DEPARTMENT OF HOMELAND SECURITY

6 CFR Part 37

[Docket No. TSA–2023–0002]

RIN 1652–AA76

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

AGENCY: Transportation Security Administration (TSA), Department of Homeland Security (DHS).

ACTION: Final rule.

SUMMARY: The Department of Homeland Security (DHS) is amending the REAL ID regulations to waive, on a temporary and State-by-State basis, the regulatory requirement that mobile or digital driver's licenses or identification cards (collectively ''mobile driver's licenses'' or ''mDLs'') must be compliant with REAL ID requirements to be accepted by Federal agencies for official purposes, as defined by the REAL ID Act, when full enforcement of the REAL ID Act and regulations begins on May 7, 2025.

DATES: *Effective date:* This rule is effective November 25, 2024.

Incorporation by Reference: The incorporation by reference of certain material listed in the rule is approved by the Director of the Federal Register as of November 25, 2024. The incorporation by reference of certain other material listed in the rule was approved by the Director of the Federal Register as of January 14, 2016.

FOR FURTHER INFORMATION CONTACT:

Technical questions: George Petersen, Senior Program Manager, REAL ID Program, Enrollment Services and Vetting Programs, Transportation Security Administration; telephone: (571) 227–2215; email: *george.petersen@tsa.dhs.gov.*

Legal questions: Anurag Maheshwary, Attorney Advisor, Office of Chief Counsel, Transportation Security Administration; telephone: (571) 227–4812; email: *anurag.maheshwary@tsa.dhs.gov.*

SUPPLEMENTARY INFORMATION:

Availability of Rulemaking Document

You can find an electronic copy of this rulemaking using the internet by accessing the Government Publishing Office's web page at *https://www.govinfo.gov/app/collection/FR/* to view the daily published **Federal Register** edition or accessing the Office of the Federal Register's web page at *https://www.federalregister.gov.* Copies are also available by contacting the individual identified for ''Technical Questions'' in the **FOR FURTHER INFORMATION CONTACT** section. Make sure to identify the docket number of this rulemaking.

Abbreviations and Terms Used in This Document

AAMVA—American Association of Motor Vehicle Administrators
CA/Browser Forum—Certification Authority Browser Forum
CISA—Cybersecurity and Infrastructure Security Agency
DHS—U.S. Department of Homeland Security
EDL—Enhanced driver's license and identification card
FIPS—Federal Information Processing Standards
HSM—Hardware security module
IBR—Incorporation by reference or Incorporate by reference
IEC—International Electrotechnical Commission
ISO—International Organization for Standardization
IT—Information technology
mDL—Mobile driver's license and mobile identification card
NIST—National Institute for Standards and Technology
NPRM—Notice of proposed rulemaking
OFR—Office of Federal Register
OMB—Office of Management and Budget
PUB—Publication
RFI—Request for information
SP—Special publication
TSA—Transportation Security Administration

Table of Contents

I. Executive Summary

A. Purpose of This Rulemaking

This rule is part of an incremental, multi-phased rulemaking that will culminate in the promulgation of comprehensive requirements that enable States to issue mobile driver's licenses and mobile identification cards (collectively ''mDLs'') that comply with the REAL ID Act of 2005 (''REAL ID Act'' or ''Act'') and regulations [1] [hereinafter ''REAL ID-Compliant'']. In this first phase, the Transportation Security Administration (TSA) is making two changes to the current regulations in 6 CFR part 37, ''REAL ID Driver's Licenses and Identification Cards.'' First, TSA is adding definitions for, among others, mobile driver's licenses and mobile identification cards. These definitions provide a precise explanation of those terms as referenced in the REAL ID Act, which applies to only State-issued driver's licenses and State-issued identification cards.[2] Any other types of identification cards, such

[1] The REAL ID Act of 2005, Division B Title II of the FY05 Emergency Supplemental Appropriations Act, as amended, Public Law 109–13, 119 Stat. 302 (May 11, 2005) (codified at 49 U.S.C. 30301 note) [hereinafter ''REAL ID Act'']; 6 CFR part 37. Effective May 22, 2023, authority to administer the REAL ID program was delegated from the Secretary of Homeland Security to the Administrator of TSA pursuant to DHS Delegation No. 7060.2.1.

[2] *See* sec. 201 of the REAL ID Act (defining a ''driver's license'' to include ''driver's licenses stored or accessed via electronic means, such as mobile or digital driver's licenses, which have been issued in accordance with regulations prescribed by the Secretary''; mirroring definition for ''identification card'').

as those issued by a Federal agency, or commercial, educational, or non-profit entity, are beyond the scope of the REAL ID Act and regulations, and hence this rulemaking, because they do not meet the definition of driver's license or identification card as defined by the REAL ID Act. The definition of ''mDL'' as used in this rulemaking is limited strictly to the REAL ID Act and regulations and does not include ''mDLs'' as defined by other entities.

Second, TSA is establishing a temporary waiver process that permits Federal agencies to accept mDLs for official purposes,[3] as defined in the REAL ID Act and regulations, on an interim basis when full enforcement begins on May 7, 2025,[4] but only if TSA has issued a waiver to the State. To qualify for the waiver, this final rule requires States to (1) be in full compliance with all applicable REAL ID requirements as defined in subpart E of this part, and (2) submit an application demonstrating that they meet the requirements specified in this rule, which are drawn from 19 industry standards and government guidelines. The rulemaking incorporates by reference (IBRs) those standards and guidelines, which cover technical areas such as mDL communication, digital identity, encryption, cybersecurity, and network/information system security and privacy.

As noted above, this final rule is part of an incremental rulemaking that temporarily permits Federal agencies to accept mDLs for official purposes until TSA issues a subsequent rule that would set comprehensive requirements for mDLs. TSA believes it is premature to issue such requirements before the May 7, 2025 deadline due to the need for emerging industry standards and government guidelines [5] to be finalized.

The need for this rulemaking arises from TSA's desire to accommodate and foster the rapid pace of mDL innovation, while ensuring the intent of the REAL ID Act and regulations are met. Secure driver's licenses and identification cards are a vital component of our national security framework. In the REAL ID Act, Congress acted to implement the 9/11 Commission's recommendation that the Federal Government ''set standards for the issuance of sources of identification, such as driver's licenses.'' Under the REAL ID Act and regulations, a Federal agency may not accept for any official purpose a State-issued driver's license or identification card, either physical or an mDL, that does not meet specified requirements, as detailed in the REAL ID regulations (*see* Part II.A., below, for more discussion on these requirements).

This final rule will result in the development of mDLs with a higher level of security, privacy, and interoperability features necessary for Federal acceptance for official purposes. Because the current regulatory provisions do not include requirements that would enable States to issue REAL ID-compliant mDLs, several States are investing significant resources to develop mDLs based on varying and often proprietary standards, many of which may lack security and privacy safeguards commensurate with REAL ID requirements and the privacy needs of users. Without timely regulatory guidance concerning potential requirements for developing a REAL ID-compliant mDL, States risk investing in mDLs that are not aligned with emerging industry standards and government guidelines that may be IBR'd in a future rulemaking. States, therefore, may become locked-in to existing solutions and could face a substantial burden to redevelop products acceptable to Federal agencies under this future rulemaking.

This final rule addresses these concerns by enabling TSA to grant a temporary waiver to States whose mDLs TSA determines provide sufficient safeguards for security and privacy, pending finalization of emerging standards. Although this rule does not set standards for the issuance of REAL ID-compliant mDLs, it does establish minimum requirements that States must meet to be granted a waiver so that mDLs can be accepted by Federal agencies for official purposes. These minimum standards and requirements ensure that States' investments in mDLs provide minimum privacy and security safeguards consistent with information currently known to the TSA.

B. Summary of the Major Provisions

As further discussed in Part II.A., below, mDLs cannot be accepted by Federal agencies for official purposes when REAL ID full enforcement begins on May 7, 2025, unless 6 CFR part 37 is amended to address mDLs. This final rule establishes a process for waiving, on a temporary and State-by-State basis, the current prohibition on Federal acceptance of mDLs for official purposes, and enables Federal agencies to accept mDLs on an interim basis while the industry matures to a point sufficient to enable TSA to develop more comprehensive mDL regulatory requirements.

The current regulations prohibit Federal agencies from accepting non-compliant driver's licenses and identification cards, including both physical cards and mDLs, when REAL ID enforcement begins on May 7, 2025. Any modification of this regulatory provision must occur through rulemaking (or legislation). Until and unless TSA promulgates comprehensive mDL regulations that enable States to issue REAL ID-compliant mDLs, mDLs cannot be developed to comply with REAL ID, and Federal agencies therefore cannot accept mDLs for official purposes after REAL ID enforcement begins on May 7, 2025. The rule allows the Federal government to accept mDLs on an interim basis, but only if TSA has issued a waiver to such State based on that State's compliance with all applicable REAL ID requirements as defined in subpart E of this part, and with the minimum privacy, safety, and interoperability requirements in this rulemaking. Please see Part II.A., below, for an explanation of the REAL ID requirement that both cards and issuing States must be REAL ID compliant.

C. Need for a Multi-Phased Rulemaking

TSA recognizes both that regulations can influence long-term industry research and investment decisions, and that premature regulations can distort the choices of technologies, which could harm competition and innovation. As noted above, there are clear reasons for TSA to issue requirements for mDLs in the context of REAL ID. Simultaneously, however, TSA observes that this is a rapidly innovating market, with multiple industry and government standards and guidelines necessary to ensure mDL privacy and security still in development.[6] Accordingly, TSA has concluded that it is premature to promulgate comprehensive requirements for mDLs while key

[3] The REAL ID Act defines official purposes as including but not limited to accessing Federal facilities, boarding Federally regulated commercial aircraft, entering nuclear power plants, and any other purposes that the Secretary shall determine. *See* REAL ID Act. Notably, because the Secretary has not determined any other official purposes, the REAL ID Act and regulations do not apply to Federal acceptance of driver's licenses and identification cards for other purposes, such as applying for Federal benefits programs, submitting immigration documents, or other Federal programs.

[4] DHS, Final Rule, Minimum Standards for Driver's Licenses and Identification Cards Acceptable by Federal Agencies for Official Purposes, 88 FR 14473 (Mar. 9, 2023); DHS Press Release, DHS Announces Extension of REAL ID Full Enforcement Deadline (Dec. 5, 2022), *https://www.dhs.gov/news/2022/12/05/dhs-announces-extension-real-id-full-enforcement-deadline* (last visited July 17, 2024).

[5] *See* TSA, Notice of Proposed Rulemaking, Waiver for Mobile Driver's Licenses, 88 FR 60056, 60063–64 (Aug. 30, 2023) [hereinafter ''NPRM''].

[6] *See* NPRM, 88 FR at 60062–66.

standards are being finalized because of the risk of unintended consequences, such as chilling innovation and competition in the marketplace, and ''locking-in'' stakeholders to certain technologies. TSA is therefore establishing a temporary waiver process with clear standards and requirements to facilitate the acceptance of mDLs while the industry matures and moves to accepted standards.

TSA is proceeding with a multi-phased rulemaking approach. This ''Phase 1'' rule establishes a temporary waiver process that enables continuing Federal acceptance of mDLs for official purposes when REAL ID enforcement begins on May 7, 2025, and affords Federal agencies additional operational experience and data that would inform comprehensive regulations in the upcoming ''Phase 2'' rulemaking. The Phase 1 rule is intended to serve as a regulatory bridge until the emerging standards are finalized and a comprehensive Phase 2 rulemaking is effective.

TSA anticipates the future Phase 2 rulemaking would repeal the temporary waiver provisions established in Phase 1 and establish comprehensive requirements enabling States to issue mDLs that comply with REAL ID requirements. TSA envisions the Phase 2 rulemaking would draw heavily from pertinent parts of the emerging standards (pending review of those final, published documents) to set specific requirements for security, privacy, and interoperability. In addition, the Phase 2 rule would distinguish between existing regulatory requirements that apply only to mDLs versus physical cards. As one commenter[7] to a previously-issued Request for Information (RFI) urged (discussed in Part II.B., below), DHS is taking ''a slow and careful approach'' to regulation in order to fully understand the implications of mDLs.

This multi-phased rulemaking approach supports Executive Order (E.O.) 14058 of December 13, 2021 (Transforming Federal Customer Experience and Service Delivery to Rebuild Trust in Government), by using ''technology to modernize Government and implement services that are simple to use, accessible, equitable, protective, transparent, and responsive for all people of the United States.''[8] As highlighted above and discussed in more detail below, allowing acceptance of mDLs issued by States that meet the waiver requirements enables the public to more immediately realize potential benefits of mDLs, including greater convenience, security, and privacy.

D. Costs and Benefits

TSA estimates the 10-year total cost of the rule to be $829.8 million undiscounted, $698.1 million discounted at 3 percent ($81.8 million annualized), and $563.9 million discounted at 7 percent ($80.3 million annualized). Affected entities include States, TSA, and relying parties (Federal agencies that voluntarily choose to accept mDLs for official purposes).

States incur costs to familiarize themselves with the requirements of the final rule, purchase access to an industry standard, submit an mDL waiver application, submit mDL waiver reapplications, and comply with waiver application requirements. TSA estimates that 40 States will seek an mDL waiver over the next 10 years at a 10-year State cost of $813.1 million undiscounted, $683.7 million discounted at 3 percent, and $552.0 million discounted at 7 percent.

TSA incurs costs associated with purchasing access to industry standards, reviewing mDL waiver applications and mDL waiver reapplications, acquiring, installing, and operating mDL readers, and training transportation security officers. TSA estimates the 10-year cost to TSA is $10.13 million undiscounted, $8.87 million discounted at 3 percent, and $7.56 million discounted at 7 percent.

Relying parties will incur costs to procure mDL readers should they voluntarily choose to accept mDLs for official purposes. TSA estimates the 10-year cost to relying parties is $6.57 million undiscounted, $5.48 million discounted at 3 percent, and $4.38 million discounted at 7 percent.

TSA also identifies other non-quantified costs that affected parties may incur. States may incur incremental costs to: monitor and study mDL technology as it evolves; resolve underlying issues that could lead to a suspension or termination of an mDL waiver; report serious threats to security, privacy, or data integrity; report material changes to mDL issuance processes; remove conflicts of interest with an independent auditor; and request reconsideration of a denied mDL waiver application. TSA may incur costs to: investigate circumstances that could lead to suspension or termination of a State's mDL waiver; provide notice to States, relying parties, and the public related to mDL waiver suspensions or terminations; develop an IT solution that maintains an up-to-date list of States with valid mDL waivers; develop materials related to process changes to adapt to mDL systems; and resolve requests for reconsideration of a denied mDL waiver application. An mDL user may incur costs with additional application requirements to obtain an mDL. States may also pass on mDL related costs to the public.[9] Relying parties may incur costs to resolve any security or privacy issue with the mDL reader; report serious threats to security, privacy, or data integrity; verify the list of States with valid mDL waivers; train personnel to verify mDLs; and update the public on identification policies.

The final rule provides benefits to affected parties which include, but are not limited to: promoting higher security, privacy, and interoperability safeguards; reducing uncertainty in the mDL technology environment by helping to foster a minimum level of security, privacy and interoperability; and allowing Federal agencies to continue to accept mDLs for official purposes when REAL ID enforcement begins. Also, mDLs themselves may provide additional security benefits by offering a more secure verification of an individual's identity and authentication of an individual's credential compared to usage of physical cards.

II. Background

A. REAL ID Act, Regulations, and Applicability to mDLs

This rulemaking is authorized by the REAL ID Act of 2005 and REAL ID Modernization Act. The REAL ID Act authorizes the Secretary of Homeland Security, in consultation with the States and the Secretary of Transportation, to promulgate regulations to implement the requirements under the REAL Act.[10] The REAL ID Modernization Act amended the definitions of ''driver's license'' and ''identification card'' to specifically include mDLs that have been issued in accordance with regulations prescribed by the Secretary of Homeland Security.[11]

The REAL ID Act and implementing regulations, 6 CFR part 37, set minimum requirements for State-issued driver's licenses and identification cards accepted by Federal agencies for official purposes, including accessing Federal

[7] *See* comment from Electronic Privacy Information Center, *https://downloads.regulations.gov/DHS-2020-0028-0048/attachment_1.pdf* (last visited July 17, 2024); DHS, Request for Information, Mobile Driver's Licenses, 86 FR 20320 (Apr. 19, 2021).

[8] *See* 86 FR 71357 (Dec. 16, 2021).

[9] TSA does not possess data to quantify how States may implement a pass through or recoup costs associated with implementation of mDLs.

[10] Sec. 205 of the REAL ID Act.

[11] Sec. 1001 of the REAL ID Modernization Act, Title X of Division U of the Consolidated Appropriations Act, 2021, Public Law 116–260, 134 Stat. 2304 [hereinafter ''REAL ID Modernization Act''].

facilities, boarding Federally regulated commercial aircraft, entering nuclear power plants, and any other purposes that the Secretary shall determine.[12] The Act defines ''driver's licenses'' and ''identification cards'' strictly as State-issued documents,[13] and the regulations further refine the definition of ''identification card'' as ''a document made or issued by or under the authority of a State Department of Motor Vehicles or State office with equivalent function.'' [14] The REAL ID Act and regulations do not apply to identification cards that are not made or issued under a State authority, such as cards issued by a Federal agency or any commercial, educational, or non-profit entity.

The regulations include a schedule describing when individuals must obtain a REAL ID-compliant driver's license or identification card intended for use for official purposes, known as ''card-based'' enforcement.[15] Card-based enforcement begins on May 7, 2025.[16] On this date, Federal agencies will be prohibited from accepting a State- or territory-issued driver's license or identification card for official purposes unless the card is compliant with the REAL ID Act and regulations.[17]

On December 21, 2020, Congress passed the REAL ID Modernization Act,[18] which amended the REAL ID Act to update the definitions of ''driver's license'' and ''identification card'' to specifically include mDLs that have been issued in accordance with regulations prescribed by the Secretary, among other updates.[19] Accordingly, mDLs must be REAL ID-compliant to be accepted by Federal agencies for official purposes when card-based enforcement begins on May 7, 2025. However, States cannot issue REAL ID-compliant mDLs until the regulations are updated to include requirements to ensure that mDLs meet equivalent levels of security currently imposed on REAL ID-compliant physical cards.

[12] REAL ID Act; 6 CFR part 37.

[13] Sec. 201 of the REAL ID Act.

[14] 6 CFR 37.3.

[15] *See* 6 CFR 37.5(b). The regulations also include a schedule for State-based compliance, known as ''State-based enforcement.'' *See* 6 CFR 37.51(a).

[16] *See* 6 CFR 37.5(b).

[17] *See* 6 CFR 37.5(b). Additionally, TSA is conducting a separate rulemaking that would allow Federal agencies to implement the card-based enforcement provisions of the REAL ID regulations under a phased approach beginning on the May 7, 2025 enforcement deadline. *See* NPRM, Phased Approach for Card-Based Enforcement, 89 FR 74137 (Sept. 12, 2024).

[18] REAL ID Modernization Act, 134 Stat. 2304.

[19] Sec. 1001 of the REAL ID Modernization Act, 134 Stat. 2304.

B. Rulemaking History

In April 2021, DHS issued an RFI announcing DHS's intent to commence future rulemaking to set the minimum technical requirements and security standards for mDLs to enable Federal agencies to accept mDLs for official purposes. The RFI requested comments and information to inform DHS's rulemaking.[20] In response, DHS received 63 comments [21] through a twice-extended comment period of 180 days, which closed on October 18, 2021.

In August 2023, TSA published a Notice of Proposed Rulemaking (NPRM) [22] drawing on comments to the RFI, which are summarized at 88 FR 60056, 60071–72. The NPRM comment period closed on October 16, 2023, and TSA received 31 comments. NPRM comments are discussed in detail in Part IV, below.

C. mDL Overview

1. mDLs Generally

An mDL is generally recognized as the digital representation of an individual's identity information contained on a State-issued physical driver's license or identification card.[23] An mDL may be stored on a diverse range of portable or mobile electronic devices, such as smartphones, smartwatches, and storage devices containing memory. Like a physical card, mDL data originates from identity information about an individual that is maintained in the database of a State driver's licensing agency. An mDL has potential benefits for all stakeholders. For Federal agencies, mDLs may provide security and efficiency enhancements compared to physical cards, because mDLs rely on digital security features that are immune to many vulnerabilities of physical security features. For individuals, mDLs may provide a more secure, convenient, privacy-enhancing, and ''touchless'' method of identity verification compared to physical IDs.

Unlike physical cards that employ physical security features to deter fraud and tampering, mDLs combat fraud through the use of digital security features that are not recognizable through human inspection, such as asymmetric cryptography/public key infrastructure (PKI). As discussed in the NPRM,[24] asymmetric cryptography generates a pair of encryption ''keys'' to encrypt and decrypt protected data. One key, a ''public key,'' is distributed publicly, while the other key, a ''private key,'' is held by the State driver's licensing agency (*e.g.,* a Department of Motor Vehicles). When the driver's licensing agency issues an mDL to an individual, the agency uses its private key to digitally ''sign'' the mDL data. A Federal agency accepting an mDL validates the integrity of the mDL data by obtaining the State driver's licensing agency's public key to verify the digital signature. Private keys and digital signatures are elements of data encryption that protect against unauthorized access, tampering, and fraud. Generally, mDL-based identity verification under REAL ID involves a triad of secure communications between a State driver's licensing agency, an mDL holder, and a Federal agency. Standardized communication interfaces are necessary to enable Federal agencies to exchange information with all U.S. States and territories that issue mDLs. Please see the NPRM for a more detailed discussion.[25]

In contrast to physical driver's licenses that are read and verified visually through human inspection of physical security features, an mDL is read and verified electronically using a device known simply as a ''reader. Any Federal agency that accepts mDLs for official purposes must use readers to validate an mDL holder's identity data from their mobile device and establish trust that the mDL is secure by using private-public key data encryption.[26] An mDL reader compliant with this requirement can take multiple forms, such as an app installed on a mobile device, or a dedicated device. Although reader development is evolving, some companies already offer reader apps for free, and TSA therefore expects readers will be offered in a wide range capabilities and associated price points.[27]

[20] 86 FR 20320 (Apr. 19, 2021).

[21] The 63 total comments included three duplicates and one confidential submission.

[22] 88 FR 60056.

[23] A technical description of mDLs as envisioned by the American Association of Motor Vehicle Administrators may be found at *https://www.aamva.org/Mobile-Drivers-License/* (last visited July 17, 2024).

[24] 88 FR at 60060.

[25] 88 FR at 60060–61.

[26] Non-Federal agencies and other entities who choose to accept mDLs for uses beyond the scope of REAL ID should also recognize the need for a reader to ensure the validity of the mDL. Any verifying entity can validate in the same manner as a Federal agency if they implement the standardized communication interface requirements specified in this final rule, which would require investment to develop the necessary IT infrastructure and related processes.

[27] Readers for mDLs have specific requirements and at this time are not interchangeable with readers for other types of Federal cards, such as the Transportation Worker Identification Credential (TWIC). Although TSA is evaluating some mDLs at select airport security checkpoints, cost estimates for readers used in the evaluations are not available because those readers are non-commercially

Continued

2. State mDL Issuance and TSA Testing

As noted above, mDL issuance is proliferating rapidly among States, with at least half of all States believed to be preparing for or issuing mDLs.[28] Although detailed mDL adoption statistics are unavailable, anecdotal information and media reports indicates that mDLs are rapidly gaining public acceptance. For example, Maryland commented that it has issued more than 200,000 mDLs to residents following a pilot in 2017 and more recent expansion in 2022 and 2023.[29] Iowa commented that in the 3 months since it began offering its mDL app, it has been downloaded by more than 7,000 users.[30]

TSA understands that States are issuing mDLs using widely varying technology solutions, raising concerns whether such technological diversity provides the safeguards and interoperability necessary for Federal acceptance. Since 2022, TSA has been collaborating with States and industry to test the use of mDLs issued by participating States at select TSA airport security checkpoints.[31] As of the date of this final rule, TSA is currently testing mDLs issued by 11 States (Arizona, California, Colorado, Georgia, Hawaii, Iowa, Louisiana, Maryland, New York, Ohio, Utah) at 27 airports.[32]

D. Industry Standards and Government Guidelines for mDLs

The nascence of mDLs and absence of standardized mDL-specific requirements provide an opportunity for industry and government to develop standards and guidelines to close this void. TSA is aware of multiple such documents, published and under development, from both Federal and non-government sources. As discussed in Part III.C.8, below, this final rule amends § 37.4 by IBR'g into part 37 19 standards and guidelines that form the basis of many of the requirements in this final rule. TSA understands that these standards and guidelines discussed are the most comprehensive and relevant references governing mDLs today. TSA also acknowledges that many additional standards and guidelines are in development and may provide additional standardized mechanisms for mDLs.[33]

III. General Discussion of the Rulemaking

A. Changes Between NPRM and Final Rule

After carefully considering all comments received to the NPRM (see detailed discussion of comments and TSA's responses in Part IV, below), TSA finalizes the NPRM with several revisions in response to public comments. Table 1 summarizes the changes made in the final rule compared to the NPRM.

TABLE 1—SUMMARY OF CHANGES BETWEEN THE NPRM AND THE FINAL RULE

Section	Final rule	Reason for the change
37.3	Adds definition for "Provisioning."	Technical change to add definition of a key term to improve clarity.
37.4	Revises points of contact for the public to contact TSA; provides additional means to access certain standards that are IBR'd in this rule.	Technical changes to improve access to IBR materials.
37.4(c)(1)	Corrects title of "Cybersecurity Incident & Vulnerability Response Playbooks" to "Federal Government Cybersecurity Incident & Vulnerability Response Playbooks.".	Technical correction.
37.4(g)(4)	Updates standard NIST FIPS PUB 197 to NIST FIPS PUB 197–upd1 to reflect revised version of standard.	Technical change to reflect revisions to standard to improve public access. Revisions include editorial improvements, but no technical changes to the algorithm specified in the earlier version.
37.4(g)(7)	Corrects website address to the cited standard	Technical change to correct a typo.
37.7(a)	Clarifies conditions under which TSA will issue a waiver	Clarification regarding impact of the waiver.
37.7(b)(3)	Deleted	Deleted proposed language that would have made a State ineligible to apply for a waiver if the State issues mDLs to individuals with non-REAL ID compliant physical cards (in addition to issuing mDLs to other individuals that have compliant physical cards).
37.8(c)	Adds paragraph (c) to require Federal agencies accepting mDLs to confirm, consistent with the deadlines set forth in § 37.5, that the mDL data element "DHS_compliance" is encoded "F," as required by §§ 37.10(a)(4)(ii) & (a)(1)(vii).	Clarifies that when REAL ID enforcement begins, Federal agencies may accept mDLs from States only if the underlying physical card is REAL ID compliant.
37.8(d)	Renumbers § 37.8(c), as proposed in the NPRM, to § 37.8(d) in light of addition of new § 37.8(c).	Technical changes renumber provision from 37.8(c) to 37.8(d), update agency name and website address, and clarify the mechanics of reporting.
	Corrects website address from *dhs.gov* to *tsa.gov*	
	Adds requirement regarding protection of SSI	Provides that reports *may* contain sensitive security information (SSI)[34] and if so, would be subject to requirements of 49 CFR part 1520.

available prototypes designed specifically for integration into TSA-specific IT infrastructure that few, if any, other Federal agencies use. In addition, mDL readers are evolving and entities who accept mDLs would participate voluntarily. Accordingly, associated reader costs are not quantified at this time but TSA intends to gain a greater understanding of any costs to procure reader equipment as the technology continues to evolve.

[28] *See, e.g.,* AAMVA, Driver and Vehicle Services Data Map, *https://www.aamva.org/jurisdiction-data-maps#anchorformdlmap* (last visited July 17, 2024); PYMNTS, *States Embrace Mobile Driver's Licenses to Fight Fraud Amid Privacy Scrutiny* (Apr. 9, 2024), *https://www.pymnts.com/identity/2024/states-embrace-mobile-drivers-licenses-to-fight-fraud-amid-privacy-scrutiny/* (last visited July 17, 2024); Government Technology, *Digital IDs Are Here, but Where Are They Used and Accepted?* (Mar. 12, 2024), *https://www.govtech.com/biz/data/digital-ids-are-here-but-where-are-they-used-and-accepted* (last visited July 17, 2024).

[29] Comment by Maryland MVA, *https://www.regulations.gov/comment/TSA-2023-0002-0032* (last visited July 17, 2024).

[30] Comment by Iowa Department of Transportation, *https://www.regulations.gov/comment/TSA-2023-0002-0023* (last visited July 17, 2024).

[31] *See* NPRM, 88 FR at 60066–67.

[32] *See* TSA, Facial Recognition and Digital Identity Solutions, *https://www.tsa.gov/digital-id* (last visited Aug. 9, 2024).

[33] *See* NPRM, 88 FR at 60063–66, for a discussion of these standards.

TABLE 1—SUMMARY OF CHANGES BETWEEN THE NPRM AND THE FINAL RULE—Continued

Section	Final rule	Reason for the change
37.9(a)	Corrects agency name from DHS to TSA Corrects website address from *dhs.gov* to *tsa.gov*	Technical changes update agency name and website address.
37.9(b)	Revises "days" to "calendar days." Corrects website address from *dhs.gov* to *tsa.gov*	Clarifies that "days" means calendar days, not business days. Technical change updates agency website address.
37.9(c)	Revises "days" to "calendar days." Corrects website address from *dhs.gov* to *tsa.gov*	Clarifies that "days" means calendar days, not business days. Technical change updates agency website address.
37.9(e)(2)	Revises "days" to "calendar days." Corrects website address from *dhs.gov* to *tsa.gov* Provides a means for States to contact TSA if the State is unclear whether certain modifications to its mDL issuance processes require reporting.	Clarifies that "days" means calendar days, not business days. Technical change updates agency website address. Provides a means for States to resolve potential questions regarding reporting requirements.
37.9(e)(4)(ii)	Revises "days" to "calendar days."	Clarifies that "days" means calendar days, not business days.
37.9(e)(5)(i)	Corrects agency name from DHS to TSA	Technical change updates agency name.
37.9(e)(5)(ii)	Revises "days" to "calendar days."	Clarifies that "days" means calendar days, not business days.
37.9(g)	Adds new paragraph (g), which provides that information submitted in response to requirements to apply for and maintain a waiver *may* contain SSI, and if so, would be subject to requirements of 49 CFR part 1520.	SSI protection.
37.10(a)(1)(vii)	Replaces NPRM requirement that States must issue mDLs only to residents who have been issued physical cards that are valid, unexpired, and REAL ID-compliant with requirement that States must populate the "DHS_compliance" data field to correspond to the REAL ID-compliance status of the underlying physical driver's license or identification card, or as required by the AAMVA Guidelines.	Proposed language would have required States to issue mDLs only to individuals to whom that State previously issued a physical card that is valid, unexpired, and REAL ID-compliant. This would have denied States the discretion to issue mDLs to holders of non-compliant physical cards. Revisions require States to issue mDLs in a manner that reflects the REAL ID compliance status of the underlying physical card. This is consistent with the intent of the NPRM, which was to enable Federal agencies to determine the REAL ID-compliance status of the underlying physical card, and accept only compliant cards when enforcement begins.
37.10(a)(4)	Corrects version number of AAMVA Mobile Driver's License (mDL) Implementation Guidelines (Jan. 2023). Updates NIST FIPS PUB 197 to NIST FIPS PUB 197–upd1 to reflect revised version of standard.	Technical change corrects version number of AAMVA Guidelines. Changes reflect current version of NIST FIPS PUB 197 to ensure continuing public access. Revisions to the standard include editorial improvements, but no technical changes to the algorithm specified in the earlier version.
37.10(b)(1)	Clarifies that "independent entity" includes State employees or contractors that are independent of the State's driver's licensing agency.	Provides States additional options to select auditors. Reduces burdens without impact on security or privacy.
37.10(c)	Corrects website address from *dhs.gov* to *tsa.gov* Clarifies that TSA will publish in the **Federal Register** a notice advising of the availability of updated TSA mDL Waiver Application Guidance, which itself will be published at *www.tsa.gov/mDL/*.	Technical changes update agency website address, and clarify means of notifying and publishing updates to TSA mDL Waiver Application Guidance.
Appendix A, Throughout	Corrections to titles of: CISA Federal Government Cybersecurity Incident & Vulnerability Response Playbooks. DHS National Cyber Incident Response Plan NIST FIPS PUB 140–3 NIST Framework for Improving Critical Infrastructure Cybersecurity.	Technical corrections.
Appendix A, paragraph 1.1	Adds section numbers to certain references Deletes requirement to comply with NIST SP 800–53B	Technical changes clarify which parts of cited reference require compliance, and remove an unnecessary requirement.
Appendix A, paragraph 2.2	Revises "privileged account or service" in NPRM to "trusted role.".	Technical change corrects terminology.
Appendix A, paragraph 2.13	Adds section numbers to a certain reference	Technical change clarifies which parts of cited reference require compliance.
Appendix A, paragraph 5.13	Reduces requirements for minimum number of personnel to generate issuing authority certificate authority (IACA) root certificate keys from a minimum of three to two persons, consisting of at least one ceremony administrator and one qualified witness.	Provides States greater freedom to select products. Does not impact security, privacy, or interoperability.

