CVD), its maturity in the ecosystem, and its potential inclusion in the Framework.

Some participants confirmed CVD was an important topic in cybersecurity risk management but were unsure of how to incorporate it into the Framework. Participants also cited the National Telecommunications and Information Administration (NTIA)'s continued support of CVD multi-stakeholder processes. With the current system of CVD being cultivated by other stakeholders, participants discussed the potential for collaboration between NIST, NTIA, and the private sector in the future.

Workshop participants noted that while CVD was a mature topic, perhaps a phased integration over multiple iterations of the Framework was necessary. Some participants suggested Framework Version 1.1 was an appropriate venue to introduce CVD. Other participants suggested Version 2.0 might be more suitable for comprehensive inclusion with more time to research the intersection between CVD and the Framework.

4.4 Cybersecurity Governance

Cybersecurity risk management requires the buy in of all levels of management, including the board of directors. The Framework provides guidance as to how organizations can use a common lexicon to communicate between and among organizations. Industry has provided comments that suggest the board level of organizations requires more attention when spreading cybersecurity risk management awareness. This breakout session discussed the challenges and opportunities of cybersecurity risk management within the context of broader enterprise risk management decision making.

Participants discussed how executive leadership and security professionals can use the Framework to assess an organization's cybersecurity needs. There was agreement among participants that varying levels within an organization, including executive leadership, find the common language of the Framework approachable and easy to understand. Participants confirmed that the inclusion of the measurement section in the draft Framework Version 1.1 was important and necessary for facilitating discussion between security professionals and board members, providing an understanding of how cybersecurity affects an organization's business goals.

Many participants found the Framework to be useful as written and were wary of having too many additional subjects/topics added in future iterations. Participants suggested building on the Framework's Informative References to cover additional subject matter that may relate to governance and enterprise risk management.

4.5 Cybersecurity Insurance

This session explored how a widely used and consistent approach to understanding and communicating cybersecurity risks might benefit an evolving and growing insurance market. Participants provided their experiences with using the Cybersecurity Framework for developing and analyzing data and using the data for underwriting cybersecurity risks. The session also explored how the Framework might be helpful in communicating cybersecurity outcomes in the insurance market.

The working session began with a presentation from NIST on some of the challenges surrounding cybersecurity insurance risk, measurement, awareness, and communications. The Department of Homeland Security presented a brief overview of the Cyber Incident Data and Analysis Repository (CIDAR). This project's mission is to store and provide cyber incident data in the interest of helping the insurance sector and organizations measure and manage cybersecurity risk.

Session attendees discussed their use of the Framework to identify their cybersecurity risks, determine where insurance is needed, and communicate the risks and needs with insurance brokers and providers. There was general confirmation that the common language provided by the Framework allows for an effective discussion of an organization's gaps in cybersecurity and the areas to be insured. Session participants expressed a variety of concerns regarding their hesitancy to share data. Among these concerns was the possibility of regulators and government agencies using these shared data to bring litigation and penalties. The discussion included organizations' use of lawyers to review assessments and data for risk reduction purposes.

Participants acknowledged the use of metrics as key when identifying their business needs and risks but suggested further clarification is needed to effectively measure and accurately report their current position and needs to outside parties, including insurers.

4.6 Federal Use

The Federal Use working session discussed opportunities for using the Framework to improve risk management programs in federal agencies, and how the Framework complements existing federal cybersecurity and enterprise risk management policies, standards, guidelines, and approaches.

Participants highlighted the need for greater clarity on the relationship between the Framework and existing federal cybersecurity risk management policies and resources, including the Risk Management Framework and associated standards and guidelines. This need was expressed, in part, in the context of recently issued Executive Order 13800, *Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure*, which requires federal agencies use the Framework to manage their cybersecurity risk. Some participants suggested that the metrics language, currently in the draft Framework Version 1.1, was insufficient for implementation purposes. Session participants suggested the Framework include more federal policies, standards, and guidelines as Informative References to align to the recently issued Executive Order.

