Before the Department of Commerce
National Institute of Standards and Technology
Washington, D.C.

Request for Comments

Framework for Improving Critical
Infrastructure Cybersecurity
Version 1.1 (Draft)

COMMENTS OF CTIA

Thomas K. Sawanobori
Senior Vice President and Chief Technology Officer

John A. Marinho
Vice President, Technology and Cybersecurity

CTIA
1400 16th Street, NW, Suite 600
Washington, DC 20036
202-736-3200
www.ctia.org

April 10, 2017

TABLE OF CONTENTS

I. Executive Summary

CTIA[1] welcomes the opportunity to comment on revisions[2] to the National Institute of Standards and Technology's ("NIST's") *Framework for Improving Critical Infrastructure Cybersecurity* (*"Framework"*).[3] Since version 1.0 was released in 2014, the private sector has been using it and other resources. CTIA applauds NIST's ability to convene private expertise to build consensus. This has been central to effective, federal cybersecurity policy, which has been non-regulatory and driven by the private sector.[4]

We have seen great progress, but challenges persist. Evolving threats come from nation-states, criminal syndicates, hacktivists, and terrorists. Users, including government, lag in cyber hygiene. Recently, regulators have considered obligations that could lead to fragmentation. Measurement of cybersecurity risk management is nascent, complex, and controversial; it is not amenable to a single approach.

The information and communications technology ("ICT") ecosystem is building on cyber successes, including the *Framework*. CTIA focuses its comments on several key areas:

- NIST should reiterate the voluntary, flexible nature of its cybersecurity guidance.
- NIST should take a different approach to measurements and metrics, returning to its emphasis on self-assessments that are flexible and tailored to organizations' goals.
- NIST should emphasize the complexity of supply chain security.
- NIST should support evolving methods of authentication.
- NIST should refine its discussion of privacy and civil liberties.
- The *Framework* should be used to improve federal government IT security.

Cybersecurity policy is at an inflection point. The government must stay the course, building on successful public-private partnerships that emphasize voluntary, flexible tools.

---

[1] CTIA® (www.ctia.org) represents the U.S. wireless communications industry and the companies throughout the mobile ecosystem that enable Americans to lead a 21st century connected life. The association's members include wireless carriers, device manufacturers, suppliers as well as apps and content companies. CTIA vigorously advocates at all levels of government for policies that foster continued wireless innovation and investment. The association also coordinates the industry's voluntary best practices, hosts educational events that promote the wireless industry and co-produces the industry's leading wireless tradeshow. CTIA was founded in 1984 and is based in Washington, D.C.

[2] NIST, *Framework for Improving Critical Infrastructure Cybersecurity, Draft Version 1.1 with Markup* at 1 (proposed Jan. 10, 2017) ("*Framework Draft Version 1.1*"), https://www.nist.gov/file/344211.

[3] NIST, *Framework for Improving Critical Infrastructure Cybersecurity, Version 1.0* at 1 (Feb. 12, 2014) ("*Cybersecurity Framework Version 1.0*"), http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214.pdf.

[4] Congress recognized this, codifying NIST's work in the Cybersecurity Enhancements Act of 2014, Pub. L. No. 113-274, 128 Stat 2971 (2014).

II. The Communications Sector Has Been Using NIST's *Framework*, with Other Tools, To Address Cybersecurity as It Builds New 5G Networks.

NIST's *Framework* is a voluntary, risk-based strategy that is being widely adapted. NIST eschewed a one-size-fits-all approach in favor of voluntary risk management because "[o]rganizations will continue to have unique risks—different threats, different vulnerabilities, different risk tolerances—and how they implement the practices in the framework will vary."[5] The *Framework* has been successful because of this flexibility, and because it resulted from public-private collaboration, as instructed by Executive Order 13636.[6] The *Framework* helps companies address risk in a cost-effective way. It "jumpstarted a vital conversation between critical infrastructure sectors and their stakeholders,"[7] and provided a common taxonomy that "enable[s] security leaders to effectively communicate" about risks and practices.[8] It has become a baseline for sector and international efforts.[9]

The Communications Sector incorporates the *Framework* into efforts on cybersecurity. The Federal Communications Commission's ("FCC's") Communications Security, Reliability and Interoperability Council ("CSRIC") IV, Working Group 4 published its *Cybersecurity Risk Management and Best Practices*[10] in 2015 to help broadcast, cable, satellite, wireless, and wireline companies adapt the voluntary *Framework*. CSRIC V, Working Group 6 leveraged the *Framework* to develop a voluntary Security-by-Design report in 2016.[11]

All contributors to the Internet and wireless ecosystem share the mission of improving security. Operating System ("OS") providers work with application developers, and many OS application stores do a good job screening applications.[12] Network operators monitor traffic and combat threats.[13] Over-the-top applications add security. Industry is refining threat indicators, improving network and communications infrastructure, and addressing remediation.

---

[5] *Cybersecurity Framework Version 1.0* at 2.
[6] Exec. Order No. 13636, 78 Fed. Reg. 11739, *Improving Critical Infrastructure Cybersecurity* (Feb. 12, 2013).
[7] Press Release, NIST, *NIST Releases Cybersecurity Framework Version 1.0* (Feb. 12, 2014), http://www.nist.gov/itl/csd/launch-cybersecurity-framework-021214.cfm.
[8] PricewaterhouseCoopers, *Why you should adopt the NIST Cybersecurity Framework* at 4 (2014), https://www.pwc.com/us/en/increasing-it-effectiveness/publications/asssets/adopt-the-nist.pdf.
[9] *See, e.g.*, United Nations' International Maritime Organization, *Interim Guidelines on Maritime Cyber Risk*, http://www.imo.org/en/MediaCentre/HotTopics/piracy/Pages/default.aspx; Conference of State Bank Supervisors, *Cyber 101: A Resource Guide for Bank Executives*, http://www.csbs.org/news/press-releases/pr2014/Pages/pr-121714.aspx; Health & Human Services, *HIPAA Security Rule Crosswalk to NIST Cybersecurity Framework*, http://www.hhs.gov/sites/default/files/NIST%20CSF%20to%20HIPAA%20Security%20Rule%20Crosswalk%2002-22-2016%20Final.pdf.
[10] *Cybersecurity Risk Management and Best Practices*, CSRIC IV WG 4, Final Report (March 2015), https://transition.fcc.gov/pshs/advisory/csric4/CSRIC_IV_WG4_Final_Report_031815.pdf.
[11] *Secure Hardware and Software: Security-by-Design*, CSRIC V WG 6, Final Report (Sept. 2016), https://transition.fcc.gov/bureaus/pshs/advisory/csric5/WG6_Final_091416.docx.
[12] Google checks more than 6 billion apps and scans 400 million devices each day. Google, *Android Security 2015 Annual Report* (Apr. 2016), https://security.googleblog.com/2016/04/android-security-2015-annual-report.html.
[13] AT&T's experts see more than 30 billion vulnerability scans and 400 million spam messages cross its network every day; and 5 billion vulnerability scans and 200,000 malware events targeted at its network every day. Chris Boyer, *How the Public Safety Bureau Paper Gets Cybersecurity Wrong*, AT&T Public Policy Blog (Jan. 25, 2017), https://www.attpublicpolicy.com/cybersecurity/how-the-public-safety-bureaupaper-gets-cybersecurity-wrong/.

Additionally, global ICT companies undertake research.[14] CTIA releases White Papers[15] and research that yield tools for device management, anti-malware, browsing protection, app reputation checking, call/short message service blocking and scanning, and firewalls. The wireless and Internet ecosystems use a multilayered approach, with Internet service providers ("ISPs"), network operators, OS developers, manufacturers, and application developers contributing. This is not only effective, it is vital. Communications infrastructure is a complex "system of systems." In mobile, for example, there is an upstream segment relying on spectrum and backhaul; a transmit segment across the network; and a downstream segment relying on mobile devices.