TABLE 1—SUMMARY OF CHANGES BETWEEN THE NPRM AND THE FINAL RULE—Continued

Section	Final rule	Reason for the change
Appendix A, paragraph 5.14	Modifies requirements for minimum number of personnel to generate document signer keys. Final rule requires either at least one administrator and one qualified witness (other than a person involved in key generation), or at least 2 administrators using split knowledge processes.	Provides States greater freedom to select products. Does not impact security, privacy, or interoperability.
Appendix A, paragraph 6.3 ..	Revises ''days'' to ''calendar days	Clarifies that ''days'' means calendar days, not business days.
Appendix A, paragraph 8.6 ..	Modifies cyber incident reporting requirements to incidents as defined in the TSA Cybersecurity Lexicon available at *www.tsa.gov* that may harm state certificate systems. Corrects website address from *dhs.gov* to *tsa.gov* ..... Adds SSI protection requirements	Clarifies types of incidents that must be reported, updates agency website address, and adds SSI protection.

B. Summary of Regulatory Provisions

In addition to revising definitions applicable to the REAL ID Act to incorporate mDLs, this rule amends 6 CFR part 37 to enable TSA to grant a temporary waiver to States that TSA determines issue mDLs consistent with specified requirements concerning security, privacy, and interoperability. This rule enables Federal agencies, at their discretion, to accept for REAL ID official purposes, mDLs issued by a State that has been granted a waiver, provided that the underlying physical card upon which the mDL was based is REAL ID-compliant. The rule applies only to Federal agency acceptance of State-issued mDLs as defined in this final rule for REAL ID official purposes, but not other forms of digital identification, physical driver's licenses or physical identification cards, or non-REAL ID purposes. Any temporary waiver issued by TSA would be valid for a period of 3 years from the date of issuance.

To obtain a waiver, § 37.9(a) requires a State to submit an application, supporting data, and other documentation to establish that their mDLs meet the criteria specified in §§ 37.10(a) and (b) (discussed in Part III.C.4., below) concerning security, privacy, and interoperability. If TSA determines, upon evaluation of a State's application and supporting documents, that a State's mDL could be securely accepted under the terms of a waiver, TSA may issue such State a certificate of waiver. TSA intends to work with each State applying for a waiver on a case-by-case basis to ensure that its mDLs meet the minimum requirements necessary to obtain a waiver. This rulemaking establishes the full process for a State to apply for and maintain a waiver, including: instructions for submitting the application and responding to subsequent communications from TSA as necessary; specific information and documents that a State must provide with its application; requirements concerning timing, issuance of decisions, requests for reconsideration; and post-issuance reporting requirements and other terms, conditions, and limitations. To assist States that are considering applying for a waiver, TSA has developed guidelines, entitled, ''Mobile Driver's License Waiver Application Guidance'' (hereinafter ''TSA Waiver Guidance'' or ''the Guidance''), which provides non-binding recommendations of some ways that States can meet the application requirements set forth in this rulemaking.[35] This final rule makes several technical and administrative changes to the NPRM, as set forth in Table 1, above. These changes are as follows:

- Corrections to agency name, website address, points of contact for access and compliance with reporting requirements: *See* §§ 37.4, 37.8(d), 37.9(a)–(c), (e)(2) & (e)(5)(i), 37.10(c), and Appendix A, paragraph 8.6.
- Corrections to inadvertent omissions, typographical errors, paragraph numbering, title/version number of publications: *See* §§ 37.3, 37.4, 37.4(c)(1), 37.8(d), 37.4(g)(4) & (7), 37.10(a)(4), Appendix A, paragraphs 1.1, 2.13, 2.2, 8.4, 8.5, 8.8.
- Clarifying that ''days'' means ''calendar days'': *See* §§ 37.9(b), 37.9(c), 37.9(e)(2), (4)(i) & (5)(ii), and Appendix A, paragraph 6.3.

C. Specific Provisions

This section describes the final regulatory provisions in this rule, including the changes discussed above. Unless otherwise noted, these provisions were described in the NPRM.

1. Definitions

The final rule adds new definitions to subpart A, § 37.3, consistent with those proposed in the NPRM. In particular, new definitions for ''mobile driver's license'' and ''mobile identification card'' are necessary because the current regulations predated the emergence of mDL technology and, therefore, do not define these terms. Additionally, the definitions reflect changes made by the REAL ID Modernization Act, which amended the definitions of ''driver's license'' and ''identification card'' to specifically include ''mobile or digital driver's licenses'' and ''mobile or digital identification cards.'' The definitions in this rule provide a more precise definition of ''mobile driver's license'' and ''mobile identification card'' by clarifying that those forms of identification require a mobile electronic device to store the identification information, as well as an electronic device to read that information. The rule also adds a new definition of ''mDL'' that collectively refers to mobile versions of both State-issued driver's licenses and State-issued identification cards as defined in the REAL ID Act.

[34] SSI is information obtained or developed in the conduct of security activities, the disclosure of which would constitute an unwarranted invasion of privacy, reveal trade secrets or privileged or confidential information, or be detrimental to the security of transportation. The protection of SSI is governed by 49 CFR part 1520.

[35] The specific measures and practices discussed in the TSA Waiver Application Guidance are neither mandatory nor necessarily the ''preferred solution'' for complying with the requirements in this final rule. Rather, they are examples of measures and practices that a State issuer of mDLs may choose to consider as part of its overall strategy to issue mDLs. States have the ability to choose and implement other measures to meet these requirements based on factors appropriate to that State, so long as DHS determines that the measures implemented provide the levels of security and data integrity necessary for Federal acceptance of mDLs for official purposes as defined in the REAL ID Act and 6 CFR part 37. As provided in § 37.10(c), TSA may periodically update the Guidance as necessary to recommend mitigations of evolving threats to security, privacy, or data integrity.

The final rule includes additional definitions to explain terms used in the waiver application criteria set forth in §§ 37.10(a)–(b) and Appendix A to subpart A of this part (Appendix A). Generally, this rule defines terms that lack a common understanding or that are common terms of art for information systems, and that require an explanation to enable stakeholders to comply with the rule. The definitions were informed by TSA's knowledge and experience, as well as a publication by the National Institute of Standards and Technology (NIST).[36] For example, the rule adds definitions for ''digital certificates'' and ''certificate systems,'' which are necessary elements of risk controls for the IT systems that States use to issue mDLs. In addition, this final rule adds a definition for ''certificate policy,'' which forms the governance framework for States' certificate systems. A State must develop, maintain, and execute a certificate policy to comply with the requirements set forth in Appendix A. In addition, ''Digital Signatures'' are mathematical algorithms that States use to validate the authenticity and integrity of a message. Each of these terms is fundamental to understanding the requirements set forth in this rule.

The final rule adds a definition for ''provisioning'' which was not proposed in the NPRM. *See* § 37.3. As defined by this final rule, ''provisioning'' means the process by which a State transmits and installs an mDL on an individual's mobile device. Although TSA did not receive any comments seeking clarity or requesting the addition of this or other definitions, TSA believes provisioning is a critical concept that requires a definition in order to facilitate stakeholder compliance.

2. TSA Issuance of Temporary Waiver and State Eligibility Criteria

The final rule adds to subpart A new § 37.7, entitled ''Temporary waiver for mDLs; State eligibility.'' This waiver framework temporarily allows Federal agencies to accept for official purposes mDLs (which today are all non-compliant) issued by States with a waiver, if the mDL is based on a REAL ID-compliant physical card, when REAL ID enforcement begins on May 7, 2025 (*see* § 37.8, discussed in Part III.C.3., below). However, the waiver framework does not apply to any other requirements in 6 CFR part 37 or physical cards. Section 37.7(a) authorizes TSA to issue a temporary certificate of waiver to States that meet the waiver application criteria set forth in §§ 37.10(a) and (b). TSA's determination of whether a State satisfies these requirements will be based on TSA's evaluation of the information provided by the State in its application (*see* Part III.C.4., below), as well as other information available to TSA. Federal agencies are not required to accept mDLs, and retain discretion to determine their own policies regarding identity verification.

Although NPRM § 37.7(a) stated that a waiver would exempt a State's mDLs from meeting the card-based compliance requirement of § 37.5(b), the final rule deletes this clause because a waiver impacts Federal agency *acceptance,* not State *issuance,* of non-compliant mDLs. Stated differently, a waiver allows Federal agencies to accept non-compliant mDLs issued by States to whom TSA has granted a waiver. As discussed above in this preamble, the waiver application criteria set forth temporary security requirements commensurate with REAL ID standards for physical cards, ensuring that mDLs meeting the criteria are suitable for Federal acceptance. However, States cannot issue REAL ID-compliant mDLs until TSA sets forth such requirements in the subsequent Phase 2 rulemaking.

Section 37.7(b) sets forth criteria that a State must meet to be eligible for consideration of a waiver. These criteria require that the issuing State: (1) is in full compliance with all applicable REAL ID requirements as defined in subpart E of this part, and (2) has submitted an application, under §§ 37.10(a) and (b) demonstrating that the State issues mDLs that provide security, privacy, and interoperability necessary for Federal acceptance.[37] The NPRM proposed paragraph (b)(3) of this section, which provided an additional waiver eligibility criterion that a State must issue mDLs only to individuals who have been issued REAL ID-compliant physical cards. However, the final rule does not adopt this proposal given TSA's evaluation of public comments (see Part IV.A.) that this provision would have made a State ineligible for a waiver if the State issued mDLs to both individuals with REAL ID-compliant physical cards and individuals with non-compliant physical cards. The final rule similarly amends § 37.10(a)(1)(vii), as proposed by the NPRM, to remove a provision that would have required States to issue an mDL only to a resident who has been issued a valid, unexpired, and REAL ID-compliant physical card that underlies the mDL. *See* Part III.C.4, below.

3. Requirements for Federal Agencies that Accept mDLs

The final rule adds to subpart A new § 37.8, entitled ''Requirements for Federal agencies accepting mDLs issued by States with temporary waiver.'' This section requires that any Federal agency that elects to accept mDLs for REAL ID official purposes must meet four requirements in new § 37.8. First, under § 37.8(a), a Federal agency must confirm that the State holds a valid certificate of waiver. Agencies would make this confirmation by verifying that the State's name appears in a list of States to whom TSA has granted a waiver. TSA will publish this list on the REAL ID website at *www.tsa.gov/real-id/mDL* (as provided in § 37.9(b)(1)).

Second, § 37.8(b) requires Federal agencies to use an mDL reader to retrieve mDL data from an individual's mobile device and validate that the data is authentic and unchanged following the processes required by industry standard ISO/IEC 18013–5:2021(E).[38]

Third, under § 37.8(c), Federal agencies may accept, consistent with the deadlines set forth in § 37.5, only those mDLs that are issued based on an underlying physical card that is REAL ID compliant. Agencies would make this determination by confirming that mDL data element ''DHS_compliance'' has a value of ''F''. As discussed in Part III.C.8.a., below, the data field ''DHS_compliance'' (defined in the American Association of Motor Vehicle Administrators *Mobile Driver's License (mDL) Implementation Guidelines Version 1.2* (Jan. 2023) (AAMVA Guidelines)) enables an mDL to convey the REAL ID compliance status of the underlying physical card. TSA notes that § 37.8(c) is a new provision that was not included in the NPRM. TSA intended, in proposed §§ 37.7(b)(3) and 37.10(a)(1)(vii) of the NPRM, that Federal agencies would accept only mDLs issued by States to whom TSA has issued a waiver, and that are based on an underlying physical card that is REAL ID-compliant. Final rule § 37.8(c), together with revisions to § 37.10(a)(1)(vii) (see discussion in Part III.C.4., below), achieves that intent.

Finally, under § 37.8(d), if a Federal agency discovers that acceptance of a State's mDL is likely to cause imminent or serious threats to security, privacy, or data integrity, the agency must report the threats to TSA at *www.tsa.gov/real-id/mDL* within 72 hours of such

[36] *See* NIST, Computer Security Resource Center, *https://csrc.nist.gov/glossary* (last visited July 17, 2024).

[37] Sections 37.7(b)(1) & (2).

[38] *See* NPRM, 88 FR at 60063–64, for a discussion of this standard.

discovery. Examples of reportable threats include cyber incidents and other events that cause serious harm to a State's mDL issuance system. Reports *may* contain SSI, and if so, would be subject to requirements of 49 CFR part 1520. Although the NPRM did not propose the SSI protection provision, TSA evaluated comments to the NPRM (*see* Part IV.W., below) seeking clarification on SSI protection for other information (State waiver applications) and determined that SSI protection is warranted for Federal agency reports under this § 37.8(d), which has been added in this final rule. TSA will consider whether such information warrants suspension of that State's waiver under § 37.9(e)(4)(i)(B) (*see* discussion in Part III.C.6., below). If TSA elects not to issue a suspension, Federal agencies would continue to exercise their own discretion regarding continuing acceptance of mDLs.

4. Requirements for States Seeking To Apply for a Waiver

The final rule adds to subpart A new § 37.9, which sets forth a process for a State to request a temporary certificate of waiver established in new § 37.7. As provided in § 37.9(a), a State seeking a waiver must file a complete application as set forth in §§ 37.10(a) and (b), following instructions available at *www.tsa.gov/real-id/mDL.* Sections 37.10(a) and (b) set forth all information, documents, and data that a State must include in its application for a waiver. If TSA determines that the means that a State implements to comply with the requirements in §§ 37.10(a) and (b) provide the requisite levels of security, privacy, and data integrity for Federal acceptance of mDLs for official purposes, TSA would grant such State a waiver. This rule does not, however, prescribe specific means (other than the requirements specified in Appendix A, which is discussed further in Part III.C.4.iv, below) that a State must implement. Instead, States would retain broad discretion to choose and implement measures to meet these requirements based on factors appropriate to that State.

(i) Application Requirements

As set forth in §§ 37.10(a)(1) through (4), a State is required to establish in its application how it issues mDLs under the specified criteria for security, privacy, and interoperability suitable for acceptance by Federal agencies, as follows:

• Paragraph (a)(1) sets forth requirements for mDL provisioning. Specific requirements include:

○ Encryption of mDL data and an mDL holder's Personally Identifiable Information,

○ Escalated review of repeated failed provisioning attempts,

○ Authentication of the mDL applicant's mobile device,

○ Mobile device identification keys,

○ User identity verification controls,

○ Applicant presentation controls,

○ Encoding of the ''DHS_compliance'' data field. States must populate this data field to correspond to the REAL ID compliance status of the underlying physical driver's license or identification card that a State has issued to an mDL holder. Specifically, ''DHS_compliance'' should be populated with ''F'' if the underlying card is REAL ID compliant, or as required by American Association of Motor Vehicle Administrator (AAMVA) Mobile Driver's License (mDL) Implementation Guidelines v. 1.2, Section 3.2 (IBR'd; see § 37.4), or ''N'' if the underlying card is not REAL ID-compliant. Although § 37.10(a)(1)(vii) of the NPRM proposed requiring that States issue an mDL only to a resident who has been issued a valid, unexpired, and REAL ID-compliant physical card that underlies the mDL, the final rule does not adopt this provision, based on TSA's evaluation of public comments (see Part IV.A.), that this provision would have made a State ineligible to apply for a waiver if the State issued mDLs to both individuals with REAL ID-compliant physical cards and individuals with non-compliant physical cards,

○ Data record requirements, and

○ Records retention specifications.

• Paragraph (a)(2) specifies requirements for managing state certificate systems, which are set forth in Appendix A.

• Paragraph (a)(3) requires a State to demonstrate how it protects personally identifiable information of individuals during the mDL provisioning process.

• Paragraph (a)(4) requires a State to explain the means it uses to:

○ Issue mDLs that are interoperable with requirements set forth in standard ISO/IEC 18013–5:2021(E),

○ Comply with the ''AAMVA mDL data element set'' as defined in the AAMVA Guidelines v. 1.2, Section 3.2,[39] and

○ Use only those algorithms for encryption,[40] secure hash function,[41] and digital signatures that are specified in ISO/IEC 18013–5:2021(E), and in NIST FIPS PUB 180–4, 186–5, 197–upd1, 198–1, and 202.

(ii) Audit Requirements

Section 37.10(b) requires a State to submit an audit report prepared by an independent auditor verifying the accuracy of the information provided by the State in response to § 37.10(a), as follows:

• Paragraph (1) sets forth specific experience, qualifications, and accreditations that an auditor must meet.

• Paragraph (2) requires a State to provide information demonstrating the absence of a potential conflict of interest of the auditing entity.

The term ''independent'' does not exclude an entity that is employed or contracted by a State, so long as that entity is independent of (*i.e.,* not an employee or contractor) the State's driver's licensing agency. TSA provides this clarification at the request of commenters (see Part IV.U., below).

(iii) Waiver Application Guidance

As set forth in § 37.10(c), TSA has published Mobile Driver's License Waiver Application Guidance on the REAL ID website at *www.tsa.gov/real-id/mDL* to assist States in completing their applications. The Guidance provides TSA's recommendations for some ways that States can meet the requirements in § 37.10(a)(1). The Guidance does *not* establish legally enforceable requirements for States applying for a waiver. Instead, the Guidance provides non-binding examples of measures and practices that States may choose to consider as part of their overall strategy to issue mDLs. States continue to exercise discretion to select processes not included in the Guidance. Given the rapidly-evolving cyber threat landscape, however, TSA may periodically update the Guidance to provide additional information regarding newly published standards or other sources, or recommend mitigations of newly discovered risks to

[39] *See* NPRM, 88 FR at 60062–65, for a discussion of these standards.

[40] Encryption refers to the process of cryptographically transforming data into a form in a manner that conceals the data's original meaning to prevent it from being read. Decryption is the process of restoring encrypted data to its original state. IETF RFC 4949, internet Security Glossary, Version 2, Aug. 2007, *https://datatracker.ietf.org/doc/html/rfc4949* (last visited July 17, 2024).

[41] A function that processes an input value creating a fixed-length output value using a method that is not reversible (*i.e.,* given the output value of a function it is computationally impractical to find the function's corresponding input value).

the mDL ecosystem. TSA will publish a notice in the **Federal Register** advising that updated Guidance is available, and TSA will publish the updated Guidance on the REAL ID website at *www.tsa.gov/real-id/mDL* and provide a copy to all States that have applied for or been issued a certificate of waiver. Updates to the Guidance will not impact issued waivers or pending applications. Although the NPRM proposed that TSA would publish updated Guidance in the **Federal Register**, in addition to TSA's website, the final rule modifies this requirement to provide that the agency will publish in the **Federal Register** only a notice of availability of updated guidance, but the Guidance itself will be published on TSA's website. This change will enable TSA to more expediently provide updated guidance to the public.

(iv) Appendix A: Requirements for State mDL Issuance Systems

Appendix A sets forth fundamental requirements to ensure the security and integrity of State mDL issuance processes. More specifically, these requirements concern the creation, issuance, use, revocation, and destruction of the State's certificate systems and cryptographic keys. Appendix A consists of requirements in eight categories: (1) Certificate Authority Certificate Life Cycle Policy, (2) Certificate Authority Access Management, (3) Facility, Management, and Operational Controls, (4) Personnel Security Controls, (5) Technical Security Controls, (6) Threat Detection, (7) Logging, and (8) Incident Response and Recovery Plan. Adherence to these requirements, described below, ensures that States issue mDLs in a standardized manner with security and integrity to establish the trust necessary for Federal acceptance for official purposes.

- Certificate Authority Certificate Life Cycle Policy requirements (Appendix A, paragraph 1) ensure that a State issuing an mDL creates and manages a formal process which follows standardized management and protections of digital certificates. These requirements must be implemented in full compliance with the references cited in Appendix A: CA/Browser Forum Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates; CA/Browser Forum Network and Certificate System Security Requirements; ISO/IEC 18013–5:2021(E), Annex B; NIST Framework for Improving Critical Infrastructure Cybersecurity; NIST SP 800–53 Rev. 5; and NIST SP 800–57.[42]

- Certificate Authority Access Management requirements (Appendix A, paragraph 2) set forth policies and processes for States concerning, for example, restricting access to mDL issuance systems, policies for multi-factor authentication, defining the scope and role of personnel, and certificate system architecture which separates and isolates certificate system functions to defined security zones. These requirements must be implemented in full compliance with the references cited in Appendix A: CA/Browser Forum Network and Certificate System Security Requirements; NIST Framework for Improving Critical Infrastructure Cybersecurity; NIST 800–53 Rev. 5; NIST SP 800–63–3; and NIST SP 800–63B.[43]

Although NPRM Appendix A, paragraph 1.1, proposed requiring States to comply with NIST SP 800–53B (among other references) as part of States' development of a policy to govern their certificate systems, the final rule does not adopt the proposal requiring compliance with NIST SP 800–53B. Document NIST SP 800–53B, ''Control Baselines for Information Systems and Organizations,'' defines minimum security and privacy risk controls for Federal Government agencies to protect information security systems. In addition, the publication provides guidance, but not requirements, for other entities that implement NIST SP 800–53 Rev. 5 in their own organizations. Although TSA did not receive any public comments on NIST SP 800–53B, after re-evaluating the usefulness of this document, TSA concludes that other provisions in the final rule prescribe the necessary security and privacy requirements for States issuing mDLs, and NIST SP 800–53B only serves as guidance without providing security or privacy enhancements. Accordingly, the inclusion of NIST SP 800–53B is unnecessary, and the final rule therefore declines to adopt the NPRM's proposal.

- Under the requirements concerning Facility, Management, and Operational Controls (Appendix A, paragraph 3), States must provide specified controls protecting facilities where certificate systems reside from unauthorized access, environmental damage, physical breaches, and risks from foreign ownership, control, or influence. These requirements must be implemented in full compliance with the references cited in Appendix A: NIST SP 800–53 Rev. 5.[44]

- Personnel security controls (Appendix A, paragraph 4) require States to establish policies to control insider threat risks to certificate systems and facilities. Such policies must establish screening criteria for personnel who access certificate systems, post-employment access termination, updates to personnel security policy, training, records retention schedules, among other policies. These requirements must be implemented in full compliance with the references cited in Appendix A: NIST SP 800–53 Rev. 5 and CA/Browser Forum Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates.[45]

- Technical security controls (Appendix A, paragraph 5) specify requirements to protect certificate system networks. In addition, States are required to protect private cryptographic keys of issuing authority root certificates using dedicated hardware security modules (HSMs) of Level 3 or higher and document signer private cryptographic keys in hardware security modules of Level 2 and higher. Dedicated HSMs are used (1) solely for IACA root private key functions and no other functions within the State's certificate system, including document signer private key functions, and (2) exclusively to support a single State. States are not permitted to share with any other State an HSM that physically supports multiple States. Other controls are specified regarding certificate system architecture and cryptographic key generation processes. These requirements must be implemented in full compliance with the references cited in Appendix A: CA/Browser Forum Network and certificate system Security Requirements; CA/Browser Forum Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates; NIST Framework for Improving Critical Infrastructure Cybersecurity; NIST SP 800–53 Rev. 5; NIST SP 800–57; and NIST FIPS PUB 140–3.[46]

- Under requirements for threat detection (Appendix A, paragraph 6), States must implement controls to monitor and log evolving threats to various mDL issuance infrastructure, including digital certificate, issuance, and support systems. These requirements must be implemented in

[42] *See* NPRM, 88 FR at 60062–65, for a discussion of these standards.

[43] *See* NPRM, 88 FR at 60062–65, for a discussion of these standards.

[44] *See* NPRM, 88 FR at 60065, for a discussion of this standard.

[45] *See* NPRM, 88 FR at 60062–63 & 60065, for a discussion of these standards.

[46] *See* NPRM, 88 FR at 60062–63 & 60065, for a discussion of these standards.

full compliance with the references cited in Appendix A: CA/Browser Forum Network and certificate system Security Requirements; NIST Framework for Improving Critical Infrastructure Cybersecurity; and NIST SP 800–53 Rev. 5.[47]

- Logging controls (Appendix A, paragraph 7) require States to record various events concerning certificate systems, including the management of cryptographic keys, and digital certificate lifecycle events. The controls set forth detailed requirements concerning specific types of events that must be logged, as well as timeframes for maintaining such logs. These requirements must be implemented in full compliance with the references cited in Appendix A: CA/Browser Forum Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates; NIST Framework for Improving Critical Infrastructure Cybersecurity; and NIST SP 800–53 Rev. 5.[48]
- Incident Response and Recovery Plan (Appendix A, paragraph 8) requires States to implement policies to respond to and recover from security incidents. States must act on logged events, issue alerts to relevant personnel, respond to alerts within a specified time period, perform vulnerability scans, among other things. In particular, States must report to TSA at *www.tsa.gov/real-id/mDL* within 72 hours of discovering a reportable cybersecurity incident. In response to comments to the NPRM seeking clarity on the reporting requirements (*see* Part IV.V.5.c., below), the final rule adds a provision that reportable incidents are those defined in the TSA Cybersecurity Lexicon at *www.tsa.gov* that could compromise the integrity of a certificate system. These requirements must be implemented in full compliance with the references cited in Appendix A: CA/Browser Forum Network and Certificate System Security Requirements; CISA Federal Government Cybersecurity Incident & Vulnerability Response Playbooks; [49] DHS National Cyber Incident Response Plan; NIST SP 800–53 Rev. 5; and NIST Framework for Improving Critical Infrastructure Cybersecurity.[50] Information submitted in response to this section *may* contain SSI, and if so, would be subject to requirements of 49 CFR part 1520. Although the NPRM did not propose the SSI protection provision, TSA evaluated comments to the NPRM (see Part IV.W., below) seeking clarification on SSI protection for other information (State waiver applications) and determined that SSI protection is warranted for State reports under this Appendix paragraph 8, which has been added in this final rule.

5. Decisions on Applications for Waiver

Section 37.9(b) establishes a timeline and process for TSA to issue decisions on a waiver application. Under this paragraph, TSA endeavors to provide States a decision on initial applications within 60 calendar days, but not longer than 90 calendar days. TSA will provide three types of written notice via email: approved, insufficient, or denied.

If TSA approves a State's application for a waiver, TSA will issue a certificate of waiver to that State, and include the State in a list of mDLs approved for Federal use, published by TSA on the REAL ID website at *www.tsa.gov/real-id/mDL.*[51] A certificate of waiver will specify the date that the waiver becomes effective, the expiration date, and any other terms and conditions with which a State must comply, as provided under § 37.9(d). A State seeking to renew its certificate beyond the expiration date must reapply for a waiver, as provided in § 37.9(e)(6).

If TSA determines that an application is insufficient, did not respond to certain information required in §§ 37.10(a) or (b), or contains other deficiencies, TSA will provide an explanation of such deficiencies and allow the State an opportunity address the deficiencies within the timeframe specified in § 37.9(b)(2). TSA will permit States to submit multiple amended applications if necessary, with the intent of working with States individually to enable their mDLs to comply with the requirements of §§ 37.10(a) and (b).

As provided in § 37.9(b)(3), if TSA denies an application, TSA will provide the specific grounds for the basis of the denial and afford the State an opportunity to submit a new application or to seek reconsideration of a denied application. Under § 37.9(c)(1), States will have 90 calendar days to file a request for reconsideration, and TSA will provide its final determination within 60 calendar days. Instructions for seeking reconsideration are provided by TSA on the REAL ID website at *www.tsa.gov/real-id/mDL.* As provided in § 37.9(c)(2), an adverse decision upon reconsideration would be considered a final agency action. However, a State whose request for reconsideration has been denied may submit a new application for a waiver.

6. Limitations, Suspension, and Termination of Certificate of Waiver

Section 37.9(e) sets forth various terms regarding a certificate of waiver. Specifically, under paragraph (e)(1) of this section, a certificate of waiver is valid for a period of three years from the date of issuance. This period was selected to align with the frequency of States' recertification under § 37.55(b).

Paragraph (e)(2) requires that a State must report to TSA if, after it receives a waiver, it makes significant modifications to its mDL issuance processes that differ in a material way from information that the State provided in its application. If the State makes such modifications, it is required to report such changes, at *www.tsa.gov/real-id/mDL,* 60 calendar days before implementing the changes. This requirement is intended to apply to changes that may undermine the bases on which TSA granted a waiver. The reporting requirement is not intended to apply to routine, low-level changes, such as systems maintenance and software updates and patches. States that are uncertain about whether a change would trigger the reporting requirements should contact TSA as directed at *www.tsa.gov/real-id/mDL.* The final rule added this provision to contact TSA to provide greater certainty to States, following TSA's evaluation of public comments seeking clarification about the reporting requirements specified in the NPRM (see Part IV.S., below).

Paragraph (e)(3) requires a State that is issued a waiver to comply with all requirements specified in §§ 37.51(a) and 37.9(d)(3).

Paragraph (e)(4) sets forth processes for suspension of certificates of waiver. As provided in § 37.9(e)(4)(i)(A), TSA may suspend the validity of a certificate of waiver if TSA determines that a State:

- fails to comply with any terms and conditions (*see* § 37.9(d)(3)) specified in the certificate of waiver;
- fails to comply with reporting requirements (*see* § 37.9(e)(2)); or
- issues mDLs in a manner that is not consistent with the information the State provided in its application for a waiver under §§ 37.10(a) and (b).

Before suspending a waiver for these reasons, TSA will provide such State written notice via email that it intends to suspend its waiver, along with an explanation of the reasons, information on how the State may address the deficiencies, and a timeline for the State to respond and for TSA to reply to the

[47] *See* NPRM, 88 FR at 60062–63 & 60065, for a discussion of these standards.

[48] *See* NPRM, 88 FR at 60062–63 & 60065, for a discussion of these standards.

[49] The NPRM inadvertently omitted ''Federal Government'' from the title of this publication.

[50] *See* NPRM, 88 FR at 60062–63 & 60065, for a discussion of these standards.

[51] Section 37.9(b)(1).

State, as set forth in § 37.9(e)(4)(ii). TSA may withdraw the notice of suspension, request additional information, or issue a final suspension. If TSA issues a final suspension of a State's certificate of waiver, TSA will temporarily remove the name of that State from the list, published at *www.tsa.gov/real-id/mDL,* of mDLs approved for Federal acceptance for official purposes.[52] TSA intends to work with States to resolve the conditions that result in a final suspension, and resume validity of that State's waiver. A State receiving a final suspension may apply for a new certificate of waiver by submitting a new application following the procedures in § 37.9(a).

TSA additionally may suspend a State's waiver at any time upon discovery that Federal acceptance of a State's mDL is likely to cause imminent or serious threats to the security, privacy, or data integrity of any Federal agency, as set forth in § 37.9(e)(4)(i)(B). These are more exigent circumstances than those set forth in § 37.9(e)(4)(i)(A). Examples of such triggering events include cyber-attacks and other events that cause serious harm to a State's mDL issuance systems. If a State discovers a reportable cybersecurity incident, as defined in the TSA Cybersecurity Lexicon available at *www.tsa.gov,* that it believes could compromise the integrity of its mDL issuance systems, paragraph 8.6 of Appendix A requires States to provide written notice to TSA as directed at *www.tsa.gov/real-id/mDL,* of such incident within no more than 72 hours of discovery. If TSA determines such suspension is necessary, TSA will provide written notice via email to each State whose certificate of waiver is affected, as soon as practicable after discovery of the triggering event, providing an explanation for the suspension, as well as an estimated timeframe for resumption of the validity of the certificate of waiver.