Participants also noted the recent issuance of draft NIST IR 8170, *The Cybersecurity Framework: Implementation Guidance for Federal Agencies*. Attendees suggested that Framework mappings to current and future policies, standards, and guidelines, and federal-focused Framework Profiles would help agencies to raise cybersecurity awareness and facilitate communication across an agency, prioritize cybersecurity activities, and improve cybersecurity and enterprise risk management programs.

4.7 Financial Services Profile

The Cybersecurity Framework is intended to be tailored to the specific needs of each sector. This session focused on ways to effectively tailor the Framework in the financial services sector and included discussion of the process of developing a sector Profile.

At the start of the session, a draft Financial Services Sector Profile was introduced by the Financial Sector Roundtable. The Profile uses a "5+2" concept that maintains the current Framework Functions (Identify, Protect, Detect, Respond, and Recover) and adds two sector-specific Functions--Governance and Dependency Management.

One of the key themes of this session was the need for governance—its benefit to regulators and how it will fit within the Framework. Participants suggested that due to heavy regulations, a thorough understanding of current risks and continued dialogue with regulators is needed. The two added Functions were discussed as an avenue to a shared understanding of the sector risk. Similarly, participants suggested that the Profile was an aid to facilitate those regulator/industry discussions by providing a common language.

Identifying and assisting with the needs of small and medium-sized businesses (SMBs) was another topic of discussion during the Financial Services Profile session. Participants confirmed that SMBs play a large role in the cybersecurity ecosystem and discussed the challenges faced by SMBs and the specific need to ensure SMBs are effectively managing cybersecurity risks.

Participants suggested further assistance may be required to aid SMBs in effectively managing cybersecurity risk. The use of mentors was suggested to help guide SMBs to currently available and valuable resources.

4.8 Future of Informative References

The informative references section of the Framework began as a list of the most cited industry standards and practices to help organizations manage cybersecurity risk, but has since been updated. This session discussed how the Framework should be updated to handle a changing and growing standards landscape.

Participants confirmed the Framework Core provides a common language for expressing the desired strategic goal, objective, and outcome for managing cybersecurity risk while the Informative References serve as a translation layer, providing detailed implementation guidance that is specific to each industry sector or technology. Participants suggested the Informative References should include various industry sector authoritative sources such as frameworks, best practices, implementation guides, and families of security controls.

The session participants recognized the challenges with maintaining the Informative References up to date over the lifecycle of the Framework. Some suggested providing the content of the Informative References as a data stream separate from the traditional document format. Removing Informative References from the Framework document would allow flexibility to continuously update the content as changes are made to the industry standard frameworks, best practices, and implementation guides. Participants felt that this decoupling of the Informative References from the Framework document would increase adoption by fostering flexibility. Providing a structured data format allows organizations to quickly leverage the

content and enhance it with additional context or customize it to fit their local policy and requirements.

Participants suggested a flexible governance model to include more Informative References from diverse sources in a timely and responsive way as the framework is being adopted nationally and internationally. Specifically, participants discussed a "federated model" in which the Informative Reference owners (e.g., ISO, IEC, etc.) develop Framework mappings, work with NIST to quality check those mappings, and host those mappings at their respective Web sites. NIST would then link to their Web sites from a NIST Web page. Participants further suggested NIST use this mechanism to collaborate with the owners of the Informative References to determine when the mapping should be updated.

4.9 Identity

This session explored and discussed the proposed updates to the Framework concerning identity. There were two concurrent sessions that discussed the topic of identity: a session at the NIST main campus, and a session at the K(NO)W Identity Conference 2017 in Washington D.C. The second session was administered in recognition that many identity experts were meeting at the K(NO)W conference in close proximity to the 2017 Cybersecurity Framework Workshop. Across the two separate sessions, participants recognized the importance of keeping specific language to support backwards compatibility with previous versions of the Framework. Most participants stated agreement with the proposed changes to the draft Framework but felt some additional changes were needed.