The global ICT market relies on flexible, voluntary consensus standards, because they reflect the global market. Many groups help inform the Communications Sector:

- The **3rd Generation Partnership Project ("3GPP")** unites seven global telecom standards organizations.[16] It developed encryption standards and worked with Groupe Speciale Mobile Association ("GSMA") to develop a certification program for 3GPP's Security Assurance Methodology.
- The **Internet Engineering Task Force ("IETF")** is a community of network designers, operators, vendors, and researchers concerned with Internet operations and evolution. IETF sets international security-related standards.[17]
- The **Alliance for Telecommunications Industry Solutions ("ATIS")** fosters communication between carriers, customers, and manufacturers. The ATIS Network Performance, Reliability, and Quality of Service Committee recommends standards and publishes technical reports related to security of communications networks.[18] ATIS was part of the CSRIC IV working group that mapped the *Framework*.
- The **Institute of Electrical and Electronics Engineers ("IEEE")** launched a cybersecurity initiative to "(1) provide the go-to online presence for security and privacy

---

[14] *See Verizon 2016 Data Breach Investigations Report* (2016), http://www.verizonenterprise.com/verizon-insights-lab/dbir/2016/; *Cisco 2017 Annual Security Report* (2017), http://b2me.cisco.com/en-us-annual-cybersecurity-report-2017?keycode1=001464153; *Neustar Annual DDoS Attacks and Protection Report* (2015), https://ns-cdn.neustar.biz/creative_services/biz/neustar/www/resources/whitepapers/it-security/ddos/2015-us-ddos-report.pdf.

[15] *See, e.g.*, CTIA, *Today's Mobile Cybersecurity: Information Sharing* (September 2014) ("CTIA White Paper on Information *Sharing*"), http://www.ctia.org/docs/default-source/default-document-library/ctia_informationsharing.pdf?sfvrsn=2; *Mobile Cybersecurity and the Internet of Things: Empowering M2M Communication* (May 2014) ("*CTIA White Paper on IoT*"), http://www.ctia.org/docs/default-source/default-document-library/ctia-iot-white-paper.pdf; *Today's Mobile Cybersecurity: Industry Megatrends & Consumers* (May 2013) http://www.ctia.org/docs/default-source/default-document-library/today-s-mobile-cybersecurity-industry-megatrends-amp-consumers.pdf?sfvrsn=0; *Today's Mobile Cybersecurity: Blueprint for the Future* (February 2013), http://www.ctia.org/docs/default-source/default-document-library/cybersecurity_white_paper.pdf?sfvrsn=2; *Today's Mobile Cybersecurity: Protected, Secured and Unified*, CTIA (October 2012) http://files.ctia.org/pdf/CTIA_TodaysMobileCybersecurity.pdf.

[16] 3GPP's seven organizational partners are The Association of Radio Industries and Business, Japan; The Alliance for Telecommunications Industry Solutions, USA; China Communications Standards Association; The European Telecommunications Standards Institute; Telecommunications Standards Development Society, India; Telecommunications Technology Association, Korea; and Telecommunication Technology Committee, Japan.

[17] *See* IETF, *About the IETF*, https://www.ietf.org/about/.

[18] *See* ATIS, *PRQC Mission*, http://www.atis.org/0010/mission.asp.

(S&P) professionals; (2) improve the understanding of cybersecurity by students and educators; and (3) improve S&P designs and implementations by professionals."[19]

- The **European Telecommunications Standards Institute ("ETSI")** produces global communications standards.[20] Because "security is . . . a key to the modern connected world and a crucial factor in inspiring the consumer confidence," ETSI has done a variety of work. Its cyber security committee produced a report encouraging "secure by default" platform security and on countermeasures.[21]
- **GSMA's Fraud and Security Group ("FASG")** aims to "drive the industry's management of fraud and security matters related to [mobile] technology, networks and services, with the objective to maintain or increase the protection of mobile operator technology and infrastructure and customer identity, security and privacy."[22]

The Communications Sector shares information.[23] Efforts are not always public-facing, but they are critical. Cybersecurity is supported by public-private forums like the National Cybersecurity and Communications Integration Center ("NCCIC"), the Communications Information Sharing and Analysis Center ("Comm-ISAC"), the Communications Sector Coordination Council ("CSCC"), and the National Security Telecommunications Advisory Committee ("NSTAC").[24] ISACs and Information Sharing and Analysis Organizations ("ISAOs")[25] help prevent, respond, and recover. The Cybersecurity Information Sharing Act of 2015 ("CISA") also facilitates information sharing.[26] This contributes to relatively low malware rates in the United States, as compared with much of the world.[27]

The ICT industry is building security into 5G, which will foster growth in the Internet of Things ("IoT"). As with 2G, 3G, and 4G, the ecosystem is working on 5G security and cutting edge solutions. Industry drives innovation in vulnerability scans, advanced technology standards, enhancements to security policies and risk management, and monitoring specific cyber threats.[28] It designs with security in mind, incorporating the latest security into underlying hardware and infrastructure. Chip manufacturers, which provide chips for millions of IoT

---

[19] *See* IEEE, IEEE Cyber Security About Page, http://cybersecurity.ieee.org/about/.
[20] ETSI, *About ETSI*, http://www.etsi.org/about.
[21] ETSI, *Annual Report* at 12 (2016), http://www.etsi.org/images/files/AnnualReports/etsi-annual-report-april-2016.pdf.
[22] GSMA, Working Groups, *Fraud and Security Group*, http://www.gsma.com/aboutus/leadership/committees-and-groups/working-groups/fraud-security-group.
[23] McAfee, *McAfee Labs Threats Report* at 2 (March 2016), http://www.mcafee.com/us/resources/ reports/rp-quarterly-threats-mar-2016.pdf ("Intel Security interviewed almost 500 security professionals … 97% of those who share cyber threat intelligence see value in it.").
[24] *See CTIA White Paper on Information Sharing* at 13.
[25] Exec. Order No. 13691, 80 Fed. Reg., 9,349, *Promoting Private Sector Cybersecurity Information Sharing*, § 1 (Feb. 13, 2015), directs DHS to encourage ISAOs, because "[o]rganizations engaged in the sharing of information related to cybersecurity risks and incidents play an invaluable role in the collective cybersecurity" of the nation.
[26] Pub. L. 114-113, 6 U.S.C. § 1501.
[27] *See* Verizon, *2015 Data Breach Investigations Report* at 19-20 (2015), http://www.verizonenterprise.com/resources/reports/rp_data-breach-investigation-report_2015_en_xg.pdf ("An average of 0.03% of smartphones per week—out of tens of millions of mobile devices on the Verizon network—were infected with 'higher-grade' malicious code. This is an even tinier fraction than the overall 0.68% infection rate reported.").
[28] *See CTIA White Paper on IoT* at 15 ("The industry manages M2M cybersecurity through 24/7 monitoring and threat assessment; design and testing; encryption; vulnerability management; and policy/data sharing.").

devices, are hard at work to deliver a roadmap of integrated hardware and software products to meet IoT security demands. This is critical, as the private sector can innovate faster than any agency.

III. Because the *Framework* Has Become a Global Baseline, NIST Should Make Few Changes and Should Reiterate Its Voluntary Nature for the Private Sector.