Under § 37.9(e)(5)(i), TSA may terminate a certificate of waiver for serious or egregious violations. More specifically, TSA may terminate a waiver if TSA determines that a State:

- does not comply with REAL ID requirements in § 37.51(a);
- is committing an egregious violation of any terms and conditions (*see* § 37.9(d)(3)) specified in the certificate of waiver and is unwilling to cure such violation;
- is committing an egregious violation of reporting requirements (*see* § 37.9(e)(2)) and is unwilling to cure such violation; or
- provided false information in its waiver application.

As required in § 37.9(e)(5)(ii), before terminating a certificate of waiver, TSA will provide written notice via email of intent to terminate, including findings supporting the termination and an opportunity for the State to present information. As specified, a State would have 7 calendar days to respond to the notice, and TSA will respond via email within 30 calendar days. TSA may withdraw the notice of termination, request additional information, or issue a final termination. Under § 37.9(e)(5)(iii), if TSA issues a final termination of a State's certificate of waiver, TSA will remove the name of that State from the list of mDLs approved for Federal acceptance for official purposes. A State whose certificate of waiver has been terminated may apply for a new certificate of waiver by submitting a new application.

Section 37.9(g) provides that information provided by States in response to paragraphs (a), (b)(2), (c), (e)(2), (e)(4)(ii), and (e)(5)(ii) of this section, which concern requirements on States to apply for and maintain a waiver, *may* contain SSI and therefore must be handled and protected in accordance with 49 CFR part 1520. Although the NPRM did not propose § 37.9(g), the final rule adds this provision based on TSA's evaluation of comments to the NPRM (see Part IV.W., below) seeking clarification on SSI protection for information in State waiver applications. TSA determined that a provision concerning SSI protection is warranted not only for information in State waiver applications, but also for other information provided by States in response to §§ 37.9(b)(2), (c), (e)(2), (e)(4)(ii), and (e)(5)(ii), which has been added in this final rule.

7. Effect of Status of Waiver on REAL ID Compliance

Section 37.9(f) clarifies that the status of a State's issued certificate of waiver, including the status of a pending application for a waiver, has no bearing on TSA's determination of that State's compliance or non-compliance with any other section of this part. A certificate of waiver that TSA has issued to a State is not a determination that the State is in compliance with any other section in this part. Similarly, an application for a waiver that TSA has deemed insufficient or denied, or a certificate of waiver TSA has suspended or terminated, or that has expired, is not a determination that the State is not in compliance with any other section in this part.

8. Incorporation by Reference

Sections 37.8(b) and 37.10(a) and Appendix A of this final rule provide that States must comply with applicable sections of specified industry standards and government guidelines. The Office of Federal Register (OFR) has published regulations concerning IBR.[53] These regulations require that, for a final rule, agencies must discuss in the preamble to the rule the way in which materials that the agency IBRs are reasonably available to interested persons, and how interested parties can obtain the materials. Additionally, the preamble to the rule must summarize the material.[54]

The final rule amends subpart A, § 37.4, by revising the introductory paragraph and adding new IBR material specified below. TSA has worked to ensure that IBR materials are reasonably available to the class of persons affected. All materials may be obtained from their publisher, as discussed below, and certain materials as noted are available in the Federal Docket Management System at *https://www.regulations.gov,* docket number TSA–2023–0002. In addition, all but one of the IBR'd standards (ISO/IEC 18013–5:2021(E), discussed in Part II.D., below) are available to the public for free at the hyperlinks provided, and all are available for inspection on a read-only basis at TSA. Please contact TSA at Transportation Security Administration, Attn.: OS/ESVP/REAL ID Program, TSA Mail Stop 6051, 6595 Springfield Center Dr., Springfield, VA 20598–6051, (866) 289–9673, or visit *www.tsa.gov.* You may also contact the REAL ID Program Office at *REALID-mDLwaiver@tsa.dhs.gov* or visit *www.tsa.gov/REAL-ID/mDL.*[55]

The rule revises the introductory paragraph proposed in the NPRM to clarify availability of IBR materials. Specifically, the final rule replaces DHS with TSA as a location where IBR material is available for inspection, and provides additional points of contact at TSA. TSA also notes that certain material is available in the Federal Docket Management System at *https://regulations.gov,* docket number TSA–2023–0002. The final rule makes these revisions given TSA's evaluation of public comments concerning access to IBR materials (see Part IV.K., below).

The final rule IBRs the following material:

[52] Section 37.9(e)(4)(iii).

[53] 1 CFR part 51.

[54] 1 CFR 51.5(b).

[55] The National Archives and Records Administration (NARA) maintains the official Federal copy of the IBR'd standards, but does not provide or distribute copies. *See www.archives.gov/federal-register/cfr/ibr-locations.htm* (last visited Sept. 17, 2024).

a. American Association of Motor Vehicle Administrators

In September 2022, the American Association of Motor Vehicle Administrators (AAMVA) published *Mobile Driver's License (mDL) Implementation Guidelines Version 1.2* (Jan. 2023) (AAMVA Guidelines), American Association of Motor Vehicle Administrators, 4401 Wilson Boulevard, Suite 700, Arlington, VA 22203, available at *https://aamva.org/getmedia/b801da7b-5584-466c-8aeb-f230cef6dda5/mDL-Implementation-Guidelines-Version-1-2_final.pdf* (last visited July 17, 2024). The AAMVA Guidelines are available to the public for free at the link provided above. The AAMVA Guidelines adapt industry standard ISO/IEC 18013–5:2021(E) (discussed in Part II.D.4., below), for State driver's licensing agencies through the addition of more qualified recommendations, as the ISO/IEC standard has been developed for international purposes and may not meet all purposes and needs of States and the Federal Government. For example, Part 3.2 of the AAMVA Guidelines modify and expand the data elements specified in ISO/IEC 18013–5:2021(E), in order to enable the mDL to indicate the REAL ID compliance status of the underlying physical card, as well as to ensure interoperability necessary for Federal acceptance. AAMVA has added mDL data fields ''DHS_compliance'' and ''DHS_temporary_lawful_status.'' These data fields provide the digital version of the requirements for data fields for physical cards defined in 6 CFR 37.17(n) [56] and 6 CFR 37.21(e),[57] respectively. As discussed generally in Part III.C.4, below, §§ 37.10(a)(1) and (4) of this rule require a State to explain, as part of its application for a waiver, how the State issues mDLs that are compliant with specified requirements of the AAMVA Guidelines.

b. Certification Authority Browser Forum

The Certification Authority Browser Forum (CA/Browser Forum) is an organization of vendors of hardware and software used in the production and use of publicly trusted certificates. These certificates are used by forum members, non-member vendors, and governments to establish the security and trust mechanisms for public key infrastructure-enabled systems. The CA/Browser Forum has published two sets of requirements applicable for any implementers of PKI, including States that are seeking to deploy certificate systems that must be publicly trusted and used by third parties:

- *Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates* v. *1.8.6* (December 14, 2022), available at *https://cabforum.org/wp-content/uploads/CA-Browser-Forum-BR-1.8.6.pdf* (last visited July 17, 2024), establishes a set of fundamental controls for the management of publicly trusted certificate authorities, including the controls and processes required for the secure generation of digital signing keys; and
- *Network and Certificate System Security Requirements* v. *1.7* (April 5, 2021), available at *https://cabforum.org/wp-content/uploads/CA-Browser-Forum-Network-Security-Guidelines-v1.7.pdf* (last visited July 17, 2024), establishes a broad set of security controls needed to securely manage a publicly trusted certificate authority and key infrastructure management system.

CA/Browser Forum, 815 Eddy St, San Francisco, CA 94109, (415) 436–9333. To issue mDLs that can be trusted by Federal agencies, each issuing State must establish a certificate system, including a root certification authority that is under control of the issuing State. TSA believes the CA/Browser Forum requirements for publicly trusted certificates have been proven to be an effective model for securing online transactions. As discussed generally in Part III.C.4, below, Appendix A, paragraphs 1, 2, and 4–8, require compliance with specified requirements of the CA/Browser Forum Baseline Requirements and/or Network and Certificate System Security Requirements.

c. DHS and Cybersecurity and Infrastructure Security Agency

DHS protects the nation from multiple threats, including cybersecurity, aviation and border security, among others. The Cybersecurity and Infrastructure Security Agency (CISA), a component of DHS, is the operational lead for Federal cybersecurity and the national coordinator for critical infrastructure security and resilience. DHS and CISA have published two guidelines which are relevant to the operations of States' mDL issuance systems:

- *DHS, National Cyber Incident Response Plan* (Dec. 2016), available at *https://www.cisa.gov/uscert/sites/default/files/ncirp/National_Cyber_IncidentResponse_Plan.pdf* (last visited July 17, 2024), further standardizes the response process for cyber incidents including the preparation, detection and analysis, containment, eradication and recovery, and post-incident activities. Department of Homeland Security, 2707 Martin Luther King Jr. Ave. SE, Washington, DC 20528; (202) 282–8000; and
- *CISA, Federal Government Cybersecurity Incident & Vulnerability Response Playbooks* (Nov. 2021),[58] available at *https://www.cisa.gov/sites/default/files/publications/Federal_Government_Cybersecurity_Incident_and_Vulnerability_Response_Playbooks_508C.pdf* (last visited July 17, 2024), was developed consistent with the direction of Presidential Policy Directive 41 (PPD–41) to establish how the U.S. responds to and recovers from significant cyber incidents which pose a risk to critical infrastructure, including the identity issuance infrastructure operated by U.S. States issuing mDLs.

Cybersecurity and Infrastructure Security Agency, Mail Stop 0380, 245 Murray Lane, Washington, DC 20528–0380, (888) 282–0870. These guidelines, available for free at the links provided above and in the Federal Docket Management System at *https://www.regulations.gov,* docket number TSA–2023–0002, provide details on best practices for management of systems during a cybersecurity incident, providing recommendations on incident and vulnerability response. Management of cybersecurity incidents and vulnerabilities is critical to maintenance of a State's mDL issuance IT infrastructure. As discussed generally in Part III.C.4, below, Appendix A, paragraph 8, requires compliance with specified requirements of the DHS National Cyber Incident Response Plan and the CISA Federal Government Cybersecurity Incident & Vulnerability Response Playbooks.

d. International Organization for Standardization and International Electrotechnical Commission

International standards-setting organizations, the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC),[59] are jointly drafted

[56] Section 37.17(n) provides, ''The card shall bear a DHS-approved security marking on each driver's license or identification card that is issued reflecting the card's level of compliance as set forth in § 37.51 of this Rule.''

[57] Section 37.21(e) provides, ''Temporary or limited-term driver's licenses and identification cards must clearly indicate on the face of the license and in the machine readable zone that the license or card is a temporary or limited-term driver's license or identification card.''

[58] The NPRM inadvertently omitted ''Federal Government'' from the title of this publication.

[59] ISO is an independent, non-governmental international organization with a membership of 164 national standards bodies. ISO creates documents that provide requirements,

international standards specific to mDLs.[60] In September 2021, ISO and IEC published ISO/IEC 18013, Part 5, entitled, ''Personal identification—ISO-compliant driving licence.'' ISO/IEC 18013–5:2021(E), *Personal identification—ISO-compliant driving licence—Part 5: Mobile driving licence (mDL) application* (Sept. 2021), International Organization for Standardization, Chemin de Blandonnet 8, CP 401, 1214 Vernier, Geneva, Switzerland, +41 22 749 01 11, *www.iso.org/contact-iso.html.* This standard is available for inspection at TSA as discussed above. In addition, TSA is working with the American National Standards Institute (ANSI), a private organization not affiliated with DHS, to add this standard to the ANSI IBR Standards Portal which provides free, read-only access.[61] TSA has participated in the development of these standards as a non-voting member of the United States national body member of the Joint Technical Committee.[62]

Standard ISO/IEC 18013–5:2021(E) standardizes communications interfaces between an mDL holder and an entity seeking to read an individual's mDL for identify verification purposes, and between a verifying entity and a State driver's licensing agency. This standard also sets full operational and communication requirements for both mDLs and mDL readers. Standard ISO/IEC 18013–5:2021(E) applies to ''attended'' mode verification, in which both the mDL holder and an officer or agent of a verifying entity are physically present together during the time of identity verification.[63] TSA believes ISO/IEC 18013–5:2021(E) is critical to enabling the interoperability, security, and privacy necessary for wide acceptance of mDLs by Federal agencies for official purposes. Specifically, § 37.8 of this rule requires Federal agencies to validate an mDL as required by standard ISO/IEC 18013–5:2021(E), and § 37.10(a)(4) requires a State to explain, as part of its application for a waiver, how the State issues mDLs that are interoperable with this standard to provide the security necessary for Federal acceptance.

e. National Institute for Standards and Technology

The National Institute of Standards and Technology (NIST), part of the U.S. Department of Commerce, promotes U.S. innovation and industrial competitiveness by advancing measurement science, standards, and technology in ways that enhance economic security and quality of life. As part of this mission, NIST produces measurements and standards relied on by the U.S. agencies and industry.

i. Federal Information Processing Standards

NIST maintains the Federal Information Processing Standards (FIPS) which relate to the specific protocols and algorithms necessary to securely process data. This suite of standards includes:

- NIST FIPS PUB 140–3, *Security Requirements for Cryptographic Modules* (March 22, 2019), available at *https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.140-3.pdf* (last visited July 17, 2024), specifies the security requirements for cryptographic modules that are used to secure the keys which are used in digitally signing mDLs, and properly securing these keys is essential to creating a publicly trusted certificate authority for mDL issuance;
- NIST FIPS PUB 180–4, *Secure Hash Standard (SHS)* (August 4, 2015), available at *https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.180-4.pdf* (last visited July 17, 2024), specifies the secure hash standard, a cryptographic algorithm necessary to provide message and data element integrity while using the transaction modes specified in ISO/IEC 18013–5:2021(E) for mDL data transmission;
- NIST FIPS PUB 186–5, *Digital Signature Standard (DSS)* (February 3, 2023), available at *https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.186-5.pdf* (last visited July 17, 2024), specifies digital signature standards used in ISO/IEC 18013–5:2021(E) standard to provide data integrity for mDL data elements issued by states; and
- NIST FIPS PUB 197–upd1, *Advanced Encryption Standard (AES)* (May 9, 2023) available at *https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.197-upd1.pdf* (last visited July 17, 2024), specifies the Advanced Encryption Standard, which is a cryptographic algorithm used to securely encrypt data messages used in the transmission of mDL data in ISO/IEC 18013–5:2021(E).

Although the NPRM proposed to IBR the prior (2001) version, NIST FIPS PUB 197, the final rule IBRs the current (May 2023) updated version, NIST FIPS PUB 197–upd1, which NIST confirms makes editorial improvements, but no technical changes to the version specified in the NPRM.[64] TSA has reviewed the updates and confirms they are formatting and stylistic clarifications. Although the public had an opportunity to comment, no such comments were received. Given the absence of public comments, no substantive changes to the updated standard, and to ensure continuing public access to this standard, the final rule IBRs the updated version, NIST FIPS PUB 197–upd1, which is consistent with the NPRM's proposal to IBR the previous version. TSA concludes that the compliance impact on stakeholders of both versions of this standard is identical.

- NIST FIPS PUB 198–1, *The Keyed-Hash Message Authentication Code (HMAC)* (July 16, 2008) available at *https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.198-1.pdf* (last visited July 17, 2024), specifies the keyed hash message authentication code which is an essential cryptographic algorithm to create a properly interoperable mDL using ISO/IEC 18013–5:2021(E); and
- NIST FIPS PUB 202, *SHA–3 Standard: Permutation-Based Hash and Extendable-Output Functions* (August 4, 2015) available at *https://*

specifications, guidelines or characteristics that can be used consistently to ensure that materials, products, processes and services are fit for their purpose. The IEC publishes consensus-based international standards and manages conformity assessment systems for electric and electronic products, systems and services, collectively known as ''electrotechnology.'' ISO and IEC standards are voluntary and do not include contractual, legal or statutory obligations. ISO and IEC standards contain both mandatory requirements and optional recommendations, and those who choose to implement the standards must adopt the mandatory requirements.

[60] ISO defines an International Standard as ''provid[ing] rules, guidelines or characteristics for activities or for their results, aimed at achieving the optimum degree of order in a given context. It can take many forms. Apart from product standards, other examples include: test methods, codes of practice, guideline standards and management systems standards.'' *www.iso.org/deliverables-all.html* (last visited July 17, 2024).

[61] ANSI, IBR Standards Portal, *https://ibr.ansi.org/* (last visited July 17, 2024).

[62] A member of TSA serves as DHS's representative to the Working Group.

[63] Part 7 of Series ISO/IEC 18013, entitled ''mDL add-on function,'' is an upcoming technical specification that will standardize interfaces for ''unattended'' mode verification, in which the mDL holder and officer/agent of the verifying agency are not physically present together, and the identity verification is conducted remotely. Unattended identity verification is not currently considered a REAL ID use case. ISO defines a ''Technical Specification'' as ''address[ing] work still under technical development, or where it is believed that there will be a future, but not immediate, possibility of agreement on an International Standard. A Technical Specification is published for immediate use, but it also provides a means to obtain feedback. The aim is that it will eventually be transformed and republished as an International Standard.'' ISO, Deliverables, *www.iso.org/deliverables-all.html* (last visited July 17, 2024).

[64] *See https://csrc.nist.gov/News/2023/nist-updates-fips-197-advanced-encryption-standard* (last visited July 17, 2024); *https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.197-upd1.pdf* (last visited July 17, 2024) at 37; *https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.197.pdf* (last visited July 17, 2024) at 1.

nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.202.pdf (last visited July 17, 2024), specifies the secure hash algorithm 3, a cryptographic algorithm necessary to provide message and data element integrity in ISO/IEC 18013–5:2021(E) for mDL data transmission.

National Institute of Standards and Technology, U.S. Department of Commerce, 100 Bureau Drive, Gaithersburg, MD 20899. This suite of FIPS standards, available in the Federal Docket Management System at *https://www.regulations.gov,* docket number TSA–2023–0002, are critical to the transactions required for mDLs, and any Federal systems which interact with or are used to verify an mDL for REAL ID official purposes will be required to use the algorithms and protocols defined. As discussed generally in Part III.C.4, below, § 37.10(a)(4) requires compliance with specified requirements of NIST FIPS PUB 180–4, 186–5, 197–upd1, 198–1, and 202, and Appendix A, paragraph 5, requires compliance with FIPS PUB 140–3.

ii. Security and Privacy Controls for Information Systems and Organizations; Key Management

NIST has published several guidelines to protect the security and privacy of information systems:

- NIST SP 800–53 Rev. 5, *Security and Privacy Controls for Information Systems and Organizations* (September 2020), available at *https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf* (last visited July 17, 2024), specifies a broad set of security and privacy controls which states must use to manage the information systems involved in the issuance and management of mDLs;
- NIST SP 800–57 Part 1, Rev. 5, *Recommendation for Key Management: Part 1—General* (May 2020), available at *https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-57pt1r5.pdf* (last visited July 17, 2024), provides general recommendations for states managing cryptographic keys that are used to securely issue mDLs;
- NIST SP 800–57 Part 2, Rev. 1, *Recommendation for Key Management: Part 2—Best Practices for Key Management Organizations* (May 2019), available at *https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-57pt2r1.pdf* (last visited July 17, 2024), provides best practices states must follow while managing cryptographic keys; and
- NIST SP 800–57 Part 3, Rev. 1, *Recommendation for Key Management, Part 3: Application-Specific Key Management Guidance* (January 2015) available at *https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-57Pt3r1.pdf* (last visited July 17, 2024), provides for application specific controls for the management of cryptographic keys.

National Institute of Standards and Technology, U.S. Department of Commerce, 100 Bureau Drive, Gaithersburg, MD 20899. All of these documents are available in the Federal Docket Management System at *https://www.regulations.gov,* docket number TSA–2023–0002.

All four of these standards relate to the administration of a certificate system including: access management; certificate life-cycle policies; operational controls for facilities and personnel; technical security controls; and vulnerability management such as threat detection, incident response, and recovery planning. Due to the sensitive nature of State certificate system processes and the potential for significant harm to security if confidentiality, integrity, or availability of the certificate systems is compromised, the minimum risk controls specified in Appendix A require compliance with the NIST SP 800–53 Rev. 5 ''high baseline'' as set forth in that document, as well as compliance with the specific risk controls described in Appendix A. In addition, and as discussed generally in Part III.C.4, below: Appendix A, paragraphs 1–8, require compliance with NIST SP 800–53 Rev. 5; paragraphs 1 and 5 require compliance with NIST SP 800–57 Part 1, Rev. 5; paragraph 1 requires compliance with NIST SP 800–57 Part 2 Rev. 1; and paragraph 1 requires compliance with NIST SP 800–57 Part 3, Rev. 1.

iii. Digital Identity Guidelines

NIST has published NIST SP 800–63–3, which covers technical requirements for Federal agencies implementing digital identity: NIST Special Publication 800–63–3, *Digital Identity Guidelines* (June 2017), National Institute of Standards and Technology, U.S. Department of Commerce, 100 Bureau Drive, Gaithersburg, MD 20899, available at *https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63-3.pdf* (last visited July 17, 2024)and in the Federal Docket Management System at *https://www.regulations.gov,* docket number TSA–2023–0002.

The *Digital Identity Guidelines* define technical requirements in each of the areas of identity proofing, registration, user authentication, and related issues. Because TSA is not aware of a common industry standard for mDL provisioning that is appropriate for official REAL ID purposes today, TSA views the *Digital Identity Guidelines* as critical to informing waiver application requirements for States regarding provisioning. As discussed generally in Part III.C.4, below, under § 37.10(a)(2) of the final rule, which requires compliance with Appendix A, a State must explain, as part of its application for a waiver, how the State issues mDLs that are compliant with NIST SP 800–63–3 to provide the security for mDL IT infrastructure necessary for Federal acceptance.

NIST has also published Special Publication 800–63B, *Digital Identity Guidelines: Authentication and Lifecycle Management* (June 2017), National Institute of Standards and Technology, U.S. Department of Commerce, 100 Bureau Drive, Gaithersburg, MD 20899, available at *https://nvlpubsnist.gov/nistpubs/specialpublications/nist.sp.800-63b.pdf* (last visited July 17, 2024) and in the Federal Docket Management System at *https://www.regulations.gov,* docket number TSA–2023–0002. This document, which is a part of NIST SP 800–63–3, provides technical requirements for Federal agencies implementing digital identity services. The standard focuses on the authentication of subjects interacting with government systems over open networks, establishing that a given claimant is a subscriber who has been previously authenticated and establishes three authenticator assurance levels. As discussed generally in Part III.C.4, below, § 37.10(a)(2) of this rule requires compliance with Appendix A, which requires a State to explain, as part of its application for a waiver, how the State manages its mDL issuance infrastructure using authenticators at assurance levels provided in NIST SP 800–63B.

iv. Framework for Improving Critical Infrastructure Cybersecurity

NIST has published *Framework for Improving Critical Infrastructure Cybersecurity* v. *1.1* (April 16, 2018), National Institute of Standards and Technology, U.S. Department of Commerce, 100 Bureau Drive, Gaithersburg, MD 20899, available at *https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf* (last visited July 17, 2024). This document, available in the Federal Docket Management System at *https://www.regulations.gov,* docket number TSA–2023–0002, provides relevant information for cybersecurity for States issuing mDLs. As discussed generally in Part III.C.4, below, certain requirements from the NIST Framework for Improving

Critical Infrastructure Cybersecurity have been adopted in Appendix A, paragraphs 1, 2, and 5–8.

D. Impacted Stakeholders

This final rule applies to State driver's licensing agencies issuing mDLs that seek a temporary waiver from TSA for its mDLs. The waiver established by this rule enables Federal agencies to accept such mDLs for official purposes, defined in the REAL ID Act as accessing Federal facilities, entering nuclear power plants, boarding Federally regulated commercial aircraft, and any other purposes that the Secretary shall determine. Any Federal agency that chooses to accept mDLs for official purposes must procure a reader in order to receive an individual's identity data.

This final rule does not apply to:

- States that do not seek a waiver for mDLs;
- Non-State issuers of other forms of digital identification; or
- Federal agencies that elect not to accept mDLs.

A State seeking a waiver for Federal acceptance of its mDLs for official purposes is required to file with TSA a complete application and supporting documents.[65] A State must demonstrate how its mDLs meet the requirements for a waiver set forth in §§ 37.10(a) and (b) when completing the application.

E. Use Cases Affected by This Rule

This final rule applies only to Federal acceptance of mDLs for official purposes, defined by the REAL ID regulations as accessing Federal facilities, entering nuclear power plants, and boarding Federally regulated commercial aircraft. Any other purpose is beyond the scope of this rulemaking. For example, a waiver issued under this rule does not apply to any of the following:

- mDL acceptance by Federal agencies for non-REAL ID official uses (*e.g.,* applying for Federal benefits);
- mDL acceptance by non-Federal agencies (*e.g.,* State agencies, businesses, private persons);
- Commercial transactions; or
- Physical driver's licenses or identification cards.

Nothing in this rule *requires* Federal agencies to accept mDLs, as each Federal agency retains the discretion to determine its identification policies. Additionally, nothing in this rule *requires* a State to seek a waiver or issue mDLs.

F. Severability

TSA notes that these changes impact multiple provisions that are not necessarily interrelated and can function independent of one another. As such, TSA believes that some of the provisions of each new part can function sensibly independent of other provisions. Therefore, in the event that any provisions in this rulemaking action as finalized are invalidated by a reviewing court, TSA intends remaining provisions to remain in effect to the fullest extent possible.

IV. Discussion of Comments

TSA published the NPRM on August 30, 2023,[66] and the deadline for public comments was October 16, 2023. TSA received 31 comments,[67] including some comments that were submitted shortly after the comment period closed. TSA carefully considered every comment received as part of the official record, including those that were submitted late. Comments and TSA's responses are as summarized by topic below.

A. Waiver Eligibility

Comments: Several State driver's licensing agencies, an association, and some vendors expressed concerns that under §§ 37.7(b)(3) and 37.10(a)(1)(vii) of the NPRM, TSA would issue waivers to States that issued mDLs only to holders of REAL ID-compliant physical cards, but a State that issues mDLs to two groups of individuals—both holders of REAL ID-compliant AND non-compliant physical cards—would be ineligible for a waiver because of issuance to the latter group. Stated differently, a State's issuance of mDLs to holders of non-compliant physical cards alone would remove the State's eligibility to apply for a waiver.

Another commenter requested clarification regarding whether a State may still apply for and receive a waiver after enforcement of the REAL ID Act and regulations begins on May 7, 2025.

TSA Response: TSA agrees with commenters and is revising the final rule to clarify that a State will not be excluded from eligibility to apply for a waiver if a State issues mDLs to both REAL ID compliant and non-compliant physical cardholders. The intended purpose of TSA's requirement is for States to ensure that an individual's mDL matches the compliance status of the underlying physical card, and for States to issue an mDL in a manner that enables a verifying Federal agency to confirm the underlying physical card's REAL ID compliance status.

Consistent with that intent, and to address commenters' concerns, the final rule makes three changes to the NPRM. First, this final rule deletes § 37.7(b)(3), as proposed by the NPRM, which provided as a criterion of waiver eligibility that a State must issue mDLs only to individuals who have been issued REAL ID-compliant physical cards.

Second, the final rule deletes a similar requirement from § 37.10(a)(1)(vii), as proposed by the NPRM, which provided that States must issue an mDL only to a resident who has been issued a valid, unexpired, and REAL ID-compliant physical card that underlies the mDL. The final rule modifies this provision to require States to populate this data field to correspond to the REAL ID compliance status of the underlying physical driver's license or identification card that a State has issued to an mDL holder. Specifically, § 37.10(a)(1)(vii)(A) requires mDL data element ''DHS_compliance'' to be populated with ''F'' if the underlying card is REAL ID-compliant, or as required by the AAMVA Guidelines,[68] Section 3.2. In addition, § 37.10(a)(1)(vii)(B) requires mDL data element ''DHS_compliance'' to be populated ''N'' if the underlying card is not REAL ID-compliant.

Third, the final rule adds new § 37.8(c), which requires Federal agencies to confirm that the physical card underlying the mDL is REAL ID-compliant, as Federal agencies will only be permitted to accept mDLs if the underlying card is REAL ID-compliant. Federal agencies would make that determination by reviewing data element ''DHS_compliance'' and confirming that it has been marked ''F.'' These changes ensure—without compromising a State's waiver eligibility—that an individual's mDL matches the compliance status of the physical card, and that Federal agency will accept only those mDLs that are based on a REAL ID-compliant underlying physical card.

Separately, in response to the commenter's question regarding waiver applications after REAL ID enforcement begins on May 7, 2025, TSA confirms that a State indeed may apply for and receive a waiver after enforcement begins.

B. Conditions on Federal Agencies Accepting mDLs

Comments: An association requested clarification concerning requirements

[65] Section 37.9(a).

[66] *See* 88 FR 60056.

[67] The 31 total comments include one duplicate, one correction, and one confidential submission.

[68] The AAMVA Guidelines require, among other things, that if the 'EDL_credential' element is present, the 'DHS_compliance' element shall have a value of ''F.''

on Federal agencies that choose to accept mDLs. Specifically, the commenter noted that the preamble provided that one of the ''conditions for TSA acceptance'' is that TSA has determined the mDL issuing State is REAL ID-compliant. The commenter sought clarification on the timing of when this compliance determination is made, specifically, whether this is a one-time determination, whether it is made at the time when TSA is reviewing a State's application, or if the State's re-certification schedule is applicable.

TSA Response: First, TSA notes that this rule does not set conditions only for ''TSA Acceptance.'' Instead, the rule sets forth requirements for all Federal agencies who choose to accept mDLs for official purposes as defined in the REAL ID Act. Second, TSA clarifies that determination of a State's REAL ID compliance status is not a requirement for other Federal agencies to make. The only conditions on Federal agencies who accept mDLs are set forth in § 37.8, which requires the agency to: (1) confirm the State holds a valid waiver by reviewing the specified TSA website, (2) use an mDL reader to communicate with and validate an individual's mDL, (3) confirm that the underlying physical card is REAL ID-compliant, and (4) notify TSA within 72 hours of the discovery of specified security, privacy, or data integrity threats. A State's compliance status is an element of a State's eligibility to apply for a waiver, as set forth in § 37.7(b)(1), and TSA will make this determination when reviewing a State's application. However, TSA acknowledges that the preamble to the NPRM states that a Federal agency must make this compliance determination. TSA has revised the preamble to this final rule to reflect the intended requirements.

In response to comments, TSA also provides further clarification on the timing of its determination of a State's compliance status. TSA will make an initial determination of State compliance status at the time of application, but this is *not* a one-time determination. States have a continuing obligation, under 6 CFR 37.55(b), to maintain their compliance status by recertifying compliance every 3 years, an obligation which continues throughout the duration of the waiver. If recertification occurs after a State is issued a waiver and TSA determines the State is no longer in compliance, the waiver may be subject to review pursuant to § 37.9(e)(5).

C. Waiver Application Criteria

1. Personally Identifiable Information and Privacy

Comments: An association remarked that § 37.10(a)(1)(i) introduces additional requirements concerning individuals' Personally Identifiable Information (PII) that are not related to mDL issuance and exceed existing requirements in the regulations. The commenter advised that the rule should not expand REAL ID requirements that are unrelated to mDLs.

The association further noted that although privacy is an important concept, it applies mostly to the agreement between an issuing State and the mDL holder, and that the only applicability to verifying Federal agencies is ensuring that the agency receives only the information necessary for identity verification. The commenter therefore recommended updating § 37.10(a)(3) so that States are only required to provision mDLs to digital wallets in a manner that will release only the data requested by the verifier. Additional privacy requirements, the commenter submitted, while important to individuals and States, may not affect verifying agencies.

