NIST Roadmap for Improving Critical Infrastructure Cybersecurity Version 1.1 April 25, 2019

1. Introduction

This companion Roadmap to the *Framework for Improving Critical Infrastructure Cybersecurity* (Cybersecurity Framework or the Framework) describes 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 Roadmap reflects revisions to the original planning document released in February 2014¹ when Version 1.0 of the Framework was released, and contains updates corresponding with Framework Version 1.1 issued in April 2018.

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 Analysis⁵ on March 24, 2016;
- Hosted a Workshop⁶ on April 6-7, 2016, in Gaithersburg, Maryland;
- Published a proposed Draft Version 1.17 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

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

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

- analysis⁹ on May 15, 2017;
- Hosted a workshop on May 16-17, 2017, to further discuss the proposed draft revisions¹⁰ and published a summary of the workshop;¹¹
- Published for public comment a proposed Draft 2 of Version 1.1. of the Cybersecurity Framework on December 5, 2017;
- Published Cybersecurity Framework Version 1.1 on April 16, 2018; and
- Hosted the NIST Cybersecurity Risk Management conference in November 7-9, 2018.

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

Considering the 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 Cybersecurity Framework Version 1.1. These focus areas may be included 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;
- Internet of Things;
- Measuring Cybersecurity;
- Referencing Techniques;
- Secure Software Development;
- 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 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.

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

A continued focus on cybersecurity 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 and Access 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. Focus Areas

NIST has identified and targeted several focus areas for continued coordination and collaboration of cybersecurity guidelines and principles:

- 4.1. Federal Agency Cybersecurity Alignment;
- 4.2. International Aspects, Impacts, and Alignment; and
- 4.3. Small Business Awareness and Resources.

4.1. 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)¹² 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) Circular A-130,¹³ 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 Infrastructure¹⁴ requires each

¹² [LINK] https://www.congress.gov/bill/113th-congress/senate-bill/2521/text

¹³ [LINK] https://www.whitehouse.gov/sites/whitehouse.gov/files/omb/circulars/A130/a130revised.pdf

¹⁴ [LINK] https://www.whitehouse.gov/the-press-office/2017/05/11/presidential-executive-order-strengthening-cybersecurity-federal

federal agency to use the Cybersecurity Framework to manage cybersecurity risk; and

• The May 2017 OMB Memorandum 17-25,15 which provides EO 13800 reporting guidance to federal agencies.

While the Framework was developed with private 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.

NIST issued draft report NISTIR 8170, *Approaches to Using the Cybersecurity Framework within Federal Agencies*¹⁶, 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 to provide additional guidance on how to use the Risk Management Framework and the Cybersecurity Framework to improve agency management of cybersecurity and privacy risks. NIST sees the RMF and the CSF as complementary risk management approaches that can be used alongside each other. NIST also understands that it sometimes can be confusing to users and those exploring whether or how to put these frameworks to good use. That includes information about how organizations can put both frameworks to optimum use.

The larger suite of NIST security and privacy risk management publications also will be updated in consideration of general Cybersecurity Framework value.

Anticipated future NIST activities include:

- Identify additional areas of alignment between the Cybersecurity Framework and existing and emerging standards, guidelines, frameworks, and other programs;
- Finalize and publish NISTIR 8170, Approaches to Using the Cybersecurity Framework within Federal Agencies; and
- Identify and share lessons learned from use of the Framework by federal departments and agencies.

4.2. 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

¹⁵ [LINK] https://www.whitehouse.gov/sites/whitehouse.gov/files/omb/memoranda/2017/M-17-25.pdf

¹⁶ [PDF] http://csrc.nist.gov/publications/drafts/nistir-8170/nistir8170-draft.pdf

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 requirements 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 practices, 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 2014¹⁷ 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 regional and bi-lateral dialogs with governments of other nations and with standards developing organizations.

NIST increasingly engages actively with the international community in an effort to increase utilization of the Cybersecurity Framework and further alignment with international standards. NIST has participated in many government-to-government interactions regarding the Framework. These efforts have resulted in or supported some countries and international entities using the Framework or considering adopting a similar approach towards cybersecurity. Examples of activities and resources include:

- The Information-technology Promotion Agency (IPA) translation of the Framework to Japanese;
- The Italian National Framework for Cyber Security¹⁸ using the Framework as a foundation;
- The Israeli adaptation and translation of the Framework to Hebrew and its use as the basis for the Israeli incorporation into the Cyber Defense Methodology;
- 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;
- The Ontario Energy Board (OEB) use of the Framework to measure cybersecurity efforts of non-bulk electric organizations¹⁹;
- The Uruguay government's Cybersecurity Framework Version 4.0, which is based on the Framework; and

