§ 29.9 Investigation and reporting of violation of PCII procedures.

(a) *Reporting of possible violations.* Persons authorized to have access to PCII must report any suspected violation of security procedures, the loss or misplacement of PCII, and any suspected unauthorized disclosure of PCII immediately to the PCII Program Manager or a PCII Program Manager's Designee. Suspected violations may also be reported to the DHS Office of Inspector General. The PCII Program Manager or a PCII Program Manager's Designee will in turn report the incident to the appropriate security officer and to the DHS Office of Inspector General.

(b) *Review and investigation of written report.* The PCII Program Manager, or the appropriate security officer must notify the DHS Office of Inspector General of their intent to investigate any alleged violation of procedures, loss of information, and/or unauthorized disclosure, prior to initiating any such investigation. Evidence of wrongdoing resulting from any such investigations by agencies other than the DHS Inspector General must be reported to the United States Department of Justice, Criminal Division, through the CISA Office of the Chief Counsel. The DHS Office of Inspector General also has authority to conduct such investigations and will report any evidence of wrongdoing to the United States Department of Justice, Criminal Division, for consideration of prosecution.

(c) *Notification to originator of PCII.* If the PCII Program Manager or the appropriate security officer determines that a loss of information or an unauthorized disclosure of PCII has occurred, the PCII Program Manager or a PCII Program Manager's Designee must notify the person or entity that submitted the PCII, unless providing such notification could reasonably be expected to hamper the relevant investigation or adversely affect any other law enforcement, national security, or homeland security interest.

(d) *Criminal and administrative penalties.* (1) As established in 6 U.S.C. 673(f), whoever, being an officer or employee of the United States or of any department or agency thereof, knowingly publishes, divulges, discloses, or makes known in any manner or to any extent not authorized by law, any information protected from disclosure by the CII Act coming to the officer or employee in the course of his or her employment or official duties or by reason of any examination or investigation made by, or return, report, or record made to or filed with, such department or agency or officer or employee thereof, shall be fined under title 18 of the United States Code, imprisoned not more than one year, or both, and shall be removed from office or employment.

(2) In addition to the penalties set forth in paragraph (d)(1) of this section, if the PCII Program Manager determines that an entity or person who has received PCII has violated the provisions of this part or used PCII for an inappropriate purpose, the PCII Program Manager may disqualify that entity or person from future receipt of any PCII or future receipt of any sensitive homeland security information under 6 U.S.C. 482, provided, however, that any such decision by the PCII Program Manager may be appealed to the Director.

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

Subpart A—General

Sec.

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

SOURCE: 73 FR 5331, Jan. 29, 2008, unless otherwise noted.

Subpart A—General

§ 37.1 Applicability.

(a) Subparts A through E of this part apply to States and U.S. territories that choose to issue driver's licenses and identification cards that can be accepted by Federal agencies for official purposes.

(b) Subpart F establishes certain standards for State-issued driver's licenses and identification cards issued by States that participate in REAL ID, but that are not intended to be accepted by Federal agencies for official purpose under section 202(d)(11) of the REAL ID Act.

§ 37.3 Definitions.

For purposes of this part:

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

Birth certificate means the record related to a birth that is permanently stored either electronically or physically at the State Office of Vital Statistics or equivalent agency in a registrant's State of birth.

Card means either a driver's license or identification card issued by the State Department of Motor Vehicles (DMV) or equivalent State office.

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.

Certification means an assertion by the State to the Department of Homeland Security that the State has met the requirements of this part.

Certified copy of a birth certificate means a copy of the whole or part of a birth certificate registered with the State that the State considers to be the same as the original birth certificate on file with the State Office of Vital Statistics or equivalent agency in a registrant's State of birth.

Covered employees means Department of Motor Vehicles employees or contractors who are involved in the manufacture or production of REAL ID driver's licenses and identification cards, or who have the ability to affect the identity information that appears on the driver's license or identification card.

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.

Data verification means checking the validity of data contained in source documents presented under this regulation.

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.

Determination means a decision by the Department of Homeland Security that a State has or has not met the requirements of this part and that Federal agencies may or may not accept the driver's licenses and identification cards issued by the State for official purposes.

DHS means the U.S. Department of Homeland Security.

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

Digital photograph means a digital image of the face of the holder of the driver's license or identification card.

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.

DMV means the Department of Motor Vehicles or any State Government entity that issues driver's licenses and identification cards, or an office with equivalent function for issuing driver's licenses and identification cards.

Document authentication means determining that the source document presented under these regulations is genuine and has not been altered.

Domestic violence and dating violence have the meanings given the terms in section 3, Universal definitions and grant provisions, of the Violence Against Women and Department of Justice Reauthorization Act of 2005 (Pub. L. 109–162, 119 Stat. 2960, 2964, Jan. 5, 2006); codified at section 40002, Definitions and grant provisions, 42 U.S.C. 13925, or State laws addressing domestic and dating violence.

Driver's license means a motor vehicle operator's license, as defined in 49 U.S.C. 30301.

Duplicate means a driver's license or identification card issued subsequent to the original document that bears the same information and expiration date as the original document and that is reissued at the request of the holder when the original is lost, stolen, or damaged and there has been no material change in information since prior issuance.

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

Federal agency means all executive agencies including Executive departments, a Government corporation, and an independent establishment as defined in 5 U.S.C. 105.

Federally-regulated commercial aircraft means a commercial aircraft regulated by the Transportation Security Administration (TSA).

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

Full compliance means that the Secretary or his designate(s) has determined that a State has met all the requirements of Subparts A through E.

Full legal name means an individual's first name, middle name(s), and last name or surname, without use of initials or nicknames.

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.

IAFIS means the Integrated Automated Fingerprint Identification System, a national fingerprint and criminal history system maintained by the Federal Bureau of Investigation (FBI) that provides automated fingerprint search capabilities.

