COMMENTS OF THE AMERICAN CIVIL LIBERTIES UNION, CENTER FOR DEMOCRACY & TECHNOLOGY, ELECTRONIC PRIVACY INFORMATION CENTER, and ELECTRONIC FRONTIER FOUNDATION

to the

Transportation Security Administration, Dept. of Homeland Security

on

Minimum Standards for Driver's Licenses and Identification Cards Acceptable by Federal Agencies for Official Purposes; Waiver for Mobile Driver's Licenses

88 Fed. Reg. 60056 / Docket No: TSA-2023-002

October 16, 2023

The American Civil Liberties Union (ACLU), Center for Democracy & Technology (CDT), Electronic Frontier Foundation (EFF), and Electronic Privacy Information Center (EPIC) submit these comments in response to the Transportation Security Administration's (TSA) notice of proposed rulemaking on a REAL ID requirement waiver for state-issued mobile driver's licenses (mDLs).[1] TSA is proposing to establish a case-by-case system for exempting state mobile driver's license programs from REAL ID Act requirements and to impose an interim set of standards for mDLs drawn from various federal government information technology standards and standards proposed by private industry groups.

We urge the TSA not to shortcut the ongoing development of a privacy-preserving digital identity system by exempting mobile licenses from REAL ID requirements before such a system emerges. We ask: what's the hurry? There is no popular demand driving TSA adoption of mDLs,

[1] https://www.federalregister.gov/documents/2023/08/30/2023-18582/minimum-standards-for-drivers-licenses-and-identification-car-acceptable-by-federal-agencies-for.

and no reason to rush into incorporating them into the airline security process — especially given that doing so will have repercussions far beyond the airport context. At the same time, there are substantial risks to privacy, civil liberties, and a well-functioning mDL system created by defining standards for acceptable mDLs before all of the technology and infrastructure exists to support reliable, privacy-preserving digital identities. Even if the TSA chooses to go ahead despite risks of vendor and technology lock-in, the agency still should not rely on standards proposed by private groups like the American Association of Motor Vehicle Administrators (AAMVA) and the International Organization for Standardization (ISO).

For more than 100 years, the ACLU has been our nation's guardian of liberty, working in courts, legislatures, and communities to defend and preserve the individual rights and liberties that the Constitution and the laws of the United States guarantee everyone in this country. The ACLU takes up the toughest civil liberties cases and issues to defend all people from government abuse and overreach. The ACLU is a nationwide organization that fights tirelessly in all 50 states, Puerto Rico, and Washington, D.C., for the principle that every individual's rights must be protected equally under the law, regardless of race, religion, gender, sexual orientation, disability, or national origin.

CDT is the leading nonpartisan, nonprofit organization fighting to advance civil rights and civil liberties in the digital age. CDT shapes technology policy, governance, and design with a focus on equity and democratic values. Established in 1994, CDT has been a trusted advocate for digital rights since the earliest days of the internet.

EFF works to ensure that technology supports freedom, justice, and innovation for all the people of the world. EFF is a non-profit organization with more than 30,000 members. EFF

regularly advocates before administrative agencies, courts, and legislatures in support of free speech, data privacy, and other rights at the digital frontier.

EPIC is a public interest research center in Washington, D.C. EPIC was established in 1994 to focus public attention on emerging privacy and related human rights issues, and to protect privacy, the First Amendment, and constitutional values. EPIC has a particular interest in preserving the Privacy Act safeguards enacted by Congress.[2] EPIC also has an ongoing interest in CBP and DHS's use of machine learning and artificial intelligence on the databases containing personal information as well as DHS's use of biometrics, particularly the use of facial recognition.[3]

I. Background

The REAL ID Act of 2005 directed the Secretary of the Department of Homeland Security (DHS) to oversee a process compelling states to standardize both the information contained on driver's licenses and other ID cards and the process for issuing those cards. Under the REAL ID Act, federal agencies are not permitted to accept driver's licenses unless they contain the data fields required by federal law, and meet security and issuance standards in DHS

[2] *See, e.g.*, Comments of EPIC to the Department of Homeland Security, Correspondence Records Modified System of Records Notice (Dec. 23, 2011), http://epic.org/privacy/1974act/EPIC-SORN-Comments-FINAL.pdf; Comments of EPIC to the Department of Homeland Security, 001 National Infrastructure Coordinating Center Records System of Records Notice and Notice of Proposed Rulemaking, (Dec. 15, 2010), http://epic.org/privacy/fusion/EPIC_re_DHS-2010-0086_0085.pdf; Comments of EPIC to the Department of Homeland Security, Terrorist Screening Database System of Records Notice and Notice of Proposed Rulemaking, (Feb. 22, 2016), https://epic.org/apa/comments/EPIC-Comments-DHS-TSD-SORN-Exemptions-2016.pdf.