CTIA is pleased that NIST is not proposing major changes or migrating control of the *Framework*. The *Framework* already "comprises leading practices from various standards bodies that have proved to be successful when implemented."[29] NIST need not reinvent the wheel; indeed, major changes can disrupt ongoing work. Many efforts—global and domestic—are built on the *Framework*. NIST lists over 50 documents and tools that incorporate or help to implement the *Framework*.[30] The *Framework* is the baseline for international frameworks.[31] Major changes would threaten global adoption. Already, 30% of companies use the *Framework*, and that number is expected to grow to 50% by 2020.[32] Congress has been looking to build on the *Framework*. For example, a recently introduced bill would direct NIST to create guidance based on the *Framework* for small businesses facing cybersecurity risks.[33] NIST should eschew changes and focus instead on helping the private sector with use cases, profiles, and other guidance.

It is also vital that NIST continue to champion the *Framework*'s voluntary nature. The *Framework* is meant to be a tool for all organizations, "regardless of size, degree of cybersecurity risk, or cybersecurity sophistication."[34] It was created pursuant to Executive Order 13636, which focused on critical infrastructure and mandated that it "incorporate **voluntary** consensus standards and industry best practices" and "be consistent with **voluntary** international standards when such international standards will advance the objectives of this order."[35] Congress has reiterated the importance of its voluntary nature. For example, the Cybersecurity Enhancement Act of 2014 "calls on NIST to facilitate and support the development of **voluntary**, industry-led cybersecurity standards and best practices for critical infrastructure,"[36] and the recently introduced MAIN STREET Cybersecurity Act of 2017 makes clear that the small business resources that NIST would disseminate under the Act, which would be based on

---

[29] PricewaterhouseCoopers, *Why you should adopt the NIST Cybersecurity Framework* at 1.
[30] *See, e.g.*, NIST, *Cybersecurity Framework – Industry Resources* (Feb. 11, 2015), https://www.nist.gov/cyberframework/industry-resources.
[31] NIST's *2016 Cybersecurity Framework Workshop Summary* noted "multiple international organizations that have implemented the Framework" and committed to international outreach with the "optimal outcome of these interactions will be national level endorsement or adaptation of Framework for use within a given nation." NIST, *Cybersecurity Framework Feedback: What We Heard and Next Steps* at 6, 8 (June 9, 2016) ("*NIST Cybersecurity Framework Feedback*"), https://www.nist.gov/sites/default/files/documents/cyberframework/Workshop-Summary-2016.pdf .
[32] Gary Stoller, *Few adopt NIST cybersecurity guidelines, but that could change*, ThirdCertainty (Apr. 11, 2016), http://thirdcertainty.com/featured-story/few-adopt-nist-cybersecurity-guidelines-but-that-could-change/.
[33] MAIN STREET Cybersecurity Act of 2017, 115th Cong. 1 (introduced March 29, 2017).
[34] *Cybersecurity Framework Version 1.0* at 1.
[35] Exec. Order No. 13636 § 7 (emphasis added).
[36] NIST, *Cybersecurity Framework FAQs Framework Basics* (Sept. 29, 2015) (emphasis added) (referencing the Cybersecurity Enhancement Act of 2014, 15 U.S.C. § 272(c)(15)), https://www.nist.gov/cyberframework/cybersecurity-framework-faqs-framework-basics.

the *Framework*, "shall be considered **voluntary**."[37] Indeed, Senator Thune (R-SD) has on multiple occasions reiterated the critical importance of cyber policy being "truly **voluntary** and industry-led."[38] NIST understands the value of maintaining the *Framework* as a voluntary tool:

> NIST's partnership with industry to develop, maintain, and implement **voluntary** consensus standards related to cybersecurity best ensures the interoperability, security, and resiliency of the global infrastructure needed to make us all more secure. It also allows this infrastructure to evolve in a way that embraces both security and innovation – allowing a market to flourish to create new types of secure products for the benefit of all Americans.[39]

NIST highlights the voluntary nature of the *Framework,*[40] and describes its "future Framework role" in voluntary terms.[41] With the Executive Order's mandate, Congress's clear preference, and NIST's own view of the importance of the *Framework*'s voluntary nature, NIST should make clear with its revisions that it continues to be entirely voluntary for the private sector.

IV. Self-Assessments Must Be Voluntary, Flexible, and Reflect Organizations' Goals.

NIST has been discussing work on "self-assessments" for cybersecurity risk management for a while. In its June 9, 2016 report on the *Cybersecurity Framework Workshop Summary*, for example, NIST indicated it was considering refinements to the *Framework* and that it "ha[d] also begun authorship of self-assessment criteria to support organizational understanding of cybersecurity risk management business practices."[42] NIST referred to the Cybersecurity Excellence Builder, which it said "will provide detailed criteria for an organization to assess its cybersecurity risk management process. It will be based on Framework and key concepts from the Baldrige Performance Excellence Program." Given the ongoing work at NIST and elsewhere on this emerging challenge, it is surprising that measurement was added to the *Framework* in the

---

[37] MAIN STREET Cybersecurity Act of 2017, 115th Cong. 1, § 3(c)(5) (emphasis added).
[38] *The Partnership Between NIST and the Private Sector: Improving Cybersecurity*, Hearing Before the Senate Committee on Commerce, Science, and Transportation, 113th Cong. 1 (July 25, 2013) (Minority Statement, Sen. John R. Thune) (emphasis added), http://www.commerce.senate.gov/public/index.cfm/hearings?Id=481F9135-40EA-4C0C-8DB3-055E4A0C7E51&Statement_id=87077572-E660-4839-9E8D-C22004F35FB9; *see also* Building a More Secure Cyber Future: Examining Private Sector Experience with the NIST Framework, Hearing Before the Senate Committee on Commerce, Science and Transportation, 114th Cong. 1 (Feb. 4, 2015) (Majority Statement, Chairman John Thune), http://www.commerce.senate.gov/public/index.cfm/hearings?Id=eb8d0d69-bf71-4052-9675-ad6d4c507782&Statement_id=FE307132-6121-458C-93B1-EC139B22B6BC ("Our Committee's bill ensures the continuation of a voluntary and industry-led process for identifying cybersecurity standards and best practices for critical infrastructure – codifying elements of the successful process that NIST undertook to create its Cybersecurity Framework, and ensuring NIST's continued involvement in this public-private collaboration.").
[39] *Confronting the Challenge of Cybersecurity*, Hearing Before the Senate Committee on Commerce, Science and Transportation, 114th Cong. 1, at 5 (Sept. 3, 2015) (testimony of Kevin Stine, Computer Security Division, Information Technology Laboratory, NIST) ("Stine Testimony") (emphasis added), http://www.commerce.senate.gov/public/?a=Files.Serve&File_id=629B3130-C0D3-44AF-ADCE-88237096A14C.
[40] NIST, *Cybersecurity Framework FAQs Framework Basics* ("The Framework is voluntary guidance, based on existing standards, guidelines, and practices, for critical infrastructure organizations to better manage and reduce cybersecurity risk.").
[41] *Id.* ("NIST's future Framework role is reinforced by the Cybersecurity Enhancement Act of 2014 (Public Law 113-274), which calls on NIST to facilitate and support the development of voluntary, industry-led cybersecurity standards and best practices for critical infrastructure.").
[42] *NIST Cybersecurity Framework Feedback* at 8.

manner reflected in the draft version 1.1. CTIA offers some suggestions to streamline section 4.0, clarify expectations, and refocus on "self-assessments" for voluntary, tailored, and internal use.

A. Cybersecurity self-assessment is important for an organization to understand its risk management program's effectiveness.

CTIA agrees that measuring the effectiveness of a cybersecurity program can help organizations understand and improve their ability to manage risks. Even though there is no uniform approach, historically organizations have chosen process-based measurement. When an organization does measure the effectiveness of its cybersecurity program, CTIA generally agrees that quantitative measures are more informative than qualitative measurements.[43] Indeed, though it can be complex, assessing risk management within organizations is not a novel idea. Prudent organizations understand the value of measurements and metrics, and use varied approaches.

