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

In the Matter of SP 800-63-4, SP 800-63A-4, SP 800-63B-4, and 800-63C-4	)))))	Digital Identity Guidelines, Revision 4 (Draft)

COMMENTS OF CTIA

Thomas K. Sawanobori
Senior Vice President and Chief Technology Officer

John A. Marinho
Vice President, Technology and Cybersecurity

Justin C. Perkins
Manager, Cybersecurity and Policy

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

April 14, 2023

Table of Contents

I. INTRODUCTION

CTIA[1] welcomes the opportunity to provide feedback to the National Institute of Standards and Technology ("NIST") as it updates it Digital Identity Guidelines. CTIA has consistently worked with NIST on this important document,[2] and is pleased to provide the below comments on Draft Special Publication (SP) 800-63, Revision 4: Digital Identity Guidelines ("Draft Revision 4"),[3] which updates the current version of the Digital Identity Guidelines, SP 800-63 Revision 3 ("Revision 3").[4] With these comments, CTIA recommends that NIST:

- Ensure that the scope of the Digital Identity Guidelines remain focused on federal agencies without creating *de facto* requirements for the private sector;
- Promote authentication innovation;
- Encourage the adoption and risk-based deployment of multi-factor authentication ("MFA"), including the use of short message service ("SMS") and the public switched telephone network ("PSTN") in authentication, where appropriate, based on the level of risk involved;

---

[1] CTIA – The Wireless Association® (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] Comments of CTIA, Draft NIST SP 800-63-3, NIST SP 800-63B, Digital Identity Guidelines (Mar. 31, 2017) (submitted via GitHub); Comments of CTIA, NIST SP 800-63-4, Pre-Draft Call for Comments: Digital Identity Guidelines (Aug. 10, 2020); NIST SP 800-63-4, Call for Comments on Open Issues: Digital Identity Guidelines (May 14, 2021).

[3] NIST SP 800-63-4 (Draft), Digital Identity Guidelines, NIST (Dec. 2022), https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63-4.ipd.pdf ("Draft SP 800-63-4"); NIST SP 800-63A-4 (Draft), Digital Identity Guidelines: Enrollment and Identity Proofing, NIST (Dec. 2022), https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63A-4.ipd.pdf ("Draft SP 800-63A"); NIST SP 800-63B-4 (Draft), Digital Identity Guidelines: Authentication and Lifecycle Management, NIST (Dec. 2022), https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63B-4.ipd.pdf ("Draft SP 800-63B"); NIST SP 800-63C-4 (Draft), Digital Identity Guidelines: Federations and Assertions, NIST (Dec. 2022), https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63C-4.ipd.pdf ("Draft SP 800-63C").

[4] NIST SP 800-63-3, Digital Identity Guidelines, NIST (June 2017), https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63-3.pdf ("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: Federations and Assertions, NIST (June 2017), https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63c.pdf ("SP 800-63C").

- Ensure that the Digital Identity Guidelines' wireless authenticator requirements are aligned with existing standards and best practices; and
- Advance equity while also ensuring sufficient flexibility.

II. THE DIGITAL IDENTITY GUIDELINES SHOULD REMAIN FOCUSED ON FEDERAL USERS.

Federal agencies are the longstanding audience of the Digital Identity Guidelines. For example, Revision 3 spells out that "[t]his recommendation provides *agencies* with technical guidelines for digital authentication of subjects to federal systems over a network."[5] While certain sections of Draft Revision 4 rightly retain previous language explaining that the guidance is intended for federal users, and that it is voluntary for the private sector, in some cases, it appears that Draft Revision 4 is attempting to reach a broader set of entities. For example, Draft Revision 4 explains: "These guidelines lay out a model for federal programs *and other organizations* to assess and manage risks associated with digital identity systems, including the processes, policies, data, people, and technologies that support digital identity management."[6] Notably, Draft Revision 4 also makes the following change from Revision 3: "These guidelines primarily focus on ~~agency services~~ organizational services that interact with ~~the non-federal workforce~~ external users, such as citizens accessing benefits or private sector partners accessing information sharing collaboration spaces."[7] Indeed, throughout Draft Revision 4, NIST has employed the broader term "organizations," whereas the previous Revision 3 tended to use the term "agencies."[8]

---

[5] SP 800-63-3 at 2 (emphasis added).

[6] Draft SP 800-63-4 at 3 (emphasis added).

[7] *Id.* at 4; SP 800-63-3 at 4.

