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

In the Matter of	)	
	)	
SP 800-63-4 (Draft)	)	PRE-DRAFT Call for Comments:
	)	Digital Identity Guidelines
	)	

COMMENTS OF CTIA

Thomas K. Sawanobori
John A. Marinho
Melanie K. Tiano
CTIA

August 10, 2020

Table of Contents

I. INTRODUCTION AND SUMMARY

CTIA[1] appreciates the opportunity to provide feedback on the National Institute of Standards and Technology's ("NIST") pre-draft call for comments on Draft SP 800-63-4.[2] CTIA welcomes NIST's efforts to refine the four-volume Digital Identity Guidelines.

The Digital Identity Guidelines offer federal agencies guidance on ensuring that an individual is who they say they are when accessing federal systems.[3] SP 800-63-3 "provides an overview of general identity frameworks, using authenticators, credentials, and assertions together in a digital system, and a risk-based process of selecting assurance levels."[4] SP 800-63A "provides requirements for enrollment and identity proofing of applicants that wish to gain access to resources."[5] SP 800-63B "provides recommendations on types of authentication processes, including choices of authenticators."[6] SP 800-63C "provides requirements to identity

---

[1] CTIA – The Wireless Association® ("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] *See PRE-DRAFT Call for Comments: Digital Identity Guidelines*, NIST (June 2020), https://csrc.nist.gov/publications/detail/sp/800-63/4/draft ("*Pre-Draft Call For Comments*").

[3] *See* NIST SP 800-63-3: Digital Identity Guidelines, at 2, NIST (June 2017), https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63-3.pdf ("These guidelines describe the risk management processes for selecting appropriate digital identity services and the details for implementing identity assurance, authenticator assurance, and federation assurance levels based on risk.") ("*SP 800-63-3*"); NIST SP 800-63A: Digital Identity Guidelines: Enrollment and Identity Proofing, NIST (June 2017), https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63a.pdf ("*SP 800-63A*"); NIST SP 800-63B, Digital Identity Guidelines: Authentication and Lifecycle Management, NIST (June 2017), https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63b.pdf ("*SP 800-63B*"); NIST SP 800-63C, Digital Identity Guidelines: Federation and Assertions, NIST (June 2017), https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63c.pdf ("*SP 800-63C*").

[4] *SP 800-63-3* at *vi*.

[5] *SP 800-63A* at 1.

[6] *SP 800-63B* at 2–3.

providers [] and relying parties [] of federated identity systems."[7] In addition to offering guidance, these documents are referenced in other NIST publications—SP 800-171,[8] SP 800-162,[9] and Draft SP 800-172[10]—that influence government contracting requirements.

The wireless industry has been involved in digital identification and offers three pieces of feedback for NIST as it updates the Digital Identity Guidelines. *First*, NIST should maintain its focus on *federal government* security and not expand the SP 800-63-4 series to reach the private sector. *Second*, the SP 800-63-4 series should highlight innovation across the field, including in mobile authentication. *Third*, SP 800-63B should encourage broad and flexible use of multi-factor authentication, consistent with its risk-based and technology-neutral approach.

II. NIST SHOULD KEEP THE FOCUS OF 800-63-4 ON FEDERAL USERS.

The Digital Identity Guidelines rightly focus on federal users. Each Guideline contains the same disclaimer: "These guidelines provide technical requirements *for federal agencies* implementing digital identity services and are *not intended to constrain the development or use of standards outside of this purpose*."[11] The Guidelines also clarify that use "by nongovernmental organizations" is "voluntary."[12] There are good reasons for maintaining this dichotomy between federal users and industry.

---

[7] *SP 800-63C* at 1, 5.

[8] *See* SP 800-171: Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations, at 84–85, NIST (Dec. 2016), https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-171r1.pdf.

[9] *See* SP 800-162: Guide to Attribute Based Access Control (ABAC) Definition and Considerations, at 1 n.1, 27, 37, NIST (Jan. 2014), https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-162.pdf.

[10] *See* Draft SP 800-172: Enhanced Security Requirement for Protecting Controlled Unclassified Information, at 16, NIST (July 2020), https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-172-draft.pdf.

[11] *See SP 800-63-3* at iii; *SP 800-63A* at ii; *SP 800-63B* at ii; *SP 800-63C* at ii (emphasis added in each).

[12] *See SP 800-63-3* at i; *SP 800-63A* at i; *SP 800-63B* at i; *SP 800-63C* at i.