Identification card means a document made or issued by or under the authority of a State Department of Motor Vehicles or State office with equivalent function which, when completed with information concerning a particular individual, is of a type intended or commonly accepted for the purpose of identification of individuals.

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.

INS means the former-Immigration and Naturalization Service of the U.S. Department of Justice.

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.

Lawful status: A person in lawful status is a citizen or national of the United States; or an alien: lawfully admitted for permanent or temporary residence in the United States; with conditional permanent resident status in the United States; who has an approved application for asylum in the United States or has entered into the United States in refugee status; who has a valid nonimmigrant status in the United States; who has a pending application for asylum in the United States; who has a pending or approved application for temporary protected status (TPS) in the United States; who has approved deferred action status; or who has a pending application for lawful permanent residence (LPR) or conditional permanent resident status. This definition does not affect other definitions or requirements that may be contained in the Immigration and Nationality Act or other laws.

Material change means any change to the personally identifiable information of an individual as defined under this part. Notwithstanding the definition of personally identifiable information below, a change of address of principal residence does not constitute a material change.

Material compliance means a determination by DHS that a State has met the benchmarks contained in the Material Compliance Checklist.

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).

NCIC means the National Crime Information Center, a computerized index of criminal justice information maintained by the Federal Bureau of Investigation (FBI) that is available to Federal, State, and local law enforcement and other criminal justice agencies.

Official purpose means accessing Federal facilities, boarding Federally-regulated commercial aircraft, and entering nuclear power plants.

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

Passport means a passport booklet or card issued by the U.S. Department of State that can be used as a travel document to gain entry into the United States and that denotes identity and citizenship as determined by the U.S. Department of State.

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.

Personally identifiable information means any information which can be used to distinguish or trace an individual's identity, such as their name; driver's license or identification card number; social security number; biometric record, including a digital photograph or signature; alone, or when combined with other personal or identifying information, which is linked or linkable to a specific individual, such as a date and place of birth or address, whether it is stored in a database, on a driver's license or identification card, or in the machine readable technology on a license or identification card.

Principal residence means the location where a person currently resides (*i.e.*, presently resides even if at a temporary address) in conformance with the residency requirements of the State issuing the driver's license or identification card, if such requirements exist.

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.

REAL ID Driver's License or Identification Card means a driver's license or identification card that has been issued by a State that has been certified by DHS to be in compliance with the requirements of the REAL ID Act and which meets the standards of subparts A through D of this part, including temporary or limited-term driver's licenses or identification cards issued under § 37.21.

Reissued card means a card that a State DMV issues to replace a card that has been lost, stolen or damaged, or to replace a card that includes outdated information. A card may not be reissued remotely when there is a material change to the personally identifiable information as defined by the Rule.

Renewed card means a driver's license or identification card that a State DMV issues to replace a renewable driver's license or identification card.

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*.

SAVE means the DHS Systematic Alien Verification for Entitlements system, or such successor or alternate verification system at the Secretary's discretion.

Secretary means the Secretary of Homeland Security.

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).

Sexual assault and stalking have the meanings given the terms in section 3, universal definitions and grant provisions, of the Violence Against Women and Department of Justice Reauthorization Act of 2005 (Pub. L. 109–162, 119 Stat. 2960, 2964, Jan. 5, 2006); codified at section 40002, Definitions and grant provisions, 42 U.S.C. 13925, or State laws addressing sexual assault and stalking.

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*.

Source document(s) means original or certified copies (where applicable) of documents presented by an applicant as required under these regulations to the Department of Motor Vehicles to apply for a driver's license or identification card.

State means a State of the United States, the District of Columbia, Puerto Rico, the Virgin Islands, Guam, American Samoa, and the Commonwealth of the Northern Mariana Islands.

State address confidentiality program means any State-authorized or State-administered program that—

(1) Allows victims of domestic violence, dating violence, sexual assault, stalking, or a severe form of trafficking to keep, obtain, and use alternative addresses; or

(2) Provides confidential record-keeping regarding the addresses of such victims or other categories of persons.

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.

Temporary lawful status: A person in temporary lawful status is a person who: Has a valid nonimmigrant status in the United States (other than a person admitted as a nonimmigrant under the Compacts of Free Association between the United States and the Republic of the Marshall Islands, the Federated States of Micronesia, or the Republic of Palau); has a pending application for asylum in the United States; has a pending or approved application for temporary protected status (TPS) in the United States; has approved deferred action status; or has a pending application for LPR or conditional permanent resident status.

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*.

Verify means procedures to ensure that:

(1) The source document is genuine and has not been altered (*i.e.*, ''document authentication''); and

(2) The identity data contained on the document is valid (''data verification'').

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*.

[73 FR 5331, Jan. 29, 2008, as amended at 84 FR 46426, Sept. 4, 2019; 89 FR 85375, Oct. 25, 2024]

§ 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*.)

[89 FR 85376, Oct. 25, 2024]

§ 37.5 Validity periods and deadlines for REAL ID driver's licenses and identification cards.

(a) Driver's licenses and identification cards issued under this part, that are not temporary or limited-term driver's licenses and identification cards, are valid for a period not to exceed eight years. A card may be valid for a shorter period based on other State or Federal requirements.

(b) On or after May 7, 2025, Federal agencies shall not accept a driver's license or identification card for official purposes from any individual unless such license or card is a REAL ID–compliant driver's license or identification card issued by a State that has been determined by DHS to be in full compliance as defined under this subpart.

(c) Through the end of May 6, 2025, Federal agencies may accept for official purposes a driver's license or identification card issued under § 37.71. On or after May 7, 2025, Federal agencies shall not accept for official purposes a driver's license or identification card issued under § 37.71.

