Draft NIST Roadmap for Improving Critical Infrastructure Cybersecurity Version 1.1
December 5, 2017

1. Introduction

This companion Roadmap to the *Framework for Improving Critical Infrastructure Cybersecurity* (Cybersecurity Framework or the Framework) describes plans for advancing the Framework development process, discusses the National Institute of Standards and Technology's (NIST's) next steps with the Framework, and identifies key areas of development, alignment, and collaboration. This plan provides a description of anticipated future activities related to the Framework and offers stakeholders another opportunity to participate actively in the continuing Framework development process. While the plan is focused on the Cybersecurity Framework, the results of work described in this roadmap are expected to be useful to a much broader audience to improve cybersecurity risk management in much the same way that the Framework itself is useful to many sectors and organizations that are not strictly defined as part of the critical infrastructure. This Roadmap reflects revisions to the original planning document released in February 2014[1] when Version 1.0 of the Framework was released, and contains updates corresponding with draft Version 1.1 of the Framework.

2. Evolution of the Cybersecurity Framework

In accordance with Executive Order 13636,[2] NIST utilized a year-long consultative process with stakeholders to create the Cybersecurity Framework. Released February 12, 2014, the Framework is an approach to cybersecurity risk management that aligns policy requirements, business needs, and technological methodologies.

Since the release of the Cybersecurity Framework, in its role defined in the Cybersecurity Enhancement Act of 2014,[3] NIST continues to be a convener of a public-private partnership and "facilitate and support the development of a voluntary, consensus-based, industry-led set of standards, guidelines, best practices, methodologies, procedures, and processes to cost-effectively reduce cyber risks." Accordingly, NIST:

- Issued a Request for Information (RFI),[4] December 11, 2015, regarding Cybersecurity Framework use;
- Published an RFI Analysis[5] on March 24, 2016;
- Hosted a Workshop[6] on April 6-7, 2016, in Gaithersburg, Maryland;

[1] [PDF] https://www.nist.gov/sites/default/files/documents/cyberframework/roadmap-021214.pdf
[2] [LINK] https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity
[3] [LINK] https://www.congress.gov/bill/113th-congress/senate-bill/1353/text
[4] [LINK] https://www.federalregister.gov/documents/2015/12/11/2015-31217/views-on-the-framework-for-improving-critical-infrastructure-cybersecurity
[5] [LINK] https://www.nist.gov/news-events/news/2016/03/cybersecurity-framework-comments-reveal-views-framework-update-increased
[6] [LINK] https://www.nist.gov/news-events/events/2016/04/cybersecurity-framework-workshop-2016

- Published a proposed Draft Version 1.1[7] of the Cybersecurity Framework on January 10, 2017. This update sought to clarify, refine, and enhance the Framework, while minimizing change to current and potential users;
- Issued a Request for Comment (RFC),[8] through the *Federal Register*, on the Cybersecurity Framework draft proposed updates;
- Received and analyzed over 120 responses to the RFC and published an initial RFC analysis[9] on May 15, 2017;
- Hosted a workshop on May 16-17, 2017, to further discuss the proposed draft revisions[10] and published a summary of the workshop;[11] and
- Published for public comment a proposed Draft 2 of Version 1.1. of the Cybersecurity Framework on December 5, 2017. This update seeks to further clarify, refine, and enhance the Framework, while minimizing change to current and potential users.

The Cybersecurity Framework is a living document, and will continue to be updated and improved with the input and feedback from industry, government, and academia.

3. Evolution of the Roadmap

As the Framework has continued to evolve, so too has the Roadmap. Considering the continuous advancements in technology and the evolving cybersecurity landscape, the Roadmap will continue to highlight areas of development relevant to the Framework and also of broader interest. Topics previously addressed by the Roadmap such as Authentication and Supply Chain Risk Management (SCRM) have been researched, developed, and incorporated into the current draft of the Cybersecurity Framework Version 1.1. These focus areas may continue to be highlighted in future versions of the Roadmap as these areas evolve and mature or they may be replaced or supplemented by additional topics.

New topics included in this version of the Roadmap include:

- Cyber-Attack Lifecycle;
- Measuring Cybersecurity;
- Referencing Techniques;
- Small Business Awareness and Resources; and
- Governance and Enterprise Risk Management.

The new Cyber-Attack Lifecycle topic includes the Automated Indicator Sharing and Data Analytics items from the previous Roadmap, and incorporates the topic of coordinated vulnerability disclosure. The title Cyber-Attack Lifecycle reflects the importance of a holistic, approach that maximizes the value of threat intelligence, discerns threat events from the large volumes of available data, and reduces timelines to receive vulnerability information from researchers. To address a growing need for cybersecurity measurement that is aligned and supportive of organizational objectives and decisions, Measuring

[7] [LINK] https://www.nist.gov/news-events/news/2017/01/nist-releases-update-cybersecurity-framework
[8] [LINK] https://www.federalregister.gov/documents/2017/01/25/2017-01599/proposed-update-to-the-framework-for-improving-critical-infrastructure-cybersecurity
[9] [PDF] https://www.nist.gov/sites/default/files/documents/2017/05/16/rfc2-response-initial-analysis-20170515.pdf
[10] [LINK] https://www.nist.gov/news-events/events/2017/05/cybersecurity-framework-workshop-2017
[11] [PDF] https://www.nist.gov/sites/default/files/2017/07/21/cybersecurity_framework_workshop_summary.pdf

Cybersecurity is added as a Roadmap item. Referencing Techniques is added to provide Framework stakeholders an understanding of future intent for the Informative References portion of the Core, as well as the general process and methodology of relating one or more reference documents. A continued focus on cybersecurity best practices and implementation relative to small businesses is important to our Nation's cumulative cyber-posture. Finally, a continued stakeholder focus on board governance, organizational governance, and enterprise risk management necessitates a specific topic.