¹⁷ [LINK] https://www.congress.gov/bill/113th-congress/senate-bill/1353/text

^{18 [}LINK] http://www.cybersecurityframework.it

¹⁹ [PDF] https://www.oeb.ca/sites/default/files/OEB-CS-Framework-WhitePaper-20170601.pdf

Translations of the Framework into Spanish, Arabic, and Portuguese as well as earlier adaptations or translations (noted above) into Hebrew and Japanese²⁰

NIST is also actively engaged with the International Organization for Standardization (ISO) and International Electrotechnical Commission (IEC) to map existing international standards to the Framework. This work culminated in the publication of ISO/IEC Technical Report 27103 summarizing that work. NIST also continues to engage with international partners within ISO and IEC aimed at producing a technical specification on developing cybersecurity frameworks that leverages the Framework content and approach. 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;
- Encourage and support, where appropriate, industry engagements internationally; and
- Work with standards developing organizations, industry, and others to ensure the Framework's alignment and compatibility with existing and developing standards and practices.

4.3. Small Business Awareness and Resources

The vulnerability of any one small business may not seem significant to many other than to the company's owner and employees. However, there are over 30 million U.S. small businesses and nearly half of the U.S. private sector working population is employed in a small business.²¹ 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. They are crucial elements of the nation's supply chain, to multiple sectors of the U.S. economy, and to national security. Therefore, a vulnerability common to many - or even just a few, key - small businesses could pose a threat to the Nation's economic base or even its national security. 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 help address this need, NIST published NISTIR 7621 Revision 1 - Small Business Information Security - The Fundamentals.²² This report provides an overview of information security, and guidance to help small businesses manage risk to their information, systems, and networks. NIST is also collaborating with federal agency partners and other collaborators to increase small- and medium-sized businesses awareness of cybersecurity, and the Cybersecurity Framework, through webinars and other outreach mechanisms.

²⁰ [PDF]

https://www.nist.gov/sites/default/files/documents/2018/12/10/frameworkesmellrev 20181102mn clean.pdf

²¹ [PDF] https://www.sba.gov/sites/default/files/advocacy/2018-Small-Business-Profiles-US.pdf

²² [PDF] http://nvlpubs.nist.gov/nistpubs/ir/2016/NIST.IR.7621r1.pdf

In March 2019, NIST launched the Small Business Cybersecurity Corner, a web site that provides small businesses with easy access to consistent, clear, concise, and actionable information – from public and private sector organizations - that helps them to better manage cybersecurity risk. This site is one activity that meets the goals of the NIST Small Business Cybersecurity Act, which became law in August 2018.

To amplify small business awareness of cybersecurity, and of the Cybersecurity Framework, NIST plans to:

- Inventory and catalog cybersecurity resources of relevance and value to small businesses through the NIST Small Business Cybersecurity Corner;
- Develop small business CSF starter profiles tailored toward risk management of business processes important to small business owners; and
- Further promote awareness of the importance and impact of cybersecurity and resources that help address cybersecurity through public events and expanded use of social media.

5. Areas for Development, Alignment, and Collaboration

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

- 5.1. Confidence Mechanisms
- 5.2. Cyber-Attack Lifecycle
- 5.3. Cybersecurity Workforce
- 5.4. Cyber Supply Chain Risk Management
- 5.5. Governance and Enterprise Risk Management
- 5.6. Identity and Access Management
- 5.7. Internet of Things
- 5.8. Measuring Cybersecurity
- 5.9. Privacy Engineering
- 5.10. Referencing Techniques
- 5.11 Secure Software Development

While this list is not intended to be exhaustive, these are important topics identified by stakeholders that should inform future versions of the Cybersecurity 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.

5.1. Confidence Mechanisms

The output of confidence mechanisms (including traditional conformity assessment activities) 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, drive improvement, 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) has built 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) has developed 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 (e.g., conformity assessment efforts) 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.

5.2. 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 actor 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. In version 1.1 of the Framework, a new subcategory was added to address vulnerability disclosure lifecycle.

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*, ²³ 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 ISO/IEC 29147²⁴ and ISO/IEC 30111²⁵ 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.

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;
- Collaborate with private and public sector efforts to further establish and streamline CVD approaches and methodologies;

²³ [PDF] http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-150.pdf

²⁴ [LINK] <u>https://www.iso.org/standard/45170.html</u>

²⁵ [LINK] https://www.iso.org/standard/53231.html

- 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);
- Collaborate with industry stakeholders in the development of threat-based Cybersecurity Framework profiles (e.g. DDoS, and Botnet profiles);
- 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.