Session participants suggested a separate subcategory should be added to the Framework to address authentication since they felt the current treatment does not indicate the importance of authenticating users and does not recognize risk-based approaches to authentication. Acknowledging the Framework's focus on outcomes, rather than prescriptive requirements, the participants suggested language such as the following to describe the new authentication subcategory, "authentication of users, privileged users, devices, and processes is managed appropriate to the risk associated with the asset and authorizations (e.g., single, multi factor, continuous authentication)." Given the number of recent incidents that have originated with privileged users, participants suggested that authentication of privileged users may need to have its own subcategory within the Protect: Access Control Category.

With the addition of more content to the Access Control Category and the potential inclusion of language around authentication, participants suggested the inclusion of more references specific to managing identity and stated the importance of references that reflect guidance to address challenges of identity proofing, authentication, and authorization. Participants specifically requested the addition of NIST SP 800-63, *Digital Identity Guidelines* and other internationally recognized identity standards and guidance (e.g., ISO 29115, Good Practice Guide 44 & 45) to the Informative References. Participants also suggested that identity federation standards and guides be considered for future inclusion in the Informative References as they become available.

Participants also noted the challenge in implementation of Subcategory PR.AC-3, "Remote access is managed," given the Subcategory's current lack of detail. In future versions of the Framework, participants suggested revising this item to expand upon the different aspects of "managing access" and determine more granular outcomes which, when aggregated, support the idea of "managed" access.

4.10 Innovations in the Framework

The Framework has been adopted by many users in industry. Some users have incorporated pieces of the Framework into their entire cybersecurity program. This session was designed for advanced users of the Framework to discuss challenges in deep implementations and how they tailored the Framework to fit their unique cybersecurity risk environment. Participants from this session discussed challenges encountered during implementation.

The biggest challenge discussed was the current state of mappings and the Framework. Participants noted multiple efforts under way to map to the Framework and the varied nature of mappings. For example, some mappings provide a relationship from the Framework Categories to laws; other mappings provide a relationship from the Framework Subcategories to controls. While these mappings are useful as stand-alone documents within specific sectors, participants suggested the ability to reuse these documents in other sectors or contexts would be helpful.

Adding to the concern of mappings, participants noted the existence of multiple overlapping standards and regulations. Participants suggested research be conducted to understand how to maximize the reuse of these Framework mappings, citing harmonization as a desirable outcome.

4.11 International Alignment

The Framework is used increasingly by international organizations and nations to manage cybersecurity risk. This session discussed current thinking on ways to help align cybersecurity strategies globally to better combat international threat, as well as satisfy multiple regimes of divergent and sometimes inconsistent policies.

During the working session, participants agreed that the Framework supports discussions on strengthening critical infrastructure within and across nations. The discussion also included the importance of harmonization, alignment, and mapping to other frameworks. No agreement was reached concerning risk-based versus prescriptive implementation methodology of the Framework internationally. Participants suggested that some international organizations may use the Framework as a descriptive set of outcomes to be achieved in accordance with risk variables, while others may use the Framework as a prescriptive set of controls that must be implemented regardless of context.

Participants noted that some governments may be apprehensive to promote the adoption of the Framework as a form of political and cultural resistance to accepting a purely US approach

to cybersecurity. These concerns were amplified given the mandate for federal government use of the Framework in Executive Order 13800. Some nations are more likely to adopt standards from international standards development organizations than those developed by NIST.

The session discussed the derivation of NIST IR 8170 from the Framework and that both documents are very much US focused. Participants expressed concern that if NIST IR 8170 receives similar recognition as SP 800-53, *Security and Privacy Controls for Federal Information Systems and Organizations*, businesses working with the US federal government will need to adopt it. Participants also noted the potential event that NIST IR 8170 may be incorporated in or mapped to international standards, including The General Data Protection Regulation (GDPR), but much of the privacy components from GDPR are not covered in the Framework. Participants suggested aligning the international standards and regulation space.

4.12 Internet of Things (IoT)

The diverse use and rapid proliferation of connected devices creates enormous value for industry, consumers, and broader society. At the same time, emerging threats highlight the pressing need to develop and apply guidance to maintain the cybersecurity of devices and the systems where they are deployed. This session sought feedback on how the Framework may be applied to the IoT, both in terms of the devices themselves, as well as their integration into broader enterprise and network environments.