First, federal and non-federal users have divergent missions, stakeholders, and data. Federal users have broad obligations to safeguard core governmental functions. Federal users' data may implicate law enforcement, the provision of public services, or other government interests. Industry users, by contrast, serve a broader and more varied array of private purposes. These private sector use cases—which encompass a wide variety of risk profiles—will often warrant different digital identification tools and approaches than federal users.

Second, federal users and non-federal users are governed by different cybersecurity and privacy laws that were designed for different purposes. For example, federal systems are subject to the Privacy Act, which was designed to protect privacy and civil liberty interests that are implicated by the government's possession and processing of data.[13] By contrast, non-federal systems' legal obligations stem from a variety of sources, including, but not limited to, private contracts, the Federal Trade Commission Act,[14] and—in some cases—sector-specific privacy or data security laws.[15]

Third, imposing the Digital Identity Guidelines' technical requirements on the private sector would strip industry of flexibility and risks deterring ongoing innovation. While NIST applies requirements on federal users,[16] it does not do so in the private sector. And in the Cybersecurity Framework, NIST specifically chose not to create "a prescriptive standard."[17] It

---

[13] *See* 5 U.S.C. § 552a.

[14] *See Privacy and Security Enforcement*, Federal Trade Commission, https://www.ftc.gov/news-events/media-resources/protecting-consumer-privacy/privacy-security-enforcement (last visited July 28, 2020).

[15] *See e.g.*, 15 U.S.C. § 6801 (Gramm–Leach–Bliley Act); 45 C.F.R. § 164.02 *et seq.* (HIPAA privacy rules).

[16] *See, e.g.*, *SP 800-63B* at 25 ("Unless otherwise specified in the description of a given authenticator, the verifier SHALL limit consecutive failed authentication attempts on a single account to no more than 100.").

[17] NIST, Presentation: Framework for Improving Critical Infrastructure Cybersecurity (June 2017), https://csrc.nist.gov/CSRC/media/Presentations/Cybersecurity-Framework-Overview/images-media/NIST%20CSF%20Overview.pdf.

instead adopted an outcome-based approach, explaining that "[b]ecause each organization's risks, priorities, and systems are unique, the tools and methods used to achieve the outcomes described by the Framework will vary."[18] Providing industry stakeholders with flexibility and room to innovate is key to improving digital identity outcomes in the private sector.

In sum, NIST should continue to apply the Digital Identity Guidelines the way they were intended to be applied: to *federal* users.

III. THE UPDATED DIGITAL IDENTITY GUIDELINES SHOULD SHOWCASE INNOVATION ACROSS THE DIGITAL IDENTITY SPACE, PARTICULARLY IN MOBILE AUTHENTICATION.

NIST's pre-draft call for comments notes that NIST "is particularly interested in" innovation in digital identity.[19] This focus is right. Innovative solutions abound and should be highlighted throughout NIST's guidance.

Mobile identity solutions are helping to drive the digital economy.[20] "Growth in mobile digital identity solutions is now forecast to exceed 800% by 2024[.]"[21] A 2019 survey found that "88% of security leaders feel that in the near future, mobile devices will serve as a digital ID for

---

[18] NIST, Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1, at 2 (Apr. 16, 2018), https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf ("*Cybersecurity Framework*").

[19] *See Pre-Draft Call For Comments* (noting that NIST is "particularly interested in" "new developments in techniques to limit linkability and observability for federation;" "[s]ecurity and performance capabilities (e.g., presentation attack detection/liveness testing) for biometric characteristic collection to support Identity Assurance Level 2 remote identity proofing in the areas of identity evidence verification (physical/biometric comparison) or binding of authenticators;" and "[c]apabilities and innovative approaches for remote identity proofing to achieve equivalent assurance as in-person identity proofing.").

[20] *Mobile Identity Overview*, GSMA, https://www.gsma.com/identity/mobile-identity-overview (last visited July 3, 2020) ("Mobile Identity is at the heart of the digital economy.").