Three previous Roadmap topics are renamed in this update. Authentication was renamed Identity Management to account for a broader range of important technical topics including authorization and identity proofing. Technical Privacy Standards has been renamed Privacy Engineering to better align with the concepts in related NIST publications such as Interagency Report 8062 - *An Introduction to Privacy Engineering and Risk Management in Federal Systems*. Conformance Assessment has been renamed Confidence Mechanisms to reflect a broader range of activities that instill digital trust.

As NIST makes advances and receives feedback from public and private stakeholders on the Cybersecurity Framework and the Roadmap, these documents will continue to be revised and updated.

4. Areas for Development, Alignment, and Collaboration

Several high-priority areas for development, alignment, and collaboration are listed by section below.

4.1. Confidence Mechanisms
4.2. Cyber-Attack Lifecycle
4.3. Cybersecurity Workforce
4.4. Cyber Supply Chain Risk Management
4.5. Federal Agency Cybersecurity Alignment
4.6. Governance and Enterprise Risk Management
4.7. Identity Management
4.8. International Aspects, Impacts, and Alignment
4.9. Measuring Cybersecurity
4.10. Privacy Engineering
4.11. Referencing Techniques
4.12. Small Business Awareness and Resources

While this list of high-priority areas is not intended to be exhaustive, these are important topics identified by stakeholders that should inform future versions of the Framework. They require continued focus to evolve areas that have yet to be developed sufficiently or where further research into their relationship to the Cybersecurity Framework is needed.

To be effective in addressing these areas, NIST will work with stakeholders to identify primary challenges, solicit input to address those identified needs, and collaboratively develop and execute action plans for addressing them. These areas may also reflect potential capabilities in the Cybersecurity Framework Core. As progress is made in each of these areas, they can be used in conjunction with, or as part of, the Framework to enhance or improve cybersecurity programs.

4.1. Confidence Mechanisms

Previously entitled Conformity Assessment, this Roadmap section was retitled to reflect a broader range of activities that instill digital trust. Whereas conformity assessment can be used to show that a product, service, or system meets specified cybersecurity risk management requirements, Confidence Mechanisms build upon conformity assessment to include means of determining the sufficiency and efficacy of organizational cybersecurity risk management, inclusive of product, service, and systems conformity.

The output of confidence mechanisms can be used to enhance an organization's understanding of its implementation of a Framework profile. Effective confidence mechanisms provide the needed level of assurance, are efficient, and have a sustainable and scalable business case. Critical infrastructures' evolving implementation of Framework profiles should drive the identification of private sector conformity assessment activities.

NIST continues to encourage the community to build and manage confidence mechanism programs to assist stakeholders. Several organizations have begun to develop such programs. For example, the British Standards Institute (BSI) is working to build a third-party review of Cybersecurity Framework outcomes as part of an existing Certification to the International Organization for Standardization and the International Electrotechnical Commission (ISO/IEC) 27001. The Information Systems Audit and Control Association (ISACA) is developing a Cybersecurity Framework-based audit program. And the NIST Baldridge Performance Excellence Program encourages self-assessment through its Cybersecurity Excellence Builder tool. While NIST does not endorse any commercial approach, NIST does encourage and support a diverse, market-based set of approaches to instill confidence.

NIST will continue working with:

- Those who manage confidence mechanisms programs to assist industry in further leveraging these resources; and
- Private and public sector entities that have a need for conformity demonstration, to help understand how these organizations can leverage existing programs.

4.2. Cyber-Attack Lifecycle

Cybersecurity is closely linked to the threats an organization faces from those that would seek to exploit a vulnerability or weakness. Therefore, it is important to approach cybersecurity from the perspective of the cyber-attack lifecycle by identifying threat sources, threat events, and vulnerabilities that predispose an environment to attack. The cyber-attack lifecycle consists of the sequence of events that a malicious agent undertakes to successfully penetrate a network for nefarious purposes (e.g., data exfiltration, ransomware attacks, denial of service). Understanding the Tactics, Techniques and Procedures (TTP) an attacker may employ and the vulnerabilities an attacker may exploit are critical to effective cyber defense. To improve risk management capabilities, it is important that cyber threat information be readily available to support decision-making. This includes threat and vulnerability metrics that support determination of likelihood, impact, and, ultimately, risk.

Timely communication and actionable information are critical to counter threat and address vulnerability. This includes a near-real time exchange of automated threat and vulnerability indicators between organizations and information sharing communities such as Information Sharing and Analysis Centers (ISACs), Information Sharing and Analysis Organizations (ISAOs), industry peers, and supply chain partners and exchanges with security service providers. Sharing indicators based on information that is discovered prior to and during incident response activities enables other organizations to deploy measures to detect, mitigate, and possibly prevent attacks as they occur. Additionally, communication between and among vendors, researchers and industry stakeholders is paramount to prudent handling of previously unknown vulnerabilities. Understanding the severity and indicators of a vulnerability, mitigating the effects of the vulnerability, and addressing the root cause of the vulnerability are just some of the activities that require coordination among those stakeholders. Coordinated Vulnerability Disclosure (CVD) develops principles and best practices in coordinating management of vulnerabilities to benefit all stakeholders.