[8] *Compare* Draft SP 800-63-4 at 2 ("This publication and its companion volumes, [SP800-63A], [SP800-63B], and [SP800-63C], provide technical guidelines to *organizations* for the implementation of digital identity services.") (emphasis added); Draft SP 800-63A at 2 (stating same); Draft SP 800-63B at 2 (stating same); Draft SP 800-63C at 2 (stating same) *with* SP 800-63-3 at 1 ("This recommendation and its companion volumes, Special Publication (SP) 800-63A, SP 800- 63B, and SP 800-63C, provide technical guidelines to *agencies* for the implementation of digital

CTIA cautions NIST against this shift away from a focus on federal users. Importantly, federal agencies and private sector organizations differ in ways that make broader, across-the-board guidance for both types of entities less practical and applicable to the private sector. Federal and non-federal users have different missions, data, and stakeholders. Industry users often serve a wider range of purposes than federal users and face a greater variety of differing risk profiles. Federal systems are also subject to unique privacy laws—such as the Privacy Act—that do not apply to private users.[9] By the same token, some private actors are subject to Federal Trade Commission ("FTC") oversight and sector-specific privacy and data security laws.[10]

Further, the structure of the Digital Identity Guidelines—which historically distinguished between different levels of priority using the terms SHALL, SHOULD, MAY, and CAN—makes sense for federal agencies, which are required to use the document.[11] However, this inflexible language is confusing—and could be misleading—for private sector users, for whom the guidance is not mandatory. Beyond being confusing and misleading, applying Draft Revision 4's guidance to non-federal users could remove flexibility from industry and deter authentication innovation.

---

authentication.") (emphasis added); NIST SP 800-63B (stating same). Additionally, Draft SP 800-63-4 uses the word "organization" or "organizations" over 150 times, while SP 800-63-3 uses the term just 36 times.

[9] *See* 5 U.S.C. § 552a.

[10] *See e.g.*, 15 U.S.C. § 6801 (Gramm–Leach–Bliley Act); 45 C.F.R. § 164.02 *et seq.* (HIPAA privacy rules); *Privacy and Security Enforcement*, FTC, https://www.ftc.gov/news-events/media-resources/protecting-consumer-privacy/privacy-security-enforcement (last visited Apr. 13, 2023).

[11] Office of Management and Budget Memorandum for Heads of Executive Departments and Agencies, M-19-17, at 2, 7-10 (May 21, 2019), https://www.whitehouse.gov/wp-content/uploads/2019/05/M-19-17.pdf; *Policies & Priorities: Identity, Credentialing, and Access Management (ICAM)*, CIO.gov, https://www.cio.gov/policies-and-priorities/ICAM/ (last visited Apr. 6, 2023). Moreover, Draft Revision 4 also does not contain the historical section, "Requirements Notation and Conventions," which normally explains these differences to users. *See* SP 800-63-3 at iii. NIST should ensure that this helpful language is included in Revision 4, and when it reinserts this language, it should further explain that the notation and conventions create requirements for federal agencies only, and that the guidance is voluntary for the private sector.

Accordingly, NIST should adjust Draft Revision 4 to ensure that it remains properly focused on federal agencies. Throughout Draft Revision 4, NIST should aim to use terminology more aligned with previous revisions to ensure consistency with past practice; specifically, NIST should refer to "federal agencies" or "agencies," rather than "organizations." Narrower language will result in recommendations that are clearer and more targeted for the intended audience of the series: federal agencies. Alternatively, if NIST continues to shift its focus to "organizations," it should include more language in the introductory sections that stress that the Digital Identity Guidelines are voluntary for the private sector, and that some of the guidance tailored for federal agencies will apply differently in private-sector contexts.

III. NIST SHOULD PROMOTE AUTHENTICATION INNOVATION, INCLUDING MOBILE IDENTITY ADVANCEMENTS, WHICH CONTINUE TO DRIVE THE MODERN ECONOMY.

CTIA encourages NIST to continue to promote technical innovation in authentication and digital identity solutions. In its 2020 Pre-Draft Call for Comments, NIST specifically sought comment on "agency and industry implementations, industry and market innovation and the current threat environment."[12] NIST was right to ask questions about innovation, and it should continue to pursue innovative security practices as it refines Draft Revision 4.

A. The Wireless Industry Fuels Authentication Innovation.

CTIA's members—and the wireless industry more generally—are developing and deploying mobile identity and identity access management solutions. CTIA member Cisco supports over 40,000 customers in over 100 countries through its Cisco Secure authentication applications and services, including Duo MFA solutions.[13] MFA can also be combined with

[12] *See Pre-Draft Call for Comments: Digital Identity Guidelines*, NIST, https://csrc.nist.gov/publications/detail/sp/800-63/4/archive/2020-06-08 (last visited Apr. 6, 2023).

[13] *About*, Duo, https://duo.com/about (last visited Apr. 6, 2023).

hardware tokens for enhanced security and authentication, as provided by CTIA member Qualcomm.[14] Device manufacturers have long used biometric authentication, and devices are utilizing various advanced methods for identifying fingerprints as well as facial recognition.[15] Adaptive authentication and access solutions can dynamically respond to risks by evaluating threat levels in real time.[16] Oracle also provides several single sign-on solutions, which provide unified authentication methods that allow access to multiple applications while enabling consistent access security.[17] Additionally, Oracle Cloud Infrastructure is an identity as a service ("IDaaS") platform that allows users to connect to and use identity management services from the cloud.[18]

Further, industry has developed new and innovative authentication tools and approaches fueled by 5G. For example, CTIA member Cisco offers an Identity Services Engine that combines Private 5G security with existing enterprise security solutions to create "contextual identity with attributes such as user, time, location, threat, vulnerability, and access type. IT administrators can centrally define a policy that differentiates guests from registered users and devices or specific IOT devices versus laptops. Regardless of their location, users and endpoints are allowed access to private networks based on role and policy."[19] As another example, the 3rd

---

[14] *Assured identity*, Qualcomm, https://www.qualcomm.com/products/government/assured-identity (last visited Apr. 6, 2023).