[3] *See e.g.*, Comments of EPIC to the Transportation Security Administration, Intent to Request Revision of Agency Information Collection Activity Under OMB Review: TSA PreCheck (June 22, 2020), https://epic.org/apa/comments/EPIC-TSA-PreCheck-FRT-Comment-June2020.pdf; Comments of EPIC to the Department of Homeland Security, Agency Information Collection Activities: Biometric Identity, (Jul. 24, 2018), https://epic.org/documents/agency-information-collection-activities-biometric-identity/.

regulations.[4] In the nearly 20 years since, many states alongside civil society groups resisted the imposition of the REAL ID Act, and only recently have all states prepared to issue REAL ID compliant licenses.[5] As a result, the mandate for federal agencies, including TSA, to accept only REAL ID compliant cards has been stalled since the Act's passage. TSA now anticipates a May 7, 2025 deadline for REAL ID enforcement to begin, though the agency has repeatedly delayed similar deadlines in the past.[6]

But the REAL ID Act only prescribes requirements for physical ID cards; it is silent about digitized credentials, like a mobile driver's license (mDL). In 2020, the REAL ID Modernization Act was passed, giving the federal agencies the authority to accept mDLs only if they have been "issued in accordance with regulations prescribed by the Secretary."[7] The REAL ID Modernization Act makes clear that mDLs must be subject to the same applicable standards as physical licenses, and that DHS must go through a regulatory process before accepting any mDL. As the TSA notes, current REAL ID regulations do not address mDLs. *See* 6 C.F.R. part 37.

Now, various states have started issuing mobile driver's licenses, and other states are exploring the proposition. Although some states like Louisiana have already made mDLs available, there is little consensus on the details of how an mDL system should be designed.

---

[4] REAL ID Driver's Licenses and Identification Cards, 6 C.F.R. § 37 (2023), https://www.ecfr.gov/current/title-6/chapter-I/part-37.

[5] *See e.g.*, Allie Bohm, *Yes, the States Really Reject Real ID*, ACLU (Mar. 27, 2012), https://www.aclu.org/news/national-security/yes-states-really-reject-real-id; EPIC Comments to DHS Information Collection on State Compliance with REAL ID (Jun. 17, 2019), https://epic.org/wp-content/uploads/apa/comments/EPIC-Comments-DHS-REAL-ID-June2019.pdf; EFF, "Real ID," https://www.eff.org/issues/real-id.

[6] *DHS announces extension of REAL ID full enforcement deadline*, TSA (Dec. 5, 2022), https://www.tsa.gov/news/press/releases/2022/12/05/dhs-announces-extension-real-id-full-enforcement-deadline.

[7] REAL ID Act of 2005, as amended, § 201 (1)(B), [Public Law 109–13] [As Amended Through P.L. 116–260, Enacted December 27, 2020], https://www.govinfo.gov/content/pkg/COMPS-16376/pdf/COMPS-16376.pdf.

Several states have adopted the ISO/IEC mDL technical standard, although several key elements of that standard are still under development.

In this proposed rulemaking, TSA would not enact permanent regulations to provide states lasting clarity on how to design and implement mobile driver's license systems. Instead, the agency proposes to establish a state-by-state waiver process where each mDL implementation will be measured against 19 technical standards incorporated by reference (IBR) in the rulemaking. At some time in the future, TSA intends to undertake a second phase rulemaking to establish the final regulations needed for federal agencies to accept mDLs. In the meantime however, not just TSA, but agencies across the federal government will be authorized to accept mDLs from states that have passed the waiver process.