TSA Response: Sections 37.10(a)(1)(i) and (a)(3) of this rule extend to mDLs PII protections that are analogous to those in the existing regulations regarding physical cards. This rule is adding mirroring PII provisions because mDLs involve a new data set and additional elements that must be protected, which are not addressed in the current regulations. Section 37.10(a)(1)(i) requires encryption of PII, and § 37.10(a)(3) requires an explanation of the means used to protect PII during processing, storage, and destruction of mDL records and provisioning records. Nothing in this final rule modifies or imposes new requirements regarding physical cards. While TSA concurs that there is a privacy interest between individuals and States, verifying Federal agencies have an equally important privacy interest in trusted mDL transactions.

2. Provisioning

Comments: An association contended that although the intended goal of §§ 37.10(a)(1)(iii)–(vi) is the step of ''binding,'' which means ensuring that an mDL is provisioned to the correct mDL holder's device, binding has no value to verifying Federal agencies, other than copy protection, at the time of identity verification. The association questions, therefore, the need for these requirements.

TSA Response: ''Binding,'' a critical step in mDL provisioning, refers to the process where the issuing State binds, or pairs, the mDL data to a specific device through the generation of the device key and signing of the mobile security object. Binding is critically important to all stakeholders involved in an mDL transaction, including verifying Federal agencies, as they share a strong interest in a secure, trusted mDL ecosystem in which identity data is protected during mDL provisioning, provided only to the rightful holder of the data, bound to that holder's device, and resists cloning to other devices unless approved by the issuing State. Section 37.10(a)(1) sets forth requirements for provisioning, and the requirements specified in § 37.10(a)(1)(iii)-(vi) provide the requisite security and privacy protections to achieve secure binding. The TSA Waiver Guidance also sets forth recommendations for provisioning and binding. To clarify the relationship between provisioning and binding, the final rule adds a new definition to § 37.3 for ''provisioning.''

3. AAMVA mDL Implementation Guidelines

Comments: AAMVA noted that § 37.10(a)(4) refers to version 1.1 of the AAMVA Guidelines, conflicting with § 37.4, which incorporates by reference version 1.2 of this document.

TSA Response: TSA agrees that § 37.10(a)(4) of the NPRM inadvertently listed version 1.1, instead of version 1.2, of the AAMVA Guidelines. TSA notes that the NPRM correctly cited version 1.2 in all other instances [69] where it referenced the AAMVA Guidelines, and only made a typographical error to version ''1.1'' in a single instance, in § 37.10(a)(4). TSA did not receive any comments to the contrary. Accordingly, the final rule has made a technical correction in § 37.10(a)(4) to address this typographical error and correctly refer to version 1.2.

4. Resident Address Data Element

Comments: AAMVA submitted that § 37.10(a)(4)(i) of the NPRM characterizes the ''resident_address'' data element as ''optional,'' despite that the AAMVA Guidelines define this data element as mandatory.

TSA Response: TSA clarifies that the ''resident_address'' data element required in § 37.10(a)(4)(i) refers to the data element as defined in the ISO/IEC 18013–5:2021(E) standard namespace ''org.iso.18013.5.1,'' not any data

[69] *See* 88 FR 60056, 60062, 60068, 60071, 60085, & 60087 (Aug. 30, 2023).

elements defined in the AAMVA Guidelines. The use of the term ''optional'' in § 37.10(a)(4)(i) reflects ISO/IEC's designation of that data element as defined in ISO/IEC 18013–5:2021(E). For clarification, despite ISO/IEC's designation of ''resident_address'' as an ''optional'' data field in ISO/IEC 18013–5:2021(E), § 37.10(a)(4)(i) of this final rule mandates inclusion of that data field.

D. TSA Waiver Application Guidance

Comments: An association recommended that the TSA Waiver Guidance should include references to the corresponding sections of the rule. The association further recommended that the documents incorporated by reference in § 37.4 should be moved to the Guidance to facilitate efficient updates as new standards are published. A State noted that the Guidance was not available at the website specified in § 37.10(c).

TSA Response: TSA agrees that the Guidance would be more helpful if it references the applicable provisions in the final rule to which the Guidance applies. The Guidance has been revised to specifically include the corresponding regulatory provisions where possible. TSA appreciates the commenter's perspective and this opportunity to provide clarity to the public and stakeholders.

Regarding the recommendation to move the standards from § 37.4 to the Guidance to reflect updated or newly-published standards, TSA notes that the Guidance is non-binding and does not establish any legally enforceable requirements. All security measures, practices, and metrics set forth are simply illustrative, non-exclusive examples for States to consider as part of their overall strategy to address the requirements under § 37.10(a). Any legally enforceable requirements must be set forth in regulatory text. Moreover, as provided in § 37.10(c), TSA may update this Guidance as necessary to provide additional information or address evolving threats to security, privacy, or data integrity.

TSA also clarifies that the Guidance was available during the comment period at the public rulemaking docket at *www.regulations.gov,* and continues to be available. The website specified in § 37.10(c), and throughout the rule, was under development at the time of the NPRM but is now live.

E. General Concerns About mDLs

Comments: Some public interest organizations posited that public demand for mDLs is ''non-existent'' and ''conjectural.'' However, some States disagreed. One State commented that it has issued more than 200,000 mDLs to residents following a pilot in 2017 and more recent expansion in 2022 and 2023. Another State commented that in the 3 months since it began offering its mDL app, it has been downloaded more than 7,000 times. Other commenters questioned the claimed mDL benefits concerning security, privacy, consumer protection, contact-free hygiene, among others, with one commenter opining that any such benefits would be realized only by those with the financial and technical means to purchase mobile devices that meet the specifications in the proposed rule. Some commenters further noted that mDLs would increase the vulnerability of driver's licensing agency databases to cyberattacks.

However, other commenters believe mDLs provide potential security and privacy benefits. One industry vendor commented that the rule would strengthen mDL integrity and security, which the commenter believes is critical to mDL holders and verifying entities. The commenter specifically noted that unlike physical cards, which require an agency's verifying officer to have specialized knowledge of potentially ''hundreds'' of different card designs of 56 issuing jurisdictions, the electronic safeguards built into mDLs obviate the need for such knowledge. The commenter further opined that mDLs provide privacy protections by empowering the mDL holder to control precisely what information is shared and with whom.

TSA Response: TSA disagrees that public demand for mDLs is weak. As discussed in Part II.C.2., above, TSA understands that more than half of all 56 issuing jurisdictions are considering or issuing mDLs, and this number continues to increase. Indeed, TSA notes that some States submitted comments disagreeing about the purported lack of demand for mDLs.

Regarding potential benefits of mDLs, TSA continues to believe that mDLs provide potential benefits, including security, privacy, efficiency, and contact-free hygiene, as discussed further in the NPRM.[70] TSA has directly observed some of these benefits through its ongoing mDL testing at airport checkpoints (discussed in Part II.C.2, above). In addition, as discussed above, some commenters agreed with TSA's view that mDLs provide potential security and privacy benefits.

TSA disagrees that the rule effectively requires the purchase of smartphones that are costly or technologically complex, which commenters contend would limit potential mDL benefits only to those with financial and technical means. The potential benefits of mDLs can be realized using nearly any smartphone available today. The only technical requirements for such devices, as a result of this final rule, are a smartphone that employs Bluetooth Low Energy and has secure hardware capability to protect the device key associated with the mDL. These technologies are widely available on most smartphones.

With respect to concerns that mDLs introduce new cyber vulnerabilities, TSA continues to believe that the minimum security requirements set forth in this rule would minimize the potential for harm resulting from such threats. As discussed in Part III.C.4.iii above, cyber threats are diverse and evolving, and TSA intends to address them by updating its Waiver Application Guidance as necessary. Some commenters agreed that this rulemaking would improve mDL security and the ability to resist cyber threats. An advocacy group shared that some States and industry today are using non-standardized technological approaches with wide substantive variances in security methodologies, thereby making some mDLs susceptible to fraud and privacy intrusions. The commenter noted that the proposed rule would overcome those concerns by providing standardized approaches to protect security and privacy.

F. Scope of Rulemaking and mDL Acceptance

Comments: An association opined that mDLs could provide benefits to Federal agencies beyond the uses discussed in the proposed rule. Specifically, the association noted that the Departments of State and Transportation could accept mDLs to improve issuance of passports and commercial driver's licenses, respectively. The commenter also sought clarification on how mDL acceptance, and REAL ID broadly, will be operationalized at TSA, both today and when enforcement of the REAL ID Act begins.

One State recommended that the definition of mDLs in the proposed rule be expanded to include Enhanced Driver's Licenses and Enhanced Identification Cards (collectively ''Enhanced Driver's Licenses'' or ''EDLs'').

TSA Response: TSA reiterates that the final rule applies only to Federal acceptance of mDLs for official purposes, defined by the REAL ID Act regulations as accessing Federal facilities, entering nuclear power plants,

[70] *See* 88 FR at 60062.

and boarding Federally regulated commercial aircraft. Any other purpose is beyond the scope of this rulemaking.

TSA further notes that each Federal agency that chooses to accept mDLs for official purposes must build its infrastructure, train its workforce, and operationalize mDL acceptance. Each Federal agency has the discretion to determine its own policies concerning acceptable IDs for access to their facilities, and for communicating this information to the public. TSA advises that questions concerning individual Federal agency identification policies and operational details should be directed to the appropriate program offices of individual agencies.

Regarding EDLs, the definition of ''mDL'' does not require modification because EDLs comply with REAL ID standards (despite that they are not governed by the REAL ID Act).[71] For that reason, this rule makes clear that mDLs issued based on EDLs will be accepted by Federal agencies under the waiver process. Indeed, the AAMVA Guidelines (incorporated by reference; see § 37.4) similarly treat EDLs as synonymous with REAL ID-compliant driver's licenses, requiring that States encode EDL-based mDLs as REAL ID-compliant. To confirm that States properly encode an EDL as REAL ID-compliant, § 37.10(a)(1)(vii)(A) of this final rule requires States to populate the ''DHS_compliance'' data element with ''F,'' indicating REAL ID-compliant, as required by the AAMVA Guidelines (*see* Part IV.A., above). This ensures that a Federal officer verifying an EDL-based mDL will correctly identify the REAL ID compliance status of the underlying EDL. TSA appreciates the commenter's perspective and this opportunity to provide clarity to stakeholders.

G. Privacy

Comments: Several public interest organizations expressed concerns that this rulemaking would establish a national digital ID that Federal agencies could use in wide ranging circumstances and purposes. They suggested that this type of ID could lead to sharing of data between State driver's licensing agencies and Federal agencies, producing serious harms to privacy and security, particularly for immigrant communities. Immigrants, the commenters argue, could suffer because many States are issuing non-compliant cards to them, and this rule could influence States to share with Federal agencies information provided in immigrant applications, potentially resulting in deportation.

Other public interest organizations noted that the proposed rule would facilitate tracking and surveillance because the rule requires ''installation of a government app on a mobile device of a certain type.'' An organization further suggested that it be allowed to view source code for these apps in order to learn their true intent. Commenters recommended that the rule should not go forward without additional privacy safeguards, noting that standard ISO/IEC 18013–5:2021(E) is not sufficient.

TSA Response: In the REAL ID Act, Congress established minimum standards for the issuance of State-issued driver's licenses and identification cards acceptable for official Federal purposes. Neither the Act nor implementing regulations, 6 CFR part 37, contemplate the creation of a sole national identification card or Federal database of driver's license information. Under the statute, the official purposes for Federal agency acceptance of mDLs relate to identity verification, and Congress neither created nor authorized a national identification card. Each individual licensing jurisdiction continues to issue its own unique licenses, maintain its own records, and control access to those records and the circumstances under which access may be provided. In addition, States continue to have full discretion to issue driver's licenses that are non-REAL ID compliant, or to issue dual classes of compliant and non-compliant cards, which some States are doing. States also have full discretion to choose not to issue mDLs at all. The REAL ID Act does not prevent compliant States from issuing driver's licenses and identification cards where the identity of the applicant cannot be assured or for whom lawful presence is not determined. This rule does not intend to interfere with existing State laws that are designed to protect driver's licensing agency data from being shared and used to enforce Federal immigration laws.

Nothing in this final rule requires a Federal agency to accept mDLs. Agencies that choose to do so will receive mDL user information only with the individual's consent, and individuals will control access and use of the mDL in their mobile devices. For example, in TSA mDL testing at airport security checkpoints, passengers present their mDLs to TSA, which uses an mDL reader to establish a secure communications channel with the passenger's mobile device to receive the passenger's mDL data. TSA's mDL readers are programmed to request access only to the relevant data needed for identity verification, which TSA cannot receive unless the passenger provides consent. Upon consent, the passenger's mobile device releases the mDL data to TSA, which automatically validates the authenticity of the information by confirming the digital signature of the issuing State driver's licensing agency (*see* discussion in Part II.C.1., above). TSA emphasizes that it receives passenger data *only* from the passenger's mobile device, and not from the issuing State driver's licensing agency. Although TSA does communicate with a driver's licensing agency, this is solely to receive the agency's private key for data validation purposes—not identity verification. TSA further emphasizes that it never communicates with driver's licensing agencies information regarding the locations or instances of passengers' mDL use. The passenger's PII is used in the same manner that biographic information from physical IDs is used. The PII that is collected from the mDL, along with the live photo taken by TSA, is overwritten when the next passenger scan occurs or when TSA switches off its ID scanner, whichever occurs first.

An mDL offers additional privacy and security benefits over physical IDs. An mDL transmits only the necessary information requested by TSA, rather than sharing all data elements found on a physical ID, and requires user's consent. All mDL data is encrypted at rest, during transfer, and during all transactions through secure channels. Nothing in this rule mandates that individuals must install a ''government'' app or any type of app at all. Nothing in this rule requires individuals to use a mobile device of any type, or to choose to receive an mDL at all. TSA appreciates the opportunity to provide a detailed explanation of the privacy protections conferred by mDLs. Additional information can be found in DHS's Privacy Impact Assessment[72] concerning privacy risks in the use of digital IDs in the identity verification process at TSA airport security checkpoints.

H. Waiver Validity Period and Renewals

Comments: An industry vendor sought clarification on whether a waiver is valid until revoked or for a defined period. An association urged that the

[71] EDLs are governed by the Western Hemisphere Travel Initiative. As explained in the 2008 Final Rule, DHS worked closely with States to ensure that EDLs would comply with REAL ID standards. 73 FR 5272, 5276 (Jan. 29, 2008). Some States mark EDLs as REAL ID compliant on the front of the card.

[72] *See* DHS, Privacy Impact Assessment for the Travel Document Checker Automation—Digital Identity Technology Pilots, *www.dhs.gov/sites/default/files/2022-01/privacy-pia-tsa051-digitalidentitytechnologypilots-january2022_0.pdf* (last visited July 17, 2024).

validity period of a waiver should be long enough such that States are not frequently submitting applications for renewals and awaiting determinations, and that the period should cover both waiver applications and State re-certifications. The association further submitted that TSA should consider a grace period to allow a waiver to remain valid for some period after the Phase 2 rule is effective. A State sought clarification of requirements for renewing a waiver if the subsequent Phase 2 rulemaking does not commence within 3 years of publication of this final rule in order to assess the resources required to prepare the renewal application. A vendor sought clarification regarding whether a new audit report is required for renewal applications if a State uses the same issuance vendors for both the initial and renewal applications.

TSA Response: Under § 37.9(e)(1), a waiver will be valid for three years from date of issuance unless suspended or terminated under §§ 37.9(e)(4) or (5). As discussed in Part III.C.6., above, this rule specifies a three-year waiver validity period because it aligns with the frequency for States to re-certify compliance with § 37.55(b). TSA believes this period is sufficient given the expedient timeframes specified in § 37.9(b) for TSA to respond to applications. As set forth therein, TSA will provide: an initial decision on applications within 60–90 calendar days, replies to States responses to notices of insufficiency within 30 calendar days, and determinations on petitions for reconsideration within 60 calendar days. These timeframes resist the commenter's concern about potentially being trapped in an enduring cycle of submitting renewal applications and waiting extensive period for TSA responses. Moreover, the three-year waiver validity period equals the three-year frequency of States to recertify compliance required by § 37.55(b), as the commenter notes.

Regarding the timing of the Phase 2 rulemaking and the need for a grace period, § 37.9(e)(6) specifies requirements for States that seek to renew waivers beyond the validity period. Renewal provides a mechanism for waivers to persist independent of the timing of future rulemakings, which obviates the need for a grace period.

With respect to audit reports for renewal applications, TSA confirms that States must submit an audit report for renewals, regardless of a State's mDL issuance vendors or system changes. Regarding the resources required for renewal applications, TSA assumes such audit costs for subsequent waiver applications will remain the same as the audit for the initial application, but TSA does estimate a 25 percent to 70 percent reduction in the renewal application cost because the State would have gained experience and collected evidence from the previously approved waiver application.[73] The processes to renew a waiver are identical to those set forth in § 37.9 for initial applications.

I. Vendor and Technology ''Lock-in'' Effects

Comments: Some public interest organizations commented that the NPRM would promote a ''lock-in'' effect, in which certain technologies and vendors would gain a durable competitive advantage that would be difficult for competitors to overcome. In particular, the commenters expressed concern that markets for digital wallets and mDL readers are likely to be harmed because of the rule's reliance on standards such as ISO/IEC 18013–5:2021(E), which the commenters believe create security, privacy, and interoperability risks. According to the commenters, digital wallets and other necessary mDL technology should be based on open standards.

TSA Response: TSA is currently testing mDLs issued by seven States who are partnering with multiple providers of digital wallets. One provider, SpruceID, is based on an open-source toolkit for developing decentralized IDs.[74] Additional digital wallet providers are expected to enter the market in the near-term, and States are expected to partner with them and seek to test their mDLs with TSA. The rule provides States broad discretion to select technology vendors of their choice, and does not prescribe any specific type of technology. This absence of prescriptive requirements is intentional, as it accommodates innovation and organic demand from consumers to facilitate technological diversity.

The final rule resists technology lock-in by providing minimum standards for security, privacy, and interoperability, while remaining technology-agnostic. The ISO/IEC 18013–5:2021(E) standard enables the required interoperability for REAL ID use cases where mDL holders present their mDLs in person to an mDL reader. Adhering to this standard for interoperability does not harm the developers of digital wallets or readers because the standard does not prohibit other standards or technologies from working alongside the ISO/IEC 18013–5:2021(E) standard. Indeed, California is pursuing this approach with SpruceID. The California mDL digital wallet, built on the open-source SpruceID toolkit, supports both ISO/IEC 18013–5:2021(E) requirements and an alternative technology, known as TruAge®, which allows the mDL to be used in broader transactions, such as age-verified purchases.[75] TSA recognizes that in a broad sense, there may be a false ''lock-in'' effect of certain types of mDLs, namely, those that meet the waiver application criteria set forth in the rule. However, this is not a true lock-in in the traditional sense of economic path dependence, in which barriers prevent innovation and deployment of equal or potentially superior alternatives. The rule requires States to demonstrate that they issue mDLs that provide security, privacy, and interoperability necessary for Federal acceptance for official purposes, but also allows States and industry wide latitude to innovate as necessary to meet the regulatory requirements.

As structured, this rule does not create dependencies on specific vendors, systems, or technologies. Instead, the rule facilitates development of more secure, privacy enhancing, and interoperable mDLs using technology-agnostic solutions. Accordingly, this rule resists the risk of true technology lock-in that otherwise may have occurred if market participants select technologies, developed by first-movers, that lack the protections necessary for Federal acceptance for official purposes.

J. Pseudonymous Validation and On-Device Biometric Matching

Comments: An individual urged that it is critical to support ''pseudonymous validation'' under standard ETSI TR 119 476. In addition, the commenter argued that mDL transactions should support biometric matching on the mobile device itself to avoid sharing biometric data. The commenter claimed these recommendations are necessary to avoid becoming ''an autocratic state.''

TSA Response: ''Pseudonymous validation'' is the concept of using a pseudonym or alias to identify an

[73] States with an established mDL program will incur a 45-hour time burden to complete an mDL waiver reapplication, down from a 60-hour time burden for the initial mDL waiver application (25 percent reduction). States without an established program may experience a 70 percent reduction in the time to complete a waiver reapplication compared to the initial mDL waiver application (from 140 hours to 45 hours). *See* § 2.4.1 of the Regulatory Impact Analysis.

[74] *See generally* SpruceID, *https://spruceid.com/products/issuing-digital-ids* (last visited July 17, 2024).

[75] *See* State of California Department of Motor Vehicles, TruAge Age-Verified Purchasing, *https://www.dmv.ca.gov/portal/ca-dmv-wallet/truage/* (last visited July 17, 2024).

individual without revealing that person's true identity. Although this may provide valuable privacy protection in some uses, it also enables an individual to operate under a consistent—but false—identity. This is contrary to the REAL ID Act and regulations' purpose of improving the security of State-issued identity cards.

On-device biometric sharing is the subject of standards ISO/IEC 23220–5 and ISO/IEC 23220–6, which are currently in development. TSA is not aware of any currently published standards enabling the establishment of trusted on-device biometric matching in the mDL ecosystem, which makes it premature to require such functionality in the final rule.

K. Access to Standards

Comments: A public interest organization contended that the NPRM failed to provide adequate access to the 19 standards incorporated by reference in the proposed rule. Specifically, the commenter noted that under the NPRM, ''the only way'' for the public to gain access was to email a request to the address specified in the rule. The commenter noted that it sent multiple emails to this address, but never received a response. The commenter also noted that the NPRM directed individuals to visit ''DHS headquarters in Washington DC'' but did not provide a specific address.

Other public interest organizations asserted that NPRM failed to provide reasonable access to ISO/IEC 18013–5:2021(E) without a substantial fee. A commenter noted that the ANSI link providing free access to the standard was not helpful, and that attempts ''to even load the standards on a modern computer failed completely.'' Further, the commenter stated that ANSI required ''an unnecessarily onerous process,'' which required signing up for an account and completing an online license agreement form, and that access was on a view-only basis.

TSA Response: TSA regrets that the commenter's multiple emails seeking access were not answered. However, TSA notes that the NPRM specified multiple mechanisms for the public to access the standards, consistent with IBR requirements specified by the OFR.[76] All but one of the 19 standards incorporated by reference in § 37.4 are available to the public for free download, and the NPRM provided the website addresses to access each of these documents. In addition, the NPRM provided detailed information for the publisher of each of these standards, including most, if not all, of the following: publisher name, address, phone, email, and website. For the sole standard that is not publicly available for free, ISO/IEC 18013–5:2021(E), the NPRM facilitated free access via ANSI, a private organization with whom TSA has no affiliation. The NPRM specifically noted that ANSI's policy required individuals to complete an online license agreement form asking for only name, professional affiliation, and email address. The NPRM also stated that access would be available on a view-only basis, and provided publisher information for individuals who sought a greater level of access. TSA received many comments discussing the 19 standards, demonstrating that the NPRM provided sufficient notice regarding access to these standards.

Although the NPRM provided sufficient notice to access the standards, the final rule modifies access instructions in existing § 37.4 to clarify and provide additional means for access. Specifically, the final rule replaces DHS with TSA as a location where IBR material is available for inspection and provides additional points of contact at TSA. The final rule also specifies that certain IBR material is available in the Federal Docket Management System at *https://www.regulations.gov,* docket number TSA–2023–0002.

L. Standards and Standards Development Generally

Comments: Several commenters sought clarification on how TSA would update the final rule to reflect evolving industry standards and government guidelines. Commenters suggested that instead of incorporating by reference a specific version of a document, the rule should require compliance with the ''most recent version.'' Some commenters requested specificity regarding the process and timeframes given to States to conform to any updated standards.

Other commenters questioned the validity of the standards-development processes followed by ISO/IEC, AAMVA, and others. Commenters asserted that these bodies are secretive, unaccountable to the public, have onerous membership criteria, are influenced by foreign authoritarian governments, among other deficiencies.

Some commenters asserted that the documents incorporated by reference in § 37.4 of the proposed rule were insufficient because they provided only partial requirements to address security and operational issues. Commenters also criticized some of the references for their absence of protections to address: emerging threats from quantum computing, evolving risks from digital identification, outdated encryption algorithms, and digital wallet design, user experience, among other deficiencies.

TSA Response: Under applicable legal requirements, Federal agencies must seek approval from the OFR for a specific version, edition, or date of a publication that an agency seeks to IBR in a final rule.[77] Revisions or updates to a publication already IBR'd in a final rule require re-approval from the OFR, and rules therefore do not update ''dynamically'' to reflect future versions.[78] Therefore, the rule cannot exclude publication version or date information, or update dynamically to reflect future versions. States will be expected to comply with the standards as published in the final rule. TSA actively monitors evolving standards and guidelines, and may consider whether to IBR those publications (pending review of the final documents) through subsequent rulemaking.

Regarding criticisms of standards-development bodies and their deliberations generally, the standards development process for international technology standards, particularly those intended to be interoperable globally, is developed by membership-based bodies comprised of interested parties representing participants from international governmental entities, educational organizations, research groups, non-profit organizations, commercial entities, and the public at large. Each standards-development organization sets its own criteria for membership, fees, standards development processes, and publication structure.

With respect to the criticism that the chosen standards and guidelines provide insufficient protections and lack future-proofing to address unknown threats, TSA notes that due to the nature of innovation and evolving technology, and legal constraints of Federal rulemaking, it is not possible to develop ''future-proofed'' regulations. TSA acknowledged in the NPRM that this is a nascent market experiencing rapid innovation, and that many key standards and guidelines are currently being developed. Although imperfect, the chosen standards reflect industry

[76] *See* 1 CFR 51.5(a); Office of Federal Register, Incorporation by Reference Handbook (June 2023, rev'd Aug. 28, 2023), *http://www.archives.gov/federal-register/write/handbook/ibr/* (last visited July 17, 2024) [hereinafter ''IBR Handbook''].

[77] *See* 1 CFR 51.5(b) & 51.9; IBR Handbook, *http://www.archives.gov/federal-register/write/handbook/ibr/.*

[78] *See* IBR Handbook, *http://www.archives.gov/federal-register/write/handbook/ibr/.*

state-of-the-art ahead of publication of emerging standards that likely will support the subsequent Phase 2 rulemaking. TSA made a risk-based determination that the 19 standards provide the key security, privacy, and interoperability requirements necessary for trusted Federal acceptance, and are commensurate with existing REAL ID standards for physical cards. The two-phased rulemaking approach is intended to address the near-term need for established security, privacy, and interoperability requirements, while accommodating the medium-term evolution of technology and standardization.

With respect to comments regarding specific deficiencies in some of the chosen standards, TSA offers the following responses. TSA acknowledges that ISO/IEC 18013–5:2021(E) was developed broadly for international consumption and does not fully address the needs for REAL ID use cases in the U.S. The waiver application criteria set forth in § 37.10(a), therefore, adapt ISO/IEC 18013–5:2021(E) for REAL ID use cases by supplementing this standard with requirements from other references as set forth in this rule. For example, §§ 37.10(a)(1) and (a)(3) address the provisioning and privacy requirements not covered by ISO/IEC 18013–5:2021(E). Other issues relevant to mDL transactions that are not addressed in ISO/IEC 18013–5:2021(E), such as device user experience and digital wallet design are beyond the scope of this rule and intentionally omitted.

M. TSA's Identity Verification Policies

Comments: A public interest organization raised questions regarding TSA's identity verification policies at the screening checkpoint.

TSA Response: This rulemaking is focused on allowing Federal agencies to accept mDLs for Federal official purposes as defined by the REAL ID Act. Issues regarding TSA's identify verification processes unrelated to mDLs are beyond the scope of this rulemaking.:

N. Paperwork Reduction Act

Comments: A public interest organization argued that every mDL transaction with a Federal agency is a collection of information subject to the Paperwork Reduction Act (PRA), and that no exemptions apply. The organization further contended that because neither TSA nor any other Federal agency has sought approval from the Office of Management and Budget (OMB) for these collections, any use of mDLs violates the PRA. Without an approved information collection, the commenter noted that it is not able to determine the costs or purposes of this information collection.

TSA Response: TSA disagrees with the commenter's assertion that every mDL transaction with a Federal agency is a collection of information subject to the PRA because a request for identify verification is not the ''soliciting . . . of facts or opinions . . . calling for . . . answers to identical questions.'' 44 U.S.C. 3502(3) (defining ''collection of information''); *cf.* 5 CFR 1320.3(h)(1) (excepting from the definition information affirmations or certifications that ''entail no burden other than that necessary to identify the respondent''). This final rule establishes a process for States to apply to TSA for a temporary waiver that enables Federal agencies to accept mDLs issued by those States when REAL ID enforcement begins on May 7, 2025. This rule does not, however, require any mDL transactions with a Federal agency or set requirements for the use of mDL information. Therefore, this comment is beyond the scope of this rulemaking.

O. Legal Authority

Comments: A public interest organization questioned the legality of DHS's delegation of authority to TSA to administer the REAL ID program because the public was deprived of an opportunity to comment on it. The commenter further argued that it is improper for TSA, a transportation-focused agency, to regulate use of mDLs by other Federal agencies for non-transportation uses.

Other public interest organizations posited that neither the REAL ID Act, nor subsequent amendments in the REAL ID Modernization Act, authorize issuance of the waiver as set forth in the NPRM. The commenters argued that DHS is statutorily authorized only to prescribe standards, certify State compliance, and extend time to facilitate compliance, and the implementing regulations prevent DHS from waiving any mandatory minimum standards.

TSA Response: Generally, Federal agencies' delegations of duties and authority are exempt from notice-and-comment requirements of the Administrative Procedure Act because they are matters of ''agency management'' and ''rules of agency organization, procedure or practice.'' [79] Matters involving internal agency organization, procedure, practice, and delegations of duties and authority are directed primarily towards improving the efficiency and effectiveness of agency operations, and therefore are not required to be posted for public comment. DHS's delegation of authority to TSA to administer the REAL ID program falls within this exemption, obviating the need for public comment.

TSA further clarifies that the REAL ID Act, as amended, authorizes the Secretary to promulgate regulations to implement the requirements under the REAL ID Act.[80] And the REAL ID Modernization Act amended the definitions of ''driver's license'' and ''identification card'' to specifically include mDLs that have been issued in accordance with regulations prescribed by the Secretary of Homeland Security.[81] TSA is adopting the waiver process established in this final rule pursuant to its authority to implement the requirements of the REAL ID Act as amended, and the final rule is consistent with all statutory requirements.'' The waiver application criteria specify issuance-related security and privacy requirements that are commensurate with requirements for physical cards. The final rule further provides that these are temporary requirements that will be superseded by a subsequent rulemaking setting forth more comprehensive requirements after emerging industry standards are published over the next few years.

P. Economic Impact Analysis

1. Alternatives

Comments: Several commenters, including a State, associations, and an individual, commented on various aspects of the assessment regarding the costs and benefits of available regulatory alternatives.[82] Some commenters recommended that TSA should accept Alternatives 1, 3, or 4 compared to the proposed rule. The commenter recommending acceptance of Alternative 1 stated the proposed rule does not address the market failures associated with a lack of common standards, such as increased complexity of mDL use across States, and may result in larger costs in the long run when formal mDL standards are finalized. The commenter supporting Alternative 3 recommended that TSA promulgate comprehensive mDL regulations that enable States to develop and issue REAL ID-compliant mDLs, as well as a process for Federal agencies to accept them. The commenter recommending acceptance of Alternative 4 stated it would eliminate the time and expense required to

[79] 5 U.S.C. 553(a)(2), (b)(A).

[80] Sec. 205 of the REAL ID Act.

[81] Sec. 1001 of the REAL ID Modernization Act, 134 Stat. 2304.

[82] *See* NPRM, 88 FR at 60079–80.

prepare and submit a waiver application and audit report, and another commenter sought clarification on how the scope of Alternative 4 differs from the proposed rule.

TSA Response: Regarding Alternative 1, TSA reiterates that this rule establishes requirements for States to issue mDLs that provide specified levels of security, privacy, and interoperability, which provides guidance and direction for State mDL issuance systems and reduces the complexity of mDL use across different jurisdictions. The mDL waiver application criteria would likely form the foundation of the more comprehensive requirements in the Phase 2 rulemaking. While States may have to incur cost to alter their mDL programs when more comprehensive requirements are issued, they are less likely to have to make significant changes and incur larger costs under this rule than under Alternative 1.