5.3. Cybersecurity Workforce

A skilled cybersecurity workforce is needed to meet the Nation's cybersecurity needs. There is a well-documented shortage of cybersecurity practitioners.²⁶ As threats, vulnerabilities, and technology environments evolve, the cybersecurity workforce must adapt to design, develop, implement, maintain and continuously improve cybersecurity practices within critical infrastructure and across the broader economy environments.

Various efforts, including the NIST-led 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).²⁷ 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 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

 $^{^{26}}$ [LINK] <u>http://cyberseek.org/</u> - Interactive jobs heat map and career pathways portal 27 [LINK] <u>https://doi.org/10.6028/NIST.SP.800-181</u>

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 public working groups.²⁸ These activities may include further definition of how NICE Framework work roles, tasks, and KSAs help to fulfill Cybersecurity Framework outcomes.

- 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.

5.4. 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. C-SCRM, especially product and service integrity, is an emerging discipline characterized by diverse perspectives, disparate bodies of knowledge, and fragmented standards and best practices.

Increasing adoption of C-SCRM 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 cyber supply chain community has advanced both technical guidance and related tools to support better management of supply chain risks.

²⁸ [LINK] https://www.nist.gov/itl/applied-cybersecurity/nice/about/working-group

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*, ²⁹ which provides guidance on identifying, assessing, and mitigating supply chain risks at all organizational levels. The April 2018 release of NIST IR 8179, *Criticality Analysis Process Model*: ³⁰ was engineered to help organizations prioritize programs, systems and components.

C-SCRM concepts have been integrated throughout several key NIST cybersecurity risk management resources including NIST SP 800-37, Revision 2, Risk Management Framework for Information Systems and Organizations³¹ and draft NIST SP 800-53 Rev. 5 - Security and Privacy Controls for Information Systems and Organizations³² controls. Additionally, C-SCRM was integrated throughout the April 2018 release of version 1.1 of the Cybersecurity Framework. This integration included an expanded section 3.3, *Communicating Cybersecurity Requirements with Stakeholders*, to help users better understand C-SCRM; a new section 3.4, Buying Decisions, which highlights use of the Framework in understanding risk associated with commercial off-the-shelf products and services; additional C-SCRM criteria in the Implementation Tiers; and a new C-SCRM category and multiple subcategories in the Framework Core.

International standards also advanced C-SCRM and related topics with stakeholders. Of note, ISO/IEC 27036³³ was published in April 2014 to help organizations address *Information Security for Supplier Relationships*, and ISO/IEC 20243³⁴ 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, 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, and that may be considered for inclusion in future Cybersecurity Framework updates. NIST will continue to raise awareness on this topic. Future activities will engage stakeholders to:

- Encourage broad industry engagement and leadership in SCRM discussions and activities;
- Determine the key challenges to SCRM (e.g., identifying and understanding mission critical functions and their dependencies, and conducting and validating prioritization) to enable more effective Framework implementation;
- Develop Best Practice Principles guidance for C-SCRM, and continue to develop C-SCRM industry case studies;
- Develop a quantitative supplier interdependency analysis process and tool;

_

²⁹ [PDF] http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-161.pdf

³⁰ [PDF] https://nvlpubs.nist.gov/nistpubs/ir/2018/NIST.IR.8179.pdf

³¹ [PDF] https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-37r2.pdf

³² [PDF] http://csrc.nist.gov/publications/drafts/800-53/sp800-53r5-draft.pdf

^{33 [}LINK] https://www.iso.org/standard/59648.html

^{34 [}LINK] https://www.iso.org/standard/67394.html

- Develop a Web-based tool for measuring and assessing cyber and supply chain risk; and
- Evolve the NIST C-SCRM publications and Cybersecurity Framework as informed by the above activities.

5.5. 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. An important distinction must be made between an organization simply complying with existing regulations versus an informed, data-driven, risk-based approach to information security. 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.35

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 enables easy translation of how those larger enterprise risk decisions affect cybersecurity. Those with 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 Enterprise Risk Management (ERM) and governance, and the on-going focus of these topics in the larger ecosystem, Governance and ERM is 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*³⁶ and the Kogod Cybersecurity Governance Center.³⁷ 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

^{35 [}LINK] https://www.whitehouse.gov/the-press-office/2017/05/11/presidential-executive-order-strengtheningcybersecurity-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."

³⁷ [LINK] http://www.american.edu/kogod/research/cybergov/

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 1.1. 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. Version 1.1 was published in March 2019.