II. There is no urgency for TSA to accept mDLs now, when the technology and standards are still developing.

The NPRM cites a variety of concerns motivating TSA to move forward with this "multi-phased rulemaking" even though the agency admits that it is "premature to issue final, comprehensive requirements" because significant technologies and associated technical standards for mDLs are likely to be developed in the near future.[8] TSA's stated concerns are conflicting and the agency's actions in this rulemaking run counter to those concerns.

a. *The current state of digital identity is immature and cannot support even interim adoption of mDLs in a privacy-preserving manner.*

First, the agency argues that because states are moving forward with mDLs now, there is a substantial risk that states will develop a patchwork of mDL systems that may lack uniform

[8] 88 Fed. Reg. 60058, "At the same time, however, TSA believes it is premature to issue final, comprehensive requirements for mDLs given the rapid pace of innovation in this nascent market, and the multiple emerging industry and government standards and guidelines necessary to ensure mDL privacy and security that are still in development."

standards and may not be interoperable.[9] While this concern is real, the agency's proposed waiver system will do little to address that concern and understates TSA's role in pushing states to adopt mDLs. As the rulemaking itself states, "it is premature to issue final, comprehensive requirements for mDLs given the rapid pace of innovation in this nascent market, and the multiple emerging industry and government standards and guidelines necessary to ensure mDL privacy and security that are still in development."[10]

TSA recognizes that sufficient standards and available technologies to guarantee privacy for mDL users do not yet exist. The core of TSA's proposed mDL design is the ISO/IEC standard for mobile driver's licenses, currently ISO/IEC 18013–5:2021, but these standards are incomplete, not readily accessible or accountable to the public, and currently govern only some aspects of an mDL digital identity system. The current standards govern how an mDL should transmit information from the phone to the verifying party (e.g. the TSA agent in the airport), and they govern how an mDL reader should verify the validity of the license.[11] But the standards do not govern provisioning (how states install an mDL on a phone). They do not provide sufficient protections for data storage on the phone, sufficient guidance for mobile wallet design or user experience, or accountable constraints that would limit invasive or unwarranted requests from abusive mDL verifiers. Standards for the issuing authority to load mDLs onto a phone are in development as the ISO/IEC 23220 series.[12] Standards for digital wallet privacy, security, and consent management are even less developed.

---

[9] *Id.*
[10] 88 Fed. Reg. 60058, https://www.govinfo.gov/content/pkg/FR-2023-08-30/pdf/2023-18582.pdf - page=3.
[11] Am. Ass'n of Motor Vehicle Administrators, Mobile Driver's License Implementation Guidelines, r 1.2 at 7-8 (Jan. 2023), https://www.aamva.org/getmedia/b801da7b-5584-466c-8aeb-f230cef6dda5/mDL-Implementation-Guidelines-Version-1-2_final.pdf.
[12] 88 Fed. Reg. 60064, https://www.govinfo.gov/content/pkg/FR-2023-08-30/pdf/2023-18582.pdf#page=9.

While the ISO standard for mDL readers is final, it still leaves major open questions such as whether the issuer should be directly involved with each verification, how an mDL reader's own identity should be structured, and how it should prove to the mDL that it is authorized to ask for credentials in the first place. Other standards that might govern the device, such as NIST's FIPS and Digital Identity Guidelines, are likely to be updated soon. mDL reader lock-in could leave states with tech they can't use or constrain the available options for mDL development in the future, running counter to TSA's stated interest in speeding up technology development.

If the TSA were to grant waivers to multiple states that use different, incompatible subsets of ISO 18013–5:2021, would each TSA checkpoint be obliged to purchase multiple mDL readers, and each TSA agent be trained to operate each one of them and to know when to use one rather than another? Or would one TSA checkpoint accept an mDL that would be rejected by another checkpoint? There is no indication in the prospective rulemaking that the TSA will contemplate these risks as part of the waiver granting process. To the extent that the waiver-granting process does consider mutual compatibility, the decisions made by the first grantee will effectively impose constraints on subsequent applications.

The situation in the mobile wallet market is grounds for even greater concern. The market is currently divided between companies advocating for a more open and fully interoperable set of wallets through the Open Wallet Foundation, and single actors like Apple[13] and Idemia[14] that are looking to carve out more exclusive positions.[15] Without endorsing any of these actors, we note

[13] For example, Georgia's mDL is currently only available through the Apple Wallet.
[14] Oklahoma's mDL can only be loaded onto Idemia's proprietary mobile wallet, on both iOS and Android phones. OK Dep't of Pub. Safety, Mobile ID (Jul. 21, 2021), https://oklahoma.gov/dps/real-id/mobile-id.html.
[15] Gordon Graham, Why the World Needs an Open Source Digital Wallet Right Now, Open Wallet Foundation (Feb. 2023), https://project.linuxfoundation.org/hubfs/LF%20Research/OpenWallet%20Open%20Digital%20Wallet%20-%20Report.pdf?hsLang=en.

that significant disparities in how mobile wallets are designed and how they interact with smartphones have not been resolved. The fact that the TSA has already partnered with Apple in several states also brings into question the amount of influence proprietary options have over open solutions.[16] Such concerns should be addressed before TSA puts more pressure on states to issue mDLs, especially because there is limited information available to states to allow them to design mobile credentials that can be loaded into any properly developed wallet. And for license-holders, this situation provides neither the protection of publicly vetted and tested wallets subject to strong standards nor the opportunity to select the most privacy-preserving wallet from a variety of options. This is not the right time to tip the scales towards wider adoption of mDLs.