Participants affirmed IoT is not a revolutionary development warranting unprecedented tools, guidance, and regulations. However, participants acknowledged that IoT widens the threat landscape and presents new challenges. These include a shift in how computing is used, determining how to manage the growing number of devices being added into networks, and the increasing likelihood of cybersecurity exploits that can lead to physical harm. Participants confirmed that a one-size-fits-all approach is not feasible and IoT is too large to be viewed as a single issue. Even within individual industries, there are diverse needs and use cases – each with a different threat landscape and varying security and privacy risks.

Session participants discussed various options for addressing IoT security, including addressing IoT more explicitly in the next Framework update, leveraging Framework Profiles, regulating the environments in which devices are deployed, standards-based certifications, and international standards. One suggestion involved taking a threat-based approach to IoT and considering the environment in which a device is deployed. For example, while a connected teapot poses few security risks in the home environment, it could introduce a significant threat in an environment where the network is purposely air-gapped. Another major discussion on the threat-based approach was the potential to examine different sectors and use cases, identify common threats, and create cross-cutting threat-based approaches (including Profiles).

Participants suggested that a sector-based approach was a good start and that the federal government could be the first sector for a use case. There is a large range of federal use cases and deployment environments, existing IoT efforts, and the opportunity to look at procurement practices, shared services, and shared security responsibility. Panelists and participants

suggested different strategies for the "federal government as a consumer" use case. The three most common suggestions were: include IoT in future Framework updates; create Framework Profiles for federal use cases; and use a Framework-like approach of convening the public and private sectors to collaboratively create an IoT-specific document.

4.13 Measurement

This session explored and discussed the proposed updates to the Framework concerning measurement, including the correlation of business results to cybersecurity risk management metrics and measures.

Much of the discussion centered on potential uses of Framework for self-assessment. Participants suggested self-assessment could be performed through any combination of internal assessment, external audit, and conformity assessment. Generally, participants felt there is no one-size-fits-all method of cybersecurity measurement, because of the varying business and mission needs of sectors, subsectors, and individual organizations. Participants discussed possible application of cybersecurity measures including understanding and reducing risk within an organization, in vendor organizations, and representing risk in appropriate and meaningful ways for partners. Many participants expressed concerns about the use and protection of measurements by external parties.

Participants confirmed that measurement is an important component of cybersecurity risk management. The session discussed the level of abstraction of the measurement taking place, suggesting that there were multiple levels at which to measure—for example, indicators, process, policy, financial, and sector measurement. Participants suggested that the Framework can be valuable in measuring all of these dimensions. The discussion confirmed that relating measurements to business or mission objectives will ensure continued use of the Framework as a risk-based approach versus a compliance-based approach. Participants affirmed that each individual organization must determine *how* to measure relative to its unique mission and business objectives.

Participants discussed separating measurement from the Framework document, suggesting that cybersecurity risk measurement was so critical to successful risk management that a separate effort was needed to ensure measurement received adequate attention. Participants further suggested that characteristics of metrics should be included in any discussion of measurement to guide organizations. Participants reiterated that the focus of metrics should be on the importance of knowing what to measure and why they are measuring.

4.14 Policy and Law

The Framework allows organizations to tie their regulatory and legal requirements to cybersecurity risk management. This session highlighted how to effectively use the Framework within the legal and policy arenas to effectively identify, assess, and manage cybersecurity risk.

Many workshop participants expressed interest in the topic of Policy and Law relative to the Framework. Participants anticipated that the Framework could provide a needed, common language by which lawyers and IT professionals could overcome confusion when expressing cybersecurity requirements. However, they expressed concern for how Executive Order 13800 and its requirement of Framework implementation for Federal agencies would affect Framework users.

Many participants suggested that great care should be taken in how the Framework section on measurement and metrics is written, namely, that measurement and metrics should be clearly defined and represented in a non-prescriptive manner. Participants suggested that the introduction of measurement and metrics in the Framework could ultimately lead to a general mandate for the entire community. This prompted suggestions to re-iterate the voluntary nature of the Framework.