[73 FR 5331, Jan. 29, 2008, as amended at 79 FR 77838, Dec. 29, 2014; 84 FR 55019, Oct. 15, 2019; 85 FR 23208, Apr. 27, 2020; 86 FR 23240, May 3, 2021; 88 FR 14476, Mar. 9, 2023]

§ 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.

[89 FR 85377, Oct. 25, 2024]

§ 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.

[89 FR 85377, Oct. 25, 2024]

§ 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.

[89 FR 85377, Oct. 25, 2024]

§ 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.

[89 FR 85377, Oct. 25, 2024]

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

Paragraph	Requirement
	• 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.
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:

Paragraph	Requirement
	• 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.
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.

Paragraph	Requirement
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; 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.

Paragraph	Requirement
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 • 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;

Paragraph	Requirement
	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; • 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.

Paragraph	Requirement
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.
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.

Paragraph	Requirement
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.

[89 FR 85380, Oct. 25, 2024]

Subpart B—Minimum Documentation, Verification, and Card Issuance Requirements

§ 37.11 Application and documents the applicant must provide.

(a) The State must subject each person applying for a REAL ID driver's license or identification card to a mandatory facial image capture, and shall maintain photographs of individuals even if no card is issued. The photographs must be stored in a format in accordance with § 37.31 as follows:

(1) If no card is issued, for a minimum period of five years.

(2) If a card is issued, for a period of at least two years beyond the expiration date of the card.

(b) *Declaration.* Each applicant must sign a declaration under penalty of perjury that the information presented on the application is true and correct, and the State must retain this declaration. An applicant must sign a new declaration when presenting new source documents to the DMV on subsequent visits.

(c) *Identity.* (1) To establish identity, the applicant must present at least one of the following source documents:

(i) Valid, unexpired U.S. passport.

(ii) Certified copy of a birth certificate filed with a State Office of Vital Statistics or equivalent agency in the individual's State of birth.

(iii) Consular Report of Birth Abroad (CRBA) issued by the U.S. Department of State, Form FS–240, DS–1350 or FS–545.

(iv) Valid, unexpired Permanent Resident Card (Form I–551) issued by DHS or INS.

(v) Unexpired employment authorization document (EAD) issued by DHS, Form I–766 or Form I–688B.

(vi) Unexpired foreign passport with a valid, unexpired U.S. visa affixed accompanied by the approved I–94 form documenting the applicant's most recent admittance into the United States.

(vii) Certificate of Naturalization issued by DHS, Form N–550 or Form N–570.

(viii) Certificate of Citizenship, Form N–560 or Form N–561, issued by DHS.

(ix) REAL ID driver's license or identification card issued in compliance with the standards established by this part.

(x) Such other documents as DHS may designate by notice published in the FEDERAL REGISTER.

(2) Where a State permits an applicant to establish a name other than the name that appears on a source document (for example, through marriage, adoption, court order, or other mechanism permitted by State law or regulation), the State shall require evidence of the name change through the presentation of documents issued by a court, governmental body or other entity as determined by the State. The State shall maintain copies of the documentation presented pursuant to §37.31, and maintain a record of both the recorded name and the name on the source documents in a manner to be determined by the State and in conformity with §37.31.

(d) *Date of birth.* To establish date of birth, an individual must present at least one document included in paragraph (c) of this section.

(e) *Social security number (SSN).* (1) Except as provided in paragraph (e)(3) of this section, individuals presenting the identity documents listed in §37.11(c)(1) and (2) must present his or her Social Security Administration account number card; or, if a Social Security Administration account card is not available, the person may present any of the following documents bearing the applicant's SSN:

(i) A W–2 form,

(ii) A SSA–1099 form,

(iii) A non-SSA–1099 form, or

(iv) A pay stub with the applicant's name and SSN on it.

(2) The State DMV must verify the SSN pursuant to §37.13(b)(2) of this subpart.

(3) Individuals presenting the identity document listed in §37.11(c)(1)(vi) must present an SSN or demonstrate non-work authorized status.

(f) *Documents demonstrating address of principal residence.* To document the address of principal residence, a person must present at least two documents of the State's choice that include the individual's name and principal residence. A street address is required except as provided in §37.17(f) of this part.

(g) *Evidence of lawful status in the United States.* A DMV may issue a REAL ID driver's license or identification card only to a person who has presented satisfactory evidence of lawful status.

(1) If the applicant presents one of the documents listed under paragraphs (c)(1)(i), (c)(1)(ii), (c)(1)(iii), (c)(1)(iv), (c)(1)(vii) or (c)(1)(viii) of this section, the issuing State's verification of the applicant's identity in the manner prescribed in §37.13 will also provide satisfactory evidence of lawful status.

(2) If the applicant presents one of the identity documents listed under paragraphs (c)(1)(v) or (c)(1)(vi), or (c)(1)(ix) of this section, the issuing State's verification of the identity document(s) does not provide satisfactory evidence of lawful status. The applicant must also present a second document from §37.11(g)(1) or documentation issued by DHS or other Federal agencies demonstrating lawful status as determined by USCIS. All documents shall be verified in the manner prescribed in §37.13.

(h) *Exceptions Process.* A State DMV may choose to establish a written, defined exceptions process for persons who, for reasons beyond their control, are unable to present all necessary documents and must rely on alternate documents to establish identity or date of birth. Alternative documents to demonstrate lawful status will only be allowed to demonstrate U.S. citizenship.

(1) Each State establishing an exceptions process must make reasonable efforts to establish the authenticity of alternate documents each time they are presented and indicate that an exceptions process was used in the applicant's record.

(2) The State shall retain copies or images of the alternate documents accepted pursuant to §37.31 of this part.

(3) The State shall conduct a review of the use of the exceptions process, and pursuant to subpart E of this part, prepare and submit a report with a copy of the exceptions process as part of the certification documentation detailed in §37.55.