More broadly, even the incomplete ISO standard is only one of a number of approaches to digital identity that are being developed around the world. Others, such as the W3C Verifiable Credentials standards, are regarded as superior by many in the digital identity community, and should be given time to further evolve and ripen before DHS pushes a standard that is likely to become locked in.[17]

In the absence of both strong technical standards and a supporting infrastructure to ensure that digital credentials are managed properly; privacy, fraud, and misuse harms will undoubtably occur. The TSA should not provide states with more incentives to adopt mDLs before the infrastructure is in place for the public, government agencies, and corporations that might accept

[16] See e.g., Alessandro Mascellino, *TSA plans mDL acceptance for airports, starting with Apple*, Biometric Update (Dec. 22, 2021), https://www.biometricupdate.com/202112/tsa-plans-mdl-acceptance-for-airports-starting-with-apple; TSA, Press Release: TSA enables Maryland residents to use mobile driver's license or state ID for verification at Baltimore/Washington International and Reagan National Airports, tsa.gov (May 25, 2022), https://www.tsa.gov/news/press/releases/2022/05/25/tsa-enables-maryland-residents-use-mobile-drivers-license-or-state.

[17] *See* EPIC and ACLU Comments on NIST's 2023 Digital Identity Draft Guidelines § III at 10-11 (Apr. 14, 2023), https://epic.org/documents/epic-and-aclu-comments-on-nists-2023-digital-identity-draft-guidelines/; EPIC Comments on DHS RFI on mDLS (Jul. 30, 2021), https://epic.org/wp-content/uploads/apa/comments/EPIC-MDL-RFI-Comments-July-2021.pdf.

a digital ID to fully support responsible widespread use. There has already been at least one case of mDL-based fraud, when a Louisiana man managed to load a currently incarcerated person's driver's license onto his own phone, and then used the credential to open bank accounts at 7 different banks and obtain several different loans.[18] There are real harms to rushing ahead with a digital identity system, including risks of novel forms of financial fraud and reputational harm.

With its nationwide reach and enormous power to define the standards for federal acceptance of a digital identity, and the current state of the technology, the agency should not be leading the emergence of a digital ID system.

b. ***An American identity standard must not only be secure and privacy-protective, but also completely open.***

It is also vital that any identity system adopted as a standard in the United States, and recognized by the TSA, be based on public and open standards that are free from dominance by any particular private companies and are not encumbered by patents without royalty-free licensing commitments. There must be no one corporation, or small handful of corporations, that Americans are *de facto* required to deal with in order to participate in a digital identity system. Standards must give people a multiplicity of choices. Unfortunately, the proposed rule does not appear to reflect this important principle. We have grave concerns over reports that the TSA has entered into contracts that give Apple Inc. significant power over the implementation of mDL checkpoints. Documents obtained by a journalist indicate, for example, that for unclear and

[18] Peter Strozniak, *Louisiana Man Uses Digital Driver's License to Defraud Credit Unions & Banks*, Credit Union Times (Mar. 16, 2023), https://www.cutimes.com/2023/03/16/louisiana-man-uses-digital-drivers-license-to-defraud-credit-unions-banks/.

puzzling reasons the TSA signed over to Apple the agency's patents governing the operation of its airport mDL checkpoints.[19]

The market for digital wallet apps is one example of the dangers of an insufficiently open digital ID system. In most states that have rolled out mDLs, there is only one option available. Louisiana, for example, uses a proprietary app called LA Wallet from a single third-party vendor, Envoc.[20] Louisiana's wallet system is tied into the state's welfare system, Covid-19 vaccine registry, hunting and firearms license system, and may even hold medical information. Georgia, meanwhile, will only issue an mDL onto an Apple brand phone or smartwatch through the Apple Wallet app.[21] The proposed rulemaking would do little to ensure that individuals have enough choices to ensure they can select a privacy-preserving wallet.