4.15 Supply Chain Risk Management (SCRM)

This session began with an overview of SCRM activities at NIST, including efforts in defining and standardizing SCRM concepts currently in use across industry. The overview established a baseline of SCRM terminology and relationships between suppliers and consumers and concluded with a description of the Cybersecurity Framework Version 1.1 update criteria. NIST reminded participants that Version 1.1 is intended to enhance and clarify the concepts within the Cybersecurity Framework Version 1.0 and associated Roadmap. The overview and discussion framing the concepts for the Version 1.1 update established a robust conversation regarding SCRM and the associated Version 1.1 updates.

Participants agreed that while the addition of the SCRM Category was beneficial, aspects of supply chain risk management should be integrated throughout many other subcategories in the Core in any future versions. The discussion transitioned to the relevance of Tiers within SCRM, with a consensus that most organizations would not accept a Tier 1 or 2 supplier's goods or services. Participants agreed, however, that these decisions were ultimately for each organization to make on its own. Participants also agreed the additional SCRM guidance for each of the Tiers was useful and a good addition for the Tier definitions.

Participants identified several areas of the draft Framework Version 1.1 requiring further clarity. Most participants agreed the addition of Section 3.3, Communicating Cybersecurity Requirements with Stakeholders, helped shape SCRM activities and concerns; however, it did not go far enough in explaining the concepts and complexities within SCRM. In addition to the current Section 3.3 example of how to use Profiles for cyber SCRM purposes, several participants expressed an additional SCRM use case for Profiles—that target state Profiles could be used to establish minimum thresholds for various suppliers based on the *access requirements* to the consumer organization's systems and networks. Participants suggested NIST should provide further guidance for both use cases on how Framework Profiles could be applied. Finally, participants observed challenges in discerning the relative criticality of suppliers. They suggested NIST continue research on approaches for analyzing supply chain interdependencies and prioritizing and defining supplier criticality. Since the conclusion of the

workshop, NIST has released draft NIST IR 8179, *DRAFT Criticality Analysis Process Model: Prioritizing Systems and Components* that is NIST's initial step in helping organizations make these criticality decisions.

4.16 Small and Medium-sized Businesses (SMBs)

Cybersecurity affects all organizations; small- and medium-sized businesses (SMBs) are no exception. While the Framework was designed for organizations of all sizes, SMBs may experience challenges customizing and applying the Framework to their unique business environments. This session sought to highlight ways that SMBs are currently using the Cybersecurity Framework as well as how the Framework can be made more usable to SMBs. Discussion also touched on additional cybersecurity resources that would assist SMBs.

While participants in the working session agreed the Framework is an ideal solution for SMBs struggling with limited resources, they stressed the importance of demonstrating the relevance of the Framework to smaller businesses early in the Framework document. Workshop participants also stated that proper messaging of the Framework to SMB owners is essential. Participants suggested messaging could focus specifically on the differences between risk management vs. controls implementation. Finally, session attendees noted that every organization needs a cybersecurity champion (typically an executive) to succeed but that SMBs may need to be creative in how they get executive buy-in. Due to limited cybersecurity personnel, SMBs could consider the creation of security committees consisting of available personnel from other parts of the organization.

To make the Framework more relevant to SMB personnel, it was suggested that the overall language of the Framework document could be reworked to clearly demonstrate its positive impact on an SMB. This language might include supplemental guidance clarifying the meaning of the subcategory outcomes. Session participants suggested that SMBs may benefit from messaging via use cases—for example, illustrating how an SMB achieved improved recovery from cybersecurity incidents because of their implementation of the Framework. Other messaging suggestions included the issuance of Profile guidance for SMBs which would more clearly link business objectives to cybersecurity outcomes.

4.17 Threat Intelligence

This session explored and discussed the proposed updates to the Framework concerning threat intelligence, namely the modification of Subcategory ID.RA-2.