(i) States are not required to comply with these requirements when issuing

REAL ID driver's licenses or identification cards in support of Federal, State, or local criminal justice agencies or other programs that require special licensing or identification to safeguard persons or in support of their other official duties. As directed by appropriate officials of these Federal, State, or local agencies, States should take sufficient steps to safeguard the identities of such persons. Driver's licenses and identification cards issued in support of Federal, State, or local criminal justice agencies or programs that require special licensing or identification to safeguard persons or in support of their other official duties shall not be distinguishable from other REAL ID licenses or identification cards issued by the State.

§ 37.13 Document verification requirements.

(a) States shall make reasonable efforts to ensure that the applicant does not have more than one driver's license or identification card already issued by that State under a different identity. In States where an individual is permitted to hold both a driver's license and identification card, the State shall ensure that the individual has not been issued identification documents in multiple or different names. States shall also comply with the provisions of § 37.29 before issuing a driver's license or identification card.

(b) States must verify the documents and information required under § 37.11 with the issuer of the document. States shall use systems for electronic validation of document and identity data as they become available or use alternative methods approved by DHS.

(1) States shall verify any document described in § 37.11(c) or (g) and issued by DHS (including, but not limited to, the I–94 form described in § 37.11(c)(vi)) through the Systematic Alien Verification for Entitlements (SAVE) system or alternate methods approved by DHS, except that if two DHS-issued documents are presented, a SAVE verification of one document that confirms lawful status does not need to be repeated for the second document. In the event of a non-match, the DMV must not issue a REAL ID driver's license or identification card to an applicant, and must refer the individual to U.S. Citizenship and Immigration Services for resolution.

(2) States must verify SSNs with the Social Security Administration (SSA) or through another method approved by DHS. In the event of a non-match with SSA, a State may use existing procedures to resolve non-matches. If the State is unable to resolve the non-match, and the use of an exceptions process is not warranted in the situation, the DMV must not issue a REAL ID driver's license or identification card to an applicant until the information verifies with SSA.

(3) States must verify birth certificates presented by applicants. States should use the Electronic Verification of Vital Events (EVVE) system or other electronic systems whenever the records are available. If the document does not appear authentic upon inspection or the data does not match and the use of an exceptions process is not warranted in the situation, the State must not issue a REAL ID driver's license or identification card to the applicant until the information verifies, and should refer the individual to the issuing office for resolution.

(4) States shall verify documents issued by the Department of State with the Department of State or through methods approved by DHS.

(5) States must verify REAL ID driver's licenses and identification cards with the State of issuance.

(6) Nothing in this section precludes a State from issuing an interim license or a license issued under § 37.71 that will not be accepted for official purposes to allow the individual to resolve any non-match.

§ 37.15 Physical security features for the driver's license or identification card.

(a) *General.* States must include document security features on REAL ID driver's licenses and identification cards designed to deter forgery and counterfeiting, promote an adequate level of confidence in the authenticity of cards, and facilitate detection of fraudulent cards in accordance with this section.

(1) These features must not be capable of being reproduced using technologies that are commonly used and made available to the general public.

(2) The proposed card solution must contain a well-designed, balanced set of features that are effectively combined and provide multiple layers of security. States must describe these document security features in their security plans pursuant to § 37.41.

(b) *Integrated security features.* REAL ID driver's licenses and identification cards must contain at least three levels of integrated security features that provide the maximum resistance to persons' efforts to—

(1) Counterfeit, alter, simulate, or reproduce a genuine document;

(2) Alter, delete, modify, mask, or tamper with data concerning the original or lawful card holder;

(3) Substitute or alter the original or lawful card holder's photograph and/or signature by any means; and

(4) Create a fraudulent document using components from legitimate driver's licenses or identification cards.

(c) *Security features to detect false cards.* States must employ security features to detect false cards for each of the following three levels:

(1) *Level 1.* Cursory examination, without tools or aids involving easily identifiable visual or tactile features, for rapid inspection at point of usage.

(2) *Level 2.* Examination by trained inspectors with simple equipment.

(3) *Level 3.* Inspection by forensic specialists.

(d) *Document security and integrity.* States must conduct a review of their card design and submit a report to DHS with their certification that indicates the ability of the design to resist compromise and document fraud attempts. The report required by this paragraph is SSI and must be handled and protected in accordance with 49 CFR part 1520. Reports must be updated and submitted to DHS whenever a security feature is modified, added, or deleted. After reviewing the report, DHS may require a State to provide DHS with examination results from a recognized independent laboratory experienced with adversarial analysis of identification documents concerning one or more areas relating to the card's security.

§ 37.17 Requirements for the surface of the driver's license or identification card.

To be accepted by a Federal agency for official purposes, REAL ID driver's licenses and identification cards must include on the front of the card (unless otherwise specified below) the following information:

(a) *Full legal name.* Except as permitted in § 37.11(c)(2), the name on the face of the license or card must be the same as the name on the source document presented by the applicant to establish identity. Where the individual has only one name, that name should be entered in the last name or family name field, and the first and middle name fields should be left blank. Place holders such as NFN, NMN, and NA should not be used.

(b) *Date of birth.*

(c) *Gender,* as determined by the State.

(d) *Unique Driver's license or identification card number.* This cannot be the individual's SSN, and must be unique across driver's license or identification cards within the State.

(e) *Full facial digital photograph.* A full facial photograph must be taken pursuant to the standards set forth below:

(1) States shall follow specifically ISO/IEC 19794–5:2005(E) (incorporated by reference; see § 37.4).

(2) Photographs may be in black and white or color.

(f) *Address of principal residence,* except an alternative address may be displayed for:

(1) Individuals for whom a State law, regulation, or DMV procedure permits display of an alternative address, or

(2) Individuals who satisfy any of the following:

(i) If the individual is enrolled in a State address confidentiality program which allows victims of domestic violence, dating violence, sexual assault, stalking, or a severe form of trafficking, to keep, obtain, and use alternative addresses; and provides that the addresses of such persons must be kept confidential, or other similar program;

(ii) If the individual's address is entitled to be suppressed under State or Federal law or suppressed by a court order including an administrative order issued by a State or Federal court; or

(iii) If the individual is protected from disclosure of information pursuant to section 384 of the Illegal Immigration Reform and Immigrant Responsibility Act of 1996.