c. *Demand for mDLs is overstated and does not justify this interim rulemaking.*

TSA also argues that it needs to go forward with this rulemaking now because "anecdotal information and fragmented reporting indicates that mDLs are rapidly gaining public acceptance."[22] But the weight of the evidence leans the opposite direction. Only one state that rolled out mDLs has had substantial public sign-on, and that is because of an unrelated state law requiring identity verification to view pornography. The TSA relies on Louisiana's substantial upticks in downloads of its mobile wallet app in the past few years, but that demand occurred for state-specific reasons. Louisiana used its mobile wallet for certain types of welfare benefits

[19] Jason Mikula, *Apple's Homeland Security Deal Yields Checkpoint, KYC, Voter ID Patents, Documents Suggest,* Fintech Business Weekly (Sept. 11, 2022), https://fintechbusinessweekly.substack.com/p/apples-homeland-security-deal-yields.
[20] La. Div. of Admin., LA Wallet, (last accessed Oct. 11, 2023), https://www.doa.la.gov/doa/ots/tech-spotlight/la-wallet/.
[21] Ga. Dep't of Driver Serv., GA Digital Driver's License FAQs, (last accessed Oct. 11, 2023), https://dds.georgia.gov/mdl-faqs.
[22] 88 Fed. Reg. 60062, https://www.govinfo.gov/content/pkg/FR-2023-08-30/pdf/2023-18582.pdf#page=7.

during the Covid-19 pandemic, and now individuals in the state need to load their credentials onto the app to access pornography sites.[23] Even so, the evidence only reflects how many people downloaded the app, not how many went through the full process to get a digital credential loaded onto their phones. There is no evidence that people are clamoring to use their digital credentials at TSA checkpoints, the TSA is clear that travelers still need to carry a physical copy of a driver's license to travel.[24] A non-existent public demand for mDLs cannot support this interim rulemaking.

Nor do the TSA's own needs merit urgency in the adoption of digital identity technology. Because checking IDs is not a chokepoint in the airline security system, a move to mDLs will not speed the throughput at airline security checkpoints to help deal with increasing passenger volume, and in any case the whole enterprise of verifying IDs has a very dubious relationship to the security of aviation.[25] That means that any additional risk posed by humans or Credential Authentication Technology (CAT) machines accepting false physical identity cards is very low. The lack of importance of an mDL in the airport context is especially true since, for the

[23] Lindsay McKenzie, *Digital driver's license downloads soar in Louisiana amid porn restriction*, StateScoop (Jan. 4, 2023), https://statescoop.com/louisiana-porn-restriction-digital-drivers-license-downloads/.

[24] 88 Fed. Reg. 60067, https://www.govinfo.gov/content/pkg/FR-2023-08-30/pdf/2023-18582.pdf#page=12 "To avoid this issue, TSA strongly urges all mDL holders to carry their physical REAL ID cards in addition to their mDLs. This will ensure that mDL holders are not disenfranchised from REAL ID uses if a Federal agency does not accept mDLs. Indeed, TSA has long advised that passengers who choose to present mDLs in TSA checkpoint testing must continue to have their physical cards readily available in the event that a TSA officer requires such identification."

[25] If TSA was primarily concerned with increasing security throughput, various design and management changes to physical screening have been tested that could reduce wait times without privacy and civil liberties concerns. *See e.g.*, Stef Janssen et al., *Data-Driven Analysis of Airport Security Checkpoint Operations*, 7 Aerospace 69 (2020), https://www.mdpi.com/2226-4310/7/6/69/htm (finding that a dedicated lane designed for passengers with disabilities and other slower-moving groups improves throughput up to 12 percent).

foreseeable future, as the TSA acknowledges, fliers are expected to have a physical credential as a backup anyway.[26] Nobody will be spared from having to carry their plastic license.

The TSA's desire, the agency says, is "to accommodate and foster the rapid pace of mDL innovation."[27] But TSA should not be sitting in the driver's seat on developing nationwide digital identity systems, and certainly should not be pushing for these systems to expand before they are ready. Without accompanying legal safeguards, technical standards, and support infrastructure any such system will not meet TSA's stated goals.

III. TSA risks unintentionally triggering early technology lock-in by accepting mDLs before standards are fully developed, precisely the harms TSA seeks to avoid.