Session participants highlighted the differences between information and intelligence and referred to the refinement concepts embodied in the Data, Information, Knowledge, Wisdom (DIKW) hierarchy and other knowledge management models. There was general confirmation that the use of a common vocabulary allows organizations to describe, classify, and evaluate threats in a consistent and precise manner and to establish a shared understanding of the threat environment. Participants confirmed the importance of contextualizing and filtering the threat information that is collected within the organization and the threats identified by

external, third-party sources. Threat intelligence is produced at multiple levels, from abstract to concrete. Participants stated some threat intelligence is suitable for strategic decision making, while other intelligence is better suited for tactical and operational decision making.

Workshop participants noted the need to establish and use consistent terminology when discussing threats. They suggested that the Framework could be used to direct information to the right individual given the needs of the organization.

4.18 Implementation Tiers

This session explored and discussed the proposed updates to the Framework concerning Implementation Tiers, most notably the clarification of the relationship between Implementation Tiers and Profiles as well as the use of the Tiers in Framework implementation.

Participants discussed the need for continued refinement and clarification of the value and use of Implementation Tiers within the Framework. They noted that few organizations have shared actual Framework lessons learned (including how those organizations have used Tiers), which obscures how much the Tiers are helping. Some participants cited their attempts to measure Core outcomes using the Tiers and the difficulties they encountered.

Session participants confirmed that Tiers are not a strict “maturity model”; however, achievement of the characteristics in the higher-level Tiers indicates improving organizational maturity. The group also discussed the makeup of the Tiers (e.g., should there be a Tier 0? Why 4 vs. 5?). Participants also discussed how Tiers are applied for various types of organizations, such as small businesses. Participants stated that incentives for Framework adoption continue to be a challenge; while a key driver for improving (i.e., moving to higher Tiers) continues to be fear of exposure to organizational risk.

Participants stated the draft supply chain language that has been added to the Tiers language is not helpful and that detailed criteria in the Tiers reduces their value as an expeditious and easy evaluation method. They suggested that sharing additional lessons learned would better support comparisons within industries.

5 NIST Next Steps

NIST has received a tremendous amount of feedback through stakeholder outreach. This feedback is essential for effective evolution of the Framework and related work. NIST is committed to increasing the value of the Framework over time through an open and continual stakeholder dialogue. This dialogue will help the Framework to remain relevant to changes in threats and technologies, incorporate lessons learned, and elevate common cybersecurity practices of a given community to best practice for all Framework users.

5.1 Framework Update

Based on stakeholder feedback, NIST will release a second draft of Framework Version 1.1 for public comment. Key features of this second draft will include, but not be limited to:

- An update to the measurement section to refine and summarize self-assessment concepts;
- Integration of the proposed Cyber Supply Chain Risk Management Implementation Tier language into some combination of the other three Implementation Tier properties;
- Refinement and clarification within Section 3.3, Communicating Cybersecurity Requirements with Stakeholders;
- Removal of the proposed Section 3.7 on applicability to the federal government, as this is now addressed through EO 13800 and supporting U.S. policy;
- An evaluation and possible language updates throughout the document to better accommodate IoT and Industrial Control Systems cybersecurity; and
- An additional subcategory in the PR.AC subcategory to address authentication.

This update is expected in the Fall of 2017 with a 30-day comment period to follow. The final version of the Framework 1.1 is expected in calendar year 2018.

5.2 Framework Roadmap

The NIST Roadmap for Improving Critical Infrastructure Cybersecurity (Roadmap) was released in conjunction with the Framework in February 2014[5]. The Roadmap discusses key areas for development, alignment, and collaboration identified by stakeholders in the Framework development process. The Framework is intended to be a "living document," and "will continue to be updated and improved as industry provides feedback on implementation." In response to stakeholder feedback, NIST anticipates several key Roadmap changes were identified including:

- Workshop participants acknowledged the importance of metrics when properly implemented and applied to the Framework. However, the concept of Measurement is bigger than the Framework itself and should be treated as such. Additionally, participants noted that some areas of measurement are nascent and are best developed through public-private dialogue. NIST is placing Measurement in the Roadmap in acknowledgement of the size of the topic and the need for continued development.
- Renaming Conformity Assessment to Confidence Mechanisms. Requests have been made in the past to develop assessment guidance for the Framework, and Workshop participants expressed the same desire for additional guidance. Based on working sessions over the last few workshops, the Conformity Assessment discussion has expanded from solely centralized standards and measures to include a distributed and market-based approach. This shift precipitates the need to re-organize the discussion around what users need to express confidence in a Framework implementation.