There is no one-size-fits-all solution to self-assessments, just as there is no single solution for cybersecurity in general.[44] Individual organizations—even within the same industry—will choose different goals and tools. Key Performance Indicators (KPI) will vary, as will Key Risk Indicators (KRI)—assuming organizations use that terminology. The *Framework* already recognizes that a one-size-fits-all approach does not work for specifying cyber risk management processes in general. The *Framework* is flexible, including informative references from different process standards, which serve to help guide organizations in the development of *Framework*-consistent risk management procedures that are most applicable to their specific requirements. NIST should follow this flexible approach with version 1.1. Because NIST is supposed to rely on voluntary consensus standards, the lack of agreement about the best approach to metrics or assessment should give NIST pause before it acts. In the absence of consensus, rather than promoting a particular approach, NIST should guide organizations to various helpful practices, but make clear that there is no agreement on best approach.

B. NIST should explicitly reference the complexities of measurement, emphasizing flexibility and tailoring.

CTIA has concerns about the way NIST incorporated the concept of self-assessments into the *Framework*. CTIA urges NIST to reconsider its approach, and specifically to (1) add clarity to the notoriously complex area of cybersecurity measures and metrics, and (2) emphasize flexible voluntary use and tailoring to organizations' goals.

---

[43] See D. Hubbard, *How to Measure Anything in Cybersecurity Risk* (2016). According to Hubbard, various qualitative approaches, which may be superficially appealing, can lead to flawed decision making. This means that various forms of risk matrices are flawed. He proposes that the Key Performance Indicator for cybersecurity risk management should be "risk tolerance exceedance." According to Hubbard, loss exceedance curves should be the medium for discussing and visualizing risks. The book proposes different approaches, including an Operation Security Metrics Maturity Model. Suggested benefits of this approach are that (i) it scales down and up and (ii) will not require an investment in big data analytics. NIST should consider this approach.

[44] Department of Defense, Defense Science Board, *Report, Task Force on Cyber Deterrence* at 9 (Feb. 2017), https://insidecybersecurity.com/sites/insidecybersecurity.com/files/documents/mar2017/cs2017_0078.pdf. Cybersecurity must be tailored to assessed threats. This is why, for example, the DoD calls for tailored approaches, recognizing that "for U.S. cyber deterrence (as with deterrence more broadly), one size will not fit all." Planning must be "tailored" and "should consider the 'most likely' types of attacks." *Id.*

First, NIST must clarify its discussion, referencing the complexities, as well and the ongoing efforts, in this area. Version 1.0 is a model of simplicity. This has allowed it to become a critical baseline for cybersecurity in this country and across the globe. Unfortunately, the discussion of measures and metrics in version 1.1 strays from this simplicity. It is verbose and confusing. As an expert observed in the context of cybersecurity risk management, there is substantial uncertainty and imprecision about the "concept of measurement" in cybersecurity.[45] Rather than serving to elucidate, NIST's effort adds to the uncertainty and imprecision.

NIST's difficulty in writing this section clearly derives from the inherent complexity of cybersecurity measurement and assessment. This complexity has vexed researchers, industry, and government alike. As DHS described, "[d]efining effective metrics for information security (and for trustworthiness more generally) has proven very difficult… general community agreement on meaningful metrics has been hard to achieve, partly because of the rapid evolution of information technology (IT), as well as the shifting locus of adversarial action."[46] Douglas Hubbard, an expert in qualitative analysis and author of *How to Measure Anything in Cybersecurity Risk*, devotes *chapters* to explaining varied approaches to cybersecurity measurement. He demonstrates that there is no consensus on methodologies or even the inherent measurability of certain aspects of cybersecurity.[47] The *2016 Federal Cybersecurity Research and Development Strategic Plan* confirms this, stating that "[i]n the current state of the art, scientifically established and well-understood solutions exist unevenly in various security subdomains. Most techniques are domain- and context-specific, often not validated as mathematically and empirically sound, and rarely take into account efficacy and efficiency."[48] This yields, among other things, "process-oriented metrics,"[49] many of which may not be suitable for use across industries and sectors or between organizations.

NIST should contend with this complexity head-on rather than glossing over it. Doing so will provide helpful context to *Framework* users, and ultimately will clarify NIST's position. Additionally, in developing its final guidance on measurements and metrics, NIST should consider this complexity and the evolving nature of the field, and take pause before promoting (or even appearing to promote) a particular approach.

At a minimum, NIST should examine, reference, and support ongoing work on cybersecurity risk management program assessment from experts and academics, standards bodies, and the insurance industry, among others. As an example of such work in just one sector—the Communications Sector—the FCC's CSRIC V, Working Group 6 compiled a list of

---

[45] Hubbard, *How to Measure Anything in Cybersecurity Risk* at 19.
[46] DHS, *A Roadmap for Cybersecurity Research* at 13 (Nov. 2009), https://www.dhs.gov/sites/default/files/publications/CSD-DHS-Cybersecurity-Roadmap.pdf (describing need for enterprise-level metrics).
[47] *See, e.g.*, Hubbard, *How to Measure Anything in Cybersecurity Risk* at 19. Therein, a guest commenter notes that "the topic of quantifying risk in the information security realm can generate significant debate and even hostility." *Id*. at 107.
[48] Executive Office of the President of the United States, National Science and Technology Council, *Federal Cybersecurity Research and Development Strategic Plan: Ensuring Prosperity and National Security* at 30 (Feb. 2016), https://www.nitrd.gov/cybersecurity/publications/2016_Federal_Cybersecurity_Research_and_Development_Strategic_Plan.pdf.
[49] *Id.*

cyber assessment standards, tools, and best practices;[50] and the Comm-ISAC and Communications Sector Coordinating Council industry leaders are currently looking at assessment. It would serve NIST well to become intimately acquainted with these efforts.

A variety of information security frameworks have been developed, which can inform NIST's effort to incorporate self-assessment. NIST should look to these as informative references for self-assessment. Examples include:

- efforts by private entities (*e.g.*, COBIT 5 by ISACA, 27001/2:2013 by ISO, 27004 by ISO/IEC, CIS Critical Security Controls);
- efforts by governmental entities (*e.g.*, NIST itself in the U.S, ENISA in the European Union, ASD in Australia);
- and efforts by industry-sponsored entities (*e.g.*, Payment Card Industry Council).[51]

Take, for example, ISO/IEC 27004, which has a different approach to measures than NIST's *Framework* version 1.1. ISO/IEC 27004 recognizes the need for tailoring and flexibility. It notes that "[c]areful selection and justification of the method used" for measurement is "important to ensure that excessive resources are not devoted to these activities … to the detriment of others."[52] For this reason, "size and complexity of the business in combination with the importance of information security affect the extent of measurement needed."[53] ISO recognizes that it is important to carefully select what is measured and what is communicated; "[a]n excessive number of reported measurement results will impact the ability of the decision-maker to focus efforts and prioritize future improvement activities." Further, ISO focuses such measurements on the specifics of the risk management program implemented within the organization; "measurement results should be prioritized based on the importance of corresponding information needs and associated [] objectives" chosen by the organization.[54] The NIST *Framework* is informed by ISO 27004; it should take a consistent approach to measurement.

NIST itself has done significant work regarding measures and metrics, but that work does not seem to be incorporated or referenced in its new treatment of the topic in version 1.1. NIST's involvement in this area includes the CyberChain survey effort,[55] the Baldrige Cybersecurity Excellence Builder,[56] and NIST Special Publication 800-55 v.1, *Performance Measurement Guide for Information Security*.[57] Specifically, The Baldrige Cybersecurity Excellence Builder, which is based on the Baldrige Excellence Framework and NIST

---

[50] https://transition.fcc.gov/bureaus/pshs/advisory/csric5/WG6_Final_091416.docx.