TSA claims that absent an interim rulemaking and waiver process, states will not have enough guidance to implement privacy-protective and interoperable mDLs. The agency foregrounds valid concerns about vendor and technology lock-in leaving states stuck with costly and ineffective technology that won't align with future standards. But those precise concerns suggest the need to slow the rollout of mDLs, not to start using a system that hasn't yet matured. We should also learn from the recent history of rushing to adopt new technology over concerns of perceived harm if they are not implemented as soon as possible.[28]

We applaud the TSA for seeking to "encourage the development of mDLs with a higher level of security, privacy, and interoperability."[29] We likewise applaud the agency for its concern

[26] 88 Fed. Reg. 60067 "To avoid this issue, TSA strongly urges all mDL holders to carry their physical REAL ID cards in addition to their mDLs. This will ensure that mDL holders are not disenfranchised from REAL ID uses if a Federal agency does not accept mDLs. Indeed, TSA has long advised that passengers who choose to present mDLs in TSA checkpoint testing must continue to have their physical cards readily available in the event that a TSA officer requires such identification."
[27] 88 Fed. Reg. 60057.
[28] *See for example*, the costly proprietary application Excelsior, adopted by New York State for vaccine credentials without much impact. Sharon Otterman, *New York's Vaccine Passport Could Cost Taxpayers $17 Million*, N.Y. Times (June 9, 2021), https://www.nytimes.com/2021/06/09/nyregion/excelsior-pass-vaccine-passport.html.
[29] 88 Fed. Reg. 60058, https://www.govinfo.gov/content/pkg/FR-2023-08-30/pdf/2023-18582.pdf#page=3.

that individual states may choose identity solutions with insufficient privacy safeguards. But given the feverish pace of development of identity technologies, the TSA is more likely to short-circuit the emergence of a strong privacy-protective standard than it is to advance a good digital identity system.

While the TSA professes to recognize the immaturity of the current identity landscape, and stresses the interim nature of its proposed approach, that approach is likely to end up strongly guiding the development of a locked-in identity system. After TSA finalizes this rulemaking, the agency will need to buy more mDL readers for its airport security stations, and other federal agencies may likewise begin purchasing readers. States will also see more TSA action as motivation to purchase their own systems, leading to more widespread adoption at a point when the market is not fully developed.

IV. TSA should be careful not to overstep its regulatory authority under the REAL ID Modernization Act by adopting interim standards.

The Real ID Modernization Act, 49 U.S.C. 30301 note, authorizes the Secretary of the Department of Homeland Security to promulgate standards to accept Real-ID compliant mDLs. The text of the bill makes clear that the Modernization Act was intended to facilitate federal agencies accepting mobile driver's licenses only with the issuance of regulations governing the process. An interim waiver process fails to comply with this directive, potentially putting DHS outside the bounds of authority granted to the agency. In addition, we note that the TSA is at best an awkward fit to implement this directive, which was assigned specifically to the Secretary.

Under the Real ID Act of 2005 and the Modernization Act of 2021, the Secretary of DHS is directed to certify that driver's licenses, including electronically stored driver's licenses, are in compliance with minimum issuance and documentation standards covering information included

on the card and security features.[30] Mobile driver's licenses are not the same as physical licenses, which TSA currently accepts even if they are not REAL ID compliant. The Modernization Act is silent as to whether TSA may even subject mDLs to a waiver procedure. The statute requires that any "driver's licenses stored or accessed via electronic means, such as a mobile or digital driver's licenses" must have been "issued in accordance with regulations prescribed by the Secretary". While such final regulations are forthcoming, the TSA should be careful not to accept mDLs that have only been through an interim waiver process, as such a process may not meet the agency's legislative mandate.

V. TSA's 19 chosen standards are not sufficient to guarantee privacy and often display a serious lack of transparency.

The TSA proposes to incorporate by reference (IBR) 19 standards that run the gamut from secretive privately developed standards and industry guidance to long-standing federal guidance documents that were not written with digital identity systems in mind.

The ISO/IEC standard that the TSA proposes to incorporate into federal regulations was developed by a secret committee within the ISO whose American members seem to consist primarily of representatives of corporations, the American Association of Motor Vehicles, and government agencies. We do not know what foreign authoritarian governments may also have been involved in formation of the standard, since ISO, a private entity, refuses to make public the members of this committee, and the members are bound by non-disclosure agreements not to reveal the details of its deliberations or the membership list. Even the text of the standard itself is copyrighted, not available to the public without a substantial fee, and generally very difficult to obtain.

[30] REAL ID Act of 2005, as modified, 49 U.S.C. 30301 note.