Organizations use a combination of standard and proprietary mechanisms to exchange indicator and vulnerability information. These mechanisms have differing strengths and weaknesses and often require organizations to maintain specific process, personnel, and technical capabilities. To make these efforts more effective, appropriate guidelines and standards need to be defined and then adopted in products to enable organizations of various levels of capability and size to make use of indicators and other related information.

To support this growing need, NIST SP 800-150 - *Guide to Cyber Threat Information Sharing,*[12] was published in October 2016 and provides high-level guidance on how to form, join, and effectively participate in information sharing communities. Also, standards such as the International Organization for Standardization ISO/IEC 29147[13] and ISO/IEC 30111[14] have been developed to outline CVD best practices.

Creation of useful and necessary threat information requires the ability to analyze big data effectively and efficiently. This is achieved through data analytics, which is the compilation and analysis of various types of information with the goal of using this information to drive decision-making. The analysis of complex behaviors in large scale-systems can begin to address issues of provenance, attribution, and discernment of attack patterns. Possible applications of data analytics in this field include integration of threat feeds from varying sources, automated triage, data filtering, indicator tracking, visualization, and reporting.

Several significant challenges must be overcome for the extraordinary potential of big data analytics to be realized, including the lack of: taxonomies for big data; mathematical and measurement foundations; analytic tools; measurement of integrity of tools; and correlation and causation. More importantly, the privacy implications in the use of these analytic tools must be addressed for legal and public confidence reasons.

[12] [PDF] http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-150.pdf
[13] [LINK] https://www.iso.org/standard/45170.html
[14] [LINK] https://www.iso.org/standard/53231.html

In continued collaboration with DHS and other relevant government participants, NIST plans to continue its Cyber-Attack Lifecycle research and participate in guidance development activities such as:

- Express cyber threat information using machine-readable formats and developing automated mechanisms for exchanging cyber threat information;
- Raise awareness of CVD among industry stakeholders;
- Support private and public sector efforts to further establish and streamline CVD approaches and methodologies;
- Support information sharing initiatives by public and private sector organizations such as Information Sharing and Analysis Centers (ISACs) and Information Sharing and Analysis Organizations (ISAOs);
- Benchmark and measure some of the fundamental scientific elements of big data (algorithms, machine learning, topology, graph theory, etc.) through means such as research, community evaluations, datasets, and challenge problems; and
- Develop NIST Special Publications on the secure application of big data analytic techniques in such areas as access control, continuous monitoring, attack warning and indicators, and security automation.

4.3. Cybersecurity Workforce

A skilled cybersecurity workforce is needed to meet the unique cybersecurity needs of critical infrastructure. There is a well-documented shortage of cybersecurity practitioners;[15]; there is an even more serious shortage of qualified cybersecurity practitioners who also have an understanding of the unique challenges facing critical infrastructure owners and operators. As threats, vulnerabilities, and technology environments evolve, the cybersecurity workforce must continue to adapt to design, develop, implement, maintain and continuously improve the necessary cybersecurity practices within critical infrastructure environments.

Various efforts, including the National Initiative for Cybersecurity Education (NICE), are fostering the education and training of a cybersecurity workforce for the future and establishing an operational, sustainable and continually improving cybersecurity education approach to provide a pipeline of skilled workers for the private sector and government. Organizations must understand their current and future cybersecurity workforce needs and develop hiring, acquisition, and training resources to raise the level of technical competence of those who build, operate, and defend data, systems, and networks delivering critical infrastructure services.

Building on several years' work with the Department of Defense (DoD) and the Department of Homeland Security (DHS), and via extensive public-private partnerships, NIST has published the NICE Cybersecurity Workforce Framework (NICE Framework).[16] The NICE Framework provides a fundamental reference resource for describing and sharing information about cybersecurity work roles, the discrete tasks performed by staff within those roles, and the knowledge, skills, and abilities (KSAs) needed to complete the tasks

[15] [LINK] http://cyberseek.org/ - Interactive jobs heat map and career pathways portal
[16] [LINK] https://doi.org/10.6028/NIST.SP.800-181

successfully. The NICE Framework provides a common lexicon to categorize and describe cybersecurity work, improving communication about how to identify, recruit, develop, and retain cybersecurity staff.

Many of the outcomes described in the Cybersecurity Framework Core are directly related to the roles, activities, and responsibilities of organizational personnel. The NICE Framework provides a complementary approach, describing the work roles that support accomplishment of the Cybersecurity Framework outcomes. In using the Cybersecurity Framework's steps to develop a measurable action plan, organizations can identify the specific tasks and KSAs needed by those who will fulfill the functions, categories, and subcategories described in the Cybersecurity Framework Core. Appendix D.1 of the NICE Framework includes examples of this integration.