[51] *See* Oleg Bogomolniy, *Cyber Insurance Conundrum: Using CIS Critical Security Controls for Underwriting Cyber Risk*, SANS Reading Room (Jan. 27, 2017), https://www.sans.org/reading-room/whitepapers/legal/cyber-insurance-conundrum-cis-critical-security-controls-underwriting-cyber-risk-37572.

[52] International Standards Organization, *Information Technology—Security Techniques—Information Security management: Measurement*, ISO/IEC 27004:2009(E) at 0.2 (Dec. 2009), https://www.iso.org/standard/42106.html.

[53] *Id.*

[54] *Id*. at 7.2.

[55] CyberChain, https://cyberchain.rhsmith.umd.edu/.

[56] NIST is convening stakeholders about its proposed "assessment tool" for use of the *Framework*. This may affect revisions to the *Framework*, including possible inclusion of metrics—so NIST should go slow in this area.

[57] NIST, *Performance Measurement Guide for Information Security*, Special Publication 800-55 v.1 at viii (July 2008) ("*NIST SP 800-55 v.1*"), http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-55r1.pdf.

Framework, is a voluntary self-assessment tool that "helps leaders of organizations to identify opportunities for improvement based on their cybersecurity risks, needs, and objectives, as well as their larger organizational environment, relationships, and outcomes."[58] The Excellence Builder is "adaptable and scalable" and "does not prescribe how an organization should structure its cybersecurity policies and operations."[59] SP 800-55v.1 guides federal agencies in "establishing a relationship between an information system and program security activities… to demonstrate the value of information security to their organization;" it also emphasizes that such "measures indicate **effectiveness of security controls** applied to information systems and security programs" and that "[s]uch measures are used to facilitate decision making, and increase accountability through the collection, analysis, and reporting of performance-related data—providing a way to tie the implementation, efficiency, and effectiveness of information system and program security controls to an agency achieving its mission."[60]

The *Commission on Enhancing National Cybersecurity* called for NIST and the National Cybersecurity Public-Private Program ("NCP[3]") to establish a Cybersecurity Framework Metrics Working Group.[61] This would yield metrics that may be used by industry voluntarily to assess risk, and to inform insurance coverage needs by measuring the effectiveness of risk management programs. NIST should consider engaging in this effort *before* incorporating measures and metrics into the *Framework*. Doing so will allow NIST to clarify its approach and draw from the voluminous and evolving body of work around measures and metrics.

Second, any discussion of self-assessment should emphasize tailoring to organizations' goals. As drafted, Section 4.0 contains too much detail and not enough flexibility. For example, the draft refers to leading and lagging metrics;[62] NIST need not get into such details. Instead, NIST should encourage organizations to think about outcomes. The "outcome" that an organization should be concerned about is the overall effectiveness of its Risk Management Program as a support of its business goals. Organizations need to resist the desire for arbitrary or "feel good" metrics.[63] Desired outcomes will vary greatly—from sector to sector, within a given sector, and within organizations. While NIST should encourage organizations to think about outcomes, it is impossible to capture the variability of desired outcomes. Attempting to do so may erode the *Framework's* utility as a broad tool that any organization can utilize.

In other settings the government recognizes the need for risk management to be tailored and outcome-oriented. The Office of Foreign Assets Control tells entities trying to comply that "[i]t is often difficult to balance the demands of Federal and State bank examiners with limitations on time, resources, and manpower. . . . no one compliance program can be

---

[58] Baldrige Cybersecurity Excellence Builder FAQs, https://www.nist.gov/baldrige/products-services/baldrige-cybersecurity-initiative.
[59] *Id.*
[60] *NIST SP 800-55 v.1*, at viii (emphasis added).
[61] Commission on Enhancing National Cybersecurity, *Report on Securing and Growing the Digital Economy* at 19 (Dec. 1, 2016) ("*WH Cyber Commission Report*"), https://www.nist.gov/sites/default/files/documents/2016/12/02/cybersecurity-commission-report-final-post.pdf.
[62] *Framework Draft Version 1.1* at 21 ("While it is important to measure whether or not a business objective was achieved through lagging measurement, it is typically more important to understand the likelihood of achieving a future objective through a leading measurement.").
[63] Take for example a metric like the "number of malicious emails blocked," which may seem impressive, but that does not provide much insight into an organization's risk management program's effectiveness.

prepackaged . . . . Every program must be tailored to meet the needs and structure of individual financial institutions."[64] Likewise, with the International Traffic in Arms Regulations, the methodology for managing controlled items should be "specifically tailored to corporate structure, organization, and functions."[65] This guidance is more apt for cybersecurity, where desired outcomes are fluid.

A good example of outcome-oriented, tailored risk management using the *Framework* is the privacy and security plan developed for the National Emergency Address Database ("NEAD"), a key component of the new wireless 9-1-1 location accuracy framework.[66] NEAD used the "NIST Cybersecurity Framework (v. 1.0) and the ISO 27001 Information Security Management Standard … in the development of controls designed to maintain the confidentiality, availability, and integrity of the NEAD Platform's networks, systems, and data."[67] Its "operations will be subject to a program of regular audits and assessments to enable ongoing governance, compliance, and risk management."[68] The plan explains that the NEAD will take steps, tailored to its risk profile and setting, to assure security of the information and infrastructure used to provide the location information database. [69] Aspects of the NEAD Platform will obtain certification under the ISO 27001 Information Security Management Standard. This approach was developed based on risks unique to the NEAD. Each part of the risk management program is tailored to the operational goals and threats that are important to the NEAD. The risk profile of the NEAD is based on the E911 critical infrastructure threat landscape as reflected in the Plan submitted to the FCC. In addition, "the sufficiency of any safeguards in place to control those risks will also be assessed at least annually."[70] The plan looks to "outcomes" in the form of policies and standards that match its operational needs. The key metric for NEAD is "availability" of the system 24 *x* 7 *x* 365. For the NEAD, relevant measures are the specific KPIs that measure the effectiveness of the risk management program. NIST should encourage organizations using the *Framework* to pursue this sort of approach, rather than encouraging users to benchmark themselves against the *Framework* or its Informative References.

---

[64] *OFAC Regulations for the Financial Community* at 2 (Jan. 24, 2012), https://www.treasury.gov/resource-center/sanctions/Documents/facbk.pdf.

[65] Department of State, Bureau of Political Military Affairs, *Compliance Program Guidelines* at 2, https://www.pmddtc.state.gov/compliance/documents/compliance_programs.pdf.

[66] NEAD, LLC, AT&T, T-Mobile USA, Sprint Corporation, and Verizon, *NEAD Privacy and Security Plan*, PS Docket No. 07-114 (Feb. 3, 2017) ("NEAD Privacy and Security Plan"), https://ecfsapi.fcc.gov/file/1020387572432/170203%20NEAD%20Privacy%20and%20Security%20Plan.pdf.

[67] *Id*. at 2.

[68] *Id.*

[69] Key components, described in the NEAD Privacy and Security Plan, include: A governance structure; Inventory of critical assets and software; Secure configuration of assets and devices, including Access controls, Segmentation, and Separation; Continuous risk assessment; Incident detection, mitigation and response plans; Boundary defenses; Encryption and Other Data Protection Measures; Sourcing and Supply Chain Restrictions; Penetration Testing; Application Security; Business continuity and disaster recovery plans; Personnel management and training; Audit & tracking; Process for continuous improvement and lessons learned.

[70] NEAD Privacy and Security Plan at 8.