Repeated requests by some groups, such as the Identity Project, to view a copy of these standards in order to comment upon them, were reportedly not honored. While the notice claims that the American National Standards Institute is providing temporary public access to the ISO/IEC 18013–5:2021 standard, it has not done so in a way that enables effective review. Attempts by some of our organizations to even load the standards on a modern computer failed completely. As noted by the DC Court of Appeals, these "reading rooms" do not provide convenient access or allow the functionality necessary for review (downloading, searching, printing, etc.).[31] Accessibility failures encumber or prevent access altogether to people with print disabilities.[32]

The American Association of Motor Vehicles published a set of "Mobile Driver's License Implementation Guidelines" for states implementing the ISO/IEC mDL standard. AAMVA's guidance mainly duplicates the ISO standard, and includes policy decisions that, because AAMVA is also a private organization, have likewise not been subject to a proper public comment process or other public input. For example, the AAMVA standard follows the ISO standard in allowing a phone-home credential verification method, also known as the "server retrieval" method.[33] But after urging from EPIC, EFF and the ACLU, the TSA laudably stated in this NPRM that "TSA does not believe server retrieval mode is appropriate for Federal

[31] Am. Soc'y for Testing & Materials v. Public.Resource.Org, Inc., No. 22-7063 at 6 (D.C. Cir. 2023), https://www.cadc.uscourts.gov/internet/opinions.nsf/0/5A2E1191A4B2D49785258A28004F2532/$file/22-7063-2016393.pdf.
[32] Blake E. Reid, Amicus Brief of Prime Access Consulting Inc. in support of appellee Public.Resource.Org, Inc. (Dec. 2022), https://www.eff.org/document/amicus-brief-prime-access-consulting.
[33] Mobile Driver's License Implementation Guidelines, r1.2, AAMVA at 7, 9, 30 (Jan. 2023), https://www.aamva.org/getmedia/b801da7b-5584-466c-8aeb-f230cef6dda5/mDL-Implementation-Guidelines-Version-1-2_final.pdf.

acceptance for official purposes at this time."[34] But states remain free to adopt a phone-home mDL implementation that creates greater risks of centralized tracking, which should be avoided in the design of any mDL system.[35]

In another example, AAMVA has decided that "Flash pass" use of mDLs (using the technology to display a human-readable version of an ID) is not permitted under their guidelines that are proposed be incorporated into federal regulation. AAMVA argues that "flash pass" is not as secure — but that denies verifiers the opportunity to decide for themselves whether they are satisfied with a lesser level of security if they deem that to be an adequate security/convenience tradeoff in some circumstances. Whatever the right answer is, there was no public discussion on whether that option ought to be provided. AAMVA made the decision itself — and the TSA would extend that decision to all Americans.

Why is this document, created by a private, non-governmental entity, being incorporated as official US policy? It contains many decisions that are questionable and that have not been democratically decided or even subject to public comment and review. This is no way to make policy, especially on such a momentous matter as the identity system that Americans will have to live under. Technical standards may be useful to incorporate by reference when those standards were developed through an open, multi-stakeholder process and where that process was procedurally legitimate and included adequate participation from the public and from public-interest and advocacy organizations. Our organizations regularly engage in such open processes for technical standard-setting for the Internet and the Web, specifically to bring full review of the

[34] 88 Fed. Reg. 60072, https://www.govinfo.gov/content/pkg/FR-2023-08-30/pdf/2023-18582.pdf#page=17.
[35] Jay Stanley, Identity Crisis: What Digital Driver's Licenses Could Mean for Privacy, Equity, and Freedom, ACLU at 12 (May 2021), https://www.aclu.org/report/identity-crisis-what-digital-drivers-licenses-could-mean-privacy-equity-and-freedom.

implications for privacy and civil liberties of technologies that may be foundational. But neither those procedural nor substantive protections are present in this particular standard that the TSA would effectively endorse. The implications of the TSA's decisions here potentially reach far beyond the airport context, extending to the process for how people present ID in every small town and city in America for decades to come.

The remaining standards are a piecemeal assembly of existing requirements that were not developed for the specific challenge of mDL use and are often in the process of being updated.

