



EXEMPTION FROM TSA REGULATIONS

SUBJECT: Exemption from Certain Security Threat Assessment and Fee Requirements Codified in 49 CFR Part 1572

COVERED PERSONS: Individuals Applying for a Hazardous Materials Endorsement Who Hold a Valid Transportation Worker Identification Credential, the States, and the District of Columbia

EFFECTIVE DATE: March 1, 2020

I. SUMMARY

The Transportation Security Administration (TSA) issues this exemption as an interim measure to conform regulatory requirements to a recent statute¹ that permits the States and the District of Columbia to issue a hazardous materials endorsement (HME) to an individual who holds a valid Transportation Worker Identification Credential (TWIC[®]). TSA intends to revise the pertinent regulations to make conforming changes to them. However, until the process to revise the regulations is complete, it is necessary to issue this exemption so that individuals, the States, and the District of Columbia may comply with the new statutory language and remain in compliance with TSA's regulations.

II. BACKGROUND

A. The Hazardous Materials Endorsement and Transportation Worker Identification Credential Vetting Programs

The Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 (USA PATRIOT Act)² provides that no State may

¹ TSA Modernization Act, Division K – Title I of the FAA Reauthorization Act, Pub. L. 115-254, 132 Stat. 3186 (Oct. 5, 2018).

² See Pub. L. 107-56, 115 Stat. 272 (October 26, 2001); codified at 49 U.S.C. 5103a.

issue an HME for a commercial driver's license until TSA notifies a State or the District of Columbia (hereinafter "the States") that the applicant does not pose a security threat. Further, the Act requires TSA to conduct a security threat assessment (STA) consisting of criminal, immigration, and terrorism checks to determine whether an HME applicant poses a security threat. TSA implemented the HME vetting program through regulations, which are codified at title 49 of the Code of Federal Regulations (CFR), parts 1515, 1570, and 1572. The regulations prohibit the States from issuing an HME unless TSA has notified them that the individual successfully completed the STA. The regulations require HME applicants to provide biographic and biometric information to TSA, which is necessary to complete the STA. The regulations also set the fees that applicants must pay during enrollment to cover TSA's costs to conduct the HME STA, as required by statute.³

The Maritime Transportation Security Act of 2002⁴ requires TSA to conduct STAs of individuals who apply for unescorted access to certain maritime facilities and vessels. The STA must include criminal, immigration, and terrorism checks. Further, TSA must issue a TWIC[®] to individuals who successfully complete the STA and collect fees from applicants to cover TSA's costs to conduct the vetting and issue the credential. TSA implemented the TWIC[®] vetting program through regulations, which are codified at 49 CFR parts 1515, 1570, and 1572. TSA established identical vetting standards for the HME and TWIC[®] programs.

B. TSA Modernization Act Requirements

Section 1978 of the TSA Modernization Act⁵ amended the USA PATRIOT Act provisions and permits a State to issue an HME to an individual following TSA notification that he or she does not pose a threat, or "if the individual holds a valid TWIC[®] issued by TSA in accordance with 46 U.S.C. 70105." The statutory language in Section 1978 does not require States to collect information, biometrics, and fees from applicants who hold valid TWICs[®]. Also, Section 1978 does not require TSA to conduct a new STA of these individuals. Therefore, TSA's current regulations requiring collection of information, biometrics, and fees, and a new

³ See 6 U.S.C. 469.

⁴ See Pub. L. 107-295, 116 Stat. 2064 (Nov. 25, 2002); codified at 46 U.S.C. 70105.

⁵ TSA Modernization Act, Division K – Title I of the FAA Reauthorization Act, Pub. L. 115-254, 132 Stat. 3186 (Oct. 5, 2018).

STA conflict with the requirements of Section 1978 with respect to HME applicants who hold valid TWICs[®].

III. DETERMINATION

TSA may grant an exemption from a regulation if the Administrator determines the exemption is in the public interest.⁶ The Administrator has determined that it is in the public interest to grant an exemption from certain HME regulations when a State wishes to issue an HME to an applicant who holds a valid TWIC[®]. With the enactment of Section 1978, the States and individuals who hold valid TWICs[®] may now forego the submission of information, biometrics, and fees to TSA because the individual is deemed to have already completed the appropriate STA. Without this exemption, the States and HME applicants with valid TWICs[®] would be in the unreasonable position of being non-compliant with certain TSA regulations, but compliant with Section 1978. Moreover, the public interest benefits from the reduction in redundant STAs and costs to individuals, the States, and TSA.