The final rule provides benefits to States and mDL users. The waiver process will allow the continued use of mDLs for official purposes when REAL ID enforcement begins on May 7, 2025. An mDL is more secure than a physical card, affords users privacy controls over the information transmitted to the relying party, and enables contact-free transactions. TSA does not believe the waiver process delays development of industry standards and Federal guidelines. Many such standards and guidelines are in development that would inform requirements in the Phase 2 rulemaking, and this final rule will facilitate, not impede, this process. For these reasons, TSA recommends the final rule over Alternative 1.

Regarding Alternative 3, TSA believes it is premature to promulgate comprehensive mDL regulations, given that several important industry standards and Federal guidelines are in development and would likely inform future requirements in the Phase 2 rulemaking, such as requirements related to mDL provisioning. Until the subsequent rulemaking is published, this final rule sets requirements based on current, available industry standards and guidelines that serve as a basis for, and bridge towards, more comprehensive requirements.

Alternative 4 would establish interim minimum requirements, similar to the waiver application criteria, for States to issue REAL ID compliant mDLs instead of a wavier process that enables Federal agencies to accept mDLs from States that meet the waiver criteria. TSA clarifies that Alternative 4 would largely convert the waiver application criteria to requirements for the issuance of REAL ID-compliant mDLs. If States could meet those requirements, under Alternative 4, States' mDLs would be deemed REAL ID compliant. In contrast, the final rule, through the waiver process, enables Federal agencies to accept for official purposes States' mDLs that meet the waiver criteria.

As discussed further in Part VI.A.4., below, TSA rejects this alternative because it effectively would codify standards that may become obsolete in the near future, thereby implying a degree of certainty that TSA believes is premature given emerging standards that are still in development. Although Alternative 4 eliminates the waiver process, TSA would continue to require a mechanism to validate that a State's mDLs complies with the established standards under Alternative 4. Thus, States would still need to provide information to TSA similar to the waiver process, including audit reports, to demonstrate compliance with the requirements. TSA believes the time and expense to provide such information under Alternative 4 would be similar to the waiver process under the final rule, and a waiver process provides more flexibility and allows States and TSA to gain insight and experience in the mDL environment.

2. Familiarization and Training Costs

Comments: A vendor recommended inclusion in Table 2 of the NPRM (Total Costs of the Rule to States) of States' Familiarization Cost in years 2–5 to reflect evolving standards, and a similar inclusion in Table 3 (Total Cost of the Rule to DHS) for DHS, but did not provide any cost estimates.[83] The vendor further recommended inclusion of States' training or continuing education costs in Table 2, which the vendor believes should be similar to DHS's training costs set forth in Table 3 ($5 million over 10 years). The commenter also requested clarification of the definition of training costs in Table 3, and whether it includes State training related to certificate systems and record maintenance.

An association posited that the economic analysis did not address TSA's costs, training requirements, and process changes to adapt to an mDL system.

TSA Response: TSA does not believe a State's familiarization or training cost estimates require modification. The familiarization cost estimate represents the cost and time burden for States to review the final rule. All State driver's licensing agencies would incur this cost in the first year after the publication of the rule. Although familiarization costs do not include time spent reviewing new standards, the NPRM does discuss, qualitatively, potential State costs to monitor and study mDL technology as it evolves including standards development and other relevant factors. TSA did not receive any cost estimates related to reviewing new standards.

The training costs in Table 3 relate to costs TSA would incur to train Transportation Security Officers (TSOs) to verify mDLs for identification purposes at airport security checkpoints. As such, States would not incur similar costs of roughly $5 million for such training. TSA is unclear as to the type of or specific training or continuing education the commenter refers and what may be needed in the future. However, for clarification, any such training and certifications have been added to the qualitative discussion of potential additional State costs (section 3.1.5 of the RIA).

TSA believes the costs related to training and process changes to adapt to an mDL system are accounted for and quantified where available. TSA quantifies the costs for TSOs to undertake training to verify mDLs for identification purposes at the security checkpoint, and for additional clarity, TSA has also added the cost to TSA to provide such training for TSOs. TSA also quantifies the costs related to the equipment that must be acquired to integrate the use of mDLs for identity verification in section 2.6 of the RIA. In addition, TSA added a qualitative discussion in the economic analysis (section 3.2.5) regarding costs TSA may incur related to process changes to adapt to an mDL system, such as changes to standard operating procedures and informational campaigns.

3. Estimated Time To Complete Waiver Applications; Estimated Costs for mDL Readers

Comments: An industry vendor recommended increasing the estimated time to complete waiver applications from 20 hours, as set forth in the NPRM, to 80 hours, and increasing the estimated cost for mDL readers by 35 percent, for both DHS and other Relying Parties.

TSA Response: TSA clarifies that the total time burden to complete a waiver application does not require modification because the estimate includes two components: (1) the time to complete the application and provide the information required under § 37.10(a), and (2) the time to gather all supporting documentation. TSA estimates completing the application

[83] *See* NPRM, 88 FR at 60074–76.

will require an average of 20 hours. Separately, the time burden estimate for gathering supporting documentation can range from 40 to 120 hours. TSA estimates States with existing mDL solutions (15 States) will require a total of 40 hours, while States considering mDLs but lacking mDL solutions (25 States) will require a total 120 hours for their initial waiver application submission. Thus, TSA estimates an average time burden of 110 hours to complete a waiver application, by adding the time to complete application materials (20 hours) and a weighted average time to gather supporting documentation (90 hours).[84] TSA also estimates States will incur an average time burden of 47.5 hours to complete a waiver resubmission, which is separate from the initial waiver application. *See* Section 2.4 of the Regulatory Impact Analysis (RIA) for additional details.

The cost of mDL readers is uncertain given evolving technology, and could vary up or down by 35 percent compared to TSA's current estimate. For example, within TSA specifically, TSA may integrate mDL readers in existing infrastructure, and TSA's costs are different than other relying parties (other Federal agencies that choose to accept mDLs for official purposes). For TSA mDL reader costs, TSA structures its estimate around internal data on actual procurement to quantify the cost of its mDL reader equipment, which also includes the cost of quarterly updates. Given the uncertainty of mDL reader costs, the final rule expands the range of possible reader costs for relying parties up and down by the comment suggested 35 percent of the TSA internal estimate which results in a range of about $260 to $540 with a midpoint of $400. While TSA does not change its primary estimate based on the estimated cost of a smartphone which is assumed to be used in combination with an application to serve as the mDL reader, it does recognize that such costs could range from $2.1 million to $4.4 million over 10 years.[85]

4. Cost-Benefit Analysis Generally

Comments: A public interest organization suggested that the cost-benefit analysis was hastily prepared and speculative.

TSA Response: TSA recognizes mDLs are an emerging market with uncertain costs and benefits. Nonetheless, TSA quantifies costs where it is able to with the best available data along with assumptions, proxies, and subject matter expert estimates, and TSA discusses potential additional costs qualitatively where TSA was unable to quantify the costs. TSA observes that the commenter did not offer specific recommendations to improve estimates of future costs, urging only that TSA should delay this rulemaking in light of the uncertainty. However, TSA believes there may be additional costs to stakeholders by delaying the rule. For example, mDL users would not be able to use mDLs for official purposes when full enforcement of REAL ID begins on May 7, 2025, which would delay or deny realization of the security, privacy, convenience, and contact-free hygiene benefits mDLs. States and industry would risk continued investments based on non-standardized processes that lack the security, privacy, and interoperability necessary for Federal acceptance for official purposes. Federal agencies would be delayed in realizing the security and privacy benefits conferred by mDLs compared to physical cards. In addition, through continued and increased mDL usage enabled by this final rule, TSA will gain insight and data that could better inform costs and benefits of the Phase 2 rulemaking.

Q. Communicating Status of Waiver; System Disruptions

Comments: Some commenters sought clarification on how the status of a waiver, specifically, suspensions and terminations, would be communicated to Federal agencies. Another commenter asked whether TSA would provide support mechanisms to communicate information about system disruptions that could impact mDL acceptance by Federal agencies.

TSA Response: As provided in §§ 37.9(b)(1), (e)(4)(iii), and (e)(5)(iii), TSA will publish, at *www.tsa.gov/real-id/mDL,* a list of States that hold valid waivers, including updates to note any final suspensions and terminations. As required by § 37.8, any Federal agency that elects to accept, for REAL ID official purposes, mDLs issued by States with a waiver must regularly review the specified website to confirm that a State holds a valid waiver. Suspensions and terminations will occur only for the violations specified in § 37.9(e), which TSA anticipates will be rare instances.

Regarding support mechanisms for system outages and other disruptions to mDL acceptance, each Federal agency that elects to accept mDLs for official purposes will be responsible for maintaining and supporting its mDL acceptance infrastructure. With respect to Federal agency access to the State mDL waiver list at *www.tsa.gov/real-id/mDL,* DHS and TSA IT systems already provide the necessary level of support to reduce the risk of widespread impacts from a temporary system outage. To further reduce risk of potential disruptions, TSA strongly encourages all mDL holders to carry their physical REAL ID cards in addition to their mDLs.

R. Impact of Waiver on States Currently Testing mDLs With TSA

Comments: A State that is currently testing mDLs with TSA sought clarification regarding the extent to which the waiver application criteria align with or differ from terms in the TSA-State testing agreement. The State sought this comparison to assess the amount of additional resources that the State may require to meet the waiver criteria.

TSA Response: Due to confidentiality provisions in TSA's contracts with States, TSA cannot publicly disclose the terms of such agreements or compare any differences with the waiver application criteria. However, to assist any States who have entered into such agreements with TSA, the agency encourages such States to contact TSA for further discussions. All States are subject to the requirements of this rule to obtain a waiver, and TSA intends to work with States that are testing mDLs with TSA to help ensure a smooth transition.

Regarding concerns about the time and resources necessary to successfully apply for a waiver, TSA estimates the 10-year cost to all States seeking a waiver is approximately $814 million. On a per-State basis, TSA estimates the average cost to complete a waiver application is approximately $40,000 (this includes the cost to complete the initial application and resubmission; *see* Table 2–8 in the RIA), and the average cost to comply with the application criteria $3.13 million in the initial year of a State's application (as discussed in Section 2.5 of the RIA).

S. Notice for Changes to mDL Issuance Processes

Comments: A State requested clarification regarding whether § 37.9(e)(2) requires States to provide 60 calendar days' advance notice before adding a new digital wallet provider.

TSA Response: In some circumstances, the addition of a new digital wallet provider may trigger the

[84] Weighted average time to gathering supporting documentation of 90 hours = ((15 States × 40 hours) + (25 States × 120 hours)) ÷ (15 States + 25 States).

[85] DHS multiplies the total number of mDL readers relying parties will procure over 10 years of 8,174.9 (Table 2–11: Relying Party mDL Reader Procurement in the Final Regulatory Impact Analysis) by a low mDL reader cost of $261.30 and high mDL reader cost of $542.70.

requirement under § 37.9(e)(2) to provide notice to TSA, depending on the extent of the changes required to the State's mDL issuance processes. This is especially true as more standards are developed in the area of mDL provisioning. Although States are responsible for assessing if any changes are significant and trigger the reporting requirements, TSA recognizes that it is not possible to define precise circumstances that require, or do not require, reporting. To assist States in determining whether changes in their specific circumstances warrant notification under § 37.9(e)(2), the final rule revises this section by adding the following sentence at the end: ''If a State is uncertain whether its particular changes require reporting, the State should contact TSA as directed at *www.tsa.gov/real-id/mDL.*'' TSA will collaborate with States to facilitate a determination of whether reporting is required. TSA appreciates this opportunity to provide clarity and reduce potential burdens on the entities directly regulated by this final rule.

T. Clarification Regarding ''*Days*''

Comments: A vendor requested clarification whether § 37.9(b) of the NPRM, under which TSA would provide decisions on waiver applications ''within 60 days'' and ''in no event longer than 90 days,'' means ''calendar days'' or ''business days.''

TSA Response: TSA clarifies that all references in this rulemaking to ''days'' means calendar days, not business days. The final rule revises the following NPRM provisions to implement this clarification: §§ 37.9(b), (c) & (e), and Appendix A, paragraph 6.3.

U. Audit Requirements

1. Questionable Necessity; Excessive Costs; Alternatives to Independent Auditor

Comments: An association recommended that the requirement for an independent, third-party audit was unnecessary and should be optional, not mandatory, and further suggested that an audit could be a substantiating element together with any self-certification that a State already presents to TSA under REAL ID requirements. Another commenter posited that an audit (and the waiver application process) is extraneous for States that have invested in mDLs and entered into testing agreements with TSA. Several States and an association expressed concerns about the costs of, and need for, an independent evaluator, noting the timing of budgetary requests and varying ability among States to afford the costs.

Some commenters recommended alternatives to independent auditors, including internal State-conducted audits, an audit conducted in conformity with the AAMVA Digital Trust Service (DTS), and processes in lieu of audits entirely. Another commenter recommended specifying detailed criteria, based on a set of established industry requirements and/or guidelines, along with relevant Root Program or industry policies, against which auditors would perform an assessment.

TSA Response: TSA clarifies that the term ''independent entity'' in § 37.10(b)(1) is intended to include entities that are employed or contracted by a State and independent of the State's driver's licensing agency. This final rule revises the proposed § 37.10(b)(1) to include this clarification.

TSA disagrees that an independent audit is unnecessary or of questionable importance. The purpose of the audit is to validate the accuracy of the information that a State provides to TSA in support of its application for a waiver. This validation ensures TSA has correct information to efficiently evaluate the sufficiency of a State's application. TSA believes an independent auditor that meets the requirements of § 37.10(b) can provide a defensible level of accuracy that cannot be achieved via other means, such as a self-certification.

TSA also disagrees that costs for independent audits will be excessive. As discussed in section 2.4.1 of the RIA, TSA estimates the audit cost range is between $5,000 and $60,000 on a per-State basis.

TSA disagrees that an audit conducted in conformity with requirements for a State to participate in AAMVA's DTS is an acceptable alternative to the audit requirements specified in this rule. The requirements imposed on States to participate in the AAMVA DTS are not identical to the requirements imposed in this rule. In particular, the AAMVA DTS requirements lack the specific cybersecurity risk control requirements addressed in § 37.10(a)(2) to establish public trust in States' mDL issuance systems. Finally, establishing specific audit criteria may be the subject of the upcoming Phase 2 rulemaking that will set forth detailed requirements that would enable States to issue mDLs that comply with the REAL ID Act.

2. Auditor Qualifications

Comments: One association recommended that the rule should allow an auditor with credentials that are more closely aligned to certification of systems management, ethics, and business practice. Alternatively, the commenter recommended that instead of requiring any specific license, the rule should only require that the name of the auditor be listed.

TSA Response: Regarding auditor qualifications, the requirement in § 37.10(b) that auditor must hold a Certified Public Accountant (CPA) license provides the necessary duty of care to report accurately and truthfully in the State in which the audit occurs, and TSA has not identified any suitable alternatives. TSA understands that auditors experienced in certification of systems management, ethics, and business practice are not an equivalent substitute to auditors who are CPAs, who possess additional qualifications as specified through their Certified Information Technology Professional credential. Similarly, merely listing the name of the auditor is not sufficient. The certification requirements in § 37.10(b) are common in auditing technical and information systems and provide proof of expertise.

V. Appendix A to Subpart A: mDL Issuance Requirements

1. Compliance With Full Reference or Specific Provisions

Comments: An association noted that some Appendix A provisions require full compliance with the cited references instead of specific parts of those references. For illustration, the association provided some non-exhaustive examples, including the CA/Browser Forum's *Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates* and *Network and Certificate System Security Requirements.* The association and another commenter requested specifying pertinent parts of the cited references that are applicable to compliance with requirements in this rule.

TSA Response: TSA agrees that the agency can provide paragraph or section numbers for some of the references cited in Appendix A to aid in understanding which parts of the references require compliance. TSA made the following technical corrections in the final rule:

- In Appendix A, paragraph 1.1, the CA/Browser Forum Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates were qualified with the addition of the following identifiers: sections 2, 4.3, 4.9, 5, and 6. TSA also qualified ISO/IEC 18013–5:2021(E) with the addition of Annex B to provide guidance on requirements for a certificate policy and to clarify its

applicability. Compliance with ISO/IEC 18013–5:2021(E) Annex B is already required by § 37.10(a)(4), and inclusion here reduces burden by providing States greater specificity on certificate profiles to include in their mDL certificate policy. For NIST SP 800–57, Part 1, Rev. 5, the final rule adds qualifications for sections 3 and 5–8. For NIST SP 800–57, Part 3, Rev. 1, the final rule adds qualifications for sections 2–4 and 8–9.

• In Appendix A, paragraph 2.13, the final rule adds a qualification to section 4.2 of NIST SP 800–63B to provide further clarity on the specific requirements for AAL2 authenticators.

Regarding the CA/Browser Forum Network and Certificate System Security Requirements document, the final rule requires full compliance with this document because these requirements define a minimum set of security controls to establish publicly trusted certificate systems. This model has proven successful as the basis for securing the certificate systems used to secure the global internet.

2. Paragraph 2.2: Changing Authentication Keys and Passwords

Comments: An association commented that the terms ''privileged account'' and ''service account'' in this paragraph are undefined.

TSA Response: The terms ''privileged account'' and ''service account'' fall under the definition of ''trusted role'' in § 37.3. Accordingly, the final rule has revised proposed Appendix A, paragraph 2.2, to replace ''privileged account'' and ''service account'' with ''trusted role.'' TSA appreciates the feedback and the opportunity to provide this clarification.

3. Paragraphs 2.11–2.14: Multifactor Authentication

Comments: An association requested clarification as to whether the Multifactor Authentication (MFA) required by paragraphs 2.11–2.14 of Appendix A is PKI-based or crypto-based phishing-resistant MFA.

TSA Response: Appendix A, paragraphs 2.11–2.14, do not require PKI-based or crypto-based phishing resistant MFA. While phishing resistant cryptographic authenticators are a best practice to achieve the highest level of assurance for multi-factor authentication, for the purposes of demonstrating compliance with Appendix A requirements in paragraphs 2.11–2.14, MFA is achievable through a combination of technologies and methods covered by NIST SP 800–63B section 4.2. TSA believes this approach optimally balances mitigation of risks associated with access to certificate systems with costs of implementation.

4. Paragraph 3: Facility, Management, and Operational Controls

Comments: An industry vendor questioned whether the requirements in paragraph 3 of Appendix A mean that only U.S. citizens or lawful permanent residents are qualified to be authorized personnel who can access such systems. The commenter sought further clarification on whether the specified controls apply to ''as a service'' offerings on *www.GovCloud.com.*

TSA Response: TSA clarifies that Appendix A, paragraph 3.3, does not require that only U.S. citizens or lawful permanent residents can serve as personnel authorized to access state certificate systems. This provision requires States to specify the controls for employees, contractors, and delegated third parties, including any cloud service providers, necessary to prevent risks posed by foreign ownership, control, or influence. Regarding applicability to other cloud-based services, this provision also requires States to specify the security controls for all ''as-a-service'' providers, who are considered to be delegated third parties.

5. Paragraph 4: Personnel Security

a. Background Checks

Comments: A commenter sought clarification regarding whether this section requires a Federal fingerprint background check, State fingerprint background check, or other non-fingerprint based background check.

TSA Response: Appendix A, paragraph 4, does not specify any particular types of screening procedures. Instead, States are responsible for specifying screening procedures for employees, contractors, and delegated third parties in trusted roles. Title 6 CFR 37.45 specifies requirements for background checks and applies to covered employees, and this final rule does not alter those requirements.

b. Paragraph 4.1: Coordination Among States; Applicable Laws

Comments: A commenter sought clarification regarding how ''coordination among State entities'' applies to a policy to control security risks from insider threats. The commenter sought further clarification of the requirement in this paragraph that a State's policy must comply with ''all applicable laws, executive orders, directives, regulations, policies, standards, and guidelines.''

TSA Response: TSA clarifies that under Appendix A, paragraph 4.1, the term ''State entities'' refers to the agencies and offices that comprise the State's governmental operations. Coordination among State entities is intrastate for the purposes of State-run insider threat programs, not interstate coordination among different States. TSA believes that States are likely familiar, from decades of experience issuing physical driver's licenses under the requirements of § 37.45, as well as familiarity with other State-specific information and security laws, with the applicable legal requirements governing policies to address risks from insider threats, many of which are State-specific.

c. Timeframe To Disable System Access; Cybersecurity Incident Reporting

Comments: A State commented that Appendix A, paragraph 4.5, which requires a State to disable an employee's system access within 4 hours of the employee's termination, conflicts with Appendix A, paragraph 8.6, which requires States to provide notice to TSA within 72 hours after discovery of a cyber incident. The State recommends that time periods in both sections be amended to 24 hours, urging that disabling an employee's system access within 4 hours of termination is overly aggressive in situations where termination is amicable, such as retirements or transfers.

TSA Response: TSA maintains that a 4-hour requirement to disable system access, as set forth in Appendix A, paragraph 4.5, is essential in all termination situations. A coordinated and prompt surrender of logical and physical access for all departing employees is a critical component of a program to address insider threats. It is highly unlikely that a State would allow employees to have physical access to buildings or other infrastructure after termination. Disabling access to logical systems is as critical as requiring the surrender of keys and media providing physical access. When an employee is terminated for misconduct or other exigent circumstances that could compromise security, timely denial of system access is critical. Although amicable termination situations may present fewer security risks, States have sufficient time, in these circumstances, to pre-plan for the prompt disabling of system access before the employee's final day, similar to how States pre-plan the recovery of any physical keys or key cards for building access.

TSA further maintains that the proposed requirement for States to report cybersecurity incidents within 72

hours of discovery, as set forth in Appendix A, paragraph 8.6, is appropriate, and TSA therefore declines the recommendation to shorten the timeframe to 24 hours. While TSA has established in other contexts outside of this rulemaking a shorter timeframe for reporting by certain transportation owners or operators, that timeframe reflects the potential impact of cybersecurity incidents that could jeopardize the safety of individuals and property. In that context, early reporting is critical to ensure the ongoing availability of critical operational capabilities. Here, in contrast, the requirement for reports to be made within no more than 72 hours is appropriate given TSA's assessment of the operational impact of a cybersecurity incident on a State's mDL issuance infrastructure. In addition, the 72-hour requirement is consistent with the timeframe required for the rulemaking by CISA under the Cyber Incident Reporting for Critical Infrastructure Act of 2022.[86] The 72-hour reporting requirement supports the policy objective of regulatory harmonization, to the greatest extent possible.

In light of the comments, TSA also seeks to provide greater clarity regarding the types of incidents that must be reported, and the mechanics of reporting. Accordingly, this final rule makes several clarifying edits to Appendix A, paragraph 8.6. First, the final rule modifies the requirement for reporting ''a significant cyber incident or breach'' to ''any reportable cybersecurity incident, as defined in the TSA Cybersecurity Lexicon available at *www.tsa.gov*.'' This modification provides greater certainty and assurance regarding events that would trigger reporting. Second, the final rule modifies the requirement for reporting ''within 72 hours'' to ''within no more than 72 hours'' to encourage more timely reporting, as recommended by a commenter. Third, the final rule modifies the requirement that regulated entities ''provide written notice to TSA'' at the specified website, to requiring that ''[r]eports must be made as directed'' at that website, which clarifies that the website will include information concerning the format or content of the report. Finally, the final rule adds a provision that reports *may* contain SSI, and if so, would be subject to requirements of 49 CFR part 1520. TSA made similar edits to a requirement concerning Federal agency reporting, § 37.8(d), to add that reports must be made to TSA ''as directed'' at the specified website, and that reports may be subject to the requirements of 49 CFR part 1520 if they contain SSI. The SSI protection provisions were not proposed in the NPRM and were added in response to public comments, discussed below in Part IV.W., below.

d. Paragraph 4.7: Training for Personnel Performing Certificate Systems Duties

Comments: A commenter sought clarification on whether training item 2 in paragraph 4.7 of Appendix A, which concerns authentication and vetting, applies to States that issue certificates to other entities as described in the CA/Browser Forum Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates. The commenter believes that this training is not applicable because in the mDL context, States do not issue document signer certificates to anyone beyond the State.

TSA Response: TSA appreciates the commenter's perspective, but notes that the training required under Appendix A, paragraph 4.7, is essential for State personnel in executing their duties regarding certificate systems. Although it is correct that States do not issue document signer certificates to other States, States issue document signer certificates to support their own mDLs, namely, to sign and establish public trust. In particular, training on authentication and vetting processes for employees, contractors, and other delegated third parties is a critical component of a well-developed insider threat program because each employee will be aware of the processes for employment and will be aided in identifying potential suspicious activity.

6. Paragraph 5.4: Hardware Security Modules (HSMs)

Comments: A commenter sought clarification as to whether the term ''dedicated hardware security modules'' in paragraph 5.4 of Appendix A requires HSMs to be dedicated to root certificate private keys and/or dedicated only to the issuing State. The commenter also asked whether this requirement excludes the use of an HSM that physically supports multiple States, but is partitioned into segments controlled by individual States.

TSA Response: Under Appendix A, paragraph 5.4, the term ''dedicated'' means that a State must use one HSM solely for IACA root private key functions and no other functions within the State's certificate system. TSA clarifies that Appendix A, paragraph 5.6, requires a State to use a separate HSM for document signer private key functions, but this HSM does not have to be ''dedicated'' solely to that function and may be used to support additional functions within the State's certificate system. TSA further clarifies that Appendix A, paragraphs 5.4 and 5.6, require ''sole control'' (as defined in § 37.3) of an HSM, which does not permit multiple States to share a single HSM, but States are permitted to use multi-tenant cloud-based HSMs, where each tenant-State is separated with logical and physical controls.

In an effort to further enable the availability of cloud HSMs, TSA is revising related NPRM Appendix A, paragraphs 5.13 and 5.14, which are related to Appendix A, paragraphs 5.4 and 5.6. Paragraphs 5.13 and 5.14 set forth requirements to generate IACA root certificate key pairs, and document signer key pairs, respectively. NPRM Appendix A, paragraph 5.13 proposed requiring two administrators (hereinafter ''multi-administrator split knowledge key generation'') and one witness to perform this function, and paragraph 5.14 proposed requiring at least two administrators. However, TSA understands that although States have strong competitive procurement options for local HSMs that support multi-administrator split knowledge key generation, suitable options for multi-tenant cloud HSMs may not exist for many States. States that are unable to procure such devices potentially would have been forced by the NPRM requirement to purchase local HSMs, which are not only costlier than cloud HSMs, but potentially less secure for States that lack HSM management capabilities. TSA understands that generally, security provided by cloud HSM services exceeds the capabilities that most States can afford to provide for local HSMs. After carefully considering a number of factors, including potential security and privacy risks, TSA believes that proposed Appendix A, paragraphs 5.13 and 5.14, imposed unnecessarily restrictive requirements concerning the minimum personnel required to perform multi-administrator split knowledge key generation. Accordingly, the final rule declines to adopt those proposals, and revises the requirement in the proposed Appendix A, paragraph 5.13, to reduce the number of administrators required to generate IACA root key pairs from two to one. The final rule similarly revises the proposed Appendix A, paragraph 5.14, to allow for the generation of document signer key pairs using one administrator and one witness as an alternate to using two administrators with split knowledge key

[86] Public Law 117–103, Div. Y (2022) (as codified at 6 U.S.C. 681–681g).

generation. TSA believes this reduction in personnel maximizes States' competitive procurement options, reflects current industry state-of-the-art, reduces burdens on regulated stakeholders, and does not compromise security, privacy, or interoperability.

7. Certificate Policies and Practices

Comments: A vendor noted that standard ISO/IEC 18013–5:2021(E) defines profiles for online certificate status protocol (OCSP) and certificate revocation list (CRL), but the standard does not mandate their implementation. The vendor recommended that the rule should specify which of the methods is required, including implementation requirements for certificate type. According to the vendor, it is important to immediately revoke a certificate when the issuing State's private key shows signs of compromise.

The vendor also recommended that the rule should require States to maintain a Certificate Practice Statement (CPS), in addition to the requirement in the NPRM to maintain a certificate policy. A CPS, the vendor explained, should follow a format specified by standard IETF RFC 3647 format, which covers certificate issuance, revocation, and renewal.

TSA Response: Although both OCSP and CRL are methods for validating the revocation status of a certificate, OCSP is out-of-scope for the IACA root and document signer certificates for mDLs, as that protocol is not part of a certificate validation process because mDLs must work in an offline environment. In addition, standard ISO/IEC 18013–5:2021(E) specifies that CRL is mandatory, not optional, and the standard fully defines the profiles and implementation requirements. Section 37.10(a)(2) of this rule requires States to explain the means used for revocation of their certificate systems in compliance with applicable requirements of Appendix A. Paragraphs 1, 5, and 8 of the Appendix set forth requirements applicable to certificate revocation. As discussed in Part IV.V.1, above, the final rule revised Appendix A, paragraph 1.1, as proposed in the NPRM, by adding specific provisions of the cited references with which States must comply. This addition provides greater clarity to States regarding requirements for a certificate policy.

Regarding the recommendation to require States to maintain a CPS following standard IETF RFC 3647,[87] paragraph 1.1 of Appendix A of this final rule already specifies that requirement. The provision requires a State to adopt certificate policies that meet the requirements in CA/Browser Forum Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates section 2. In addition, the provision requires a State to develop a CPS based on requirements set forth in standard IETF RFC 3647.

8. mDL Lifecycle Management

Comments: A commenter recommended that the rule implement requirements on States to manage the lifecycle of issued mDLs. Examples of such lifecycle management practices include validity periods, refresh periods, push-based updates, harmonized expiration dates of mDL and physical cards, and limitations on the numbers of devices to which a given mDL can be provisioned.

TSA Response: Because mDL issuance and Federal agency experience are still in their infancies, together with an absence of standardized mechanisms to implement certain lifecycle management tasks and minimal data to support specific requirements, TSA believes it is premature to prescribe requirements that the commenter recommends. Imposing such requirements now, while technologies are unsettled and evolving, risks upsetting this rule's equilibrium between security and privacy on the one hand, and innovation on the other. TSA also notes that mDL lifecycle management is addressed in the AAMVA mDL Implementation Guidelines.

W. Protection of Sensitive Security Information in Waiver Applications

Comments: A commenter sought clarification on procedures for protecting any SSI that may be included in waiver applications.

TSA Response: TSA has comprehensively re-evaluated the need to protect SSI that may be included in response to requirements throughout this rule. TSA believes that SSI protection is warranted not only for information included in waiver applications, but also in response to other requirements in this rule (§§ 37.9(b)(2), (c), (e)(2), (e)(4)(ii) & (e)(5)(ii), and Appendix A, paragraph 8.6). Accordingly, this final rule revises NPRM § 37.9 to add new paragraph (g), which provides that information provided in response to §§ 37.9(a), (b)(2), (c), (e)(2), (e)(4)(ii), and (e)(5)(ii), and Appendix A, paragraph 8.6, *may* contain SSI and therefore must be handled and protected in accordance with 49 CFR part 1520.

V. Consultation With States and the Department of Transportation

Under section 205 of the REAL ID Act, issuance of REAL ID regulations must be done in consultation with the Secretary of Transportation and the States. During the development of this final rule, DHS and TSA consulted with the Department of Transportation and other Federal agencies with an interest in this rulemaking via regular meetings. DHS and TSA also consulted with State officials through meetings with their representatives to AAMVA.

VI. Regulatory Analyses

A. Economic Impact Analyses

1. Regulatory Impact Analysis Summary

Changes to Federal regulations must undergo several economic analyses. First, E.O. 12866 (Regulatory Planning and Review),[88] as affirmed by E.O. 13563 (Improving Regulation and Regulatory Review),[89] and as amended by E.O. 14094 (Modernizing Regulatory Review),[90] directs Federal agencies to propose or adopt a regulation only upon a reasoned determination that the benefits of the intended regulation justify its costs. Second, the Regulatory Flexibility Act of 1980 (RFA)[91] requires agencies to consider the economic impact of regulatory changes on small entities. Third, the Trade Agreement Act of 1979[92] prohibits agencies from setting standards that create unnecessary obstacles to the foreign commerce of the United States. Fourth, the Unfunded Mandates Reform Act of 1995[93] (UMRA) requires agencies to prepare a written assessment of the costs, benefits, and other effects of proposed or final rules that include a Federal mandate likely to result in the expenditure by State, local, or tribal governments, in the aggregate, or by the private sector, of $100 million or more (adjusted for inflation) in any one year.