In the next one-to-three years NIST intends to continue and to 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;
- Align and integrate Cybersecurity Framework concepts and principles into NIST's portfolio of risk management standards and guidelines; and
- Promote and update NIST publications such as the BCEB and the Framework.

5.6. Identity and Access Management

Identity and Access 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 are aimed at bringing 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 a report that "81% of hacking-related breaches [leveraging] either stolen and/or weak passwords.³⁸"

Although the use and adoption of identity and access management 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 Special Publication 800-63, *Digital Identity Guidelines*. This guideline and extensive stakeholder feedback informed refinements in Cybersecurity Framework version 1.1 to better account for authentication, authorization, and identity proofing. More specifically, NIST renamed the Access Control category to Identity Management and Access Control (PR.AC) and added subcategories for

³⁸ [LINK] 2017 Verizon Data Breach Report Executive Summary, http://www.verizonenterprise.com/resources/reports/rp DBIR 2017 Report execsummary en xg.pdf

Authentication and Identity Proofing.

As threats and risks continue to evolve, a static approach to identity no longer suffices. Identity and access 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 developing its standards and guidance, 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 its National Cybersecurity Center of Excellence (NCCoE) 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 anticipates:

- Conducting focused research to better understand new and emerging technologies, their impact on existing standards, and the implementation of identity management solutions;
- Continuing active participation in national and international identity management standards, guidance, best practices, profiles, and frameworks to create an enhanced, interoperable suite of secure, privacy-enhancing solutions, including authentication and authorization within the Internet of Things (IoT); and
- Evolving NIST identity and access management guidelines and publications as informed by the above activities.

5.7. Internet of Things

There is no consensus amongst industry on how to define the Internet of Things (IoT). With a shared responsibility between manufacturers and consumers, the IoT ecosystem poses cybersecurity risks that extend beyond traditional data security. A single enterprise can have hundreds if not thousands of sensors, and monitoring for attacks in real time is resource-intensive. Traditional IT security systems offer very little defense against these cyber-attacks that can shut down power grids, smart traffic systems, and automobiles. The ubiquity of IoT devices poses challenges for managing the personal information they collect and helping people understand how that information is processed by a system. IoT can – intentionally or unintentionally – lead to the direct collection of sensitive personal information such as geolocation, financial account numbers, and health information. Many consumers are unaware that devices already in homes can surreptitiously record and process their information.

NIST's Cybersecurity for IoT Program [Program] supports the development and application of standards, guidelines, and related tools to improve the cybersecurity of connected devices and the environments in which they are deployed. To understand the current state of IoT and challenges faced by stakeholders, NIST has engaged with and received input from diverse stakeholders at various workshops and events. In response to the feedback received, NIST published draft NISTIR 8228³⁹, *Considerations for Managing IoT Cybersecurity and Privacy Risks* in September of 2018, which provides guidance to help

_

³⁹ [LINK] https://csrc.nist.gov/publications/detail/nistir/8228/draft

organizations address common high-level cybersecurity and privacy risks for IoT, and to introduce practical risk management considerations for IoT product selection, deployment, protection, and operation. This guidance identifies Cybersecurity Framework subcategories impacted by cybersecurity and privacy risks for protecting device security, data security and individuals' privacy. Following on that work, NIST is developing a core cybersecurity capability baseline for IoT devices that will outline those capabilities that should be found in all IoT devices while considering the aspects of IoT relevant to cybersecurity highlighted in NISTIR 8228. This subsequent work is focused at manufacturers of IoT devices but will have applications and implications throughout the product chain and ecosystem. Furthermore, NIST will continue working on projects to demonstrate secure IoT cybersecurity solutions through efforts undertaken by the NCCoE, such as the *Mitigating IoT-Based DDoS* project [Project], and Security for IoT Sensor Networks project [Project]. Feedback received and experiences gained through NIST's Cybersecurity for IoT program will inform future improvements to the Cybersecurity Framework to ensure it continues to be applicable to IoT technologies.

Anticipated future activities in IoT include:

- Publication of the *Core Cybersecurity Capabilities Baseline for IoT Devices* that continues from a discussion essay on the topic⁴⁰;
- Extension of the baseline work to address IoT challenges faced by the Federal Government and participation in key multi-stakeholder, private-sector led activities as identified in *A Road Map Towards Resilience Against Botnets*⁴¹;
- Demonstrating example solutions to IoT cybersecurity challenges with technology specific implementations working with the community of interest and industry collaborators at the NCCoE, and
- Continued interaction with stakeholders through public and private sector organizations, standards development organizations, and academia in this emerging field to present NIST's work and stay up-to-date on the challenges they face when developing or using IoT to inform the groups future work.