[21] *Identity in the Digital Ecosystem*, GSMA, https://www.gsma.com/identity/identity-programme (last visited July 3, 2020).

accessing enterprise apps and data."[22] More than 75% of those leaders agree that "mobile devices secured by biometric authentication methods present the best option for replacing passwords."[23]

Mobile identity and authentication have become more important as industry stakeholders have begun implementing zero trust principles. "Zero trust security models assume that an attacker is present on the network and that an enterprise-owned network infrastructure is no different—or no more trustworthy—than any nonenterprise-owned network."[24] Incorporating zero trust principles increases the need for efficient authentication because users may need to be authenticated more often to access discrete assets in a zero trust architecture.[25] The wireless ecosystem supports innovative digital identity solutions, including:

- Federated Identity: Mobile solutions can "[p]rovide[] a mechanism for a single set of credentials (a single digital identity) to be used across multiple IT systems or websites, rather than the user having to register and remember credentials for each."[26] SP 800-63C's guidance is specifically intended for stakeholders that support "federated identity systems."[27]

- Single Sign-On: CTIA members—such as Oracle—support single sign-on ("SSO") solutions, which provide a unified authentication method that supports access to multiple applications.[28] As NIST explained, federated identity systems can "be used to support single sign on, where subscribers authenticate once to an [identity provider] and

---

[22] IDG & MobileIron, Say Goodbye to Passwords, at 4 (2019), https://www.mobileiron.com/en/resources-library/surveys-and-studies/say-goodbye-passwords ("*Say Goodbye to Passwords*").

[23] *Id.* at 3.

[24] Draft (2nd) SP 800-207: Zero Trust Architecture, at 1, NIST (Feb. 2020), https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-207-draft2.pdf.

[25] *See id.* at 1 ("In zero trust, these protections usually involve minimizing access to resources (such as data and compute resources and applications) to only those users and assets identified as needing access as well as *continually authenticating and authorizing the identity and security posture of each access request.*" (emphasis added)); *see also Adaptive Multi-Factor Authentication (MFA)*, Cisco, https://www.cisco.com/c/en/us/products/security/adaptive-multi-factor-authentication.html#~for-small-business (last visited July 9, 2020) ("Duo's multi-factor authentication (MFA) and device trust is a great start for enterprises to secure the workforce on their zero-trust journey.").

[26] *Mobile Identity Overview*, GSMA, https://www.gsma.com/identity/mobile-identity-overview (last visited July 3, 2020).

[27] *SP 800-63C*, at 1.

[28] *See, e.g.*, *Oracle Enterprise Single Sign-On*, Oracle, https://www.oracle.com/middleware/identity-management/enterprise-sso/ (last visited July 8, 2020).

subsequently obtain services from multiple [relying parties]."[29] SSO in turn enhances organizational efficiency "by reducing the number of authentication steps," while at the same time enhancing security by "support[ing] a diverse set of credentials, enabling a[n] [organization] to choose an authentication solution that best meets its individual needs."[30]

- Mobile Digital Signature: "The SIM . . . is an apt tool for supporting digital signatures."[31]

- Authentication Applications and Services: CTIA member Cisco supports *500 million* authentications every month to over 20,000 customers.[32] Others offer applications to provide mobile authentication through "Public-Key cryptography and open standards,"[33] as well as contextual identifiers that may be unique to mobile devices, such as GPS data and paired companion devices.[34]

- Biometric Authentication: Device manufacturers have long enabled biometric authentication using fingerprint sensors and are turning to "other biometrics such as face and iris scanning[.]"[35]

- Adaptive Authentication: Adaptive authentication "attempts to match the required authentication credentials to the perceived risk of the connection or authorizations requested."[36] Industry first movers are already offering cutting-edge adaptive authentication services that allows users to "create custom access policies based on role, device, location, and many other contextual factors."[37]

---

[29] *Id.* at 2.

[30] *See* SP 1800-13: Mobile Application Single Sign-On: Improving Authentication for Public Safety First Responders (Second Draft), NIST NCCoE (May 2019), https://www.nccoe.nist.gov/sites/default/files/library/sp1800/psfr-mobile-sso-nist-sp1800-13-draft-v2.pdf ("*NCCoE Public Safety SSO Second Draft*"); *see also Why is single sign-on important?*, Onelogin, https://www.onelogin.com/learn/why-sso-important (last visited July 8, 2020) ("SSO reduces the number of attack surfaces because users only log in once each day and only use one set of credentials.").

[31] *Mobile Identity Overview*, GSMA, https://www.gsma.com/identity/mobile-identity-overview (last visited July 3, 2020).

[32] *See About Us*, Duo, https://duo.com/about (last visited July 9, 2020).

[33] *Why HYPR*, HYPR, https://www.hypr.com/why-hypr/ (last visited July 3, 2020).