Through NICE, NIST promotes cybersecurity workforce development activities via a public working group structure.[17] These activities may include further definition of how NICE Framework work roles, tasks, and KSAs help to fulfill Cybersecurity Framework objectives. Additional future activities are expected to include:

- Continue to extend and integrate NICE activities across critical infrastructure sectors to raise awareness of workforce development tools;
- Emphasize coordination of K-12, higher education, and local employers in regions across the nation;
- Identify and support applied research opportunities in areas including cybersecurity education, training, and workforce; and
- Convene conferences, workshops, webinars, and other events that support the development of cybersecurity education, training, and workforce resources; and
- Evolve NICE publications and resources as informed by the above activities.

4.4. Cyber Supply Chain Risk Management

Supply chains consist of organizations that design, produce, source, and deliver products and services. All organizations are part of, and dependent upon, product and service supply chains. Supply chain risk is an essential part of the risk landscape that should be included in organizational risk management programs.

Cyber Supply Chain Risk Management (C-SCRM) is the process of identifying, assessing, and mitigating the risks associated with the distributed and interconnected nature of technology product and service supply chains. It covers the entire lifecycle of a system (including design, development, distribution, deployment, acquisition, maintenance, and destruction) as supply chain threats and vulnerabilities may intentionally or unintentionally compromise a technology product or service at any stage.

Although many organizations may have robust internal risk management processes, supply chain criticality and dependency analysis, collaboration, information sharing, supplier management, and trust mechanisms remain a challenge. Organizations can struggle to identify their risks and prioritize their actions leaving the weakest links susceptible to penetration and disruption. Supply chain risk management, especially product and service

[17] [LINK] https://www.nist.gov/itl/applied-cybersecurity/nice/about/working-group

integrity, is an emerging discipline characterized by diverse perspectives, disparate bodies of knowledge, and fragmented standards and best practices.

Increasing adoption of supply chain risk management standards, practices and guidelines requires greater awareness and understanding of the risks associated with the time-sensitive interdependencies throughout the supply chain, including in and between critical infrastructure sectors/subsectors. This understanding is vital to enable organizations to assess their risk, prioritize, and allow for timely mitigation.

In recent years, the private-public supply chain community has advanced both technical guidance and related tools to support better management of supply chain risks. Some of these activities culminated in the October 2015 release of NIST SP 800-161*, Supply Chain - Risk Management Practices for Federal Information Systems and Organizations*,[18] which provides guidance on identifying, assessing, and mitigating supply chain risks at all organizational levels. The July 2017 draft *Criticality Analysis Process Model* (draft NISTIR 8179[19]) was engineered to work in conjunction with the SP 800-161 concepts. SCRM concepts also have been integrated throughout draft NIST SP 800-53 Rev. 5 - Security and Privacy Controls for Information Systems and Organizations[20] controls. NIST, the General Services Administration (GSA), and the University of Maryland Robert H. Smith School of Business continue to collaborate and learn from CyberChain,[21] a Web tool for measuring and assessing supply chain risk.

International standards also advanced C-SCRM and related topics with stakeholders. Of note, ISO/IEC 27036[22] was published in April 2014 to help organizations address *Information Security for Supplier Relationships*, and ISO/IEC 20243[23] was released in September 2015 to guide organizations on how to *Mitigate Maliciously Tainted and Counterfeit Products.*

However, challenges remain, particularly in organizational awareness of supply chain risks as well as awareness about the standards, best practices, guidance, and related tools available for use to mitigate many of these risks.

As information and maturity around C-SCRM advances, NIST will remain focused on identifying, evaluating and developing effective technologies, tools, techniques, practices and guidance that help secure an organization's supply chain. NIST will continue to raise awareness on this topic. Future activities will engage stakeholders to:

- Encourage broad industry engagement and leadership in supply chain risk management discussions and activities;
- Promote the mapping of existing supply chain risk management standards, practices and guidelines to the Framework Core;
- Identify challenges in Framework adoption and determine appropriate support to enable effective supply chain risk management;

[18] [PDF] http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-161.pdf
[19] [LINK] https://csrc.nist.gov/publications/detail/nistir/8179/draft
[20] [PDF] http://csrc.nist.gov/publications/drafts/800-53/sp800-53r5-draft.pdf
[21] [LINK] https://cyberchain.rhsmith.umd.edu
[22] [LINK] https://www.iso.org/standard/59648.html
[23] [LINK] https://www.iso.org/standard/67394.html

- Determine the key challenges to supply chain risk management (e.g., identifying and understanding mission critical functions and their dependencies, and conducting and validating prioritization) to enable more effective Framework implementation; and
- Evolve the NIST supply chain and criticality publications as informed by the above activities.

4.5. Federal Agency Cybersecurity Alignment

Several federal requirements directly apply to how federal agencies implement cybersecurity and the Framework:

- The Federal Information Security Management Act (FISMA)[24] requires federal agencies to implement agency-wide programs to provide information security for the information and information systems that support the operations and assets of the agency, including those provided or managed by another agency, contractor, or other source;
- The July 2016 update of Office of Management and Budget (OMB) A-130 Circular,[25] which establishes the complementary relationship between the NIST Risk Management Framework and the Cybersecurity Framework;
- Section 1(c)(ii) of the May 2017 Executive Order (EO) 13800 - Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure[26] - requires each federal agency to use the Cybersecurity Framework to manage cybersecurity risk; and
- The May 2017 OMB Memorandum 17-25,[27] which provides EO 13800 reporting guidance to federal agencies.