5.8. 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.

https://www.nist.gov/sites/default/files/documents/2019/02/01/final_core_iot_cybersecurity_capabilities_baseline_considerations.pdf

⁴⁰ [PDF]

^{41 [}PDF] https://www.commerce.gov/sites/default/files/2018-11/Botnet%20Road%20Map%20112918%20for%20posting 0.pdf

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 beginning focused work on cybersecurity measurement to align technical 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.* 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.

5.9. 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. ⁴³ Coordination between privacy and information security strategist and implementation efforts should be considered. 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

_

^{42 [}LINK] https://csrc.nist.gov/publications/detail/sp/800-55/rev-1/final

⁴³ [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.

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 Systems, 44 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.⁴⁵ In addition, NIST has integrated guidance for privacy into its existing guidance for cybersecurity risk management, including an update 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. 46/47 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.

In October 2018, NIST initiated a process to develop a Privacy Framework.⁴⁸ This voluntary framework is envisioned as an enterprise risk management tool to help organizations to better identify, assess, manage and communicate privacy risks. NIST is developing the framework in an open, collaborative process with stakeholders modeled after the Cybersecurity Framework. Additionally, in response to initial public input, NIST proposes a structure for the Privacy Framework that would enable a risk- and outcome-based approach and is aligned to the structure of the Cybersecurity Framework to reduce complexity for organizations that already use the Cybersecurity Framework.

NIST will continue to work with stakeholders in the federal privacy community, academia, and the private sector to develop additional 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 NIST risk management guidance;
- Engage with standards development organizations to advance privacy engineering standards;
- Work collaboratively with other NIST programs including Cybersecurity for IoT to advance integrated privacy and cybersecurity processes; and
- Promote the use and improvement of tools and solutions to engineer privacy protections into systems through its Privacy Engineering Collaboration Space, an

^{44 [}PDF] http://nvlpubs.nist.gov/nistpubs/ir/2017/NIST.IR.8062.pdf

⁴⁵ LINK https://www.nist.gov/itl/applied-cybersecurity/privacy-engineering

⁴⁶ [PDF] https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-37r2.pdf

⁴⁷ [PDF] https://csrc.nist.gov/csrc/media/publications/sp/800-53/rev-5/draft/documents/sp800-53r5-draft.pdf

⁴⁸ [LINK] For more information and a development schedule, visit https://www.nist.gov/privacy-framework.

online platform open to the public where practitioners can discover, share, discuss, and improve upon open source tools, solutions, and processes that support privacy engineering and risk management.⁴⁹

5.10. 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 on-line format. NISTIR draft 8204 was developed to provide guidance to potential Reference Authors on how to complete the Reference Template and submit a proposed reference for review. 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; and
- Integrate existing technology security practices to security control catalog.

5.11. Secure Software Development

As software is frequently integrated with systems to support business functions in the form of applications and services, a vulnerability in one application can become an attack vector through which a malicious actor may gain access to other applications, data or systems. A

⁴⁹ [LINK] https://www.nist.gov/itl/applied-cybersecurity/privacy-engineering/collaboration-space

^{50 [}LINK] https://csrc.nist.gov/publications/detail/nistir/8204/draft

focus on security by design throughout the software development process is paramount to application and data confidentiality, integrity, and availability. Careless or negligent software development can result in significant security vulnerabilities. As such, it is important for organizations to build security into their development processes. Code developed with security in mind may provide important beneficial results such as approaches for cost-effective risk-based mitigation for the development and software testing practices while reducing the number of product vulnerability incident responses and associated patches.

NIST plans to develop a NIST cybersecurity white paper for Secure Software Development which highlights particularly important practices that should apply to any secure software development approach; any software development lifecycle (SDLC) model, standard, or methodology; any programming language or development environment; and any operating environment. This flexibility will support agile and DevOps methodologies. NIST plans to continue its Secure Software Development research and participate in guidance development activities such as:

- Raising awareness of secure software development;
- Encouraging the academic and training sectors through the National Initiative for Cybersecurity Education (NICE) to fully integrate secure coding practices into computer science and related programs⁵¹;
- Supporting private and public sector efforts to further establish and streamline secure software development approaches and methodologies;
- Developing NIST Special Publications on secure software development techniques and best practices;
- Demonstrating these practices with technology specific implementations working with the community of interest and industry collaborators at the National Cybersecurity Center of Excellence; and
- Informing improvements and refinements to the Cybersecurity Framework related to secure software development.

 $^{^{51}\}left[PDF\right] \underline{\ https://www.commerce.gov/sites/default/files/media/files/2018/eo_13800_botnet_report_-_finalv2.pdf$