[34] Sarbari Gupta, *Next-generation identity assurance for mobile environments* (May 23, 2019), https://gcn.com/articles/2019/05/23/mobile-authentication.aspx.

[35] Joel Snyder, *Using biometrics for authentication in Android*, Samsung (Mar. 23, 2020), https://insights.samsung.com/2020/03/23/using-biometrics-for-authentication-in-android/.

[36] *Adaptive Authentication*, Secret Double Octopus, https://doubleoctopus.com/security-wiki/authentication/adaptive-authentication/ (last visited July 9, 2020).

[37] *See Adaptive Access Policies*, Duo, https://duo.com/product/adaptive-access-policies (last visited July 9, 2020).

The wireless ecosystem collaborates with the government on digital identity. CTIA members Verizon and Intel—with other industry partners—collaborated with NIST's National Cybersecurity Center of Excellence ("NCCoE") to "demonstrate[] how organizations can provide multifactor authentication for users to access [Personal Identity Verification (PIV)]-enabled websites from mobile devices that lack PIV Card readers."[38] Other stakeholders—including CTIA members Motorola Solutions and Nok Nok Labs—collaborated with NCCoE on the second draft of SP 1800-13, which "describes a reference design for multifactor authentication (MFA) and mobile single sign-on (MSSO) for native and web applications while improving interoperability among mobile platforms, applications, and identity providers, regardless of the application development platform used in their construction."[39]

In addition to collaboration with the public sector, the wireless industry is working with standards-setting bodies on digital identification. Stakeholders—like Cisco, Google, and Nok Nok Labs—are advancing FIDO2 specifications, aimed at standardizing authentication solutions across the Internet.[40] The FIDO Alliance's Internet of Things ("IoT") Technical Working Group—co-chaired by representatives from CTIA members Intel and Qualcomm[41]—is working "to provide a comprehensive authentication framework for IoT devices" by developing "IoT

---

[38] SP 1800-12: Derived Personal Identity Verification (PIV) Credentials, NIST NCCoE, at 1 (Aug. 2019), https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.1800-12.pdf; *see also Derived PIV Credentials*, NIST NCCoE, https://www.nccoe.nist.gov/projects/building-blocks/piv-credentials (last visited July 3, 2020) (listing "Collaborating Vendors").

[39] *NCCoE Public Safety SSO Second Draft* at ii.

[40] *See W3C and FIDO Alliance Finalize Web Standard for Secure, Passwordless Logins*, FIDO Alliance (Mar. 4, 2019), https://fidoalliance.org/w3c-and-fido-alliance-finalize-web-standard-for-secure-passwordless-logins/.

[41] *See Working Groups*, FIDO Alliance, https://fidoalliance.org/members/working-groups/ (last visited July 9, 2020).

device attestation/authentication profiles to enable interoperability between service providers and IoT devices[.]"[42]

NIST should recognize these innovations in digital identity. The wireless industry, with significant experience in digital identity, looks forward to collaborating with NIST.

IV. NIST SHOULD CONTINUE TO ENCOURAGE MULTI-FACTOR AUTHENTICATION.

NIST is interested in the "[c]ontinued use of short message service (SMS) and public switched telephone networks (PSTN) as restricted authentication channels for out-of-band authenticators."[43] Consistent with the risk-based and technology-neutral approach of the SP 800-63 series, NIST should encourage broad and flexible use of multi-factor authentication, including via SMS as appropriate.

A. Multi-Factor Authentication Has Clear Security-Enhancing Benefits.

NIST allows single-factor authentication only at Authenticator Assurance Level ("AAL") 1, requiring multi-factor Authentication for AAL2 and AAL3.[44] NIST's NCCoE explained last year that multi-factor authentication helps "reduce the risk of account takeovers," "reduce the risk of system-administrator account security breaches," and, "increase consumer confidence."[45] NIST is right. There is widespread acceptance among security professionals that using passwords alone introduces vulnerabilities.[46]

---

[42] *Internet of Things (IoT)*, FIDO Alliance, https://fidoalliance.org/internet-of-things/ (last visited July 9, 2020).

[43] *Pre-Draft Call For Comments*.

[44] *See SP 800-63B* at 2–3.

[45] *See* SP 1800-17: Multifactor Authentication for E-Commerce: Risk-Based, FIDO Universal Second Factor Implementations for Purchasers, NIST NCCoE (July 2019), https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.1800-17.pdf.