(3) In areas where a number and street name has not been assigned for U.S. mail delivery, an address convention used by the U.S. Postal Service is acceptable.

(g) *Signature.* (1) The card must include the signature of the card holder. The signature must meet the requirements of the AAMVA Specifications (incorporated by reference; see § 37.4). This standard includes requirements for size, scaling, cropping, color, borders, and resolution.

(2) The State shall establish alternative procedures for individuals unable to sign their name.

(h) *Physical security features,* pursuant to § 37.15 of this subpart.

(i) *Machine-readable technology on the back of the card,* pursuant to § 37.19 of this subpart.

(j) *Date of transaction.*

(k) *Expiration date.*

(l) *State or territory of issuance.*

(m) *Printed information.* The name, date of birth, gender, card number, issue date, expiration date, and address on the face of the card must be in Latin alpha-numeric characters. The name must contain a field of no less than a total of 39 characters, and longer names shall be truncated following the standard established by ICAO 9303 (incorporated by reference; see § 37.4).

(n) 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.

[73 FR 5331, Jan. 29, 2008, as amended at 88 FR 44192, July 12, 2023]

§ 37.19 Machine readable technology on the driver's license or identification card.

For the machine readable portion of the REAL ID driver's license or identification card, States must use ISO/IEC 15438:2006(E) (incorporated by reference; see § 37.4). The PDF417 bar code standard must have the following defined minimum data elements:

(a) Expiration date.

(b) Full legal name, unless the State permits an applicant to establish a name other than the name that appears on a source document, pursuant to § 37.11(c)(2).

(c) Date of transaction.

(d) Date of birth.

(e) Gender.

(f) Address as listed on the card pursuant to § 37.17(f).

(g) Unique driver's license or identification card number.

(h) Card design revision date, indicating the most recent change or modification to the visible format of the driver's license or identification card.

(i) Inventory control number of the physical document.

(j) State or territory of issuance.

[73 FR 5331, Jan. 29, 2008, as amended at 88 FR 44192, July 12, 2023]

§ 37.21 Temporary or limited-term driver's licenses and identification cards.

States may only issue a temporary or limited-term REAL ID driver's license or identification card to an individual who has temporary lawful status in the United States.

(a) States must require, before issuing a temporary or limited-term driver's license or identification card to a person, valid documentary evidence, verifiable through SAVE or other DHS-approved means, that the person has lawful status in the United States.

(b) States shall not issue a temporary or limited-term driver's license or identification card pursuant to this section:

(1) For a time period longer than the expiration of the applicant's authorized stay in the United States, or, if there is no expiration date, for a period longer than one year; and

(2) For longer than the State's maximum driver's license or identification card term.

(c) States shall renew a temporary or limited-term driver's license or identification card pursuant to this section and §37.25(b)(2), only if:

(1) the individual presents valid documentary evidence that the status by which the applicant qualified for the temporary or limited-term driver's license or identification card is still in effect, or

(2) the individual presents valid documentary evidence that he or she continues to qualify for lawful status under paragraph (a) of this section.

(d) States must verify the information presented to establish lawful status through SAVE, or another method approved by DHS.

(e) 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.

§37.23 Reissued REAL ID driver's licenses and identification cards.

(a) *State procedure.* States must establish an effective procedure to confirm or verify an applicant's identity each time a REAL ID driver's license or identification card is reissued, to ensure that the individual receiving the reissued REAL ID driver's license or identification card is the same individual to whom the driver's license or identification card was originally issued.

(b) *Remote/Non-in-person reissuance.* Except as provided in paragraph (c) of this section a State may conduct a non-in-person (remote) reissuance if State procedures permit the reissuance to be conducted remotely. Except for the reissuance of duplicate driver's licenses and identification cards as defined in this rule, the State must reverify pursuant to §37.13, the applicant's SSN and lawful status prior to reissuing the driver's license or identification card.

(c) *In-person reissuance.* The State may not remotely reissue a driver's license or identification card where there has been a material change in any personally identifiable information since prior issuance. All material changes must be established through an applicant's presentation of an original source document as provided in this subpart, and must be verified as specified in §37.13.

§37.25 Renewal of REAL ID driver's licenses and identification cards.

(a) *In-person renewals.* States must require holders of REAL ID driver's licenses and identification cards to renew their driver's licenses and identification cards with the State DMV in person, no less frequently than every sixteen years.

(1) The State DMV shall take an updated photograph of the applicant, no less frequently than every sixteen years.

(2) The State must reverify the renewal applicant's SSN and lawful status through SSOLV and SAVE, respectively (or other DHS-approved means) as applicable prior to renewing the driver's license or identification card. The State must also verify electronically information that it was not able to verify at a previous issuance or renewal if the systems or processes exist to do so.

(3) Holders of temporary or limited-term REAL ID driver's licenses and identification cards must present evidence of continued lawful status via SAVE or other method approved by DHS when renewing their driver's license or identification card.

(b) *Remote/Non-in-person renewal.* Except as provided in (b)(2) a State may conduct a non-in-person (remote) renewal if State procedures permit the renewal to be conducted remotely.

(1) The State must reverify the applicant's SSN and lawful status pursuant to §37.13 prior to renewing the driver's license or identification card.

(2) The State may not remotely renew a REAL ID driver's license or identification card where there has been a material change in any personally identifiable information since prior issuance. All material changes must be established through the applicant's presentation of an original source document as provided in Subpart B, and must be verified as specified in §37.13.