While the Framework was developed with critical infrastructure owners and operators as the primary stakeholders, federal standards and guidelines were often cited by non-federal participants during development of the Framework as useful in managing cybersecurity risk. For that reason, the Framework includes controls from NIST SP 800-53 -*Security and Privacy Controls for Federal Information Systems and Organizations*, as informative references in the Framework Core.

To assist federal agencies with integrating the Cybersecurity Framework and the Risk Management Framework, NIST issued a discussion draft of SP 800-37 - Revision 2, *Risk Management Framework for Information Systems and Organizations,* [28] which includes incorporation of key Cybersecurity Framework, privacy risk management and systems security engineering concepts.[29] NIST held an open workshop for additional stakeholder

[24] [LINK] https://www.congress.gov/bill/113th-congress/senate-bill/2521/text
[25] [LINK] https://www.whitehouse.gov/sites/whitehouse.gov/files/omb/circulars/A130/a130revised.pdf
[26] [LINK] https://www.whitehouse.gov/the-press-office/2017/05/11/presidential-executive-order-strengthening-cybersecurity-federal
[27] [LINK] https://www.whitehouse.gov/sites/whitehouse.gov/files/omb/memoranda/2017/M-17-25.pdf
[28] [PDF] https://csrc.nist.gov/CSRC/media/Publications/sp/800-37/rev-2/draft/documents/sp800-37r2-discussion-draft.pdf
[29] [LINK] https://csrc.nist.gov/publications/detail/sp/800-160/final

engagement and feedback on the discussion draft of the Risk Management Framework, including its consideration of the Cybersecurity Framework.

NIST issued draft report NISTIR 8170 - *The Cybersecurity Framework: Implementation Guidance for Federal Agencies*[30] to support agency heads and senior cybersecurity leadership in Framework implementation planning. The draft summarizes eight private sector uses of the Framework, which may be applicable for federal agencies. By leveraging NISTIR 8170, agencies can better understand how to implement the Framework in conjunction with other NIST cybersecurity risk management standards and guidelines.

To advance and evolve an integrated federal approach to cybersecurity risk management, NIST is also updating its suite of cybersecurity and privacy risk management publications (*e.g.,* SP 800-39 - *Managing Information Security Risk*[31]) to provide additional guidance on how to integrate implementation of the Framework. Similarly, the larger suite of NIST security and privacy risk management publications will be updated in consideration of NISTIR 8170 feedback and general Framework value.

Anticipated future NIST activities include:

- Reconcile public comments and publishing final versions of NISTIR 8170 and SP 800-37 revision 2; and
- Identify additional areas of alignment between existing and emerging standards, guidelines, frameworks, and other programs (e.g., Continuous Diagnostics and Mitigation) and the Framework.

4.6. Governance and Enterprise Risk Management

From its inception, the Cybersecurity Framework was designed to focus on and encourage a risk management approach within and among enterprises. As part of that strategy, NIST has aimed to support senior executive decision making with regard to cybersecurity risks. Additionally, private and public-sector participants involved in developing the Framework recognized and stressed at the outset that leadership "buy-in" to the approach was crucial to improving the nation's cybersecurity. At the federal level, the importance of active engagement of senior leaders in cybersecurity risk management and the Cybersecurity Framework, has been reinforced by a May 11, 2017, Executive Order.[32]

The Framework's language, structure, and components offer a natural integration of cybersecurity and enterprise risk management, enhancing senior executive decision making and engagement. More specifically, the Framework stages consideration of cybersecurity in larger enterprise risk management discussion, and also enable easy translation of how those larger enterprise risk decisions affect cybersecurity. Those with

[30] [PDF] http://csrc.nist.gov/publications/drafts/nistir-8170/nistir8170-draft.pdf
[31] [PDF] http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-39.pdf
[32] [LINK] https://www.whitehouse.gov/the-press-office/2017/05/11/presidential-executive-order-strengthening-cybersecurity-federal - The recent Executive Order 13800 on strengthening cybersecurity is another reinforcement about the crucial role of the heads of organizations: "Effective risk management requires agency heads to lead integrated teams of senior executives with expertise in IT, security, budgeting, acquisition, law, privacy, and human resources." That Order also directs: "Effective immediately, each agency head shall use The Framework for Improving Critical Infrastructure Cybersecurity (the Framework) developed by the National Institute of Standards and Technology, or any successor document, to manage the agency's cybersecurity risk."

enterprise risk management responsibilities in an organization typically include C-suite officers (chief executive officers, chief operating officers, chief financial officials, chief information officers, etc.), while directors within a board must govern the organization through oversight of those officers.

Given the importance of supporting senior executive risk decisions, the Framework's native support of enterprise risk management, the close relationship between ERM and governance, and the on-going focus of these topics in the larger ecosystem, Governance and Enterprise Risk Management will be a Roadmap topic area.

Inroads have been made in achieving these goals. For example, several organizations representing the interests of business leaders have incorporated the Cybersecurity Framework in relevant guidance. These include: the National Association of Corporate Directors, which has issued a *Cyber Risk Oversight Handbook*[33] and the Kogod Cybersecurity Governance Center.[34] Key among the considerations which appear to be influential and driving increased attention by boards and "C-suite" executives are the legal, regulatory, and media implications of their organizations' risk management approaches - and how implementation of these strategies brings management of risk to practice.