[5] https://www.nist.gov/sites/default/files/documents/cyberframework/roadmap-021214.pdf

- In keeping with continued focus on the small business community, Small Business Awareness and Resources will become a Roadmap item. This initiative will include efforts to educate and customize the Framework for small business use.
- A new Roadmap item will be added to address the relationship of one document to another, such as defining the relationship between the Framework and ISO 27001. These relationships are commonly referred to as mappings or crosswalks. This Roadmap area will also reflect NIST and stakeholder efforts to develop and publish on-line Informative References, as well as apply those references in ways that yield efficiencies. Potential work in the Roadmap area includes but is not limited to mapping vocabulary, ontology, data structures, and automation.

The updated Roadmap will be available at the same time as the Framework update for review and consideration. In accordance with the previous Roadmap document, this iteration of the Roadmap will be published as a final document, with ongoing feedback, dialogue, and collaboration between the government and stakeholders.

5.3 Program Focus

Based on stakeholder feedback, NIST will maintain continued focus on the small business, regulatory and international communities. Given the recent requirement for federal agencies to use the Framework, NIST will add federal agencies as a focus area.

NIST is evaluating how best to expand outreach to small businesses in the U.S. Specifically, NIST is currently evaluating the feasibility of a train-the-trainer (TTT) outreach model. Historically, NIST has partnered with the Small Business Administration and the Federal Bureau of Investigation to offer small businesses cybersecurity awareness and risk assessment training. This curriculum could be expanded to include cybersecurity risk management using the Framework. Supportive materials and TTT instruction would then be offered to organizations wishing to bring NIST content to their pre-existing small business outreach.

Workshop participants noted that many small businesses may have challenges customizing the Framework for their use. To help address these challenges, NIST is developing Framework "starter Profiles" for commonly-occurring small business types and business processes (e.g., manufacturer, e-Commerce Web merchant, medical office). The objective is to create Framework Profiles that require no customization for initial use. Small businesses would be welcome to customize those Profiles over time to better suit their needs.

At the request of Workshop participants and RFC respondents, NIST will continue advocacy within the regulatory community to promote the value of using a universal and voluntary set of cybersecurity objectives. To advance the use of voluntary approaches by regulators, NIST's National Cybersecurity Center of Excellence (NCCoE) will continue partnership with the U.S. Coast Guard to produce Framework Profiles. In the past, this effort produced a voluntary Framework Profile in collaboration with and for the bulk liquid transport segment of the

maritime industry. NCCoE and the U.S. Coast Guard will create Profiles for other segments of the maritime industry, including passenger vessel and mobile off-shore drilling segments.

Workshop participants highlighted use of the Framework as a tool to support alignment of international policy. This alignment helps stakeholders reduce the burden of international regulatory and legal regimes, leading to a reduced cost of operation. To promote this objective, many private sector organizations engage foreign governments to encourage their consideration of the Framework or publication of complementary national frameworks. NIST will continue reinforcing those private sector discussions with government-to-government dialogue. NIST is also working through the American National Standards Institute (ANSI) in collaboration with the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC) to align international standards. Supported by NIST participants, joint working groups of ISO and IEC have launched studies on the relevance of the Framework to ISO/IEC standards. The desired outcome of this work will likely be the creation of an ISO/IEC Technical Report mapping the Framework to ISO/IEC Standards, increasing the use of the Framework internationally.