[15] *Which biometric authentication method is most secure?*, Samsung (May 25, 2021), https://insights.samsung.com/2021/05/25/which-biometric-authentication-method-is-most-secure-3/; *Authentication and identity*, Qualcomm, https://www.qualcomm.com/products/government/authentication-identity (last visited Apr. 6, 2023).

[16] *Adaptive access policies*, Duo, https://duo.com/product/adaptive-access-policies (last visited Apr. 6, 2023).

[17] *Oracle Access Management*, Oracle, https://www.oracle.com/security/identity-management/access-management/ (last visited Apr. 6, 2023).

[18] *OCI Identity and Access Management*, Oracle, https://www.oracle.com/security/cloud-security/identity-cloud/#rc30p4 (last visited Apr. 6, 2023).

[19] Cisco's Private 5G Solution Security Overview: Design Principles and Capabilities, Cisco, at 14 (2023) https://www.cisco.com/c/en/us/products/collateral/wireless/cisco-private-5g-solution-wp.pdf.

Generation Partnership Project ("3GPP") is working to define industry specifications for Multi-SIM, which would allow for multiple authenticators for a single device—for example, a mobile network operator could authenticate a SIM for commercial network access and another SIM could be used for private network access to an enterprise deployed 5G network.[20]

B. 5G Technology Features Significant Security Improvements, Including More Advanced Authentication.

To date, 5G is the most secure generation of wireless technology, with security features and enhancements built into the standard. The wireless industry is building on this 5G foundation and working to continuously improve security, to meet the fast-paced and ever-changing threat landscape. Indeed, industry is currently working through 3GPP and the Federal Communications Commission's ("FCC") Communications Security, Reliability, and Interoperability Council ("CSRIC"), among other venues, to further enhance security through the deployment of 5G. For example, CTIA launched its 5G Security Test Bed, which brings together "wireless providers, equipment manufacturers, cybersecurity experts, academia, and government agencies to demonstrate and validate how 5G security will work, using real 5G networks."[21] The 5G Security Test Bed creates a practical environment to test recommendations and security solutions.[22]

With respect to authentication, historically since 2G, wireless providers have used a universal subscriber identity module ("USIM") with a unique cryptographic key to authenticate and authorize each subscriber on their networks; however, the 5G standard contains significant

---

[20] *Support for Multi-SIM devices for LTE/NR*, 3GPP (Aug. 8, 2022), https://www.3gpp.org/technologies/support-for-multi-sim-devices-for-lte-nr.

[21] 5G Security Test Bed, https://5gsecuritytestbed.com/ (last visited Apr. 6, 2023).

[22] The 5G Security Test Bed: Enhancing Product Security & Threat Response in a Real-World Testing Environment, 5G Security Test Bed (June 14, 2022) https://5gsecuritytestbed.com/wp-content/uploads/2022/06/STB-One-Pager_061422.pdf.

authentication advancements. Drawing on "zero trust" principles,[23] the 3GPP technical specifications feature enhanced authentication,[24] and 5G's unified authentication framework can enhance security for 3GPP and non-3GPP access networks. In particular:

- The authentication framework specified by the Extensible Authentication Protocol ("EAP") has the potential to support exchange of authentication information between the device and the authenticating server.[25] 5G has three authentication protocols, two more than 4G: 5G-AKA, EAP-AKA', and EAP-TLS. Each of these protocols provide additional layers of security to both users and networks.[26]
- 5G's Authentication and Key Agreement protocol ("AKA") provides heightened signal security by using a symmetric key shared between a user and the 5G network to provide mutual authentication and avoid man-in-the-middle attacks.[27]
- Transport Layer Security ("TLS") is a 5G protocol that provides encryption for data transmitted over the internet.[28]
- 5G requires mutual authentication, whereby both the device and the network authenticate each other before they start the communication.
- Finally, and only in 5G, the user's permanent identity is always concealed with encryption when it is transmitted over the air, which ensures privacy protection of the user.

These and other advancements help make 5G the most secure generation of wireless.

---

[23] *See* Defining Zero Trust: Industry Approaches and Policy Frameworks for Strong Wireless Network Security, CTIA, at 11-12 (Jan. 9, 2023), https://api.ctia.org/wp-content/uploads/2023/01/Defining-Zero-Trust-White-Paper-2023.pdf.

[24] *See* 3GPP, TS 33.501 V16.13.0, Security architecture and procedures for 5G System (Release 16), ESTI (Jan. 2023), https://www.etsi.org/deliver/etsi_ts/1 33500_133599/133501/16.11.00_60/ts_133501v161100p.pdf.