§ 37.27 Driver's licenses and identification cards issued during the age-based enrollment period.

Driver's licenses and identification cards issued to individuals prior to a DHS determination that the State is materially compliant may be renewed or reissued pursuant to current State practices, and will be accepted for official purposes until the validity dates described in § 37.5.

[73 FR 5331, Jan. 29, 2008, as amended at 79 FR 77838, Dec. 29, 2014]

§ 37.29 Prohibition against holding more than one REAL ID card or more than one driver's license.

(a) An individual may hold only one REAL ID card. An individual cannot hold a REAL ID driver's license and a REAL ID identification card simultaneously. Nothing shall preclude an individual from holding a REAL ID card and a non-REAL ID card unless prohibited by his or her State.

(b) Prior to issuing a REAL ID driver's license,

(1) A State must check with all other States to determine if the applicant currently holds a driver's license or REAL ID identification card in another State.

(2) If the State receives confirmation that the individual holds a driver's license in another State, or possesses a REAL ID identification card in another State, the receiving State must take measures to confirm that the person has terminated or is terminating the driver's license or REAL ID identification card issued by the prior State pursuant to State law, regulation or procedure.

(c) Prior to issuing a REAL ID identification card,

(1) A State must check with all other States to determine if the applicant currently holds a REAL ID driver's license or identification card in another State.

(2) If the State receives confirmation that the individual holds a REAL ID card in another State the receiving State must take measures to confirm that the person has terminated or is terminating the REAL ID driver's license or identification card issued by the prior State pursuant to State law, regulation or procedure.

Subpart C—Other Requirements

§ 37.31 Source document retention.

(a) States must retain copies of the application, declaration and source documents presented under § 37.11 of this part, including documents used to establish all names recorded by the DMV under § 37.11(c)(2). States shall take measures to protect any personally identifiable information collected pursuant to the REAL ID Act as described in their security plan under § 37.41(b)(2).

(1) States that choose to keep paper copies of source documents must retain the copies for a minimum of seven years.

(2) States that choose to transfer information from paper copies to microfiche must retain the microfiche for a minimum of ten years.

(3) States that choose to keep digital images of source documents must retain the images for a minimum of ten years.

(4) States are not required to retain the declaration with application and source documents, but must retain the declaration consistent with applicable State document retention requirements and retention periods.

(b) States using digital imaging to retain source documents must store the images as follows:

(1) Photo images must be stored in the Joint Photographic Experts Group (JPEG) 2000 standard for image compression, or a standard that is interoperable with the JPEG standard. Images must be stored in an open (consensus) format, without proprietary wrappers, to ensure States can effectively use the image captures of other States as needed.

(2) Document and signature images must be stored in a compressed Tagged Image Format (TIF), or a standard that is interoperable with the TIF standard.

(3) All images must be retrievable by the DMV if properly requested by law enforcement.

(c) Upon request by an applicant, a State shall record and retain the applicant's name, date of birth, certificate numbers, date filed, and issuing agency

in lieu of an image or copy of the applicant's birth certificate, where such procedures are required by State law.

§ 37.33 DMV databases.

(a) States must maintain a State motor vehicle database that contains, at a minimum—

(1) All data fields printed on driver's licenses and identification cards issued by the State, individual serial numbers of the card, and SSN;

(2) A record of the full legal name and recorded name established under § 37.11(c)(2) as applicable, without truncation;

(3) All additional data fields included in the MRZ but not printed on the driver's license or identification card; and

(4) Motor vehicle driver's histories, including motor vehicle violations, suspensions, and points on driver's licenses.

(b) States must protect the security of personally identifiable information, collected pursuant to the REAL ID Act, in accordance with § 37.41(b)(2) of this part.

Subpart D—Security at DMVs and Driver's License and Identification Card Production Facilities

§ 37.41 Security plan.

(a) *In General.* States must have a security plan that addresses the provisions in paragraph (b) of this section and must submit the security plan as part of its REAL ID certification under § 37.55.

(b) Security plan contents. At a minimum, the security plan must address—

(1) Physical security for the following:

(i) Facilities used to produce driver's licenses and identification cards.

(ii) Storage areas for card stock and other materials used in card production.

(2) Security of personally identifiable information maintained at DMV locations involved in the enrollment, issuance, manufacture and/or production of cards issued under the REAL ID Act, including, but not limited to, providing the following protections:

(i) Reasonable administrative, technical, and physical safeguards to protect the security, confidentiality, and integrity of the personally identifiable information collected, stored, and maintained in DMV records and information systems for purposes of complying with the REAL ID Act. These safeguards must include procedures to prevent unauthorized access, use, or dissemination of applicant information and images of source documents retained pursuant to the Act and standards and procedures for document retention and destruction.

(ii) A privacy policy regarding the personally identifiable information collected and maintained by the DMV pursuant to the REAL ID Act.

(iii) Any release or use of personal information collected and maintained by the DMV pursuant to the REAL ID Act must comply with the requirements of the Driver's Privacy Protection Act, 18 U.S.C. 2721 *et seq.* State plans may go beyond these minimum privacy requirements to provide greater protection, and such protections are not subject to review by DHS for purposes of determining compliance with this part.

(3) Document and physical security features for the card, consistent with the requirements of § 37.15, including a description of the State's use of biometrics, and the technical standard utilized, if any;

(4) Access control, including the following:

(i) Employee identification and credentialing, including access badges.

(ii) Employee background checks, in accordance with § 37.45 of this part.

(iii) Controlled access systems.

(5) Periodic training requirements in—

(i) Fraudulent document recognition training for all covered employees handling source documents or engaged in the issuance of driver's licenses and identification cards. The fraudulent document training program approved by AAMVA or other DHS approved method satisfies the requirement of this subsection.

(ii) Security awareness training, including threat identification and handling of SSI as necessary.