As an added tool to help drive the enterprise risk management process as well as the applicability of the Cybersecurity Framework at all levels within an organization, NIST produced the *Baldrige Cybersecurity Excellence Builder (BCEB)*, Version 1.0. This self-assessment tool is intended to help organizations better understand the effectiveness of their cybersecurity risk management efforts and identity improvement opportunities in the context of their overall organizational performance. The Builder blends organizational assessment approaches from the Baldrige Performance Excellence Program with the concepts and principles of the Cybersecurity Framework. Developed with industry input, including public comments on a draft version, the Builder was released in April 2017.

In the next one-to-three years NIST intends to continue and enhance its efforts to engage the leadership ranks of private and public sector organizations, partnering with and leveraging other organizations. Among other things, NIST will engage stakeholders in discussions about how best to:

- Stage cybersecurity's consideration in enterprise risk management decision making;
- Describe the difference between corporate governance and board governance;
- Determine how best to depict and describe the board-to-senior executive dialog; and
- Evolve NIST publications such as the BCEB and the Framework given the above dialogs.

[33] [LINK] https://www.nacdonline.org/cyber
[34] [LINK] http://www.american.edu/kogod/research/cybergov/

4.7. Identity Management

Identity Management solutions have continued to evolve and improve since the Framework's initial release, with both the public and private sectors making progress toward developing and implementing stronger standards, processes, technologies, and protocols. In particular, multi-factor authentication (MFA) solutions are increasingly used to augment passwords. New protocols – such as those defined by the Fast Identity Online (FIDO) and the World Wide Web Consortium (W3C) will bring easy-to-use and cost-effective MFA solutions to the consumer masses, with support by nearly every major browser and mobile manufacturer. These technologies are also being paired with biometric technology to make strong authentication more common and user-friendly, and increasingly, password-less. While adoption is trending in the right direction, the rate falls short of what is needed to best protect against cybersecurity threats, especially with "81 of hacking-related breaches [leveraging] either stolen and/or weak passwords35."

Although the use and adoption of identity technologies is evolving, challenges remain in aligning technology with risk management processes. This is exemplified by the plethora of personal information now available on social media or due to massive breaches of consumer data. To better align technology and risk management processes, NIST published a substantial 2017 update to the Special Publication 800-63 suite. NIST also continues development of associated implementation guides and National Cybersecurity Center of Excellence (NCCoE) reference models.

As threats and risks continue to evolve, a static approach to identity no longer suffices. Identity management needs to become more risk-aligned, adaptive, and contextual with guidance capable of supporting flexibility, modularity, and agility – while never sacrificing personal privacy to achieve better outcomes. To support this, NIST continues to evolve processes for its standards and guidance efforts, including increasing use of approaches and tools to maximize stakeholder engagement and be responsive to a rapidly changing threat landscape. In addition, NIST will leverage the National Cybersecurity Center of Excellence to bring together important identity management and cybersecurity requirements that are needed to address specific business cybersecurity challenges.

To positively participate and impact the growing identity ecosystem, NIST will:

- Inform the development and enhancement of standards, guidelines, implementations and technology gaps through targeted NCCoE use cases, reference implementations, and technology deployments;
- Conduct focused research to better understand new and emerging technologies, their impact on existing standards, and the implementation of identity management solutions;
- Pilot innovative identity proofing technologies and processes so that a range of demographics can prove their identity remotely and access digital services;
- Continue active participation in national and international identity management standards, guidance, best practices, profiles, and frameworks to create an enhanced,

[35] [LINK] 2017 Verizon Data Breach Report Executive Summary, http://www.verizonenterprise.com/resources/reports/rp_DBIR_2017_Report_execsummary_en_xg.pdf

interoperable suite of secure, privacy-enhancing solutions, including authentication and authorization within the IoT; and

- Continue to foster the growth, adoption, and scaling of technology, such as MFA and identity proofing, by partnering with commercial, federal, and international stakeholders to overcome adoption barriers;
- Evolve NIST identity management guidelines and publications as informed by the above activities.

4.8. International Aspects, Impacts, and Alignment

Globalization and advances in technology have driven unprecedented increases in innovation, competitiveness, and economic growth. Critical infrastructure has become dependent on these enabling technologies for increased efficiency and new capabilities. Many governments are proposing and enacting strategies, policies, laws, and regulations covering information technology for critical infrastructure as a result. Because many organizations and most sectors operate globally or rely on the interconnectedness of the global digital infrastructure, these requirements are affecting, or may affect, how organizations operate, conduct business, and develop new products and services. Diverse or specialized requirements can impede interoperability, result in duplication, harm cybersecurity, and hinder innovation. In turn, this can significantly reduce the availability and use of innovative technologies to critical infrastructures in all industries and hamper the ability of organizations to operate globally and to effectively manage new and evolving risks.

Currently, no common language or taxonomy exists among international entities relative to cybersecurity. Many countries are working to develop their own, unique standards and best practices which may make interoperability at the international level a more challenging and sometimes onerous process. To this end, international collaboration and alignment would lead to greater innovation and a more effective and efficient utilization of resources. Because the Framework references globally accepted standards, guidelines and practice, organizations domiciled inside and outside of the United States can use the Framework to efficiently operate globally and manage new and evolving risks.