[25] *See* Report on Recommendations for Identifying Optional Security Features that Can Diminish the Effectiveness of 5G Security, CSRIC VII, Working Group 3, at 14 (Mar. 10, 2021), https://www.fcc.gov/file/20606/download; *see also* John A. Marinho, *CSRIC: A Crucial Cybersecurity Partnership Protecting Wireless Consumers, and Federal Agencies*, CTIA (Mar. 10, 2021), https://www.ctia.org/news/blog-csric-a-crucial-cybersecurity-partnership-protecting-wireless-consumers-and-federal-agencies.

[26] *See, e.g.*, *A Comparative Introduction to 4G and 5G Authentication*, Cable Labs (2019), https://www.cablelabs.com/insights/a-comparative-introduction-to-4g-and-5g-authentication (last visited Apr. 6, 2023).

[27] *See* Xiaoting Huang et al., *Authentication Mechanisms in the 5G System*, 9 Journal of ICT Standardization 61, 62 (2021), https://journals.riverpublishers.com/index.php/JICTS/article/view/5707/5725; Shane Fonyi, *Overview of 5G Security and Vulnerabilities*, 5 Cyber Defense Review 117, 127 (2020), https://cyberdefensereview.army.mil/Portals/6/CDR%20V5N1%20-%2008_%20Fonyi_WEB.pdf.

[28] *See TLS Basics*, Internet Society, https://www.internetsociety.org/deploy360/tls/basics/ (last visited Apr. 6, 2023).

IV. NIST SHOULD PROMOTE THE RISK-BASED DEPLOYMENT OF MULTI-FACTOR AUTHENTICATION.

It is critical that NIST continue to promote the use of MFA, as MFA is a cybersecurity best practice. Indeed, NIST's National Cybersecurity Center of Excellence ("NCCoE") has explained that MFA helps "reduce the risk of system-administrator account security breaches" and "increase consumer confidence,"[29] and CISA has noted that "MFA adds a strong protection against account takeover by greatly increasing the level of difficulty for adversaries."[30] Additionally, CISA has launched its "More than a Password" campaign to promote use of MFA.[31]

While NIST already promotes MFA in the Digital Identity Guidelines,[32] it could further promote MFA—consistent with its longstanding risk-based and technology-neutral approach—by promoting the broad and flexible implementation of MFA, including via SMS or the PSTN, as appropriate. Specifically, NIST has indicated that it considers these authentication methods to be vulnerable (e.g., from account hijacking and SIM swap, SS7 attacks, and capture/relay attacks), and has noted that it is considering additional guidance for addressing these risks, such as mobile account tenure checks or SIM swap detection APIs.[33] However, rather than requiring prescriptive and inflexible rules with respect to a particular channel, NIST should (1) encourage

---

[29] NIST SP 1800-17, Multifactor Authentication for E-Commerce: Risk-Based, FIDO Universal Second Factor Implementations for Purchasers, NIST NCCoE, at 3 (July 2019), https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.1800-17.pdf.

[30] Multi-Factor Authentication Fact Sheet, CISA (January 2022), https://www.cisa.gov/sites/default/files/publications/MFA-Fact-Sheet-Jan22-508.pdf.

[31] *More than a Password: Protect Yourself from Malicious Hackers with Multifactor Authentication*, CISA, https://www.cisa.gov/mfa (last visited Apr. 6, 2023).

[32] NIST allows single-factor authentication only at Authenticator Assurance Level ("AAL") 1 and requires MFA for AAL2 and AAL3. SP 800-63B at 2-3; Draft SP 800-63B, at 2-3.

[33] NIST's Digital Identity Guidelines Update – Kicking off Revision 4!, NIST Information Technology Lab, at 37 (Jan. 12, 2023), https://www.nccoe.nist.gov/sites/default/files/2023-01/digital-identity-guidelines-kickoff-revision-4-presentation.pdf.

organizations to conduct risk assessments to determine what channel and/or form of MFA is most appropriate for any given context, and (2) make clear that SMS-based MFA may be used—as appropriate—based on the nature and sensitivity of information being accessed. Doing so would align with NIST's longstanding technology-neutral approach to the Cybersecurity Framework;[34] it would best promote the broad and flexible deployment of MFA, consistent with cybersecurity best practices; and it would be consistent with the risk-based approach long taken by NIST,[35] as well as other agencies.[36] In particular, SMS is an important option for deploying MFA, and while no communication channel is a perfect security, NIST should consider SMS's ongoing security enhancements and its ubiquitous nature when discussing approaches to MFA under the Digital Identity Guidelines.

Industry Works Diligently to Continue to Enhance SMS Security. Industry is well aware of the threats associated with SMS and works hard to address these threats and mitigate

[34] NIST's CSF explains that cybersecurity guidance is most effective and supports technological innovation when guidance is technology neutral. Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1, at 2, NIST (Apr. 16, 2018), https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf.