(6) Emergency/incident response plan;

(7) Internal audit controls;

(8) An affirmation that the State possesses both the authority and the means to produce, revise, expunge, and protect the confidentiality of REAL ID driver's licenses or identification cards issued in support of Federal, State, or local criminal justice agencies or similar programs that require special licensing or identification to safeguard persons or support their official duties. These procedures must be designed in coordination with the key requesting authorities to ensure that the procedures are effective and to prevent conflicting or inconsistent requests. In order to safeguard the identities of individuals, these procedures should not be discussed in the plan and States should make every effort to prevent disclosure to those without a need to know about either this confidential procedure or any substantive information that may compromise the confidentiality of these operations. The appropriate law enforcement official and United States Attorney should be notified of any action seeking information that could compromise Federal law enforcement interests.

(c) *Handling of Security Plan*. The Security Plan required by this section contains Sensitive Security Information (SSI) and must be handled and protected in accordance with 49 CFR part 1520.

§ 37.43 Physical security of DMV production facilities.

(a) States must ensure the physical security of facilities where driver's licenses and identification cards are produced, and the security of document materials and papers from which driver's licenses and identification cards are produced or manufactured.

(b) States must describe the security of DMV facilities as part of their security plan, in accordance with § 37.41.

§ 37.45 Background checks for covered employees.

(a) *Scope*. States are required to subject persons who are involved in the manufacture or production of REAL ID driver's licenses and identification cards, or who have the ability to affect the identity information that appears on the driver's license or identification card, or current employees who will be assigned to such positions (''covered employees'' or ''covered positions''), to a background check. The background check must include, at a minimum, the validation of references from prior employment, a name-based and fingerprint-based criminal history records check, and employment eligibility verification otherwise required by law. States shall describe their background check process as part of their security plan, in accordance with § 37.41(b)(4)(ii). This section also applies to contractors utilized in covered positions.

(b) *Background checks*. States must ensure that any covered employee under paragraph (a) of this section is provided notice that he or she must undergo a background check and the contents of that check.

(1) *Criminal history records check*. States must conduct a name-based and fingerprint-based criminal history records check (CHRC) using, at a minimum, the FBI's National Crime Information Center (NCIC) and the Integrated Automated Fingerprint Identification (IAFIS) database and State repository records on each covered employee identified in paragraph (a) of this section, and determine if the covered employee has been convicted of any of the following disqualifying crimes:

(i) *Permanent disqualifying criminal offenses*. A covered employee has a permanent disqualifying offense if convicted, or found not guilty by reason of insanity, in a civilian or military jurisdiction, of any of the felonies set forth in 49 CFR 1572.103(a).

(ii) *Interim disqualifying criminal offenses*. The criminal offenses referenced in 49 CFR 1572.103(b) are disqualifying if the covered employee was either convicted of those offenses in a civilian or military jurisdiction, or admits having committed acts which constitute the essential elements of any of those criminal offenses within the seven years preceding the date of employment in the covered position; or the covered employee was released from incarceration for the crime within the five years preceding the date of employment in the covered position.

(iii) *Under want or warrant.* A covered employee who is wanted or under indictment in any civilian or military jurisdiction for a felony referenced in this section is disqualified until the want or warrant is released.

(iv) *Determination of arrest status.* When a fingerprint-based check discloses an arrest for a disqualifying crime referenced in this section without indicating a disposition, the State must determine the disposition of the arrest.

(v) *Waiver.* The State may establish procedures to allow for a waiver of the requirements of paragraphs (b)(1)(ii) or (b)(1)(iv) of this section under circumstances determined by the State. These procedures can cover circumstances where the covered employee has been arrested, but no final disposition of the matter has been reached.

(2) *Employment eligibility status verification.* The State shall ensure it is fully in compliance with the requirements of section 274A of the Immigration and Nationality Act (8 U.S.C. 1324a) and its implementing regulations (8 CFR part 274A) with respect to each covered employee. The State is encouraged to participate in the USCIS E-Verify program (or any successor program) for employment eligibility verification.

(3) *Reference check.* Reference checks from prior employers are not required if the individual has been employed by the DMV for at least two consecutive years since May 11, 2006.

(4) *Disqualification.* If results of the State's CHRC reveal a permanent disqualifying criminal offense under paragraph (b)(1)(i) or an interim disqualifying criminal offense under paragraph (b)(1)(ii), the covered employee may not be employed in a position described in paragraph (a) of this section. An employee whose employment eligibility has not been verified as required by section 274A of the Immigration and Nationality Act (8 U.S.C. 1324a) and its implementing regulations (8 CFR part 274A) may not be employed in any position.

(c) *Appeal.* If a State determines that the results from the CHRC do not meet the standards of such check the State must so inform the employee of the determination to allow the individual an opportunity to appeal to the State or Federal government, as applicable.

(d) Background checks substantially similar to the requirements of this section that were conducted on existing employees on or after May 11, 2006 need not be re-conducted.

Subpart E—Procedures for Determining State Compliance

§ 37.51 Compliance—general requirements.

(a) *Full compliance.* To be in full compliance with the REAL ID Act of 2005, 49 U.S.C. 30301 note, States must meet the standards of subparts A through D or have a REAL ID program that DHS has determined to be comparable to the standards of subparts A through D. States certifying compliance with the REAL ID Act must follow the certification requirements described in § 37.55. States must be fully compliant with Subparts A through D on or before January 15, 2013. States must file the documentation required under § 37.55 at least 90 days prior to the effective date of full compliance.

(b) *Material compliance.* States must be in material compliance by January 1, 2010 to receive an additional extension until no later than May 10, 2011 as described in § 37.63. Benchmarks for material compliance are detailed in the Material Compliance Checklist found in DHS' Web site at *http://www.dhs.gov*.