In December 2014, the Cybersecurity Enhancement Act of 2014 affirmed NIST's role in driving global alignment in consultation with international organizations, as well as governments of other nations. To support the law and Framework stakeholders, NIST has engaged in international alignment through both bi-lateral dialogs with governments of other nations and engagement with standards developing organizations.

NIST continues to actively engage with the international community in an effort to increase utilization of the Cybersecurity Framework and further alignment with international standards. To date, NIST has participated in more than 30 government-to-government interactions to determine philosophy and disposition regarding Framework. These efforts have resulted in or supported some countries and international entities using the Framework or considering adopting a similar approach towards cybersecurity. For example:

- The Information-technology Promotion Agency (IPA) translation of the Framework to Japanese;
- The Italian National Framework for Cyber Security[36] using the Framework as a foundation;
- The Israeli adaptation and translation of the Framework to Hebrew;
- The Bermuda Cybersecurity Framework Workshop, where the Bermudian government confirmed their use of the Framework and encouraged the voluntary use of Framework in private sector; and
- The Ontario Energy Board (OEB) using the Framework to measure cybersecurity efforts of non-bulk electric organizations.[37]

NIST is also actively engaged with the ISO and IEC to map existing international standards to the Framework. This work is expected to culminate in the publication of an ISO/IEC Technical Report summarizing that work. NIST will expand its efforts to communicate the intent and approach of the Framework to the international community, with the goal of seeking greater alignment and use. Among other things, NIST will:

- Continue to engage foreign governments and international organizations directly to explain the Framework and seek alignment of approaches when possible;
- Work with industry stakeholders to assist with their international engagement; and
- Exchange information and working with standards development organizations, industry, and sectors to ensure the Framework alignment and compatibility with existing and developing standards and practices.

4.9. Measuring Cybersecurity

Every organization wants to gain maximum value and effect for its finite cybersecurity-related investments. This includes reducing risk and optimizing the potential reward of cybersecurity. Organizations frequently make go-ahead decisions, comparing scenarios that differ in projected cost, and estimated benefit and risk reduction. However, these scenarios are often based on "best guess." Increasingly, senior executives are asking for a more accurate and quantitative portrayal of these factors and how they might change. Providing more accurate and quantifiable answers to these questions requires an aligned, modular, and systemic approach to cybersecurity measurement, so that measurement at more technical levels is supportive of high-level decision making.

Since development work on the Framework was begun in 2013, measurement has been a recurrent area of interest and much discussion. That discussion, including a desire to have better information and tools to assess the effectiveness of cybersecurity strategies and actions, reflects the broader issue of measurement within the cybersecurity community. This is an under-developed topic, one in which there is not even a standard taxonomy for terms such as "measurement" and "metrics." The development of reliable ways to measure risk and effectiveness would be a major advancement and contribution to the cybersecurity community.

NIST is initiating a cybersecurity measurement program focusing on aligning technical

[36] [LINK] http://www.cybersecurityframework.it
[37] [PDF] https://www.oeb.ca/sites/default/files/OEB-CS-Framework-WhitePaper-20170601.pdf

measures to determine effect on high-level organizational objectives, as well as to support decision making by senior executives and oversight by boards of directors. The initiative will build on existing research and approaches, and will involve consultation with the research, business, and government sectors, including those already offering measures. The program will also rely on previous work such as NIST SP 800-55 - *Performance Measurement Guide for Information Security.*[38] Likely activities within this program include:

- Research to understand challenges, insights, and gaps in cybersecurity measurement;
- Preliminary work to define a basic vocabulary and subdivide the diverse cybersecurity measurement topic space;
- Discussion of those work products and other critical topics at one or more public workshops; and
- Evolution of NIST SP 800-55 as informed by the above activities.

4.10. Privacy Engineering

A key challenge for the privacy field has been the difficulty of determining how to design information technologies and systems that protect individuals' privacy, and by extension, civil liberties in an increasingly connected world. The Fair Information Practice Principles (FIPPs) - developed in the early stages of computerization and data aggregation to address the handling of individuals' personal information - have been used as a basis for a number of laws, regulations, and frameworks in the U.S. and around the world. The FIPPs, as principles, provide an important set of general policy considerations, but lack the quantifiable elements necessary for system engineers to develop, implement, and assess privacy protections at a system level.

Although cybersecurity provides some degree of privacy protection, individuals' privacy cannot be achieved solely by securing personally identifiable information (PII). Privacy risks also can arise from the intentional or authorized processing of PII, including when cybersecurity measures are processing PII to provide increased security.[39] Research is being conducted in the public and private sectors to improve current privacy practices, but many gaps remain. In particular, there are few identifiable technical standards or implementation guidelines to mitigate the impact of cybersecurity activities on individuals' privacy or civil liberties.

To address these circumstances, NIST is contributing to the development of the discipline of privacy engineering as a bridge between privacy policy and system-level implementation. NIST has established a program for privacy engineering with the goals of advancing 1) a lexicon to describe the field and 2) the development of widely adopted frameworks, models, methodologies, tools, and standards. In January 2017, NIST published NISTIR 8062 - *An Introduction to Privacy Engineering and Risk Management in Federal*

[38] [LINK] https://csrc.nist.gov/publications/detail/sp/800-55/rev-1/final

[39] [PDF] https://www.nist.gov/sites/default/files/documents/cyberframework/cybersecurity-framework-021214.pdf - For example, security measures such as persistent activity monitoring can create concerns about the degree to which information is revealed about individuals that is unrelated to cybersecurity purposes. See section 3.5 of the CSF for additional considerations.