[35] Revision 3 rightly emphasizes the risk-based nature of cybersecurity. SP 800-63-3 at vi, ("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." "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." 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." 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."). Draft Revision 4 continues to direct agencies to engage in digital identity risk management processes. *See* Draft SP 800-63-4 at 23. A similar risk-based approach should be promoted for selecting a method for MFA.

[36] As the FTC recently recognized with respect to SMS-based MFA in updating its Safeguards Rules: "[i]n some cases, use of SMS text messages as a factor may be the best solution because of its low cost and easy use, if its risks do not outweigh those benefits under the circumstances. In other instances, however, the use of SMS text messages may not be a reasonable solution, such as when extremely sensitive information can be obtained through the access method being controlled, or when a more secure method can be used for a comparable price. A financial institution will need to evaluate the balance of risks for its situation." *Standards for Safeguarding Customer Information*, Final Rule, 86 Fed. Reg. 70272, 70277 (Dec. 9, 2021), https://www.govinfo.gov/content/pkg/FR-2021-12-09/pdf/2021-25736.pdf (provision set forth in 16 C.F.R. § 314).

risks. Overall, the wireless industry is committed to enhancing the security of SMS, as the security and reliability of networks is the backbone of everything that the wireless sector does.

With respect to the threat of fraudulent SIM swaps, promoting device and account security to prevent fraudulent SIM swapping is in the wireless industry's best interest, because protecting security protects customers and maintains trust in carrier networks. That said, it is critical to understand that wireless providers cannot be the only line of defense against fraudulent SIM swapping schemes; indeed, all actors across the mobile and Internet ecosystem—including financial and social media companies whose users' accounts are often targeted—must work together to thwart the bad actors that perpetrate these crimes. For its part, wireless industry tactics to combat fraud abound, and they include:

- **Account passcodes.** Providers offer SIM and wireless PINs or passcodes to protect accounts.
- **Account locking.** Providers offer customers the ability to lock or freeze their accounts to protect against unauthorized access.
- **Leveraging technology solutions to identify and combat unauthorized SIM swaps.** Providers work with partners across the ecosystem to help provide fraud detection and risk score tools, to help organizations identify and manage SIM swap risks in real time.[37]
- **MFA.** SIM swapping is deterred by using MFA when account changes are requested. While some are worried that SMS-based MFA is vulnerable to SIM swapping, the SIM swapping process itself can be protected by an initial MFA process.

[37] *See, e.g.*, *Lookup SIM Swap Overview*, Twilio, https://www.twilio.com/docs/lookup/lookup-sim-swap (last visited Apr. 7, 2023) ("Lookup SIM Swap provides real-time authoritative data, directly sourced from mobile network operators, telling you if the SIM linked to a mobile phone number has recently changed."); *Zumigo Secures Increasing Use of Mobile Banking and e-Commerce Transactions Due to COVID-19 Pandemic*, Zumigo, (July 14, 2020), https://zumigo.com/zumigo-secures-increasing-use-of-mobile-banking-and-e-commerce-transactions-due-to-covid-19-pandemic/ ("To protect against SIM hijacking or SIM swap fraud, Zumigo verifies for banks and merchants in real-time if it's safe to communicate with their customers' mobile phones during a transaction requiring user verification, or if there have been SIM or network changes to the users' mobile phone account, making the transaction risky."); *Prove Trust Score™: Fighting the Rising Threat of SIM Swap Fraud in the UK and Eliminating False Positives*, Prove (July 15, 2021), https://www.prove.com/blog/prove-trust-score-fighting-rising-threat-sim-swap-fraud-uk-eliminating-false-positives ("Trust Score is a real-time measure of a phone number's reputation that uses behavioral and phone intelligence signals to measure fraud risk and identity confidence. When a Prove client asks if a phone number is safe to send a text message to or engage with, Prove will perform many real-time checks, including a SIM swap check, to calculate a real-time Trust Score.").

- **Customer notification and reporting tools.** Providers notify customers when SIM swaps or port outs are requested to avoid fraud. Additionally, customers can report fraud using a variety of resources, such as fraud hotlines.[38]
- **Employee training.** Providers educate employees with the training necessary to identify the telltale signs of fraudulent SIM swapping and port-out requests, as well as the policies and procedures for combatting fraud.

In addition to these wireless provider practices, CTIA has published resources for wireless account protections that educate consumers about leveraging MFA, establishing a PIN, and downloading a provider's mobile app to stary abreast of security updates.[39] And consistent with the above examples, in the FCC's recent proceeding on SIM swapping,[40] the record demonstrates that wireless providers engage in ongoing threat evaluation and analysis related to authentication,[41] but, again, wireless providers cannot be the only line of defense against this ecosystem-wide issue.