C. Section 4.0 should be revised to avoid a compliance mindset that can lead to misuse.

Without the clarifications and changes suggested above, the approach put forth in version 1.1 may do more harm than good. The draft could be read to encourage users to treat assessment as a compliance matter by cataloging their use of the *Framework*. This would be the wrong approach. NIST should make clear that it is recommending that organizations using the *Framework* assess their own performance; *not* that organizations must earn a specific "grade" in their implementation of the *Framework*, or that one organization's "grade" can be compared to another's. Because of the variability in desired outcomes between sectors, within sectors, and within organizations, it is unrealistic to try to make meaningful comparisons about cybersecurity effectiveness. Instead, NIST should make clear that measurements and metrics are *not* tools to monitor compliance with the *Framework* or to comparatively assess organizations.

The current draft also runs the risk of misuse. First, regulators and litigators, who may not appreciate the complexity of cybersecurity measurement, may try to use self-assessments to assign responsibility and obligations. Attaching a value to cyber practices—at a time when litigation is picking up steam and agencies may feel obliged to act—may turn NIST's voluntary and flexible guidance into a *de facto* standard of care. Emphasizing the complexity of assessment can help ensure measurement does not inadvertently foster litigation and regulation. Second, the draft may increase security concerns due to possible public disclosure of measurement information. While risk assessments and detailed security planning are valuable,[71] these activities are highly sensitive and, for private companies, proprietary. In the wrong hands, such information can be dangerous. NIST should address the security concern posed by collecting information about organizations' cyber preparation and efficacy. Emphasizing the internal use of assessments would help avoid these unintended consequences.

D. NIST should re-draft its discussion.

NIST should take the opportunity to re-draft its discussion.

- NIST should make clear that its inclusion of measurement is intended to support a common taxonomy for voluntary self-assessment of the effectiveness of a risk management program. NIST should re-name the section "Self-Assessment."
- NIST should acknowledge that measurement is evolving and there is no consensus around metrics or measures.
- NIST should explain that self-assessment tools should be chosen to measure the effectiveness of the risk management program within individual organizations.
- NIST should state, throughout the *Framework*, including in Sections 3.2 and 4.0, that measures are intended to be used internally and protected from external use.

[71] Some companies are developing their own ways to measure and assess risk and security, and are offering services to the marketplace. Such innovation should be rewarded.

V. Supply Chain Risk Management Is Complex and Variable.

A. The draft rightly addresses SCRM, but should explain its complexities.

Version 1.1 is meant to "[e]nhance guidance for applying the Framework for supply chain risk management."[72] NIST explained that "[t]o assist users wanting to apply the framework to cyber supply chain risk management, the authors developed a vocabulary so all organizations working together on a project can clearly understand cybersecurity needs."[73]

CTIA appreciates NIST's effort to provide a common taxonomy for supply chain risk management ("SCRM"). But the current draft dives into a discussion of SCRM without providing adequate context.[74] The draft could be improved by adding a section at the beginning of Section 3.3 that describes the basics of SCRM. NIST should describe the depth of the complexities and challenges associated with SCRM. SCRM is highly complex and variable from organization to organization and sector to sector. The U.S. Chamber of Commerce has described businesses as "linked together through a global web of interconnected, predictable, and efficient supply chains," which are relied upon "to access international consumers and compete in the global marketplace."[75] NIST must recognize this complexity, and promote a reduction in cybersecurity supply chain risks "without compromising the interconnectivity that makes networks useful."[76]

Some complexities exist across sectors. For example, supply chain expectations may impact legacy systems. NIST must recognize that many organizations maintain legacy systems whose provenance may not be known or relevant. Also legacy contracts may be difficult to amend. Organizations may not always have the ability to control or monitor the cybersecurity practices of third parties. To some extent, the draft recognizes this in its newly-added Section 3.4 on Buying Decisions;[77] however, this is an issue that must be taken into account beyond buying decisions, including with suppliers.

---

[72] NIST, *Cybersecurity Framework Virtual Events* (Mar. 1, 2017) ("March 2017 Webinar"), https://www.nist.gov/news-events/events/2017/03/cybersecurity-framework-webinars.

[73] Press Release, NIST, *NIST Releases Update to Cybersecurity Framework* (Jan. 10, 2017), https://www.nist.gov/news-events/news/2017/01/nist-releases-update-cybersecurity-framework.

[74] *Framework Draft Version 1.1* expands Section 3.3—*Communicating Cybersecurity Requirements with Stakeholders*—to help users understand SCRM. It adds SCRM as a property of the Implementation Tiers. It also adds SCRM as a category to the *Framework* Core. *Framework Draft Version 1.1*at *ii.*

[75] Letter from R. Bruce Josten, U.S. Chamber of Commerce, to The Honorable Max Baucus and The Honorable Orrin Hatch Regarding S. 662, the "Trade Facilitation and Trade Enforcement Reauthorization Act of 2013," (May 19, 2013), https://www.uschamber.com/letter/letter-regarding-s-662-trade-facilitation-and-trade-enforcement-reauthorization-act-2013%E2%80%9D.

[76] *Cybersecurity: An Examination of the Communications Supply Chain*, Hearing Before the Subcommittee on Communications and Technology of the House Committee on Energy and Commerce, 113th Cong. 1 (May 21, 2013) (statement of Rep. Walden, Chairman, House Subcommittee on Communications and Technology) ("Supply Chain Hearing").

[77] *See Framework Draft Version 1.1*§ 3.4 ("[I]t may not be possible to impose a set of cybersecurity requirements on the supplier. . . . Therefore, a product or service is typically purchased with known gaps to the Target Profile.").

Some complexities are unique to sectors or organizations. For example, in the mobile ICT sector, there are differences in hardware and software sourcing.[78] Supply chains are global, constant, dispersed, and "include supply chains for physical components, integrated components such as network routers, and software."[79] A main difference between hardware and software is that while "[h]ardware specifications can be verified on delivery in most instances, . . . software functionality cannot . . . . [and] may exhibit undesired behavior when confronted with conditions not considered during development. . . ."[80]

NIST should make clear that there is no one-size-fits-all approach to SCRM.[81] Organizations should use flexible, market-driven solutions. "Since the technology underlying both the U.S. infrastructure and cyber-attacks can change rapidly, protective measures must evolve rapidly, as well."[82] NIST should rely on guidance already developed, such as:

- 3GPP SA Working Group 3, identifying security assurance methodologies for 3GPP network elements;[83]
- ISO/IEC 15408, creating Common Criteria for Information Technology Security Evaluation and the internationally-recognized Common Criteria Recognition Agreement;[84] and
- ISO/IEC 27036, offering guidance for organizations on securing information and information systems within the context of the supply chain.[85]

NIST has written extensively on supply chain issues, and should clearly cross reference and provide mapping to ensure that the addition of SCRM to the *Framework* does not confuse organizations that might look to NIST for guidance.