In support of federal use of the Framework, NIST has embarked on a transformation process for our cybersecurity risk management publications, and a corresponding education process. This effort began with the release of draft NIST IR 8170, *The Cybersecurity Framework: Implementation Guidance for Federal Agencies*[6]. The formal comment period for NIST IR 8170 closed on 30 June 2017, and the document will be revised based on comments received. Comments will also shape how the Framework is included in other NIST risk management publications. NIST is currently updating SP 800-37, *Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach* to revision 2, which will include the Framework and how it supports the Risk Management Framework. Other NIST risk management publications will be addressed after the update of SP 800-37. Accompanying all publication updates, NIST is interacting with the federal community through a combination of meetings and speaking engagements to both receive feedback and educate stakeholders about document evolution.

Over the upcoming several months, NIST will launch “online Informative References” to account for additional, and sometimes topic specific, Informative References. Workshop participants discussed a federated model where parties wishing to contribute a mapping of their Informative Reference to the Framework Core will host and maintain the mapping at their Web site. NIST will evaluate those mappings for accuracy with regard to the Framework, and then link to those mappings from the Framework Web site.

In response to several RFC and workshop comments, NIST will publish processes for evolving the Framework and Roadmap documents to new versions. These processes will include qualifying criteria for additions, modifications, and deletions.

[6] https://beta.csrc.nist.gov/News/2017/Draft-NISTIR-8170,-Cybersecurity-Framework-Impleme

Framework workshops are most valuable when they align with stakeholder needs. NIST intends to organize future workshops via public calls for abstracts. Stakeholders whose abstracts are selected by NIST will organize that portion of the program. NIST will continue to organize program content regarding the evolution of the Framework and Roadmap publications. NIST offered a topic-specific satellite working session at the 2017 workshop. Satellite working sessions allow NIST to bring a specific topic to a pre-established conference for round table discussion. This mechanism was effective at obtaining subject matter expert feedback on the Framework. NIST will consider this mechanism for future workshops.

5.4 Actions Recommended to Stakeholders

The Framework ecosystem shows continued signs of health. Framework stakeholders are increasing efforts to share Framework-related information and practices. NIST applauds these activities as propagation through the broader community magnifies the positive benefits of the Framework. The following activities are recommended for stakeholders:

- Share your Framework experiences within and outside of your sector or community. Whether on a local, national, or international scale, this action will help your organization use the Framework with other organizations, and it also helps the larger ecosystem. Beyond informal sharing, consider hosting Framework-based informational meetings, workshops, and conferences as they are great ways to help others understand and refine use of the Framework.
- Publish a sector or community crosswalk. Mappings of important legislation, regulation, or guidelines to the Framework Categories or Subcategories are considered a crosswalk. These artifacts are important because they are the basis for cybersecurity requirements reconciliation and prioritization. Consider mailing a hyperlink of your on-line crosswalk to cyberframework@nist.gov for consideration as an on-line Informative Reference.
- Customize the Framework for your sector or community and publish that work in the form of a Profile. This activity might involve a) determining parts of the Framework that are more, or less, applicable to your sector or community, and b) suggesting generalized cybersecurity priorities based on your sector or community's needs. Publication of Profiles is extremely beneficial to the ecosystem because it helps other organizations accelerate their customization process.
- Publish case studies of your Framework implementation. The entire Framework ecosystem will benefit from your confirmation of Framework use, understanding the ways you customized and are using the Framework, understanding the positive results you are achieving, and identifying areas for improving the Framework.
- Submit a paper during the NIST call for abstracts for the next Framework workshop. Your ideas will help to inform Framework stakeholders on summaries of use, noteworthy resources and Informative References, and valuable perspectives on cybersecurity risk management using the Framework.
- Share your Framework resources with NIST.

6 Feedback and Engagement

NIST is committed to maintaining an open dialogue. The community is encouraged to participate in this public-private partnership through workshop attendance, responses to RFIs and RFCs, and emailing questions to the Framework alias: cyberframework@nist.gov.

National Security Archive,

Suite 701, Gelman Library, The George Washington University,

2130 H Street, NW, Washington, D.C., 20037,

Phone: 202/994-7000, Fax: 202/994-7005, nsarchiv@gwu.edu