---

[38] *See, e.g.*, *SIM Swapping*, Verizon, https://www.verizon.com/about/account-security/sim-swapping (last visited Apr. 7, 2023); *Account Security and Fraud Claims*, Verizon, https://www.verizon.com/about/account-security/overview#:~:text=In%20the%20unfortunate%20event%20that%20your%20account%20has%20been%20taken,any%20instances%20of%20fraudulent%20activity (last visited Apr. 7, 2023); *Online safety and cybersecurity.*, T-Mobile, https://www.t-mobile.com/privacy-center/education/online-safety-cybersecurity#:~:text=Report%20directly%20to%20the%20companies,8997%20from%20any%20other%20device (last visited Apr. 7, 2023); *Customer Care*, T-Mobile, https://www.t-mobile.com/customers/customer-care#:~:text=Our%20customer%20support%20team%2C%20including,Mobile%20phone%20number%20when%20prompted (last visited Apr. 7, 2023); *Report an unauthorized AT&T account or an account change*, AT&T, https://www.att.com/support/article/my-account/KM1159583/ (last visited Apr. 7, 2023).

[39] *Protecting Your Wireless Account Against SIM Swap Fraud,* CTIA Consumer Resources, https://www.ctia.org/protecting-against-sim-swap-fraud (last visited Apr. 6, 2023).

[40] *Protecting Consumers from SIM Swap and Port-Out Fraud*, Notice of Proposed Rulemaking, 36 FCC Rcd 14120 (rel. Sept. 30, 2021), https://docs.fcc.gov/public/attachments/FCC-21-102A1.pdf.

[41] *See, e.g.*, Comments of AT&T, WC Docket No. 21-341, at 6 (filed Nov. 15, 2021), https://www.fcc.gov/ecfs/document/11151760309724/1 ("AT&T has leveraged data analytics to develop a sophisticated risk-scoring model for certain postpaid transactions. The model assigns a real-time transaction-specific risk score to certain transactions requested by a customer, including SIM changes and port-outs. The assigned score may trigger heightened authentication requirements or additional fraud prevention and mitigation techniques . . . prior to allowing completion of the requested transaction."); Comments of T-Mobile, WC Docket No. 21-341, at 6 (filed Nov. 15, 2021), https://www.fcc.gov/ecfs/document/111594614578/1 ("T-Mobile engages in ongoing, proactive threat evaluation, and information collection on threats and fraud for internal purposes."); Comments of Verizon, WC Docket No. 21-341, at 2, 8 (filed Nov. 15, 2021), https://www.fcc.gov/ecfs/document/1115202045496/1 ("Verizon efficiently and effectively monitors, detects, and can respond to a constantly changing field of fraudulent activities, ensuring not only the protection of CPNI, but customers' other privacy and security interests as well. . . ." and it explains that it uses many of the authentication safeguards for SIM swapping and number porting described in the Notice of Proposed Rulemaking.).

With respect to the threat of SS7 attacks**,** industry is not blind to challenges that exist in legacy technology—such as SS7. However, generally speaking, the concern over SS7 is outdated. *First*, neither the SS7 protocol nor its successor Diameter protocol are widely used to deliver SMS messages on U.S. networks. Generally, U.S. providers employ the IP Multimedia Subsystem ("IMS")—an architectural framework based on the Session Initiate Protocol ("SIP")—to deliver SMS messages. While there are known security challenges with SIP as well, the wireless industry is well aware of them and is taking tangible steps to address and mitigate these issues.[42] *Second,* to the limited extent that SS7 is utilized to deliver messages (e.g., where international messaging is involved), the wireless industry has taken critical steps to address threats associated with SS7 and Diameter. Notably, the wireless industry has been implementing recommendations from relevant CSRIC reports and taking related measures to minimize SS7 and Diameter risks.[43] The record in the FCC's proceeding on Diameter also demonstrates that carriers had been taking action related to SS7 and Diameter for years.[44]

With respect to the threat of phishing, the wireless industry uses a variety of cutting-edge tools and approaches to combat fraudulent text messages, which can be a source of phishing attempts. For example, wireless providers' security and fraud prevention teams use innovative technologies, machine learning, and other spam mitigation tools to protect consumers through real-time analysis and other defense solutions.[45] Messaging applications also deploy new

---

[42] *See generally* CSRIC VII, Working Group 6 Report on SIP Security Challenges and Mitigations (Mar. 10, 2021), https://www.fcc.gov/file/20609/download.

[43] *See CTIA Statement on SS7 and FCC CSRIC Recommendations*, CTIA (2017), https://api.ctia.org/docs/default-source/default-document-library/ss7-statement-2017-final.pdf; John Marinho, *Report Recognizes Wireless Efforts to Protect Against Cyber Threats*, CTIA (Apr. 5, 2018), https://www.ctia.org/news/report-recognizes-wireless-efforts-to-protect-against-cyber-threats.

[44] *See* Comments of CTIA, PS Docket No. 18-99, at 5, 9-13 (filed Mar. 11, 2020), https://www.fcc.gov/ecfs/document/103110781117841/1.