Finally, SCRM challenges and solutions are different for the private sector and government. Thus, when NIST cites to its SCRM work in NIST Special Publication 800-161,[86]

---

[78] *See, e.g.*, Comments of CTIA, *Mobile Security Threats and Defenses*, Solicitation Number QTA00NS16SDI0003, at 8 (filed Aug. 22, 2016), http://www.ctia.org/docs/default-source/Legislative-Activity/ctia-filing-dhs.pdf.
[79] Robert J. Ellison, et al, *Software Supply Chain Risk Management: From Products to Systems of Systems*, Software Engineering Institute, Carnegie Mellon at 1 (Dec. 2010), https://resources.sei.cmu.edu/asset_files/TechnicalNote/2010_004_001_15194.pdf.
[80] *Id.*
[81] *See* Press Release, United States House of Representatives, Energy and Commerce Committee, *Walden Appoints Members of Bipartisan Supply Chain Working Group,* 113th Cong. 1 (May 21, 2013), http://energycommerce.house.gov/press-release/walden-appoints-members-bipartisan-supply-chain-working-group ("There is no one silver bullet and it cannot be fixed by government alone."); United States House of Representatives, Committee on Energy and Commerce, Majority Committee Staff, *Majority Memorandum for the May 21, 2013, Communications and Technology Subcommittee Hearing* at 2 (May 17, 2013) ("*House Supply Chain Memo*"), http://docs.house.gov/meetings/IF/IF16/20130521/100876/HHRG-113-IF16-20130521-SD002.pdf ("[J]ust as there is no one-size-fits-all network, there cannot be a one-size-fits-all response.").
[82] *House Supply Chain Memo* at 2.
[83] *See* 3GPP, *Draft Meeting Report for TSG SA WG3 Meeting S3#70*, at § 8.3 (Jan. 21, 2013), www.3gpp.org/ftp/tsg_sa/wg3_security/.../Report/finalMeetingReport_SA3_63.pdf.
[84] *See* Common Criteria, http://www.commoncriteriaportal.org/.
[85] *See* International Standards Organization, *Information Technology—Security Techniques—Information Security for Supplier Relationships—Part 1: Overview and Concepts*, ISO/IEC 27036-1:2014 (Apr. 2014), https://www.iso.org/standard/59648.html.

it should make clear that its guidance is for federal systems.[87] NIST has stated that it wants its guidance for federal systems to be consistent with its guidance in the *Framework*.[88] However, best practices for federal systems are not perfectly adaptable for private use. For example, federal systems are acutely concerned about SCRM in part because of insider threats,[89] but insider threats may not be similar across the private sector. An organization must assess its own risk to insider threats, and in many cases, it will be different than a federal system's risk. Where there is any difference in the guidance between the *Framework* and SP 800-161, NIST should explicitly recognize this. Similarly, NIST deals with supply chain issues in SP 800-53. The *Framework* should specifically reference this treatment and ensure that the two are consistent, or that the inconsistencies are clearly identified and explained.

B. A separate SCRM category may confuse users and overemphasize supply chain.

The new draft adds SCRM as a property of the Implementation Tiers.[90] SCRM maturity has been added to each Tier. The new draft also adds SCRM as a Category under the Identify function of the Core *Framework*.[91] By singling out SCRM, the draft overemphasizes it. The draft might inadvertently lead users to believe that SCRM is a higher priority than other practices. This could have unintended consequences, including deemphasizing the importance of general risk management, integrated risk management programs, external participation, and assessing an organization's unique vulnerabilities and risk tolerance. Rather than identifying SCRM as a standalone issue, the revised *Framework* should depict SCRM as a subset of the Risk Management Process. This will make clear that SCRM is a key part of Risk Management. NIST does this elsewhere in the document, including when it explains that "SCRM encompasses IT and OT suppliers and buyers as well as non-IT and OT partners" and that "these relationships highlight the critical role of cyber SCRM in addressing cybersecurity risk in the critical infrastructure and the broader digital economy."[92]

VI. NIST's Approach to Information Sharing Should Promote Voluntary, Meaningful Exchanges.

NIST treats a lack of information sharing as a gap and makes clear that sharing is part of tier selection.[93] NIST should make clear that even where there are benefits to the ecosystem, decisions about whether, what, and how to share rest entirely with the organization involved.

---

[86] *See, e.g.*, NIST, *Supply Chain Risk Management Practices for Federal Information Systems and Organizations*, SP 800-161, at n.10 (Apr. 2015) ("NIST SP 800-161"), http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-161.pdf.

[87] *See id.* at 3 ("The audience for this publication is federal agency personnel involved in engineering/developing, testing, deploying, acquiring, maintaining, and retiring ICT components and systems. These functions may include, but are not limited to, information technology, information security, contracting, risk executive, program management, legal, supply chain and logistics, acquisition and procurement, other related functions, and system owner. Other personnel or entities are free to make use of the guidance as appropriate to their situation.").

[88] *Cybersecurity Framework Update Webinar*, NIST (March 1, 2017).

[89] *See NIST SP 800-161*, at 27.

[90] *Framework Draft Version 1.1*at ii.

[91] *Id.*

[92] *Id.* at 17.

[93] *Id.* at 9.

NIST should promote *meaningful* efforts, not sharing for its own sake. In the measurement section, NIST appears to suggest that organizations should look to the quantity of information shared.[94] This is wrongheaded. As a RAND paper explained, "process measures of an initiative that broadly shares bad data and does so very rapidly might make the initiative look very good—large numbers of users, high usage, many reports produced, etc.—but these factors could be impeding rather than aiding the organization's actual performance."[95] NIST should avoid this trap and make clear that any sharing should be wholly voluntary and meaningful.

VII. Work on Authentication Should Not Promote Particular Solutions.

With version 1.1, NIST emphasized authentication. The Access Control Category has been refined to account for authentication, authorization, and identity proofing. A Subcategory has been added, and the Category has been renamed to Identity Management and Access Control (PR.AC). NIST expanded PR.AC.1 from "Identities and credentials are managed for authorized devices and users," to "PR.AC-1: Identities and credentials are issued, managed, verified, revoked, and audited for authorized devices, users, and processes." NIST should not prescribe details and should recognize the need for flexibility. NIST can do this by adding "as appropriate" to discussions of identity and credential management.

NIST should heed FTC recommendations[96] that authentication standards should be:

> technology-neutral and provide flexibility to private sector entities to implement a program that is compatible with their size, the nature of their business, and the specific authentication risks they face. The procedures also should be adaptable to changes that may occur over time in available technologies and the nature of the risks, including the potential harm to consumers. Finally, the standard should be one of reasonableness and not perfection, acknowledging that there is no fool-proof method of authenticating consumers and no likelihood that one will be developed in the foreseeable future.[97]

NIST should not paint with a broad brush in disfavoring approaches, such as methods of two-factor authentication ("2FA"), as it does in its proposed *Digital Authentication Guidelines*, SP 800-63B. It cannot let the perfect be the enemy of the good. It would be a major success for government, companies, and individuals to embrace 2FA of any kind, as appropriate for their setting. Relatedly, NIST should be explicit about its other work on authentication, for example, in SP 800-53, 800-82 and 800-63, and be careful not to confuse organizations that may have difficulty deciding what to follow.

---

[94] *See id.* at 23 ("Finally, the volume of threat and vulnerability information received from information 827 sharing forums and sources (ID.RA-2) is reflected in the metric, External Participation.").
[95] Brian A. Jackson, *How Do We Know What Information Sharing Is Really Worth?, Exploring Methodologies to Measure the Value of Information Sharing and Fusion Efforts,* RAND Corporation, http://www.rand.org/content/dam/rand/pubs/research_reports/RR300/RR380/RAND_RR380.pdf.
[96] FTC, *Internet of Things: Privacy & Security in a Connected World* (Jan. 2015), https://www.ftc.gov/system/files/documents/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-internet-things-privacy/150127iotrpt.pdf.
[97] FTC, *Security in Numbers—SSNs and ID Theft* at 6-7 (Dec. 2008), https://www.ftc.gov/sites/default/files/documents/reports/security-numbers-social-security-numbers-and-identity-theft-federal-trade-commission-report/p075414ssnreport.pdf.

There is no single solution. Passwords can vex consumers, and conventional wisdom changes.[98] Two-factor authentication is important, but can impact user experience. This may limit adoption or increase consumer frustration. As researchers observe, "respondents most often rejected security behaviors because they were inconvenient." In one survey, "25% (of respondents) used 2FA on all of the devices or services that offered it; 45% used 2FA on some, but not all services; and 28% never used 2FA." "Inconvenience was also the most common reason given by respondents for not using 2FA (41%)."[99] Luckily, innovation is changing authentication. "Authentication as a service" has emerged, and providers are innovating to drive use. Service providers abound.[100] Innovations (biometrics, online tools that use IP addresses or geolocation, mobile identify verification services) are promising and should be encouraged.