2. Assessments Required by E.O. 12866 and E.O. 13563

Executive Order 12866 (Regulatory Planning and Review), as affirmed by Executive Order 13563 (Improving Regulation and Regulatory Review) and

[87] Internet Engineering Task Force, Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework, Nov. 2003, *www.rfc-editor.org/rfc/rfc3647.html* (last visited July 17, 2024).

[88] 58 FR 51735 (Oct. 4, 1993).

[89] 76 FR 3821 (Jan. 21, 2011).

[90] 88 FR 21879 (Apr. 11, 2023).

[91] Public Law 96–354, 94 Stat. 1164 (Sept. 19, 1980) (codified at 5 U.S.C. 601 *et seq.,* as amended by the Small Business Regulatory Enforcement Fairness Act of 1996 (SBREFA)).

[92] Public Law 96–39, 93 Stat. 144 (July 26, 1979) (codified at 19 U.S.C. 2531–2533).

[93] Public Law 104–4, 109 Stat. 66 (Mar. 22, 1995) (codified at 2 U.S.C. 1181–1538).

amended by Executive Order 14094 (Modernizing Regulatory Review), directs agencies to assess the costs and benefits of available regulatory alternatives and, if regulation is necessary, to select regulatory approaches that maximize net benefits (including potential economic, environmental, public health and safety effects, distributive impacts, and equity). Executive Order 13563 emphasizes the importance of quantifying costs and benefits, reducing costs, harmonizing rules, and promoting flexibility.

The OMB has designated this rule a ''significant regulatory action'' as defined under section 3(f) of E.O. 12866, as amended by Executive Order 14094. Accordingly, OMB has reviewed this rule.

In conducting these analyses, TSA has made the following determinations:

(a) While TSA attempts to quantify costs where available, TSA primarily discusses the costs and benefits of this rulemaking in qualitative terms. At present, mDLs are part of an emerging and evolving industry with an elevated level of uncertainty surrounding costs and benefits. Nonetheless, TSA anticipates the final rule will not result in an effect on the economy of $200 million or more in any year of the analysis. The rulemaking will not adversely affect the economy, interfere with actions taken or planned by other agencies, or generally alter the budgetary impact of any entitlements.

(b) In accordance with the RFA, and pursuant to 5 U.S.C. 605(b), TSA certifies that the rule will not have a significant economic impact on a substantial number of small entities, including small governmental jurisdictions. The rule will only directly regulate the 50 States, the District of Columbia, and the five U.S. territories who voluntarily participate in the mDL waiver process, who under the RFA are not considered small entities.

(c) TSA has determined that the final rule imposes no significant barriers to international trade as defined by the Trade Agreement Act of 1979; and

(d) TSA has determined that the final rule does not impose an unfunded mandate on State, local, or tribal governments, such that a written statement will be required under the UMRA, as its annual effect on the economy does not exceed the $100 million threshold (adjusted for inflation) in any year of the analysis.

TSA has prepared an analysis of its estimated costs and benefits, summarized in the following paragraphs, and in the OMB Circular A–4 Accounting Statement. When estimating the cost of a rulemaking, agencies typically estimate future expected costs imposed by a regulation over a period of analysis. For this final rule's period of analysis, TSA uses a 10-year period of analysis to estimate costs.

This final rule establishes a temporary waiver process that permits Federal agencies to accept mDLs, on an interim basis, for official purposes, as defined in the REAL ID Act, when full enforcement of the REAL ID Act and regulations begins on May 7, 2025. Federal agencies that opt to accept mDLs for official purposes must also procure an mDL reader in order to validate the identity of the mDL holder. As part of the application process for the mDL waiver, States are required to submit to TSA an application, including supporting data, and other documentation necessary to establish that their mDLs meet specified criteria concerning security, privacy, and interoperability. When REAL ID Act and regulations enforcement begins on May 7, 2025, Federal agencies will be prohibited from accepting non-compliant driver's licenses and identification cards, including both physical cards and mDLs, for official purposes.

In the following paragraph TSA summarizes the estimated costs of the rule on the affected parties: States, TSA, mDL users, and relying parties (Federal agencies that voluntarily choose to accept mDLs for official purposes). TSA has also identified other non-quantified impacts to affected parties. As Table 2 displays, TSA estimates the 10-year total cost of the rule to be $829.8 million undiscounted, $698.1 million discounted at 3 percent, and $563.9 million discounted at 7 percent. The total cost to States comprises approximately 98 percent of the total quantified costs of the rule.

TABLE 2—TOTAL COST OF THE RULE BY ENTITY

[$ Thousands]

Year	States cost	TSA cost	Relying party cost	Total rule cost		
	a	b	c	d = a + b + c		
				Undiscounted	Discounted at 3%	Discounted at 7%
1	$42,876	$1,595	$79	$44,551	$43,253	$41,636
2	62,791	1,715	919	65,424	61,669	57,144
3	71,352	1,209	537	73,098	66,895	59,670
4	83,182	1,102	381	84,665	75,224	64,591
5	94,460	864	375	95,699	82,551	68,232
6	91,467	695	1,160	93,323	78,156	62,185
7	91,881	727	742	93,351	75,903	58,134
8	91,743	730	558	93,031	73,440	54,145
9	91,467	719	531	92,717	71,060	50,432
10	91,881	774	1,289	93,944	69,903	47,757
Total	813,102	10,128	6,573	829,803	698,054	563,925
Annualized					81,833	80,290

Note: Totals may not add due to rounding.

States incur costs to familiarize themselves with the requirements of the rule, purchase access to an industry standard, submit their mDL waiver application, submit an mDL waiver reapplication, and comply with waiver application criteria requirements. As displayed in Table 3, the 10-year cost to States is $813.1 million undiscounted,

$683.7 million discounted at 3 percent, and $552.0 million discounted at 7 percent.

TABLE 3—TOTAL COST OF THE RULE TO STATES
[$ Thousands]

Year	Familiarization cost	Standards cost	Waiver application cost	Reapplication cost	Escalated review cost	Infrastructure security cost	Total cost to states		
							g = a + b + c + d + e + f		
	a	b	c	d	e	f	Undiscounted	Discounted at 3%	Discounted at 7%
1	$63.3	$1.9	$592.1	$0	$7.2	$42,212	$42,876	$41,628	$40,071
2	0	1.3	394.7	0	12.0	62,383	62,791	59,186	54,844
3	0	0.6	197.4	0	14.4	71,140	71,352	65,297	58,244
4	0	0.6	197.4	413.9	16.8	82,553	83,182	73,906	63,459
5	0	0.6	197.4	275.9	19.2	93,967	94,460	81,482	67,349
6	0	0	0	138.0	19.2	91,310	91,467	76,603	60,949
7	0	0	0	551.8	19.2	91,310	91,881	74,708	57,219
8	0	0	0	413.9	19.2	91,310	91,743	72,423	53,395
9	0	0	0	138.0	19.2	91,310	91,467	70,102	49,752
10	0	0	0	551.8	19.2	91,310	91,881	68,368	46,708
Total	63.3	5.0	1,578.9	2,483.2	165.2	808,807	813,102	683,704	551,991
Annualized								80,151	78,591

Note: Totals may not add due to rounding.

TSA incurs costs associated with reviewing mDL waiver applications and mDL waiver renewals, purchasing access to industry standards, procuring mDL readers, and mDL training. As displayed in Table 4, the 10-year cost to TSA is $0.131 million undiscounted, $8.87 million discounted at 3 percent, and $7.56 million discounted at 7 percent.

TABLE 4—TOTAL COST OF THE RULE TO TSA ($ THOUSANDS)

Year	Standards cost	Application review cost	Reapplication review cost	mDL reader cost	mDL training cost	Total cost to TSA		
						f = a + b + c + d + e		
	a	b	c	d	e	Undiscounted	Discounted at 3%	Discounted at 7%
1	$0.4	$74.3	$0	$1,418.8	$101.5	$1,595.0	$1,548.5	$1,490.6
2	0	49.5	0	699.8	965.4	1,714.7	1,616.3	1,497.7
3	0	24.8	0	547.9	636.2	1,208.9	1,106.4	986.9
4	0	24.8	39.9	440.6	596.4	1,101.8	978.9	840.5
5	0	24.8	26.6	240.6	571.7	863.7	745.0	615.8
6	0	0.0	13.3	199.4	482.0	694.7	581.8	462.9
7	0	0.0	53.2	200.9	473.3	727.5	591.5	453.0
8	0	0.0	39.9	202.3	487.4	729.7	576.0	424.7
9	0	0.0	13.3	203.8	501.4	718.5	550.7	390.8
10	0	0.0	53.2	205.2	515.5	773.9	575.9	393.4
Total	0.4	198.2	239.6	4,359.4	5,330.8	10,128.4	8,870.9	7,556.4
Annualized							1,039.9	1,075.9

Note: Totals may not add due to rounding.

Relying parties represent Federal agencies that elect to accept mDLs for official purposes. Per the final rule, relying parties are required to use an mDL reader to retrieve and validate mDL data. As a result, relying parties will incur costs to procure mDL readers should they voluntarily choose to accept mDLs for official purposes. TSA is also considered a relying party, but due to the particular impact to TSA related to the requirement for REAL ID related to boarding Federally regulated commercial aircraft, those impacts are discussed separately. As displayed in Table 5, the 10-year cost to relying parties is $6.58 million undiscounted, $5.48 million discounted at 3 percent, and $4.38 million discounted at 7 percent.

TABLE 5—TOTAL COST OF THE RULE TO RELYING PARTIES ($ THOUSANDS)

79Year	mDL reader cost	Total cost to relying parties		
		b = a		
	a	Undiscounted	Discounted at 3%	Discounted at 7%
1	$79.3	$79.3	$76.9	$74.1
2	918.8	918.8	866.0	802.5

TABLE 5—TOTAL COST OF THE RULE TO RELYING PARTIES ($ THOUSANDS)—Continued

79Year	mDL reader cost	Total cost to relying parties		
		b = a		
	a	Undiscounted	Discounted at 3%	Discounted at 7%
3	537.4	537.4	491.8	438.7
4	381.3	381.3	338.8	290.9
5	375.0	375.0	323.5	267.4
6	1,160.4	1,160.4	971.9	773.3
7	741.8	741.8	603.1	461.9
8	558.3	558.3	440.7	324.9
9	531.2	531.2	407.1	288.9
10	1,289.1	1,289.1	959.2	655.3
Total	6,572.6	6,572.6	5,479.1	4,377.9
Annualized	.....	.....	642.3	623.3

Note: Totals may not add due to rounding.

TSA has also identified other non-quantified impacts to the affected entities. States may incur costs to: monitor and study mDL technology as it evolves; resolve the underlying issues that could lead to a suspension or termination of an mDL waiver; report serious threats to security, privacy, or data integrity; report material changes to mDL issuance processes; remove conflicts of interest with independent auditor; and request reconsideration of a denied mDL waiver application. TSA may incur costs to: investigate circumstances that could lead to suspension or termination of a State's mDL waiver; provide notice to States, relying parties, and the public related to mDL waiver suspensions or terminations; develop an information technology (IT) solution that maintains an up-to-date list of States with valid mDL waivers; develop materials related to the process changes to adapt to mDL systems; and resolve a request for reconsideration of a denied mDL waiver application. mDL users may incur costs with additional application requirements to obtain an mDL. Relying parties may incur costs to resolve any security or privacy issue with the mDL reader; report serious threats to security, privacy, or data integrity; verifying the list of States with valid mDL waivers; train personnel to verify mDLs; and update the public on identification policies.

TSA believes that States implementing an mDL, absent the rulemaking, would still comply with the AAMVA Guidelines. Many of the requirements of the waiver application criteria are already contained within the AAMVA Guidelines. This includes waiver application criteria concerning: data encryption; authentication; device identification keys; user identity verification; applicant presentation; REAL ID compliant physical card; data record; records retention; privacy; and interoperability. Only the waiver application criteria related to escalated review and infrastructure security/issuance are not contained with the AAMVA Guidelines. Operating under the assumption that States interested in mDLs would comply with the AAMVA Guidelines, TSA assumes the application criteria that overlap with the AAMVA Guidelines would otherwise be incurred and thus not included as a cost of the rule.

This final rule establishes waiver application criteria that serves as interim requirements regarding security, privacy, and interoperability for those States choosing to issue mDLs that can be accepted for official purposes. The waiver application criteria may help guide States in their development of mDL technologies which will provide a shared standard that could potentially improve efficiency while also promoting higher security, privacy, and interoperability safeguards.

The application criteria set requirements establishing security and privacy protections to safeguard an mDL holder's identity data. They also set interoperability requirements to ensure secure transactions with Federal agencies. States, via their mDL waiver application, must establish that their mDLs meet the application criteria thus helping to ensure adequate security and privacy protections are in place. Absent the rule, individual States may choose insufficient security and privacy safeguards for mDL technologies that fail to meet the intended security purposes of REAL ID and the privacy needs of users.

An mDL may provide additional security benefits by offering a more secure verification of an individual's identity and authentication of an individual's credential compared to physical cards. In general, mDLs use a cryptographic protocol that ensures the mDL was obtained through a trusted authority, such as a State's Department of Motor Vehicles.[94] This same protocol may prevent the alteration of mDLs and reduce the threat of counterfeit credentials.[95] An mDL also offers increased protection of personal identifiers by preventing over-collection of information. An mDL may enable the ability to share only those attributes necessary to validate the user identity with the relying party.[96] When using a physical card, the user has no ability to limit the information that is shared, regardless of the amount of information required for verification.

The waiver application criteria can help guide State development and investment in mDLs. The waiver application criteria will foster a level of standardization that would potentially reduce complexity by limiting individual State nuances while also ensuring interoperability across States and with the Federal Government. This increased interoperability reduces implementation costs by limiting the need for different protocols or

[94] Global News Wire, *Secure Technology Alliance's Mobile Driver's License Workshop Showcases mDLs Role in the Future of Identification,* Dec. 14, 2021, *https://www.globenewswire.com/en/news-release/2021/12/14/2351757/22743/en/Secure-Technology-Alliance-s-Mobile-Driver-s-License-Workshop-Showcases-mDLs-Role-in-The-Future-of-Identification.html* (last visited July 17, 2024).

[95] *Id.*

[96] Biometric Update, *Mobile ID can bring both convenience and citizen privacy,* July 15, 2021, *https://www.biometricupdate.com/202107/mobile-id-can-bring-both-convenience-and-citizen-privacy* (last visited July 17, 2024).

mechanisms to accept mDLs from individual States.

Identification of waiver application criteria that can be used across States will result in efficiency gains through multiple States pursuing similar objectives, goals, and solutions. Establishing application criteria early in the technology development process has the potential to align development activities across disparate efforts. Early guidance might also reduce re-work or modifications required in future regulations thus saving time and resources redesigning systems and functionality to adhere to subsequent Federal guidelines.

Furthermore, the waiver application criteria may potentially encourage investment in mDLs and the pooling of resources to develop mDL technology capabilities across States and address common concerns or issues. Such collaboration, or unity of effort, can help spread research and development risk and reduce inefficiencies that may arise from States working independently. Greater clarity over mDL regulations, with the rule part of an incremental, multi-phased rulemaking approach, may spur new entrants (States and technology companies) into the mDL ecosystem.

The rule allows Federal agencies to continue to accept mDLs for official purposes when REAL ID enforcement begins. This will avoid the sudden halting of mDL acceptance when REAL ID enforcement begins which will reverse trends in providing for a more customer-friendly screening experience. The experience and insight learned through the mDL waiver process could also be used to inform future standards and rulemaking.

3. OMB A-4 Statement

The OMB A-4 Accounting Statement presents annualized costs and qualitative benefits of the rule.

TABLE 6—OMB A–4 ACCOUNTING STATEMENT

[$ Millions, 2022 dollars]

Category	Estimates			Units			Notes
	Primary estimate	Low estimate	High estimate	Year dollar	Discount rate %	Period covered	
Benefits:							
Annualized Monetized ($ millions/year).	N/A	N/A	N/A	N/A	7	N/A	Not quantified.
	N/A	N/A	N/A	N/A	3	N/A	
Annualized Quantified	N/A	N/A	N/A	N/A	7	N/A	Not quantified.
	N/A	N/A	N/A	N/A	3	N/A	
Qualitative	The rule will produce benefits by reducing uncertainty in the mDL technology environment by helping to foster a minimum level of security, privacy and interoperability, and reduce potential costs through the alignment of development activities across disparate efforts.						
Costs:							
Annualized Monetized ($ millions/year).	$80.29	N/A	N/A	2022	7	10 years	NPRM Regulatory Impact Analysis (RIA).
	$81.83	N/A	N/A	2022	3	10 years	
Annualized Quantified	N/A	N/A	N/A	N/A	7	N/A	Not quantified.
	N/A	N/A	N/A	N/A	3	N/A	
Qualitative	States may incur incremental costs to: monitor and study mDL technology as it evolves; resolve the underlying issues that could lead to a suspension or termination of an mDL waiver; report serious threats to security, privacy, or data integrity; report material changes to mDL issuance processes; remove conflicts of interest with an independent auditor; and request reconsideration of a denied mDL waiver application. TSA may incur costs to: investigate circumstances that could lead to suspension or termination of a State's mDL waiver; provide notice to States, relying parties, and the public related to mDL waiver suspensions or terminations; develop an IT solution that maintains an up-to-date list of States with valid mDL waivers; develop materials related to the process changes to adapt to mDL systems; and resolve a request for reconsideration of a denied mDL waiver application. An mDL user may incur costs with additional application requirements to obtain an mDL. Relying parties may incur costs to resolve any security or privacy issue with the mDL reader; report serious threats to security, privacy, or data integrity; verifying the list of States with valid mDL waivers; train personnel to verify mDLs; and update the public on identification policies.						
Transfers:							
From/To	From:	N/A		To:	N/A		
	States may pass on costs associated with mDLs and the final rule to the public.						
Effects On: State, Local, and/or Tribal Government: The final rule will result in States incurring 552.0 million discounted at 7 percent. Small Business: None. Wages: None. Growth: Not measured.							NPRM Regulatory Flexibility Analysis (RFA).

4. Alternatives Considered

In addition to the rule, or the ''preferred alternative,'' TSA also considered four alternative regulatory options.

The first alternative (Alternative 1) represents the status quo, or no change relative to the creation of an mDL waiver. This represents a scenario without a rulemaking or a waiver process to enable mDL acceptance for official Federal purposes. Under this alternative, States would continue to develop mDLs in a less structured manner while waiting for relevant guiding standards to be published which would likely result in dissimilar

mDL implementation and technology characteristics. This alternative was not selected because it does not address the market failures associated with a lack of common standards, such as increased complexity of mDL use across States, and may result in larger costs in the long run when formal mDL standards are finalized.

The second alternative (Alternative 2) features the same requirements of the rule, including an mDL waiver process, but would allow Federal agencies to accept mDLs issued by certain States whose mDLs TSA has deemed to be ''low-risk,'' and therefore presumptively eligible to be granted a waiver. TSA would identify mDLs from States who have fulfilled the rule's minimum requirements prior to applying for the waiver and have sufficiently demonstrated (*e.g.,* via TSA initiative or recent evaluation by a trusted party) to TSA that their mDL systems present adequate interoperability and low security and privacy risk. The presumptive eligibility provision would allow Federal agencies to immediately (or conditionally) accept those ''low-risk'' mDLs for official purposes pending final approval of the respective State mDL waiver applications. However, TSA rejects this alternative because TSA believes the emerging technology underlying mDLs is insufficiently established to accept the security, privacy, and interoperability of States' mDL systems without an evaluation by TSA or another trusted party. In addition, a similar presumptive eligibility process is not available for other aspects of REAL ID and such an action would not reduce the burden on States to comply with any framework TSA develops.

Under the third alternative (Alternative 3), TSA would establish more comprehensive requirements than those in the rule to ensure mDLs comply with the REAL ID Act. States would be required to adopt the more comprehensive requirements to issue valid mDLs that can be accepted for official purposes. These technical requirements could include specific standards related to mDL issuance, provisioning, verification, readers, privacy, and other security measures. TSA rejects this alternative because promulgating more comprehensive requirements for mDLs is premature, as both industry standards and technology used by States are still evolving. Restrictive requirements could stifle innovation by forcing all stakeholders to pivot toward compliance. This could impede TSA from identifying and implementing a more efficient regulatory approach in the future.

Finally, under the fourth alternative (Alternative 4), instead of a waiver process, TSA would first establish minimum requirements for issuing REAL ID compliant mDLs before TSA later sets more comprehensive requirements as additional guidance and standards become available in the mid- and long-term. The interim minimum requirements would consist of similar requirements for security, privacy, and interoperability, based on 19 industry and government standards and guidelines, described in the rule regarding waiver applications. Alternative 4 effectively would codify standards that may become obsolete in the near future, as existing standards are revised, emerging standards publish, and new cyber threats proliferate. TSA rejects this alternative because establishing minimum requirements that may become obsolete in the near future may limit the ability for TSA to revise standards quickly and would increase the security and privacy risks of accepting mDLs. In addition, this alternative implies a degree of certainty that TSA believes is premature given emerging standards that are still in development. Also, costs under Alternative 4 would roughly be similar to costs under the rule, as both options would require audits and other compliance costs.

5. Regulatory Flexibility Act Assessment

The Regulatory Flexibility Act (RFA) of 1980, as amended,[97] was enacted by Congress to ensure that small entities (small businesses, small not-for-profit organizations, and small governmental jurisdictions) will not be unnecessarily or disproportionately burdened by Federal regulations. Section 605 of the RFA allows an agency to certify a rule in lieu of preparing an analysis if the regulations are not expected to have a significant economic impact on a substantial number of small entities.

In accordance with the RFA, pursuant to 5 U.S.C. 605(b), TSA certifies that the rule will not have a significant economic impact on a substantial number of small entities. The rule will directly impact States that voluntarily choose to apply for a waiver that will permit mDLs issued by those States to be accepted for official Federal purposes.

6. International Trade Impact Assessment

The Trade Agreement Act of 1979 prohibits Federal agencies from establishing any standards or engaging in related activities that create unnecessary obstacles to the foreign commerce of the United States. The Trade Agreement Act does not consider legitimate domestic objectives, such as essential security, as unnecessary obstacles. The statute also requires that international standards be considered and, where appropriate, that they be the basis for U.S. standards. TSA has assessed the potential effect of this rule and has determined this rule will not have an adverse impact on international trade.

7. Unfunded Mandates Reform Act Assessment

Title II of the Unfunded Mandates Reform Act of 1995 (UMRA), Public Law 104–4, establishes requirements for Federal agencies to assess the effects of their regulatory actions on State, local, and tribal governments and the private sector. Under section 202 of the UMRA, TSA generally must prepare a written Statement, including a cost-benefit analysis, for and final rules with ''Federal mandates'' that may result in expenditures by State, local, and tribal governments in the aggregate or by the private sector of $100 million or more (adjusted for inflation) in any one year.

Before TSA promulgates a rule for which a written statement is required, section 205 of the UMRA generally requires TSA to identify and consider a reasonable number of regulatory alternatives and adopt the least costly, most cost-effective, or least burdensome alternative that achieves the objectives of the rulemaking. The provisions of section 205 do not apply when they are inconsistent with applicable law. Moreover, section 205 allows TSA to adopt an alternative other than the least costly, most cost-effective, or least burdensome alternative if the final rule provides an explanation why that alternative was not adopted. Before TSA establishes any regulatory requirements that may significantly or uniquely affect small governments, including tribal governments, it must develop under section 203 of the UMRA a small government agency plan. The plan must provide for notifying potentially affected small governments, enabling officials of affected small governments to have meaningful and timely input in the development of TSA regulatory proposals with significant Federal intergovernmental mandates, and informing, educating, and advising small governments on compliance with the regulatory requirements.

When adjusted for inflation, the threshold for expenditures becomes $177.1 million in 2022 dollars. TSA has

[97] Public Law 96–354, 94 Stat. 1164 (Sept. 19, 1980) (codified at 5 U.S.C. 601 *et seq.,* as amended by the Small Business Regulatory Enforcement Fairness Act of 1996 (SBREFA)).

determined that this rule does not contain a Federal mandate as it is voluntary. Furthermore, estimated expenditures for State, local, and tribal governments do not exceed that amount in the aggregate in any one year.

B. Paperwork Reduction Act

The Paperwork Reduction Act of 1995 (PRA) (44 U.S.C. 3501 *et seq.*) requires that TSA consider the impact of paperwork and other information collection burdens imposed on the public. Under the provisions of PRA section 3507(d), TSA must obtain approval from the Office of Management and Budget (OMB) for each collection of information it conducts, sponsors, or requires through regulations. This rule calls for a collection of information under the PRA. Accordingly, TSA has submitted to OMB for review the information collections that follow below and is pending approval. *See* 5 CFR 1320.11(a). TSA has published a separate notice in the **Federal Register** soliciting comment on the PRA collection included in this final rule. As defined in 5 CFR 1320.3(c), ''collection of information'' includes reporting, recordkeeping, monitoring, posting, labeling, and other similar actions. This section provides the description of the information collection and of those who must collect the information as well as an estimate of the total annual time burden. TSA cannot request submission of waiver applications under this rule until OMB has approved the information collection.

The rule establishes a process for States to apply to TSA for a temporary waiver. Such a request is voluntary but will require the submission of an mDL waiver application, resubmission of an mDL waiver application deemed insufficient or denied, and reapplication for an mDL waiver when the term of the mDL waiver expires. All of these items are considered new information collections.

TSA uses the current State of mDL implementation to inform its estimate on how many State entities will request an mDL waiver during the period of analysis.[98] All 50 States, the District of Columbia, and five territories (collectively referred to as ''States'' hereafter) are eligible to apply for an mDL waiver as discussed in the rule. However, TSA assumes that not all States will apply for the mDL waiver. TSA assumes 15 States will apply for an mDL waiver in Year 1 of the analysis, 10 States in Year 2, and five States in Year 3.[99]

Following the State submission of its mDL waiver application, TSA determines if the application is approved, insufficient, or denied. States are allowed to amend an insufficient or denied mDL waiver application and resubmit to TSA review.

TSA assumes that all submissions will initially be deemed insufficient due to the mDL waiver criteria being new and with mDLs an emerging technology. Nonetheless, TSA intends to work individually with interested States to meet the mDL criteria to maximize the likelihood of receiving a waiver. Based on these assumptions, TSA estimates all initial mDL waiver applications will be deemed insufficient and that 90 percent of States will resubmit their mDL waiver applications.[100]

A State's mDL waivers will be valid for three years. Therefore, States granted an mDL waiver in Year 1 will need to reapply in Year 4 which is beyond the scope of this particular information collection.

TSA technology subject matter experts estimate that the mDL waiver application will take, on average, 20 hours to complete. TSA also estimates that mDL waiver resubmissions will take 25 percent of the initial mDL waiver application time which equates to 5 hours.[101] Finally, TSA estimates that mDL waiver reapplications will take 75 percent of the initial mDL waiver application time which equates to 15 hours. [102]

These hour burden estimates are combined with the number of collection activities to calculate the total and average time burden associated with the rule. TSA estimates the rule's total three-year burden for mDL waiver applications, mDL waiver resubmissions, and mDL waiver reapplications is 57 responses and 735 hours. TSA estimates an average yearly burden of 19 responses and 245 hours. Details of the calculation can be found in Table 7.

TABLE 7—PRA INFORMATION COLLECTION RESPONSES AND BURDEN HOURS

Collection activity	Number of responses						Total hours	Average annual hours
	Year 1	Year 2	Year 3	Total responses	Average annual responses	Time per response (hours)		
				d = a + b + c	e = d/3	f	g = d * f	h = g/3
mDL Waiver Application	15.0	10.0	5.0	30.0	10.0	20	600	200
mDL Waiver Resubmission	13.5	9.0	4.5	27.0	9.0	5	135	45
mDL Waiver Reapplication	0	0	0	0	0	15	0	0
Total	28.5	19.0	9.5	57.0	19.0		735	245

[98] As of December 2023, 10 States currently provide mDLs. Roughly 18 States have taken steps towards mDL implementation, including six States participating in the TSA mDL testing without a current mDL solution.

[99] Each State would submit one mDL waiver application.

[100] DHS assumes that 10 percent of applications deemed insufficient would no longer pursue an mDL waiver due to the level of effort involved to become sufficient and wait until the mDL environment is more fully developed.

[101] mDL Waiver Resubmission burden = 20 hours [initial mDL waiver application burden] × 0.25 = 5 hours.

[102] mDL Waiver Renewal burden = 20 hours [initial mDL waiver application burden] × (1 − 0.25) = 15 hours.

In addition, States will incur costs associated with audits of their mDL infrastructure. TSA estimates an average cost of $26,974 per submission. States will incur this cost for the initial mDL waiver application and mDL waiver reapplication. As there are no reapplications anticipated for this information collection request, TSA multiplies the annual average number of mDL waiver applications from Table 7 above (10) and the audit cost of $26,974 for a total mDL waiver application cost of $269,742.

C. Federalism (E.O. 13132)

A rule has implications for federalism under E.O. 13132 of August 6, 1999 (Federalism) if it has a substantial direct effect on State or local governments and would either preempt State law or impose a substantial direct cost of compliance on them. TSA analyzed this rule under this order and determined that although this rule affects the States, it does not preempt State law or impose substantial direct compliance costs.

This final rule establishes a process for States to request a temporary waiver that enables Federal agencies to accept mDLs issued by those States when REAL ID enforcement begins on May 7, 2025. The rule does not, however, require States to apply for a waiver, and does not impact States who elect not to do so.

States that elect to apply for a waiver under this rule must submit an application, supporting data, and other documentation to establish that its mDLs meet the specified criteria concerning security, privacy, and interoperability. TSA intends to work with each State a case-by-case basis to ensure that its mDLs meet the minimum requirements necessary to obtain a waiver. This rule does not impact the broad policymaking discretion that States currently exercise regarding other aspects of driver's license issuance.

DHS recognizes that States seeking a waiver will incur compliance costs for which Federal funds are generally not available. However, TSA emphasizes again that this rule does not require States to apply for a waiver, and TSA is promulgating this rule in response to States' concerns regarding mDL acceptance when REAL ID enforcement begins. To minimize States' costs, this rule affords States the maximum possible discretion consistent with the purposes of the REAL ID Act and regulations. Although the rule prescribes baseline requirements, it allows States broad discretion to implement technology decisions, tailored to each State's unique situation, that meet the requirements.

TSA therefore has determined that the rule is consistent with Executive Order 13132 and does not have these implications for federalism.

D. Customer Service (E.O. 14058)

E.O. 14058 of December 13, 2021 (Transforming Federal Customer Experience and Service Delivery to Rebuild Trust in Government), is focused on enhancing the of technology ''to modernize Government and implement services that are simple to use, accessible, equitable, protective, transparent, and responsive for all people of the United States.'' The Secretary of Homeland Security has specifically committed to testing the use of innovative technologies at airport security checkpoints to reduce passenger wait times. This rule supports this commitment. Using mDLs to establish identity at airport security checkpoints is intended to provide the public with increased convenience, security, privacy, and health benefits from ''contact-free'' identity verification. In 2022, DHS and TSA began a collaboration with States and industry to test the use of mDLs issued by participating States at select TSA airport security checkpoints (see Part II.B.2., above). As of the date of this final rule, TSA is currently testing mDLs issued by 11 States (Arizona, California, Colorado, Georgia, Hawaii, Iowa, Louisiana, Maryland, New York, Ohio, Utah) at 27 airports.[103]

E. Energy Impact Analysis (E.O. 13211)

TSA analyzed this rule under E.O. 13211 of May 18, 2001 (Actions Concerning Regulations That Significantly Affected Energy Supply, Distribution or Use), and determined that it is not a ''significant energy action'' under that E.O. and is not likely to have a significant adverse effect on the supply, distribution, or use of energy. Therefore, this rulemaking does not require a Statement of Energy Effects.