[45] *See* Reply Comments of CTIA, CG Docket No. 21-402, at 3 (filed Dec. 9, 2022), https://www.fcc.gov/ecfs/document/1209746509660/1 (citing Comments of Competitive Carriers Association, CG

reporting tools that are unique to wireless device operating systems and provide consumers with an easy method for reporting scam text messages.[46] Wireless providers also publish consumer guidance and provide tools specifically related to phishing attacks.[47]

SMS Is Ubiquitous. In addition to industry's work to enhance SMS security, texting is user-friendly and ubiquitous, which will assist with user adoption of MFA. For example, the FTC noted in its updated Safeguards Rule that "In some cases, use of SMS text messages as a factor may be the best solution because of its low cost and easy use, if its risks do not outweigh those benefits under the circumstances."[48] Organizations should be free to weigh the ease of use of SMS for MFA against the risk of account compromise. As CISA recognizes, "any form of MFA is better than no MFA," and the ease of using SMS in MFA may be the best option in some cases or help organizations ease their way into other forms of MFA.[49]

Docket No. 21-402, at 4-9 (filed Nov. 10, 2022), https://www.fcc.gov/ecfs/document/1111678810309/1); Comments of M3AAWG, CG Docket No. 21-402, at 3-4 (filed Nov. 8, 2022), https://www.fcc.gov/ecfs/document/11081168704757/1; Comments of NetNumber, CG Docket No. 21-402, at 5-6 (filed Nov. 10, 2022), https://www.fcc.gov/ecfs/document/1110011118553/1; Comments of Professional Associations for Customer Engagement (PACE), CG Docket No. 21-402, at 2 (filed Nov. 10, 2022), https://www.fcc.gov/ecfs/document/11100708003620/1; Comments of Sinch America, CG Docket No. 21-402, at 2-4 (filed Nov. 10, 2022), https://www.fcc.gov/ecfs/document/1111531902527/1; Comments of Telesign, CG Docket No. 21-402, at 3 (filed Nov. 10, 2022), https://www.fcc.gov/ecfs/document/1109139181158/1; Comments of T-Mobile USA, Inc., CG Docket No. 21-402, at 4-7, 9 (filed Nov. 10, 2022), https://www.fcc.gov/ecfs/document/1110515408223/1; Comments of Verizon, CG Docket No. 21-402, at 2-4 (filed Nov. 10, 2022), https://www.fcc.gov/ecfs/document/1110088820229/1.

[46] *See Block, filter, and report messages on iPhone*, Apple, https://support.apple.com/guide/iphone/block-filter-and-report-messages-iph203ab0be4/ios (last visited Apr. 6, 2023); *Report Spam*, Messages by Google, https://support.google.com/messages/answer/9061432?hl=en (last visited Apr. 6, 2023).

[47] *See*, *e.g.*, *Fake Email or "Phishing"*, Cyber Aware AT&T, https://about.att.com/pages/cyberaware/ae/phishing (last visited Apr. 10, 2023); *Phishing*, Verizon, https://www.verizon.com/about/account-security/phishing (last visited Apr. 10, 2023); *Help with scams, spam, and fraud*, T-Mobile, https://www.t-mobile.com/support/plans-features/help-with-scams-spam-and-fraud (last visited Apr. 10, 2023).

[48] *Standards for Safeguarding Customer Information*, Final Rule, 86 Fed. Reg. 70272, 70277 (Dec. 9, 2021), https://www.govinfo.gov/content/pkg/FR-2021-12-09/pdf/2021-25736.pdf.

[49] Implementing Phishing-Resistant MFA Fact Sheet, CISA (Oct. 2022), https://www.cisa.gov/sites/default/files/publications/fact-sheet-implementing-phishing-resistant-mfa-508c.pdf.

In short, the decision to use SMS as a channel for MFA should be a risk-based one. SMS-based MFA is not appropriate for all contexts, and there may be circumstances where agencies or other organizations desire heightened security levels and choose not to utilize SMS-based MFA—particularly for highly sensitive transactions. However, SMS can be an appropriate channel in certain circumstances, especially because it is a ubiquitous and user-friendly approach.

V. NIST SHOULD ENSURE THAT ITS WIRELESS AUTHENTICATOR REQUIREMENTS ARE RISK-BASED.

Currently, Draft NIST SP 800-63B-4, *Digital Identity Guidelines: Authentication and Lifecycle Management* ("Draft SP 800-63B") includes guidance for wireless authenticators. Specifically, Draft SP 800-63B provides recommendations for encryption and the pairing process for two types of wireless technologies: those with an effective range of one meter or more and those with an effective range of less than one meter.[50]

Wireless authenticator security approaches are highly developed and complex.[51] NIST's discussion of requirements under the Digital Identity Guidelines appears to be incomplete and not factor in the full range of risk-based approaches that are already part of industry's best

[50] Draft SP 800-63B at 39-40.