Fundamentally, NIST should not allow a focus on authentication to distract it from easier basic cyber security issues that can be addressed without much difficulty. Basic cyber hygiene needs to be improved across the government. A recent study revealed that 7% of federal employees bring jailbroken mobile devices to work and use them on federal networks.[101] A 2014 study showed that 25% of federal workers said that they do not use passwords on their work mobile devices, and 28% reported using "easy" passwords.[102] NIST should focus on basic things like MDM and common sense behavior before it addresses identity and credential authentication.

VIII. NIST Should Refine Its Discussion of Privacy and Civil Liberties.

The draft recognizes important privacy and civil liberties issues, and wisely does not offer prescriptive approaches. This is generally consistent with version 1.0 of the *Framework*. In Section 3.6, the new draft states that "Privacy and cybersecurity have a strong nexus. It is well-recognized that cybersecurity plays an important role in protecting individuals' privacy; for example, with respect to the confidentiality of assets containing personal information." CTIA agrees, because without security, we cannot protect privacy. The public expects companies, particularly in the Communications Sector, to respect their privacy. This is why the Communications Sector has repeatedly stated its commitment to consumer privacy, and why the industry supported CISA, federal cybersecurity legislation that struck a balance between private sector cybersecurity information-sharing and the protection of privacy in personal information.

---

[98] *See, e.g.*, Dan Goodin, *Frequent password changes are the enemy of security, FTC technologist says*, Ars Technica (Aug. 2, 2016), https://arstechnica.com/security/2016/08/frequent-password-changes-are-the-enemy-of-security-ftc-technologist-says/ (explaining that contrary to earlier security recommendations, "[f]requent password changes do little to improve security and very possibly make security worse by encouraging the use of passwords that are more susceptible to cracking").

[99] Elissa M. Redmiles, et al., *How I Learned to be Secure: a Census-Representative Survey of Security Advice Sources and Behavior*, University of Maryland, Johns Hopkins University (Oct. 2016), https://www.umiacs.umd.edu/~mmazurek/papers/ccs2016-learned-secure.pdf.

[100] http://searchsecurity.techtarget.com/feature/The-top-multifactor-authentication-products.

[101] Lookout.com, *Feds: You Have a BYOD Program Whether You Like It or Not* at 3, https://campustechnology.com/~/.../04D1177141F04D6C99DF8626742C7843.pdf

[102] Josh Hicks, *How safe are feds with their work mobile devices?*, Washington Post (Jan. 21, 2014) (citing a Mobile Work Exchange Study), https://www.washingtonpost.com/pb/news/federal-eye/wp/2014/01/21/how-safe-are-feds-with-their-work-mobile-devices/?outputType=accessibility&nid=menu_nav_accessibilityforscreenreader.

Against this backdrop, the draft's treatment of civil liberties could be clarified. NIST states that "an organization's cybersecurity activities also can create risks to privacy and civil liberties when personal information is used, collected, processed, maintained, or disclosed in connection with an organization's cybersecurity activities."[103] This new formulation emphasizes perceived risks and does not recognize the protections afforded in CISA. It also may confuse responsibility for privacy and civil liberties, particularly insofar as the draft elsewhere is imprecise about government and private use of the *Framework*. As a general matter, private activity does not directly impact *civil liberties*, though government action can. Because the *Framework* is to be used across all organizations—public and private—NIST should make clear that while private companies should focus on privacy impacts, its discussion of *civil liberties* applies to government organizations and activities.

IX. Federal Agency Use of the *Framework* Will Bring Needed Improvement, but Procurement Should Not Be Used To Drive Private Sector Change or Stifle Trade.

Government systems are not yet secure, as the government knows.[104] Two recent examples make this point: in 2016, hackers gained access to IRS data of more than 700,000 taxpayers,[105] and in 2015, the OPM hack exposed the personal information of 22 million current and former federal employees.[106] These attacks undermine confidence in the government's ability to protect information. As a user of ICT and a target, the government can do a better job including security into digital strategy, educating its user community, and managing mobile. New Section 3.7 is correct that "Federal agencies may find the Framework a valuable addition."[107] Using the NIST *Framework* will help agencies. As the *Commission on Enhancing National Cybersecurity* recently noted, "the majority of federal and other government agencies, are not yet taking advantage of" the *Framework*.[108] The Commission recommended that "all federal agencies should be required to use [it]."[109] NIST should devote its limited resources to helping federal IT security, harmonizing systems, and educating the user base about basic cyber hygiene.

However, it is vital that standards for government systems remain voluntary and flexible, not cemented in rigid procurement standards that act as *de facto* regulation. Voluntary, third party standards are consistent with the National Technology Transfer and Advancement Act of 1995 ("NTTA"), which requires agencies to use "technical standards that are developed or adopted by voluntary, consensus standards bodies,"[110] and OMB Circular A-119, which requires

---

[103] This section replaces previous language that observed, "privacy and civil liberties implications may arise" when personal information is used in cybersecurity activities.
[104] GAO, Report to Congressional Committee, GAO-12-757, *Information Security: Better Implementation of Controls for Mobile Devices Should Be Encouraged* at 35 (Sept. 2012), http://www.gao.gov/assets/650/648519.pdf.
[105] Kevin McCoy, *Cyber hack got access to over 700,000 IRS accounts*, USA Today (Feb. 26, 2016), http://www.usatoday.com/story/money/2016/02/26/cyber-hack-gained-access-more-than-700000-irs-accounts/80992822/.
[106] Ellen Nakashima, *Hacks of OPM databases compromised 22.1 million people, federal authorities say*, The Washington Post (July 9, 2015), https://www.washingtonpost.com/news/federal-eye/wp/2015/07/09/hack-of-security-clearance-system-affected-21-5-million-people-federal-authorities-say/.
[107] *Framework Draft Version 1.1* at 20.
[108] *WH Cyber Commission Report* at 19.
[109] *WH Cyber Commission Report*, Action Item 1.4.2 at 20.
[110] National Tech. Transfer and Advancement Act (NTTA), Pub. L. No. 104-113, § 12(d), 110 Stat. 775 (1995).

federal agencies to "use voluntary consensus standards in lieu of government-unique standards in their procurement and regulatory activities."[111] Likewise, the government should avoid any action that would turn security requirements into a trade barrier or encourage other countries to do so. Under 19 U.S.C. § 2532, "[n]o Federal agency may engage in any standards-related activity that creates unnecessary obstacles to the foreign commerce of the United States."[112] NIST should ensure that the *Framework* is not used as a trade barrier; CTIA urges NIST to be especially cognizant of this with the additions of supply chain risk management.

X. Conclusion

CTIA has worked with NIST at every stage of the *Framework*; we applaud NIST for the collaborative, voluntary, and industry-led approach it has taken. The *Framework* has been effective and successful because of those traits and NIST's continued leadership. CTIA urges NIST to stay the course, focusing on voluntary, flexible tools that can help the ecosystem improve security.

Thomas K. Sawanobori
Senior Vice President and Chief Technology Officer

John A. Marinho
Vice President, Technology and Cybersecurity

CTIA
1400 16th Street, NW, Suite 600
Washington, DC 20036
202-736-3200
www.ctia.org

[111] Executive Office of the President, OMB, OMB Circular A-119: *Federal Participation in the Development and Use of Voluntary Consensus Standards and in Conformity Assessment Activities*, at 14, 17 (Jan. 27, 2017), https://obamawhitehouse.archives.gov/sites/default/files/omb/inforeg/revised_circular_a-119_as_of_1_22.pdf.
[112] 19 U.S.C. § 2532.