1. The National Cybersecurity Incident Response Plan (2016) is currently under review and will be updated in 2025. Per a recent directive from the White House, the National Cybersecurity Strategy Implementation Plan, the Cybersecurity and Infrastructure Security Agency (CISA) is going through a process of update the Incident Response Plan. The current version of the Incident Response Plan is outdated, and does not foreground digital identity issues, which have become a much more pressing concern in the last decade. Directing states to build their systems around an old incident response plan instead of waiting for newer guidance is likely to result in outdated cybersecurity practices that will expose people to greater risks of data breach and identity theft.

2. NIST's Digital Identity Guidelines are currently under review and will be updated in late 2024. The Guidelines set baseline technical requirements for federal agencies to implement digital identity services. These guidelines are the core of how agencies assess their digital ID systems, but they are currently under revision because the 2017 Guidelines do not account for the rapid development of digital identity systems. Relying on the 2017 Guidelines for a new digital identity system not only risks developing a system that is outdated at the time of its creation, but also exposes the public to privacy and security harms that could be avoided with newer guidance.

3. Many of the Federal Information Processing Standards (FIPS) are slated for review soon. The standards for cryptographic hashing are a good example. The TSA proposes to IBR both NIST's FIPS 180-4, Secure Hash Standard (SHS) (August 4,

2015).[36] But NIST is in the process of offering a significant update to FIPS 180-4 to address known weaknesses in one of the cryptographic hashing functions approved in this standard.[37] The removal of SHA-1 is expected to result in the publication of FIPS 180-5 in the coming year, which will supersede FIPS180-4.[38] While sophisticated IT departments should already be avoiding SHA-1, incorporating FIPS 180-4 without more explicit guidance creates the risk that some state agencies will adopt outdated technologies.

Another set of TSA's chosen standards, the Digital Signature Standards, FIPS 186-5, are current but are explicitly not future-proofed.[39] As NIST recognizes, the standard approves of public key signing algorithms like RSA, ECDSA, and EdDSA that will be vulnerable to attacks when a quantum computer is developed.[40] NIST already has standards in the works for post-quantum cryptography public-key algorithms that would provide substantially more protection.[41] But these newer algorithms are not yet finalized, and are not considered in the TSA's current interim regulations, potentially leaving states with old tech if TSA incorporates the post-quantum standards in the next round of this rulemaking. Again, newer standards are imminent so locking states into older guidance makes little sense.

None of these critiques suggest that agencies should not generally rely on NIST's guidance right now, but rather that for the rollout of a new set of digital identity systems, there are substantial concerns with relying on older standards when new ones are imminent. Any mDL system that is

[36] Available at https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.202.pdf
[37] Computer Security Resource Center, *NIST Transitioning Away from SHA-1 for All Applications*, NIST (Dec. 15, 2022), https://csrc.nist.gov/news/2022/nist-transitioning-away-from-sha-1-for-all-apps.
[38] Computer Security Resource Center, *Decision to Revise FIPS 180-4, Secure Hash Standard (SHS)*, NIST (Mar. 7, 2023), https://csrc.nist.gov/news/2023/decision-to-revise-fips-180-4.
[39] FIPS 186-5, Digital Signature Standard (DSS) (Feb. 23, 2023), https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.186-5.pdf.
[40] *Id*. at 1.
[41] Computer Security Resource Center, *PQC Standardization Process: Announcing Four Candidates to be Standardized, Plus Fourth Round Candidates*, NIST (Jul. 5, 2022), https://csrc.nist.gov/News/2022/pqc-candidates-to-be-standardized-and-round-4, Computer Security Resource Center, *Post-Quantum Cryptography: Digital Signature Schemes: Workshops and Timeline*, NIST (Sept. 11, 2023), https://csrc.nist.gov/Projects/pqc-dig-sig/standardization/workshops-and-timeline.

eventually adopted should be relatively future-proof so that such a widespread system is usable for many years with only minor technical revisions. Absent a properly future-proofed system, people will lose trust in mDLs and many individuals will be left relying on outdated and vulnerable technology.

Conclusion

We urge the TSA not to go forward with this interim step that will expand the use of mDLs without concurrent privacy safeguards. In the medium term, the TSA should continue to evaluate whether mDLs serve a substantial purpose for in-person identity verification and whether the ISO/IEC standard is the best available option. Finally, the TSA should not take a role actively advancing mDLs, at the very least until the needed standards are complete.

Signed,

Jay Stanley
Senior Policy Analyst
ACLU

Jake Wiener
Counsel, Project on Surveillance Oversight
Electronic Privacy Information Center

Nick Doty
Senior Technologist
Center for Democracy & Technology

Alexis Hancock
Director of Engineering
Electronic Frontier Foundation