[51] *See, e.g.*, NIST SP 800-121, (Revision 2): Guide to Bluetooth Security, NIST (May 2017), https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-121r2-upd1.pdf (SP 800-121 is NIST's Bluetooth security standard); *About Us*, Bluetooth, https://www.bluetooth.com/about-us/ (last visited Apr. 6, 2023) (The Bluetooth Special Interest Group ("SIG") is a global organization of over 38,000 companies that develops shared technical standards for Bluetooth connected devices); *see also U.S. Government Approved Protection Profile – PP-Module for Bluetooth Version 1.0*, NIAP (Apr. 15, 2021), https://www.niap-ccevs.org/profile/Info.cfm?PPID=425&id=425 ("The scope of the Bluetooth PP-Module is to describe the security functionality of Bluetooth technology in terms of [CC] and to define functional and assurance requirements for the Bluetooth capability of mobile devices and operating systems."); *U.S. Government Approved Protection Profile Protection Profile for Mobile Device Fundamentals Version 3.3*, NIAP (Sept. 22, 2022), https://www.niap-ccevs.org/profile/Info.cfm?PPID=468&id=468 ("This assurance standard describes these essential security services provided by the Mobile Device and serves as a foundation for a secure mobile architecture. . . . If the mobile device contains Bluetooth functionality (i.e., has Bluetooth hardware), the Bluetooth connectivity shall be evaluated against the PP-Module for Bluetooth.").

practices. For example, a pairing code can be a helpful security code in a variety of situations, but there are best practices in place—depending on the context—with respect to rotating and changing the code periodically, which the NIST draft does not adequately address. Rather than implementing prescriptive rules, NIST should point to existing consensus-based standards and best practices.

VI. CTIA SUPPORTS THE ADDITION OF EQUITY CONSIDERATIONS IN THE DIGITAL IDENTITY GUIDELINES.

In Draft Revision 4, NIST includes equity-based considerations in the Digital Identity Guidelines, explaining that users should not just focus on security (i.e., keeping bad actors out), but also on ensuring that the right actors have proper access.[52] For example, Draft NIST SP 800-63A-4, *Enrollment and Identity Proofing Requirements* ("Draft SP 800-63A") requires credential service providers ("CSPs") to assess elements of identity services to identify "processes or technologies that can possibly result in inequitable access, treatment, or outcomes for members of one group as compared to others."[53] Additionally, to assist organizations with their equity considerations when conducting risk assessments, NIST provides informative, non-binding guidance sections on equity considerations throughout the suite.[54] For example, Draft 800-63B states that normative requirements have been established to address certain equity issues.[55] CTIA supports these equity-based changes. The wireless industry agrees that authentication is a complex process, and organizations need to balance a variety of considerations, including privacy, security, and equity impacts.

---

[52] *See Digital Identity Guidelines - Kicking Off Revision 4! Webinar*, NIST NCCoE, at 10:54-11:22 (Jan. 12, 2023) https://www.nccoe.nist.gov/get-involved/attend-events/digital-identity-guidelines-rev-4/post-workshop-materials.

[53] Draft SP 800-63A at 19.

[54] *Id.* at 51; Draft SP 800-63B at 74.

[55] Draft SP 800-63B at 74 ("Normative requirements have been established requiring CSPs to mitigate the problems in this area that are expected to be most common.").

As NIST continues to refine Draft Revision 4, the agency should ensure that the document builds in sufficient flexibility so that users can balance commitments to equity with privacy, security, and unique organizational goals. Already, NIST rightly recognizes that there are potential tradeoffs between security, privacy, and equity. Regarding authentication and lifecycle management, NIST notes that SMS-based out-of-band authentication may not be feasible for subscribers in rural areas, since mobile service may be unavailable.[56] Further, NIST notes that some hardware-based authenticators may not be affordable for certain subscribers.[57] CTIA agrees with NIST that contextual factors will impact equity considerations, and that there are no perfect solutions. For example, Draft 800-63B explains that "[I]t is not feasible to anticipate all potential equity problems. Potential equity problems also will vary for different applications."[58] NIST is right to recognize that guidance cannot account for all scenarios, and, as a result, anticipating all equity-related concerns is a difficult undertaking. When it comes to equity, context matters.

Overall, CTIA encourages NIST to continue to ensure that the Digital Identity Guidelines provide organizations with the flexibility to address these considerations, using established risk-based principles and processes. As was echoed at NIST's recent webinar discussing equity with respect to the Digital Identity Guidelines,[59] flexibility is critically important and will help organizations provide novel solutions that properly authenticate users while also meeting equity goals.

---

[56] *Id.*

[57] *Id.*

[58] *Id.*

[59] *See Digital Identity Webinar-Digital Identity Risk Management and Assurance Level Selection*, NIST NCCoE (Mar. 2, 2023), https://www.nccoe.nist.gov/get-involved/attend-events/digital-identity-risk-management-and-assurance-level-selection/post-workshop-materials.

VII. CONCLUSION

CTIA and its members look forward to ongoing collaboration with NIST as it updates the Digital Identity Guidelines.

Respectfully submitted,

/s/ Thomas K. Sawanobori
Thomas K. Sawanobori
Senior Vice President and Chief Technology Officer

John A. Marinho
Vice President, Technology and Cybersecurity

Justin C. Perkins
Manager, Cybersecurity and Policy

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

April 14, 2023