Systems.[40] The publication provides a foundation for the concepts of privacy engineering and risk management, and introduces a set of privacy engineering objectives and a privacy risk model. NIST also has developed a tool for organizations to use to conduct privacy risk assessments based on this privacy risk model. In addition, NIST is integrating guidance for privacy into its existing guidance for cybersecurity risk management, including current draft revisions to SP 800-37 - *Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy* and 800-53, *Security and Privacy Controls for Information Systems and Organizations*.[41/42] These activities promote repeatable and measurable approaches to privacy protection that can be communicated clearly across an organization and improve collaboration between the privacy and security teams.

NIST will continue to work with stakeholders in the federal privacy community, academia, and the private sector to develop frameworks, models, methodologies, tools, and standards that can be used to achieve more effective privacy protections in systems. NIST's activities will focus on building on its introductory work, including:

- Expand integration of privacy guidance into additional NIST risk management guidelines;
- Engage with standards development organizations to advance privacy engineering standards;
- Work collaboratively with other NIST programs such as IoT Cybersecurity efforts to advance integrated privacy and cybersecurity processes; and
- Promote the use and improvement of tools and solutions to engineer privacy protections into systems.

4.11. Referencing Techniques

Referencing Techniques has been added to this Roadmap to address the relationship of one set of cybersecurity requirements, controls, or outcomes ("references") to another, such as defining the relationship between Framework outcomes and ISO 27001 requirements. These relationships are commonly referred to as mappings or crosswalks. References range far beyond the Framework Informative References. However, Informative References serve as an easy starting point for this topic.

To handle the changing and growing cybersecurity standards, industry and sector specific recommended practices, technology specific implementation guides, and general guidelines landscape, the Informative References must adapt. These references serve as a translation layer for the principles expressed in the categories/subcategories of the Cybersecurity Framework Core. As such, additional informative references will help organizations address emerging needs when implementing the Cybersecurity Framework.

To enable expansion of the Informative Reference to exhaustive mappings and to expand the number of Informative References, NIST is transitioning Informative References into an

[40] [PDF] http://nvlpubs.nist.gov/nistpubs/ir/2017/NIST.IR.8062.pdf
[41] [PDF] https://csrc.nist.gov/CSRC/media/Publications/sp/800-37/rev-2/draft/documents/sp800-37r2-discussion-draft.pdf
[42] [PDF] https://csrc.nist.gov/csrc/media/publications/sp/800-53/rev-5/draft/documents/sp800-53r5-draft.pdf

on-line format. This catalog will provide users a basis for searching and selecting the most appropriate references to meet their needs. The resulting body of references is also viewed as foundational for future work standardizing language, mapping formats, and researching automation.

Envisioned Roadmap work items include:

- Develop an anthology for describing the controls in a standardized format;
- Develop a governance model for maintaining and administering online Informative References;
- Collaborate with the current Informative Reference document owners to expand those mappings and make them available online;
- Engage additional parties in development of online Informative References;
- Discuss referencing language, format, process, and automation with stakeholders at upcoming workshops;
- Integrate existing technology security practices to security control catalog; and
- Determine appropriate elements of the above dialog to include in NIST publications.

4.12. Small Business Awareness and Resources

The vulnerability of any one small business may not seem significant to many other than the company's owner and employees. However, there are almost 29 million U.S. small businesses and nearly half of the U.S. private sector working population is employed in a small business.[43] These businesses produce approximately 46 percent of our Nation's private sector output and create 64 percent of all net new private sector jobs in the country. Therefore, a vulnerability common to many - or even just a few, key - small businesses could pose a threat to the Nation's economic base. An information security incident can be detrimental to the business, its customers, employees, business partners and many others. It is important that small business leaders understand and have effective approaches to manage risks to their information, systems and networks.

To address this need, NIST published NISTIR 7621 Revision 1 - *Small Business Information Security.*[44] This report provides guidance on how small businesses can implement basic security for their information, systems, and networks and gives a basic overview of information security. NIST is also collaborating with the National Cyber Security Alliance (NCSA)[45] on outreach avenues to small- and medium-sized businesses (SMBs). This includes participating in a webinar series to explain NIST cybersecurity resources to SMBs.

NIST will collaborate with public and private sector partners to embark on a "listening tour" to hear first-hand from SMB owners about their cybersecurity needs. Based on these discussions, NIST will work with federal stakeholders and SMB owners and operators to address gaps in cybersecurity resources. Importantly, NIST will reflect the specific preferences of those SMBs in determining how best and at what level to provide those resources. These will leverage the capabilities of others and may include:

[43] [LINK] https://www.sba.gov/
[44] [PDF] http://nvlpubs.nist.gov/nistpubs/ir/2016/NIST.IR.7621r1.pdf
[45] [LINK] https://staysafeonline.org/

- Self-help educational material such as instructional presentations, pamphlets, guidance, and videos;
- Awareness of the importance and impact of cybersecurity and resources that help address cybersecurity through events and expanded use of social media channels; and
- "Starter" Framework Profiles specific to SMBs, tailored toward risk management of business processes important to small business owners and reducing effort necessary to customize Framework.