[46] *See, e.g.*, *Say Goodbye to Passwords* at 2 ("Among the security leaders, 86% would dump password use as an authentication method if they could. In fact, nearly half of those surveyed cited eliminating passwords as a way to cut almost half of all breach attempts.").

B. Encouraging a Diverse Range of Authentication Channels—Including SMS as Appropriate—Promotes Sound Risk-Management and Is Technology-Neutral.

NIST advocates a risk-based approach to cybersecurity. NIST's Cybersecurity Framework explains that "[b]ecause each organization's risks, priorities, and systems are unique, the tools and methods used to achieve [desired security outcomes] will vary."[47]

The SP 800-63 series emphasizes this. "SP 800-63 provides an overview of general identity frameworks, using authenticators, credentials, and assertions together in a digital system, and a *risk-based process* of selecting assurance levels."[48] "SP 800-63-A . . . provides requirements by which applicants can both identity proof and enroll at one of *three different levels of risk mitigation* in both remote and physically-present scenarios."[49] SP 800-63B's "three AALs define the subsets of options agencies can select *based on their risk profile* and the potential harm caused by an attacker taking control of an authenticator and accessing agencies' systems."[50] SP 800-63C's "three FALs reflect the options agencies can select *based on their risk profile* and the potential harm caused by an attacker taking control of federated transactions."[51]

SMS is one method used in multi-factor authentication and should be used as appropriate based on the nature and sensitivity of information being accessed, which is consistent with a risk-based approach. SMS authentication adds an extra complementary layer of security on top of passwords, reducing the ability for online data to be compromised. While there may be circumstances in which an agency desires security at an even greater level, SMS remains a

---

[47] *Cybersecurity Framework* at 2.

[48] *SP 800-63* at vi (emphasis added).

[49] *Id.* (emphasis added).

[50] *Id.* (emphasis added).

[51] *Id.* at vii (emphasis added).

valuable and user-friendly approach that could be used as appropriate based on the nature and sensitivity of the data accessed, and as one authentication method in a multi-factor authentication approach.

Many institutions use SMS as one of many methods of multi-factor authentication, in part because of its convenience and ubiquity, both of which are important to encouraging the adoption of security-enhancing practices. "[M]any organizations will struggle to persuade large numbers of users to" engage in other, less-accessible authentication methods.[52] It is commonly understood that consumers will not use—or, worse still, will seek security-damaging shortcuts around—burdensome or complex authentication solutions.[53] Indeed, NIST's NCCoE recognizes that security advantages "can be limited if complex authentication requirements hinder" users' ability to quickly access a system.[54]

Encouraging a diverse range of authentication channels is consistent with NIST's technology-neutral approach. NIST has explained that its work is "effective and supports technical innovation" when it is "technology neutral."[55] NIST should apply this approach to promoting multi-factor authentication.

---

[52] *See* Michael Mosher, *SMS two-factor authentication is alive and kicking*, OpenMarket (Mar. 6, 2019), https://www.openmarket.com/blog/sms-2-factor-authentication-alive/.

[53] *See, e.g.*, Nok Nok Labs, Multifactor Authentication Technical White Paper at 3–4 (Oct. 2016), https://noknok.com/wp-content/uploads/2017/10/wp-nnl-technical-overview-2016-09-30-english.pdf ("Users have also struggled with authentication. As the number of services used by a typical user has multiplied, so too has the number of usernames and passwords the user needs to remember. Users try to manage the problem by common or easy-to-remember passwords or simply reusing passwords. However, such passwords are more vulnerable to attack and weaken security.").

[54] *NCCoE Public Safety SSO Second Draft* at 1.

[55] *Cybersecurity Framework* at 2; *see also* SP 800-37, Rev. 2: Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy, NIST (Dec. 2018) ("The framework is policy and technology neutral, which facilitates ongoing upgrades to IT resources and to IT modernization efforts[.]").

V. CONCLUSION

The wireless industry looks forward to working with NIST as it revises the Digital Identity Guidelines. As it begins this process, CTIA urges NIST to (1) maintain a focus on federal users, not the private sector, (2) highlight innovation across the digital identity space, particularly with regard to mobile authentication, and (3) encourage a diverse range of authentication channels to best promote multi-factor authentication.

Respectfully submitted,

MelanieK.Tiano
ThomasK.Sawanobori
JohnA.Marinho

August 10, 2020