[73 FR 5331, Jan. 29, 2008, as amended at 76 FR 12271, Mar. 7, 2011]

EFFECTIVE DATE NOTE: At 74 FR 68478, Dec. 28, 2009, in § 37.51, paragraph (b) was stayed from Jan. 1, 2010, until further notice.

§ 37.55 State certification documentation.

(a) States seeking DHS's determination that its program for issuing REAL ID driver's licenses and identification cards is meeting the requirements of this part (full compliance), must provide DHS with the following documents:

(1) A certification by the highest level Executive official in the State overseeing the DMV reading as follows:

''I, [name and title (name of certifying official), (position title) of the State (Commonwealth))] of _____, do hereby certify that the State (Commonwealth) has implemented a program for issuing driver's licenses and identification cards in compliance with the requirements of the REAL ID Act of 2005, as further defined in 6 CFR par_t 37, and intends to remain in compliance with these regulations.''

(2) A letter from the Attorney General of the State confirming that the State has the legal authority to impose requirements necessary to meet the standards established by this part.

(3) A description of the State's exceptions process under §37.11(h), and the State's waiver processes under §37.45(b)(1)(v).

(4) The State's Security Plan under §37.41.

(b) After DHS's final compliance determination, States shall recertify compliance with this part every three years on a rolling basis as determined by DHS.

§37.59 DHS reviews of State compliance.

State REAL ID programs will be subject to DHS review to determine whether the State meets the requirements for compliance with this part.

(a) *General inspection authority.* States must cooperate with DHS's review of the State's compliance at any time. In addition, the State must:

(1) Provide any reasonable information pertinent to determining compliance with this part as requested by DHS;

(2) Permit DHS to conduct inspections of any and all sites associated with the enrollment of applicants and the production, manufacture, personalization and issuance of driver's licenses or identification cards; and

(3) Allow DHS to conduct interviews of the State's employees and contractors who are involved in the application and verification process, or the manufacture and production of driver's licenses or identification cards. DHS shall provide written notice to the State in advance of an inspection visit.

(b) *Preliminary DHS determination.* DHS shall review forms, conduct audits of States as necessary, and make a preliminary determination on whether the State has satisfied the requirements of this part within 45 days of receipt of the Material Compliance Checklist or State certification documentation of full compliance pursuant to §37.55.

(1) If DHS determines that the State meets the benchmarks of the Material Compliance Checklist, DHS may grant the State an additional extension until no later than May 10, 2011.

(2) If DHS determines that the State meets the full requirements of subparts A through E, the Secretary shall make a final determination that the State is in compliance with the REAL ID Act.

(c) *State reply.* The State will have up to 30 calendar days to respond to the preliminary determination. The State's reply must explain what corrective action it either has implemented, or intends to implement, to correct any deficiencies cited in the preliminary determination or, alternatively, detail why the DHS preliminary determination is incorrect. Upon request by the State, an informal conference will be scheduled during this time.

(d) *Final DHS determination.* DHS will notify States of its final determination of State compliance with this part, within 45 days of receipt of a State reply.

(e) *State's right to judicial review.* Any State aggrieved by an adverse decision under this section may seek judicial review under 5 U.S.C. Chapter 7.

§37.61 Results of compliance determination.

(a) A State shall be deemed in compliance with this part when DHS issues a determination that the State meets the requirements of this part.

(b) The Secretary will determine that a State is not in compliance with this part when it—

(1) Fails to submit a timely certification or request an extension as prescribed in this subpart; or

(2) Does not meet one or more of the standards of this part, as established in a determination by DHS under §37.59.

§37.63 Extension of deadline.

(a) A State may request an initial extension by filing a request with the Secretary no later than March 31, 2008. In the absence of extraordinary circumstances, such an extension request will be deemed justified for a period

lasting until, but not beyond, December 31, 2009. DHS shall notify a State of its acceptance of the State's request for initial extension within 45 days of receipt.

(b) States granted an initial extension may file a request for an additional extension until no later than May 10, 2011, by submitting a Material Compliance Checklist demonstrating material compliance, per §37.51(b) with certain elements of subparts A through E as defined by DHS. Such additional extension request must be filed by December 1, 2009. DHS shall notify a State whether an additional extension has been granted within 45 days of receipt of the request and documents described above.

(c) Subsequent extensions, if any, will be at the discretion of the Secretary.

[73 FR 5331, Jan. 29, 2008, as amended at 74 FR 49309, Sept. 28, 2009]

§ 37.65 Effect of failure to comply with this part.

(a) Any driver's license or identification card issued by a State that DHS determines is not in compliance with this part is not acceptable as identification by Federal agencies for official purposes.

(b) Driver's licenses and identification cards issued by a State that has obtained an extension of the compliance date from DHS per §37.51 are acceptable for official purposes until the end of the applicable enrollment period under §37.5; or the State subsequently is found by DHS under this Subpart to not be in compliance.

(c) Driver's licenses and identification cards issued by a State that has been determined by DHS to be in material compliance and that are marked to identify that the licenses and cards are materially compliant will continue to be accepted by Federal agencies after the expiration of the enrollment period under §37.5, until the expiration date on the face of the document.

Subpart F—Driver's Licenses and Identification Cards Issued Under section 202(d)(11) of the REAL ID Act

§ 37.71 Driver's licenses and identification cards issued under section 202(d)(11) of the REAL ID Act.

(a) Except as authorized in §37.27, States that DHS determines are compliant with the REAL ID Act that choose to also issue driver's licenses and identification cards that are not acceptable by Federal agencies for official purposes must ensure that such driver's licenses and identification cards—

(1) Clearly state on their face and in the machine readable zone that the card is not acceptable for official purposes; and

(2) Have a unique design or color indicator that clearly distinguishes them from driver's licenses and identification cards that meet the standards of this part.

(b) DHS reserves the right to approve such designations, as necessary, during certification of compliance.

PART 46—PROTECTION OF HUMAN SUBJECTS

Sec.