F. Environmental Analysis

DHS and its components review actions to determine whether the National Environmental Policy Act[104] (NEPA) applies to them and, if so, what degree of analysis is required. DHS Directive 023–01, Rev. 01 (Directive) and Instruction Manual 023–01–001–01,[105] Rev. 01 (Instruction Manual) establish the procedures that DHS and its components use to comply with NEPA and the Council on Environmental Quality (CEQ) regulations[106] for implementing NEPA. The CEQ regulations allow Federal agencies to establish in their NEPA implementing procedures categories of actions (''categorical exclusions'') which experience has shown normally do not individually or cumulatively have a significant effect on the human environment and, therefore, do not require an Environmental Assessment (EA) or Environmental Impact Statement (EIS).[107]

Under DHS NEPA implementing procedures, for an action to be categorically excluded, it must satisfy each of the following three conditions: (1) the entire action clearly fits within one or more of the categorical exclusions; (2) the action is not a piece of a larger action; and (3) no extraordinary circumstances exist that create the potential for a significant environmental effect.[108]

As discussed throughout this preamble, this final rule amends existing REAL ID regulations to add definitions and establish a process enabling States to apply to TSA for a temporary waiver, which would allow Federal agencies to accept, for official purposes when REAL ID enforcement begins in May 2025, mDLs issued by States to whom TSA has issued a waiver. These requirements interpret or amend an existing regulation without changing its environmental effect.

TSA therefore has determined that this final rule clearly fits within by categorical exclusion number A3 in Appendix A of the Instruction Manual. Categorical exclusion A3 applies to promulgation of rules, issuance of rulings or interpretations, and the development and publication of policies, orders, directives, notices, procedures, manuals, advisory circulars, and other guidance documents of the following nature: (a) Those of a strictly administrative or procedural nature; (b) those that implement, without substantive change, statutory or regulatory requirements; (c) those that implement, without substantive change, procedures, manuals, and other guidance documents; (d) those that interpret or amend an existing regulation without changing its

[103] TSA, Facial Recognition and Digital Identity Solutions, *https://www.tsa.gov/digital-id* (last visited July 17, 2024).

[104] *See* Public Law 91–190, 42 U.S.C. 4321- 4347.

[105] *See* DHS, Implementing the National Environmental Policy Act, *DHS Directive 023–01, Rev 01* (Oct. 31, 2014), and *DHS Instruction Manual 023–01–001–01, Rev. 01* (Nov. 6, 2014), *https://www.dhs.gov/publication/directive-023-01-rev-01-and-instruction-manual-023-01-001-01-rev-01-and-catex* (last visited July 17, 2024).

[106] 40 CFR parts 1500 through 1508.

[107] *See* 40 CFR 1501.4(a).

[108] *See* Instruction Manual, section V.B.2 (a–c).

environmental effect; (e) technical guidance on safety and security matters; or (f) guidance for the preparation of security plans.

This final rule is not a piece of a larger action. Under section V.B(2)(b) of the Instruction Manual, and as informed by the scoping requirements of 40 CFR 1501.9(e), actions must be considered in the same review if the actions are connected, meaning that an action may trigger another action, an action cannot or will not proceed unless another action is taken, or an action depends on a larger action for its justification. While TSA anticipates future rulemaking efforts to further amend REAL ID regulations and create requirements enabling States to issue REAL ID-compliant mDLs, any subsequent final rule, as well as this final rule, are each stand-alone regulatory actions. Thus, this final rule is not connected to any other action for purposes of the NEPA categorical exclusion analysis.

In accordance with the Instruction Manual's NEPA implementing procedures, TSA has completed an evaluation of this rule to determine whether it involves one or more of the ten identified extraordinary circumstances that present the potential for significant environmental impacts. TSA concludes from its analysis that no extraordinary circumstances are present requiring further environmental analysis and documentation. Therefore, this action is categorically excluded and no further NEPA analysis is required.

List of Subjects in 6 CFR part 37

Document security, Driver's licenses, Identification cards, Incorporation by reference, Licensing and registration, Motor vehicle administrations, Motor vehicle. safety, Motor vehicles, Personally identifiable information, Physical security, Privacy, Reporting and recordkeeping requirements, Security measures.

Regulatory Amendments

For the reasons set forth in the preamble, the Department of Homeland Security amends 6 CFR part 37 to read as follows:

PART 37—REAL ID DRIVER'S LICENSES AND IDENTIFICATION CARDS

■ 1. The authority citation for part 37 continues to read as follows:

Authority: 49 U.S.C. 30301 note; 6 U.S.C. 111, 112.

Subpart A—General

■ 2. Amend § 37.3 by adding the definitions for ''Administration'', ''Certificate authority'', ''Certificate management system'', ''Certificate policy'', ''Certificate system'', ''Critical security event'', ''Delegated third party'', ''Delegated third party system'', ''Denial of service'', ''Digital certificates'', ''Digital signatures'', ''Distributed denial of service'', ''Execution environment'', ''Front end system'', ''Hardware security module'', ''High security zone'', ''Identity proofing'', ''Identity verification'', ''Internal support system'', ''Issuing authority'', ''Issuing authority certificate authority'', ''Issuing system'', ''mDL'', ''Mobile driver's license'', ''Mobile identification card'', ''Multi-Factor authentication'', ''Online certificate status protocol'', ''Penetration test'', ''Provisioning'', ''Public key infrastructure'', ''Rich execution environment'', ''Root certificate authority'', ''Root certificate authority system'', ''Secure element'', ''Secure hardware'', ''Secure key storage device'', ''Secure zone'', ''Security support system'', ''Sole control'', ''State root certificate'', ''System'', ''Trusted execution environment'', ''Trusted role'', ''Virtual local area network'', ''Vulnerability'', ''Vulnerability scanning'', and ''Zone'' in alphabetical order to read as follows:

§ 37.3 Definitions.

* * * * *

Administration means management actions performed on *Certificate Systems* by a person in a *Trusted Role.*

* * * * *

Certificate authority means an issuer of *digital certificates* that are used to certify the identity of parties in a digital transaction.

Certificate Management System means a system used by a State or *delegated third party* to process, approve issuance of, or store *digital certificates* or *digital certificate* status information, including the database, database server, and storage.

Certificate policy means the set of rules and documents that forms a State's governance framework in which *digital certificates, certificate systems,* and cryptographic keys are created, issued, managed, and used.

Certificate system means the system used by a State or *delegated third party* to provide services related to *public key infrastructure* for digital identities.

Critical security event means detection of an event, a set of circumstances, or anomalous activity that could lead to a circumvention of a *zone's* security controls or a compromise of a *certificate system's* integrity, including excessive login attempts, attempts to access prohibited resources, *Denial of service* or *Distributed denial of service* attacks, attacker reconnaissance, excessive traffic at unusual hours, signs of unauthorized access, system intrusion, or an actual compromise of component integrity.

* * * * *

Delegated third party means a natural person or legal entity that is not the state and that operates any part of a *certificate system* under the State's legal authority.

Delegated third party system means any part of a *certificate system* used by a *delegated third party* while performing the functions delegated to it by the State.

Denial of service means the prevention of authorized access to resources or the delaying of time-critical operations.

* * * * *

Digital certificates identify the parties involved in an electronic transaction, and contain information necessary to validate *Digital signatures.*

* * * * *

Digital signatures are mathematical algorithms used to validate the authenticity and integrity of a message.

Distributed denial of service means a *denial of service* attack where numerous hosts perform the attack.

* * * * *

Execution environment means a place within a device processer where active application's code is processed.

* * * * *

Front end system means a system with a public IP address, including a web server, mail server, DNS server, jump host, or authentication server.

* * * * *

Hardware security module means a physical computing device that safeguards and manages cryptographic keys and provides cryptographic processing.

High security zone means a physical location where a State's or *Delegated third party's* private key or cryptographic hardware is located.

* * * * *

Identity proofing refers to a series of steps that the State executes to prove the identity of a person.

Identity verification is the confirmation that identity data belongs to its purported holder.

* * * * *

Internal support system means a system which operates on a State's internal network and communicates with the *certificate system* to provide business services related to mDL management.

Issuing authority means the State that issues a *mobile driver's license* or *mobile identification card.*

Issuing authority certificate authority means a *certificate authority* operated by or on behalf of an *issuing authority* or a State's *root certificate authority.*

Issuing system means a system used to sign *mDLs, digital certificates,* mobile security objects, or validity status information.

* * * * *

mDL means *mobile driver's license* and *mobile identification cards,* collectively.

Mobile driver's license means a *driver's license* that is stored on a mobile electronic device and read electronically.

Mobile identification card means an *identification card,* issued by a State, that is stored on a mobile electronic device and read electronically.

Multi-Factor authentication means an authentication mechanism consisting of two or more of the following independent categories of credentials (*i.e.,* factors) to verify the user's identity for a login or other transaction: something you know (knowledge factor), something you have (possession factor), and something you are (inherence factor).

* * * * *

Online certificate status protocol means an online protocol used to determine the status of a *digital certificate.*

* * * * *

Penetration test means a process that identifies and attempts to exploit vulnerabilities in systems through the active use of known attack techniques, including the combination of different types of exploits, with a goal of breaking through layers of defenses and reporting on unpatched vulnerabilities and system weaknesses.

* * * * *

Provisioning means the process by which a State transmits and installs an *mDL* on an individual's mobile device.

Public key infrastructure means a structure where a *certificate authority* uses *digital certificates* for issuing, renewing, and revoking digital credentials.

* * * * *

Rich execution environment, also known as a ''normal execution environment,'' means the area inside a device processor that runs an operating system.

Root certificate authority means the State *certificate authority* whose public encryption key establishes the basis of trust for all other *digital certificates* issued by a State.

Root certificate authority system means a system used to create a State's *root certificate* or to generate, store, or sign with the private key associated with a *State root certificate.*

* * * * *

Secure element means a tamper-resistant secure hardware component which is used in a device to provide the security, confidentiality, and multiple application environment required to support various business models.

Secure hardware means hardware provided on a mobile device for key management and trusted computation such as a *secure element* (SE) or *trusted execution environment.*

Secure key storage device means a device certified as meeting the specified FIPS PUB 140–3 Level 2 overall, Level 3 physical, or Common Criteria (EAL 4+).

Secure zone means an area (physical or logical) protected by physical and logical controls that appropriately protect the confidentiality, integrity, and availability of *certificate systems.*

Security support system means a system used to provide security support functions, which may include authentication, network boundary control, audit logging, audit log reduction and analysis, vulnerability scanning, and intrusion detection (host-based intrusion detection, network-based intrusion detection).

* * * * *

Sole control means a condition in which logical and physical controls are in place to ensure the *administration* of a *certificate system* can only be performed by a State or *delegated third party.*

* * * * *

State root certificate means a public *digital certificate* of a *root certificate authority* operated by or on behalf of a State.

System means one or more pieces of equipment or software that stores, transforms, or communicates data.

* * * * *

Trusted execution environment means an *execution environment* that runs alongside but isolated from a *rich execution environment* and has the security capabilities necessary to protect designated applications.

Trusted role means an employee or contractor of a State or *delegated third party* who has authorized access to or control over a *secure zone* or *high security zone.*

* * * * *

Virtual local area network means a broadcast domain that is partitioned and isolated within a network.

Vulnerability means a weakness in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat source.

Vulnerability scanning means a technique used to identify host attributes and associated *vulnerabilities.*

Zone means a subset of *certificate systems* created by the logical or physical partitioning of systems from other *certificate systems.*

■ 3. Revise § 37.4 to read as follows:

§ 37.4 Incorporation by reference.

Certain material is incorporated by reference into this part with the approval of the Director of the Federal Register under 5 U.S.C. 552(a) and 1 CFR part 51. All approved incorporation by reference (IBR) material is available for inspection at the Transportation Security Administration (TSA) and at the National Archives and Records Administration (NARA). Please contact TSA at Transportation Security Administration, Attn.: OS/ESVP/REAL ID Program, TSA Mail Stop 6051, 6595 Springfield Center Dr., Springfield, VA 20598–6051, (866) 289–9673, or visit *www.tsa.gov.* You may also contact the REAL ID Program Office at *REALID-mDLwaiver@tsa.dhs.gov* or visit *www.tsa.gov/REAL-ID/mDL.* For information on the availability of this material at NARA, visit *www.archives.gov/federal-register/cfr/ibr-locations.html* or email *fr.inspection@nara.gov.* The material may also be obtained from the following sources:

(a) American Association of Motor Vehicle Administrators (AAMVA) 4301 Wilson Boulevard, Suite 400, Arlington, VA 22203; phone: (703) 522–4200; website: *www.aamva.org.*

(1) 2005 AAMVA Driver's License/Identification Card Design Specifications, Annex A, section A.7.7.2., March 2005 (AAMVA Specifications); IBR approved for § 37.17.

(2) Mobile Driver's License (mDL) Implementation Guidelines, Version 1.2January 2023; IBR approved for § 37.10(a). (Available at *https://aamva.org/getmedia/b801da7b-5584-466c-8aeb-f230cef6dda5/mDL-Implementation-Guidelines-Version-1-2_final.pdf.*)

(b) Certification Authority Browser Forum (CA/Browser Forum), 815 Eddy St., San Francisco, CA 94109; phone: (415) 436–9333; email: *questions@cabforum.org;* website: *www.cabforum.org.*

(1) Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates, Version

1.8.6, December 14, 2022; IBR approved for appendix A to this subpart. (Available at *https://cabforum.org/wp-content/uploads/CA-Browser-Forum-BR-1.8.6.pdf.*)

(2) Network and Certificate System Security Requirements, Version 1.7, April 5, 2021; IBR approved for appendix A to this subpart. (Available at *https://cabforum.org/wp-content/uploads/CA-Browser-Forum-Network-Security-Guidelines-v1.7.pdf.*)

(c) Cybersecurity and Infrastructure Security Agency, Mail Stop 0380, Department of Homeland Security, 245 Murray Lane, Washington, DC 20528–0380; phone: (888) 282–0870; email: *central@cisa.gov;* website: *www.cisa.gov.*

(1) Federal Government Cybersecurity Incident & Vulnerability Response Playbooks, November 2021; IBR approved for appendix A to this subpart. (Available at *www.cisa.gov/sites/default/files/publications/Federal_Government_Cybersecurity_Incident_and_Vulnerability_Response_Playbooks_508C.pdf.*)

(2) [Reserved]

(d) Department of Homeland Security, 2707 Martin Luther King Jr. Ave. SE, Washington, DC 20528; phone: (202) 282–8000; website: *www.dhs.gov.*

(1) National Cyber Incident Response Plan, December 2016; IBR approved for appendix A to this subpart. (Available at *www.cisa.gov/uscert/sites/default/files/ncirp/National_Cyber_Incident_Response_Plan.pdf.*)

(2) [Reserved]

(e) International Civil Aviation Organization (ICAO), ICAO, Document Sales Unit, 999 University Street, Montreal, Quebec, Canada H3C 5H7; phone: (514) 954–8219; email: *sales@icao.int;* website: *www.icao.int.*

(1) ICAO 9303, ''Machine Readable Travel Documents,'' Volume 1, part 1, Sixth Edition, 2006; IBR approved for § 37.17.

(2) [Reserved]

(f) International Organization for Standardization, Chemin de Blandonnet 8, CP 401, 1214 Vernier, Geneva, Switzerland; phone: +41 22 749 01 11; email: *customerservice@iso.org;* website: *www.iso.org/contact-iso.html.* (Also available by contacting ANSI at ANSI, 25 West 43rd Street, 4th Floor, New York, New York 10036 website: *www.ansi.org.*)

(1) ISO/IEC 19794–5:2005(E) Information technology—Biometric Data Interchange Formats—Part 5: Face Image Data, dated June 2005; IBR approved for § 37.17.

(2) ISO/IEC 15438:2006(E) Information Technology—Automatic identification and data capture techniques—PDF417 symbology specification, dated June 2006; IBR approved for § 37.19.

(3) ISO/IEC 18013–5:2021(E), Personal identification—ISO-compliant driving license—Part 5: Mobile driving license (mDL) application, First Edition, September 2021; IBR approved for §§ 37.8(b); 37.10(a); and appendix A to this subpart.

(g) National Institute of Standards and Technology, 100 Bureau Drive, Gaithersburg, MD 20899; phone: (301) 975–2000; website: *www.nist.gov.*

(1) FIPS PUB 140–3, Federal Information Processing Standard Publication: Security Requirements for Cryptographic Modules, March 22, 2019; IBR approved for appendix A to this subpart. (Available at *https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.140-3.pdf.*)

(2) FIPS PUB 180–4, Federal Information Processing Standard Publication: Secure Hash Standard (SHS), August 2015; IBR approved for § 37.10(a). (Available at *https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.180-4.pdf.*)

(3) FIPS PUB 186–5, Federal Information Processing Standard Publication: Digital Signature Standard (DSS), February 3, 2023; IBR approved for § 37.10(a). (Available at *https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.186-5.pdf.*)

(4) FIPS PUB 197-upd1, Federal Information Processing Standard Publication: Advanced Encryption Standard (AES), May 9, 2023; IBR approved for § 37.10(a). (Available at *https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.197.pdf.*)

(5) FIPS PUB 198–1, Federal Information Processing Standard Publication: The Keyed-Hash Message Authentication Code (HMAC), July 2008; IBR approved for § 37.10(a). (Available at *https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.198-1.pdf.*)

(6) FIPS PUB 202, Federal Information Processing Standard Publication: SHA–3 Standard: Permutation-Based Hash and Extendable-Output Functions, August 2015; IBR approved for § 37.10(a). (Available at *https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.202.pdf.*)

(7) NIST SP 800–53 Rev.5, NIST Special Publication: Security and Privacy Controls for Information Systems and Organizations, Revision 5, September 2020 (including updates as of December. 10, 2020); IBR approved for appendix A to this subpart. (Available at *https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf.*)

(8) NIST SP 800–57 Part 1 Rev.5, NIST Special Publication: Recommendation for Key Management: Part 1—General, Revision 5, May 2020; IBR approved for appendix A to this subpart. (Available at *https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-57pt1r5.pdf.*)

(9) NIST SP 800–57 Part 2 Rev.1, NIST Special Publication: Recommendation for Key Management: Part 2—Best Practices for Key Management Organization, Revision 1, May 2019; IBR approved for appendix A to this subpart. (Available at *https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-57pt2r1.pdf.*)

(10) NIST SP 800–57 Part 3 Rev.1, NIST Recommendation for Key Management: Part 3: Application-Specific Key Management Guidance, Revision 1, January 2015; IBR approved for appendix A to this subpart. (Available at *https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-57Pt3r1.pdf.*)

(11) NIST SP 800–63–3, NIST Special Publication: Digital Identity Guidelines, June 2017; IBR approved for appendix A to this subpart. (Available at *https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63-3.pdf.*)

(12) NIST SP 800–63B, NIST Special Publication: Digital Identity Guidelines Authentication and Lifecycle Management, June 2017 (including updates as of December. 1, 2017); IBR approved for appendix A to this subpart. (Available at *https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63b.pdf.*)

(13) NIST Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1, April 16, 2018); IBR approved for appendix A to this subpart. (Available at *https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf.*)

4. Add §§ 37.7 through 37.10 to read as follows:

Sec.

§ 37.7 Temporary waiver for mDLs; State eligibility.

(a) *Generally.* TSA may issue a temporary certificate of waiver to a State

that meets the requirements of §§ 37.10(a) and (b).

(b) *State eligibility.* A State may be eligible for a waiver only if, after considering all information provided by a State under §§ 37.10(a) and (b), TSA determines that—

(1) The State is in full compliance with all applicable REAL ID requirements as defined in subpart E of this part; and

(2) Information provided by the State under §§ 37.10(a) and (b) sufficiently demonstrates that the State's mDL provides the security, privacy, and interoperability necessary for acceptance by Federal agencies.

§ 37.8 Requirements for Federal agencies accepting mDLs issued by States with temporary waiver.

Notwithstanding § 37.5(b), Federal agencies may accept an mDL for REAL ID official purposes issued by a State that has a valid certificate of waiver issued by TSA under § 37.7(a). A Federal agency that elects to accept mDLs under this section must—

(a) Confirm the State holds a valid certificate of waiver consistent with § 37.7(a) by verifying that the State appears in a list of mDLs approved for Federal use, available as provided in § 37.9(b)(1);

(b) Use an mDL reader to retrieve and validate mDL data as required by standard ISO/IEC 18013–5:2021(E) (incorporated by reference; see § 37.4);

(c) In accordance with the deadlines set forth in § 37.5, verify that the data element ''DHS_compliance'' is marked ''F'', as required by §§ 37.10(a)(4)(ii) and (a)(1)(vii); and

(d) Upon discovery that acceptance of a State's mDL is likely to cause imminent or serious threats to the security, privacy, or data integrity, the agency's senior official responsible for REAL ID compliance, or equivalent function, must report such discovery to TSA as directed at *www.tsa.gov/real-id/mDL* within 72 hours of such discovery. Information provided in response to this paragraph *may* contain SSI, and if so, must be handled and protected in accordance with 49 CFR part 1520.

§ 37.9 Applications for temporary waiver for mDLs.

(a) *Application process.* Each State requesting a temporary waiver must file with TSA a complete application as set forth in §§ 37.10(a) and (b). Application filing instructions may be obtained from TSA at *www.tsa.gov/real-id/mDL.*

(b) *Decisions.* TSA will provide written notice via email to States within 60 calendar days, to the extent practicable, but in no event longer than 90 calendar days, indicating that TSA has made one of the following decisions:

(1) *Approved.* Upon approval of an application for a temporary waiver, TSA will issue a certificate of waiver to the State, and publish the State's name in a list of mDLs approved for Federal use at *www.tsa.gov/real-id/mDL.*

(2) *Insufficient.* Upon determination that an application for a temporary waiver is incomplete or otherwise deficient, TSA will provide the State an explanation of deficiencies, and an opportunity to address any deficiencies and submit an amended application. States will have 60 calendar days to respond to the notice, and TSA will respond via email within 30 calendar days.

(3) *Denied.* Upon determination that an application for a waiver fails to meet criteria specified in §§ 37.10(a) and (b), TSA will provide the State specific grounds on which the denial is based, and provide the State an opportunity to seek reconsideration as provided in paragraph (c) of this section.

(c) *Reconsideration*—(1) *How to File Request.* States will have 90 calendar days to file a request for reconsideration of a denied application. The State must explain what corrective action it intends to implement to correct any defects cited in the denial or, alternatively, explain why the denial is incorrect. Instructions on how to file a request for reconsideration for denied applications may be obtained from TSA at *www.tsa.gov/real-id/mDL.* TSA will notify States of its final determination within 60 calendar days of receipt of a State's request for reconsideration.

(2) *Final agency action.* An adverse decision upon reconsideration is a final agency action. A State whose request for reconsideration has been denied may submit a new application at any time following the process set forth in paragraph (a) of this section.

(d) *Terms and conditions.* A certificate of waiver will specify—

(1) The effective date of the waiver;

(2) The expiration date of the waiver; and

(3) Any additional terms or conditions as necessary.

(e) *Limitations; suspension; termination*—(1) *Validity period.* A certificate of waiver is valid for a period of 3 years from the date of issuance.

(2) *Reporting requirements.* If a State, after it has been granted a certificate of waiver, makes any significant additions, deletions, or modifications to its mDL issuance processes, other than routine systems maintenance and software updates, that differ materially from the information the State provided in response to §§ 37.10(a) and (b) under which the waiver was granted, the State must provide written notice of such changes to TSA at *www.tsa.gov/real-id/mDL* 60 calendar days before implementing such additions, deletions, or modifications. If a State is uncertain whether its particular changes require reporting, the State may contact TSA as directed at *www.tsa.gov/real-id/mDL.*

(3) *Compliance.* A State that is issued a certificate of waiver under this section must comply with all applicable REAL ID requirements in § 37.51(a), and with all terms and conditions specified in paragraph (d)(3) of this section.

(4) *Suspension.* (i) TSA may suspend the validity of a certificate of waiver for any of the following reasons:

(A) *Failure to comply.* TSA determines that a State has failed to comply with paragraph (d)(3) or (e)(2) of this section, or has issued mDLs in a manner not consistent with the information provided under §§ 37.10(a) or (b); or

(B) *Threats to security, privacy, and data integrity.* TSA reserves the right to suspend a certificate of waiver at any time upon discovery that Federal acceptance of a State's mDL is likely to cause imminent or serious threats to the security, privacy, or data integrity of any Federal agency. In such instances, TSA will provide written notice via email to each affected State as soon as practicable after discovery of the triggering event, including reasons for suspension, an explanation of any corrective actions a State must take to resume validity of its certificate of waiver.

(ii) Before suspending a certificate of waiver under paragraph (e)(4)(i)(A) of this section, TSA will provide to such State written notice via email of intent to suspend, including an explanation of deficiencies and instructions on how the State may cure such deficiencies. States will have 30 calendar days to respond to the notice, and TSA will respond via email within 30 calendar days. TSA's response would include one of the following: withdrawal of the notice, a request for additional information, or a final suspension.

(iii) If TSA issues a final suspension, TSA will temporarily remove the State from the list of mDLs approved for Federal acceptance for official purposes. TSA will continue to work with a State to whom TSA has issued a final suspension to resume validity of its existing certificate of waiver. A State that has been issued a final suspension may seek a new certificate of waiver by submitting a new application following the process set forth in paragraph (a) of this section.

(5) *Termination.* (i) TSA may terminate a certificate of waiver at an earlier date than specified in paragraph (d)(2) of this section if TSA determines that a State—

(A) Does not comply with applicable REAL ID requirements in § 37.51(a);

(B) Is committing an egregious violation of requirements specified under paragraph (d)(3) or (e)(2) of this section that the State is unwilling to cure; or

(C) Provided false information in support of its waiver application.

(ii) Before terminating a certificate of waiver, TSA will provide the State written notice via email of intent to terminate, including findings on which the intended termination is based, together with a notice of opportunity to present additional information. States must respond to the notice within 7 calendar days, and TSA will reply via email within 30 calendar days. TSA's response would include one of the following: withdrawal of the notice, a request for additional information, or a final termination.

(iii) If TSA issues a final termination, TSA will remove the State from the list of mDLs approved for Federal acceptance for official purposes. A State whose certificate of waiver has been terminated may seek a new waiver by submitting a new application following the process set forth in paragraph (a) of this section.

(6) *Reapplication.* A State seeking extension of a certificate of waiver after expiration of its validity period must file a new application under paragraph (a) of this section.

(f) *Effect of status of certificate of waiver.* (1) Issuance of a certificate of waiver is not a determination of compliance with any other section in this part.

(2) An application for certificate of waiver that TSA has deemed insufficient or denied, or a certificate of waiver that TSA has deemed suspended, terminated, or expired, is not a determination of non-compliance with any other section in this part.

(g) *SSI.* Information provided in response to paragraphs (a), (b)(2), (c), (e)(2), (e)(4)(ii), and (e)(5)(ii) of this section *may* contain SSI, and if so, must be handled and protected in accordance with 49 CFR part 1520.

§ 37.10 Application criteria for issuance of temporary waiver for mDLs; audit report; waiver application guidance.

(a) *Application criteria.* A State requesting a certificate of waiver must establish in its application that the mDLs for which the State seeks a waiver are issued with controls sufficient to resist compromise and fraud attempts, provide privacy protections sufficient to safeguard an mDL holder's identity data, and provide interoperability for secure acceptance by Federal agencies under the terms of a certificate of waiver. To demonstrate compliance with such requirements, a State must provide information, documents, and/or data sufficient to explain the means, which includes processes, methodologies, or policies, that the State has implemented to comply with requirements in this paragraph (a).

(1) *Provisioning.* For both remote and in-person provisioning, a State must explain the means it uses to address or perform the following—

(i) *Data encryption.* Securely encrypt mDL data and an mDL holder's Personally Identifiable Information when such data is transferred during provisioning, and when stored on the State's system(s) and on mDL holders' mobile devices.

(ii) *Escalated review.* Review repeated failed attempts at provisioning, resolve such failures, and establish criteria to determine when the State will deny provisioning an mDL to a particular mDL applicant.

(iii) *Authentication.* Confirm that an mDL applicant has control over the mobile device to which an mDL is being provisioned at the time of provisioning.

(iv) *Device identification keys.* Confirm that the mDL applicant possesses the mDL device private key bound to the mDL during provisioning.

(v) *User identity verification.* Prevent an individual from falsely matching with the licensing agency's records, including portrait images, of other individuals.

(vi) *Applicant presentation.* Prevent physical and digital presentation attacks by detecting the liveness of an individual and any alterations to the individual's appearance during remote and in-person provisioning.

(vii) *DHS_compliance data element.* Set the value of data element ''DHS_compliance'', as required by paragraph (a)(4)(ii) of this section, to correspond to the REAL ID compliance status of the underlying physical driver's license or identification card that a State has issued to an mDL holder as follows—

(A) ''F'' if the underlying card is REAL ID-compliant, or as otherwise required by AAMVA Mobile Driver's License (mDL) Implementation Guidelines, Section 3.2 (incorporated by reference; see § 37.4); or

(B) ''N'' if the underlying card is not REAL ID-compliant.

(viii) *Data record.* Issue mDLs using data, including portrait image, of an individual that matches corresponding data in the database of the issuing State's driver's licensing agency for that individual.

(ix) *Records retention.* Manage mDL records and related records, consistent with requirements set forth in AAMVA Mobile Driver's License (mDL) Implementation Guidelines (incorporated by reference; see § 37.4).

(2) *Issuance.* A State must explain the means it uses to manage the creation, issuance, use, revocation, and destruction of the State's certificate systems and keys in full compliance with the requirements set forth in appendix A to this subpart.

(3) *Privacy.* A State must explain the means it uses to protect Personally Identifiable Information during processing, storage, and destruction of mDL records and provisioning records.

(4) *Interoperability.* A State must explain the means it uses to issue mDLs that are interoperable with ISO/IEC 18013–5:2021(E) and the ''AAMVA mDL data element set'' defined in the AAMVA Mobile Driver's License (mDL) Implementation Guidelines (incorporated by reference; see § 37.4) as follows:

(i) A State must issue mDLs using the data model defined in ISO/IEC 18103–5:2021(E) section 7 (incorporated by reference; see § 37.4), using the document type ''org.iso.18013.5.1.mDL'', and using the name space ''org.iso.18013.5.1''. States must include the following mDL data elements defined as mandatory in ISO/IEC 18103–5:2021(E) Table 5: ''family_name'', ''given_name'', ''birth_date'', ''issue_date'', ''expiry_date'', ''issuing_authority'', ''document_number'', ''portrait'', and must include the following mDL data elements defined as optional in Table 5: ''sex'', ''resident_address'', ''portrait_capture_date'', ''signature_usual_mark''.

(ii) States must use the AAMVA mDL data element set defined in AAMVA Mobile Driver's License (mDL) Implementation Guidelines, Section 3.2 (incorporated by reference; see § 37.4), using the namespace ''org.iso.18013.5.1.aamva'' and must include the following data elements in accordance with the AAMVA mDL Implementation Guidelines: ''DHS_compliance'', and ''DHS_temporary_lawful_status''.

(iii) States must use only encryption algorithms, secure hashing algorithms, and digital signing algorithms as defined by ISO/IEC 18103–5:2021(E), section 9 and Annex B (incorporated by reference; see § 37.4), and which are included in the following NIST Federal Information Processing Standards (FIPS): NIST FIPS PUB 180–4, NIST

FIPS PUB 186–5, NIST FIPS PUB 197-upd1, NIST FIPS PUB 198–1, and NIST FIPS PUB 202 (incorporated by reference; see § 37.4).

(b) *Audit report.* States must include with their applications a report of an audit that verifies the information provided under paragraph (a) of this section.

(1) The audit must be conducted by a recognized independent entity, which may be an entity that is employed or contracted by a State and independent of the State's driver's licensing agency,—

(i) Holding an active Certified Public Accountant license in the issuing State;

(ii) Experienced with information systems security audits;

(iii) Accredited by the issuing State; and

(iv) Holding a current and active American Institute of Certified Public Accountants (AICPA) Certified Information Technology Professional (CITP) credential or ISACA (F/K/A Information Systems Audit and Control Association) Certified Information System Auditor (CISA) certification.

(2) States must include information about the entity conducting the audit that identifies—

(i) Any potential conflicts of interest; and

(ii) Mitigation measures or other divestiture actions taken to avoid conflicts of interest.

(c) *Waiver application guidance*—(1) *Generally.* TSA will publish ''Mobile Driver's License Waiver Application Guidance'' to facilitate States' understanding of the requirements set forth in paragraph (a) of this section. The non-binding Guidance will include recommendations and examples of possible implementations for illustrative purposes only. TSA will publish the Guidance on the REAL ID website at *www.tsa.gov/real-id/mDL.*

(2) *Updates.* TSA may periodically update its Waiver Application Guidance as necessary to provide additional information or recommendations to mitigate evolving threats to security, privacy, or data integrity. TSA will publish a notification in the **Federal Register** advising that updated Guidance is available, and TSA will publish the updated Guidance at *www.tsa.gov/real-id/mDL* and provide a copy to all States that have applied for or been issued a certificate or waiver.

■ 5. Add appendix A to subpart A to read as follows:

Appendix A to Subpart A of Part 37—Mobile Driver's License Issuance Infrastructure Requirements

A State that issues mDLs for acceptance by Federal agencies for official purposes as specified in the REAL ID Act must implement the requirements set forth in this appendix A in full compliance with the cited references. All references identified in this appendix A are incorporated by reference, see § 37.4. If a State utilizes the services of a delegated third party, the State must ensure the delegated third party complies with all applicable requirements of this appendix A for the services provided.

Paragraph	Requirement
	1: Certificate Authority Certificate Life-Cycle Policy
1.1	Maintain a certificate policy, which forms the State's certificate system governance framework. If certificate systems are managed at a facility not controlled by the State, the State must require any delegated third party to comply with the State's certificate policy. These requirements must be implemented in full compliance with the following references: • CA/Browser Forum Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates, Sections 2, 4.3, 4.9, 5, 6, as applicable; • ISO/IEC 18013–5:2021(E), Annex B; • CA/Browser Forum Network and Certificate System Security Requirements; • NIST SP 800–57 Part 1, Rev. 5, Sections 3, 5, 6, 7, 8; • NIST SP 800–57 Part 2, Rev. 1; • NIST SP 800–57 Part 3, Rev. 1, Sections 2, 3, 4, 8, 9; • NIST 800–53 Rev. 5, AC–1, AT–1, AU–1, CA–1, CM–1, CP–1, IA–1, IR–1, MA–1, MP–1, PE–1, PL–1, PL–2, PL–8, PL–10, PM–1, PS–1, PT–1, RA–1, SA–1, SC–1, SI–1, and SR–1.
1.2	Perform management and maintenance processes which includes baseline configurations, documentation, approval, and review of changes to certificate systems, issuing systems, certificate management systems, security support systems, and front end and internal support systems. These requirements must be implemented in full compliance with the following references: • CA/Browser Forum Network and Certificate System Security Requirements; • NIST Framework for Improving Critical Infrastructure Cybersecurity PR.IP–3; and • NIST SP 800–53 Rev. 5, CM–1, CM–2, CM–3, CM–4, CM–5, CM–6, CM–8, CM–9, CM–10, CM–11, CM–12, MA–2, MA–3, MA–4, MA–5, MA–6, PE–16, PE–17, PE–18, PL–10, PL–11, RA–7, SA–2, SA–3, SA–4, SA–5, SA–8, SA–9, SA–10, SA–11, SA–15, SA–17, SA–22, SC–18, SI–6, SI–7, SR–2, SR–5.
1.3	Apply recommended security patches, to certificate systems within six months of the security patch's availability, unless the State documents that the security patch would introduce additional vulnerabilities or instabilities that outweigh the benefits of applying the security patch. These requirements must be implemented in full compliance with the following references: • CA/Browser Forum Network and Certificate System Security Requirements; • NIST Framework for Improving Critical Infrastructure Cybersecurity ID.RA–1, PR.IP–12; and • NIST SP 800–53 Rev. 5, SI–2, SI–3.
	2: Certificate Authority Access Management
2.1	Grant administration access to certificate systems only to persons acting in trusted roles, and require their accountability for the certificate system's security, in full compliance with the following references: • CA/Browser Forum Network and Certificate System Security Requirements; • NIST Framework for Improving Critical Infrastructure Cybersecurity PR.AC–4; and • NIST SP 800–53 Rev. 5, AC–1, AC–2, AC–3, AC–5, AC–6, AC–8, AC–21, AC–22, AC–24, CA–6, PS–6.
2.2	Change authentication keys and passwords for any trusted role account on a certificate system whenever a person's authorization to administratively access that account on the certificate system is changed or revoked, in full compliance with the following references: • CA/Browser Forum Network and Certificate System Security Requirements; • NIST Framework for Improving Critical Infrastructure Cybersecurity PR.AC–1; and • NIST SP 800–53 Rev. 5, AC–1, AC–2, AC–3, AC–6, IA–1, IA–2, PS–4, PS–5.

Paragraph	Requirement
2.3	Follow a documented procedure for appointing individuals to trusted roles and assigning responsibilities to them, in full compliance with the following references: • CA/Browser Forum Network and Certificate System Security Requirements; • NIST Framework for Improving Critical Infrastructure Cybersecurity PR.AC–1; and • NIST SP 800–53 Rev. 5, AC–1, AC–2, AC–3, AC–5, AC–6, IA–1, IA–2.
2.4	Document the responsibilities and tasks assigned to trusted roles and implement ''separation of duties'' for such trusted roles based on the security-related concerns of the functions to be performed, in full compliance with the following references: • CA/Browser Forum Network and Certificate System Security Requirements; • NIST Framework for Improving Critical Infrastructure Cybersecurity—PR.AC–4; and • NIST SP 800–53 Rev. 5, AC–1, AC–2, AC–5, AC–6, MP–2, PS–9.
2.5	Restrict access to secure zones and high security zones to only individuals assigned to trusted roles, in full compliance with the following references: • CA/Browser Forum Network and Certificate System Security Requirements; • NIST Framework for Improving Critical Infrastructure Cybersecurity PR.AC; and • NIST SP 800–53 Rev. 5, AC–1, AC–2, AC–3, AC–5, AC–6, MP–2, PS–1, PS–6.
2.6	Restrict individuals assigned to trusted roles from acting beyond the scope of such role when performing administrative tasks assigned to that role, in full compliance with the following references: • CA/Browser Forum Network and Certificate System Security Requirements; • NIST Framework for Improving Critical Infrastructure Cybersecurity PR.AC–1, PR.AC–4, PR.AC–6, PR.AT–2; and • NIST SP 800–53 Rev. 5, AT–2, AT–3, PM–13, PM–14.
2.7	Require employees and contractors to observe the principle of ''least privilege'' when accessing or configuring access privileges on certificate systems, in full compliance with the following references: • CA/Browser Forum Network and Certificate System Security Requirements; • NIST Framework for Improving Critical Infrastructure Cybersecurity PR.AC–4, PR.AC–2; and • NIST SP 800–53 Rev. 5, AC–1, AC–2, AC–3, AC–5, AC–6, PE–1, PE–3, PL–4.
2.8	Require that individuals assigned to trusted roles use a unique credential created by or assigned to them in order to authenticate to certificate systems, in full compliance with the following references: • CA/Browser Forum Network and Certificate System Security Requirements; • NIST Framework for Improving Critical Infrastructure Cybersecurity PR.AC–1, PR.AC–6, PR.AC–4, PR.AC–7; and • NIST SP 800–53 Rev. 5, AC–1, IA–1, IA–2, IA–3, IA–5, IA–8, IA–12.
2.9	Lockout account access to certificate systems after a maximum of five failed access attempts, provided that this security measure: 1. Is supported by the certificate system; 2. Cannot be leveraged for a denial-of-service attack; and 3. Does not weaken the security of this authentication control. These requirements must be implemented in full compliance with the following references: • CA/Browser Forum Network and Certificate System Security Requirements; • NIST Framework for Improving Critical Infrastructure Cybersecurity PR.AC–7; and • NIST SP 800–53 Rev. 5, AC–7.
2.10	Implement controls that disable all privileged access of an individual to certificate systems within 4 hours of termination of the individual's employment or contracting relationship with the State or Delegated Third Party, in full compliance with the following references: • CA/Browser Forum Network and Certificate System Security Requirements; • NIST Framework for Improving Critical Infrastructure Cybersecurity PR.AC–7; and • NIST SP 800–53 Rev. 5, AC–1, AC–2, PS–1, PS–4, PS–7.
2.11	Implement multi-factor authentication or multi-party authentication for administrator access to issuing systems and certificate management systems, in full compliance with the following references: • CA/Browser Forum Network and Certificate System Security Requirements; • NIST Framework for Improving Critical Infrastructure Cybersecurity-PR.AC–6, PR.AC–7; and • NIST SP 800–53 Rev. 5, AC–14, IA–1, IA–2, IA–3, IA–5, IA–8, IA–11.
2.12	Implement multi-factor authentication for all trusted role accounts on certificate systems, including those approving the issuance of a Certificate and delegated third parties, that are accessible from outside a secure zone or high security zone, in full compliance with the following references: • CA/Browser Forum Network and Certificate System Security Requirements; • NIST Framework for Improving Critical Infrastructure Cybersecurity PR.AC–7; and • NIST SP 800–53 Rev. 5, AC–17, AC–18, AC–19, AC–20, IA–1, IA–2, IA–3, IA–4, IA–5, IA–6, IA–8.
2.13	If multi-factor authentication is used, implement only multi-factor authentication that achieves an Authenticator Assurance Level equivalent to AAL2 or higher, in full compliance with the following references: • NIST SP 800–63–3, Sections 4.3, 6.2; • NIST SP 800–63B, Section 4.2; • NIST Framework for Improving Critical Infrastructure Cybersecurity PR.AC–7; and • NIST SP 800–53 Rev. 5, IA–5, IA–7.
2.14	If multi-factor authentication is not possible, implement a password policy for trusted role accounts in full compliance with NIST SP 800–63B, Section 5.1.1.2, Memorized Secret Verifiers, and implement supplementary risk controls based on a system risk assessment.
2.15	Require trusted roles to log out of or lock workstations when no longer in use, in full compliance with the following references: • CA/Browser Forum Network and Certificate System Security Requirements; and • NIST SP 800–53 Rev. 5, AC–11, AC–12.
2.16	Configure workstations with inactivity time-outs that log the user off or lock the workstation after a set time of inactivity without input from the user. A workstation may remain active and unattended if the workstation is otherwise secured and running administrative tasks that would be interrupted by an inactivity time-out or system lock. These requirements must be implemented in full compliance with the following references: • CA/Browser Forum Network and Certificate System Security Requirements; and • NIST SP 800–53 Rev. 5, AC–11, AC–12.

Paragraph	Requirement
2.17	Review all system accounts at least every three months and deactivate any accounts that are no longer necessary for operations, in full compliance with the following references: • CA/Browser Forum Network and Certificate System Security Requirements; • NIST Framework for Improving Critical Infrastructure Cybersecurity PR.AC–1; and • NIST SP 800–53 Rev. 5, AC–2.
2.18	Restrict remote administration or access to a State issuing system, certificate management system, or security support system, including access to cloud environments, except when: 1. The remote connection originates from a device owned or controlled by the State or delegated third party; 2. The remote connection is through a temporary, non-persistent encrypted channel that is supported by Multi-Factor Authentication; and 3. The remote connection is made to a designated intermediary device— a. located within the State's network or secured Virtual Local Area Network (VLAN), b. secured in accordance with the requirements of this Appendix, and c. that mediates the remote connection to the issuing system. These Requirements must be implemented in full compliance with the following references: • CA/Browser Forum Network and Certificate System Security Requirements; • NIST Framework for Improving Critical Infrastructure Cybersecurity PR.AC–3, PR.AC–7; and • NIST SP 800–53 Rev. 5, AC–17, AC–19, AC–20, IA–3, IA–4, IA–6.
3: Facility, Management, and Operational Controls	
3.1	Restrict physical access authorizations at facilities where certificate systems reside, including facilities controlled by a delegated third party, by: 1. Verifying individual access authorizations before granting access to the facility; 2. Controlling ingress and egress to the facility using appropriate security controls; 3. Controlling access to areas within the facility designated as publicly accessible; 4. Escorting visitors, logging visitor entrance and exit from facilities, and limiting visitor activities within facilities to minimize risks to certificate systems; 5. Securing physical keys, combinations, and other physical access devices; 6. Maintaining an inventory of physical keys, combinations, and physical access devices; conduct review of this inventory at least annually; and 7. Changing combinations and keys every three years or when physical keys are lost, combinations are compromised, or when individuals possessing the physical keys or combinations are transferred or terminated. These requirements must be implemented in full compliance with the following reference: • NIST SP 800–53 Rev. 5, PE–2, PE–3, PE–4, PE–5, PE–8.
3.2	Implement controls to protect certificate system operations and facilities where certificate systems reside from environmental damage and/or physical breaches, including facilities controlled by a delegated third party, in full compliance with the following reference: • NIST SP 800–53 Rev. 5, CP–2, CP–4, CP–6, CP–7, CP–8, CP–9, CP–10, PE–2, PE–9, PE–10, PE–11, PE–12, PE–13, PE–14, PE–15, PE–21.
3.3	If certificate systems are managed at a facility not controlled by the State, implement controls to prevent risks to such facilities presented by foreign ownership, control, or influence, in full compliance with the following reference: • NIST SP 800–53 Rev. 5, SR–2, SR–3, SR–4, SR–6.
3.4	Implement controls to prevent supply chain risks for certificate systems including: 1. Employing acquisition strategies, tools, and methods to mitigate risks; 2. Establishing agreements and procedures with entities involved in the supply chain of certificate systems; 3. Implementing an inspection and tamper protection program for certificate systems components; 4. Developing and implementing component authenticity policies and procedures; and 5. Developing and implementing policies and procedures for the secure disposal of certificate systems components. These requirements must be implemented in full compliance with the following reference: • NIST SP 800–53 Rev. 5, SR–5, SR–8, SR–9, SR–10, SR–11, SR–12.
4: Personnel Security Controls	
4.1	Implement and disseminate to personnel with access to certificate systems and facilities, including facilities controlled by a delegated third party, a policy to control insider threat security risks that: 1. Addresses the purpose, scope, roles, responsibilities, management commitment, coordination among State entities, and compliance; 2. Complies with all applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and 3. Designates an official in a trusted role to manage the development, documentation, and dissemination of the policy and procedures. These requirements must be implemented in full compliance with the following reference: • NIST SP 800–53 Rev. 5, MA–5, PS–1, PS–8.
4.2	Assign a risk designation to all organizational positions with access to certificate systems and facilities, in full compliance with the following reference: • NIST SP 800–53 Rev. 5, PS–2, PS–9.
4.3	Establish screening criteria for personnel filling organization positions with access to certificate system and facilities, in full compliance with the following reference: • NIST SP 800–53 Rev. 5, PS–2, PS–3, SA–21.
4.4	Screen individual personnel in organizational positions with access to certificate systems and facilities, in full compliance with the following reference: • NIST SP 800–53 Rev. 5, PS–3.
4.5	Upon termination of individual employment, State or delegated third party must: 1. Disable system access within 4 hours;

Paragraph	Requirement
	2. Terminate or revoke any authenticators and credentials associated with the individual; 3. Conduct exit interviews that include— a. Notifying terminated individuals of applicable, legally binding post-employment requirements for the protection of organizational information, and b. Requiring terminated individuals to sign an acknowledgment of post-employment requirements as part of the organizational termination process; 4. Retrieve all security-related organizational system-related property; and 5. Retain access to organizational information and systems formerly controlled by terminated individual. These requirements must be implemented in full compliance with the following reference: • NIST SP 800–53 Rev. 5, PS–4.
4.6	Review and update personnel security policy, procedures, and position risk designations at least once every 12 months, in full compliance with the following reference: • NIST SP 800–53 Rev. 5, PS–1, PS–2.
4.7	Provide training to all personnel performing certificate system duties, on the following topics: 1. Fundamental principles of Public Key Infrastructure; 2. Authentication and vetting policies and procedures, including the State's certificate policy; 3. Common threats to certificate system processes, including phishing and other social engineering tactics; 4. Role specific technical functions related to the administration of certificate systems; and 5. The requirements of this Appendix. These requirements must be implemented in full compliance with the following references: • CA/Browser Forum Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates, Section 5.3.3; and • NIST SP 800–53 Rev. 5, CP–3, IR–2, SA–16.
4.8	Maintain records of training as required by paragraph 4.7 of this Appendix, in full compliance with the following references: • CA/Browser Forum Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates, Sections 5.3.3, 5.4.1; and • NIST SP 800–53 Rev. 5, AT–4.
4.9	Implement policies and processes to prevent any delegated third party personnel managing certificate systems at a facility not controlled by a State from being subject to risks presented by foreign control or influence, in full compliance with the following reference: • NIST SP 800–53 Rev. 5, SR–3, SR–4, SR–6.
	5: Technical Security Controls
5.1	Segment certificate systems into networks based on their functional or logical relationship, such as separate physical networks or VLANs, in full compliance with the following references: • CA/Browser Forum Network and Certificate System Security Requirements; • NIST Framework for Improving Critical Infrastructure Cybersecurity PR.AC–5; and • NIST SP 800–53 Rev. 5, AC–4, AC–10, CA–3, CA–9, MP–3, MP–4, RA–2, RA–9, SC–2, SC–3, SC–4, SC–8.
5.2	Apply equivalent security controls to all systems co-located in the same network (including VLANs) with a certificate system, in full compliance with the following references: • CA/Browser Forum Network and Certificate System Security Requirements; • NIST Framework for Improving Critical Infrastructure Cybersecurity PR.AC–5; and • NIST SP 800–53 Rev. 5, MP–5, MP–6, MP–7, RA–2, SC–7, SC–10, SC–39.
5.3	Maintain State root certificate authority systems in a high security zone and in an offline state or air-gapped from all other network operations. If operated in a cloud environment, State root certificate authority systems must use a dedicated VLAN with the sole purpose of Issuing Authority Certificate Authority (IACA) root certificate functions and be in an offline state when not in use for IACA root certificate functions. These requirements must be implemented in full compliance with the following references: • CA/Browser Forum Network and Certificate System Security Requirements; and • NIST SP 800–53 Rev. 5, SC–32.
5.4	Protect IACA root certificate private keys using dedicated hardware security modules (HSMs), either managed on-premises or provided through cloud platforms, that are under sole control of the State or delegated third party. These requirements must be implemented in full compliance with the following references: • NIST SP 800–57 Part 1, Rev. 5; • NIST FIPS PUB 140–3; and • NIST SP 800–53 Rev. 5, SC–12, SC–13.
5.5	Protect certificate systems private keys using NIST FIPS PUB 140–3 Level 3 or Level 4 certified HSMs, in full compliance with the following references: • NIST FIPS PUB 140–3; and • NIST SP 800–53 Rev. 5, SC–12, SC–13.
5.6	Protect document signer private keys using HSMs, either managed on-premises or provided through cloud platforms, that are under sole control of the State or delegated third party. These requirements must be implemented in full compliance with the following references: • NIST SP 800–57 Part 1, Rev. 5; • NIST FIPS PUB 140–3; and • NIST SP 800–53 Rev. 5, SC–12, SC–13.
5.7	Protect certificate systems document signer keys using NIST FIPS PUB 140–3 Level 2, Level 3, or Level 4 certified HSMs, in full compliance with the following references: • NIST FIPS PUB 140–3; and • NIST SP 800–53 Rev. 5, SC–12, SC–13.
5.8	Maintain and protect issuing systems, certificate management systems, and security support systems in at least a secure zone, in full compliance with the following references: • CA/Browser Forum Network and Certificate System Security Requirements; and

Paragraph	Requirement
	• NIST SP 800–53 Rev. 5, SC–15, SC–20, SC–21, SC–22, SC–24, SC–28, SI–16.
5.9	Implement and configure: security support systems that protect systems and communications between systems inside secure zones and high security zones, and communications with non-certificate systems outside those zones (including those with organizational business units that do not provide PKI-related services) and those on public networks. These requirements must be implemented in full compliance with the following references: • CA/Browser Forum Network and Certificate System Security Requirements; and • NIST SP 800–53 Rev. 5, SC–15, SC–20, SC–21, SC–22, SC–24, SC–28, SI–16.
5.10	Configure each network boundary control (firewall, switch, router, gateway, or other network control device or system) with rules that support only the services, protocols, ports, and communications that the State has identified as necessary to its operations. These requirements must be implemented in full compliance with the following references: • CA/Browser Forum Network and Certificate System Security Requirements; and • NIST SP 800–53 Rev. 5, AC–4, SI–3, SI–8, SC–7, SC–10, SC–23, CM–7.
5.11	Configure issuing systems, certificate management systems, security support systems, and front end and internal support systems by removing or disabling all accounts, applications, services, protocols, and ports that are not used in the State's or delegated third party's operations and restricting use of such systems to only those that are approved by the State or delegated third party. These requirements must be implemented in full compliance with the following references: • CA/Browser Forum Network and Certificate System Security Requirements; • NIST Framework for Improving Critical Infrastructure Cybersecurity PR.PT–3; and • NIST SP 800–53 Rev. 5, CM–7.
5.12	Implement multi-factor authentication on each component of the certificate system that supports multi-factor authentication, in full compliance with the following references: • CA/Browser Forum Network and Certificate System Security Requirements; • NIST Framework for Improving Critical Infrastructure Cybersecurity PR.AC–7; and • NIST SP 800–53 Rev. 5, IA–2.
5.13	Generate IACA root certificate key pairs with a documented and auditable multi-party key ceremony, performing at least the following steps: 1. Prepare and follow a key generation script; 2. Require a qualified person who is in a trusted role and not a participant in the key generation to serve as a live witness of the full process of generating the IACA root certificate key pair, or record a video in lieu of a live witness; 3. Require the qualified witness to issue a report confirming that the State followed its key ceremony during its key and certificate generation process, and confirming that controls were used to protect the integrity and confidentiality of the key pair; 4. Generate the IACA root certificate key pair in a physically secured environment as described in the State's certificate policy and/or certification practice statement; 5. Generate the IACA root certificate key pair using personnel in trusted roles under the principles of multiple person control and split knowledge. IACA root certificate key pair generation requires a minimum of two persons, consisting of at least one key generation ceremony administrator and one qualified witness); 6. Log the IACA root certificate key pair generation activities, sign the witness report (and video file, if applicable), with a document signing key which has been signed by the IACA root certificate private key, and include signed files and document signing public certificate with the IACA root certificate key pair generation log files; and 7. Implement controls to confirm that the IACA root certificate private key was generated and protected in conformance with the procedures described in the State's certificate policy and/or certification practice statement and the State's key generation script. These requirements must be implemented in full compliance with the following reference: • CA/Browser Forum Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates, Section 6.1.1.1.
5.14	Generate document signer key pairs with a documented and auditable multi-party key ceremony, performing at least the following steps: 1. Prepare and follow a key generation script; 2. Generate the document signer key pairs in a physically secured environment as described in the State's certificate policy and/or certification practice statement; 3. Generate the document signer key pairs using only personnel in trusted roles under the principles of multiple person control and split knowledge. document signer key pair generation requires a, minimum of two persons, consisting of at least one key generation ceremony administrator and at least one qualified witness or at least two key generation ceremony administrators when split knowledge generation is in place; 4. If a witness observes the key generation, require a qualified person who is in a trusted role and not a participant in the key generation to serve as a live witness of the full process of generating the document signer key pair; and 5. Require the qualified witness to issue a report confirming that the State followed its key ceremony during its key and certificate generation process and confirming that controls were used to rotect the integrity and confidentiality of the key pair; 6. Log the document signer key pairs generation activities and signed witness report, if applicable; and 7. Implement controls to confirm that the document signer private key was generated and protected in conformance with the procedures described in the State's certificate policy and/or certification practice statement and the State's key generation script. These requirements must be implemented in full compliance with the following reference: • CA/Browser Forum Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates, Section 6.1.1.1.
	6: Threat Detection
6.1	Implement a System under the control of State or delegated third party trusted roles that continuously monitors, detects, and alerts personnel to any modification to certificate systems, issuing systems, certificate management systems, security support systems, and front-end/internal-support systems, unless the modification has been authorized through a change management process. The State or delegated third party must respond to the alert and initiate a plan of action within at most 24 hours. These requirements must be implemented in full compliance with the following references: • CA/Browser Forum Network and Certificate System Security Requirements;

Paragraph	Requirement
	• NIST Framework for Improving Critical Infrastructure Cybersecurity DE.CM–7; and • NIST SP 800–53 Rev. 5, CA–7, CM–3, SI–5.
6.2	Identify any certificate systems under the control of State or delegated third party trusted roles that are capable of monitoring and logging system activity, and enable those systems to log and continuously monitor the events specified in paragraph 7 of this Appendix. These requirements must be implemented in full compliance with the following references: • CA/Browser Forum Network and Certificate System Security Requirements; and • NIST SP 800–53 Rev. 5, AU–12.
6.3	Monitor the integrity of the logging processes for application and system logs using either continuous automated monitoring and alerting, or human review, to confirm that logging and log-integrity functions meet the requirements set forth in paragraph 7 of this Appendix. Alternatively, if a human review is utilized and the system is online, the process must be performed at least once every 31 calendar days. These requirements must be implemented in full compliance with the following references: • CA/Browser Forum Network and Certificate System Security Requirements; and • NIST SP 800–53 Rev. 5, AU–1, AU–6, AU–5, AU–9, AU–12.
	7: Logging
7.1	Log records must include the following elements: 1. Date and time of record; 2. Identity of the person or non-person entity making the journal record; and 3. Description of the record. These requirements must be implemented in full compliance with the following references: • CA/Browser Forum Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates Section 5.4.1; • NIST Framework for Improving Critical Infrastructure Cybersecurity PR.PT–1; and • NIST SP 800–53 Rev. 5, AU–2, AU–3, AU–8.
7.2	Log at least certificate system and key lifecycle events for IACA root certificates, document signer certificates, and other intermediate certificates, including: 1. Key generation, backup, storage, recovery, archival, and destruction; 2. Certificate requests, renewal, and re-key requests, and revocation; 3. Approval and rejection of certificate requests; 4. Cryptographic device lifecycle management events; 5. Generation of Certificate Revocation Lists and OCSP entries; 6. Introduction of new Certificate Profiles and retirement of existing Certificate Profiles; 7. Issuance of certificates; and 8. All verification activities required in paragraph 2 of this Appendix and the State's Certification System Policy. These requirements must be implemented in full compliance with the following references: • CA/Browser Forum Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates Section 5.4.1; • NIST Framework for Improving Critical Infrastructure Cybersecurity PR.PT–1; and • NIST SP 800–53 Rev. 5, AU–1, AU–2, AU–3, AU–4, AU–7, AU–10, SC–17.
7.3	Log certificate system Security events, including: 1. Successful and unsuccessful PKI system access attempts; 2. PKI and security system actions performed; 3. Security profile changes; 4. Installation, update and removal of software on a certificate system; 5. System crashes, hardware failures, and other anomalies; 6. Firewall and router activities; and 7. Entries to and exits from the IACA facility if managed on-premises. These requirements must be implemented in full compliance with the following references: • CA/Browser Forum Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates Section 5.4.1; and • NIST SP 800–53 Rev. 5, AU–2, AU–3, AU–4, AU–7, AU–10, CM–3, PE–6, SI–11, SI–12.
7.4	Maintain certificate system logs for a period not less than 36 months, in full compliance with the following references: • CA/Browser Forum Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates Section 5.4.3; and • NIST SP 800–53 Rev. 5, AU–4, AU–10, AU–11.
7.5	Maintain IACA root certificate and key lifecycle management event logs for a period of not less than 24 months after the destruction of the IACA root certificate private key, in full compliance with the following references: • CA/Browser Forum Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates Section 5.4.3; • NIST Framework for Improving Critical Infrastructure Cybersecurity PR.PT–1; and • NIST SP 800–53 Rev. 5, AU–2, AU–4, AU–10, AU–11.
	8: Incident Response & Recovery Plan
8.1	Implement automated mechanisms under the control of State or delegated third party trusted roles to process logged system activity and alert personnel, using notices provided to multiple destinations, of possible critical security events. These requirements must be implemented in full compliance with the following references: • CA/Browser Forum Network and Certificate System Security Requirements; • DHS National Cyber Incident Response Plan; • NIST Framework for Improving Critical Infrastructure Cybersecurity RS.CO–5, RS.AN–5; and • NIST SP 800–53 Rev. 5, AU–1, AU–2, AU–6, IR–5, SI–4, SI–5.

Paragraph	Requirement
8.2	Require trusted role personnel to follow up on alerts of possible critical security events, in full compliance with the following references: • CA/Browser Forum Network and Certificate System Security Requirements; • DHS National Cyber Incident Response Plan; and • NIST SP 800–53 Rev. 5, AC–5, AC–6, IR–1, IR–4, IR–7, SI–4, SI–5.
8.3	If continuous automated monitoring and alerting is utilized, respond to the alert and initiate a plan of action within 24 hours, in full compliance with the following references: • CA/Browser Forum Network and Certificate System Security Requirements; • DHS National Cyber Incident Response Plan; and • NIST SP 800–53 Rev. 5, IR–1, PM–14, SI–4.
8.4	Implement intrusion detection and prevention controls under the management of State or delegated third party individuals in trusted roles to protect certificate systems against common network and system threats, in full compliance with the following references: • CA/Browser Forum Network and Certificate System Security Requirements; • CISA Federal Government Cybersecurity Incident & Vulnerability Response Playbooks; • DHS National Cyber Incident Response Plan; • NIST Framework for Improving Critical Infrastructure Cybersecurity DE.AE–2, DE.AE–3; DE.DP–1; and • NIST SP 800–53 Rev. 5, IR–1, IR–4, IR–7, IR–8, SI–4, SI–5.
8.5	Document and follow a vulnerability correction process that addresses the identification, review, response, and remediation of vulnerabilities, in full compliance with the following references: • CA/Browser Forum Network and Certificate System Security Requirements; • CISA Federal Government Cybersecurity Incident & Vulnerability Response Playbooks; • DHS National Cyber Incident Response Plan; • NIST Framework for Improving Critical Infrastructure Cybersecurity PR.IP–9; and • NIST SP 800–53 Rev. 5, CA–5, CP–2, CP–4, CP–6, CP–7, CP–8, CP–9, CP–10, SI–1, SI–2, SI–10.
8.6	Notify TSA of any reportable cybersecurity incident, as defined in the TSA Cybersecurity Lexicon available at *www.tsa.gov*, that may compromise the integrity of the certificate systems within no more than 72 hours of the discovery of the incident. Reports must be made as directed at *www.tsa.gov/real-id/mDL*. These requirements must be implemented in full compliance with the following references: • DHS National Cyber Incident Response Plan; and • NIST SP 800–53 Rev. 5, IR–6. Information provided in response to this paragraph *may* contain SSI, and if so, must be handled and protected in accordance with 49 CFR part 1520.
8.7	Undergo a vulnerability scan on public and private IP addresses identified by the State or delegated third party as the State's or delegated third party's certificate systems at least every three months, and after performing any significant system or network changes. These requirements must be implemented in full compliance with the following references: • CA/Browser Forum Network and Certificate System Security Requirements; • DHS National Cyber Incident Response Plan; and • NIST SP 800–53 Rev. 5, CM–1, CM–4, IR–3, RA–1, RA–5.
8.8	Undergo a penetration test on the State's and each delegated third party's certificate systems at least every 12 months, and after performing any significant infrastructure or application upgrades or modifications. These requirements must be implemented in full compliance with the following references: • CA/Browser Forum Network and Certificate System Security Requirements; • DHS National Cyber Incident Response Plan; • NIST Framework for Improving Critical Infrastructure Cybersecurity PR.IP–7; and • NIST SP 800–53 Rev. 5, CA–2, CA–8, CM–4, RA–3.
8.9	Record evidence that each vulnerability scan and penetration test was performed by a person or entity with the requisite skills, tools, proficiency, code of ethics, and independence.
8.10	Review State and/or delegated third party incident response & recovery plan at least once during every 12 months to address cybersecurity threats and vulnerabilities, in full compliance with the following references: • CA/Browser Forum Network and Certificate System Security Requirements; • DHS National Cyber Incident Response Plan; and • NIST SP 800–53 Rev. 5, CP–2, IR–1, IR–2, SC–5.

Dated: October 10, 2024.

David P. Pekoske,

Administrator.

[FR Doc. 2024–23881 Filed 10–24–24; 8:45 am]

BILLING CODE 9110–05–P