IV. SPECIFIC EXEMPTIONS AND PROCEDURES

A. Exemptions for Individuals Who Hold Valid TWICs[®]

TSA exempts an HME applicant who holds a TWIC[®] that the State has determined is valid under the procedures set forth in section IV.C. below from the following regulatory requirements:

1. 49 CFR § 1572.9, Applicant information required for HME security threat assessment.
2. 49 C.F.R. § 1572.11(c), Submission of fingerprints and information.
3. 49 C.F.R. § 1572.405, Procedures for collection by TSA.

B. Exemptions for the States

TSA exempts the States from the following regulatory requirements when issuing an HME to an individual who holds a TWIC[®] that is determined to be valid under the procedures set forth in section IV.C. below:

⁶ See 49 U.S.C. 114(q).

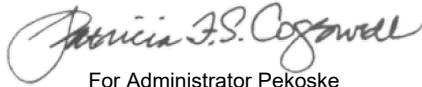
1. 49 C.F.R. § 1572.13(a) and (f), State responsibilities for issuance of hazardous materials endorsement.

2. 49 C.F.R. § 1572.403, Procedures for collection by States.

C. Procedures States Must Follow to Validate TWIC[®] and Establish HME Expiration

1. To issue an HME to an individual on the basis of a TWIC[®], the State must first verify that the TWIC[®] is valid by using both the expiration date and Visual Canceled Card List or Canceled Card List credential validation procedures listed in Appendix A to this Exemption.

2. After the State verifies that the TWIC[®] is valid, the State must set the HME expiration date to be no later than the existing TWIC[®] expiration date. The State must provide the HME data, including expiration date, to TSA in a manner, timeframe, and format suitable to TSA.



For Administrator Pecoske

David P. Pecoske, TSA Administrator

Dated: 1/8/20

APPENDIX A

PROCEDURES TO VERIFY THE VALIDITY OF A TWIC[®] FOR PURPOSES OF THIS EXEMPTION

The TWIC[®] and its associated STA can be validated using TWIC[®] security features, which include the card's printed expiration date and the card's status on the TWIC[®] Canceled Card List. For the purposes of this exemption, TSA requires States to perform card validation checks to determine that (1) the TWIC[®] and its associated STA have not expired; (2) TSA has not canceled the card; and (3) the card has not been reported lost, stolen, or damaged. Also, the States must perform basic identity verification checks to determine that the applicant is the same person to whom the TWIC[®] was issued.

A. Expiration Date Validation

States must validate whether a TWIC[®] (and respective cardholder's STA) has expired by visually checking the TWIC[®]'s expiration date printed on the front of the card. In Appendix B, the *TWIC[®] Validation Guide* provides details on overt, visible, physical security features of both versions (i.e., 2007 design and 2018 design) of the TWIC[®] design in circulation. *(Please contact for more information on other security features.)*

To validate the expiration date of the TWIC[®], the State must ensure that the year, month, and day (YYYY/MMM/DD) printed on the card is later than the current calendar date. For security, States should inspect the printed date for any indications of alteration or counterfeiting. In 2018, TSA released a new TWIC[®] design with a more secure printed date format, including a color-coded background that frames the expiration date's year. To deter counterfeiting attempts, the background color updates on an annual basis. States should consult Appendix B, *TWIC[®] Validation Guide*, for information on overt physical TWIC[®] security features.

B. Visual Canceled Card List (VCCL) and Canceled Card List (CCL) Validation

TSA communicates that a TWIC[®] has been canceled by reporting the cancellation on the TWIC[®] VCCL and CCL. TSA updates these lists daily, and the lists are available to the public online at <https://universalenroll.dhs.gov/canceled-card-lists>. The VCCL provides the Credential Identification Number (CIN) for all TWICs[®] TSA cancels. The CCL lists the Federal Agency Smart Credential Number (FASC-N) and the date the TWIC[®] FASC-N was added to the CCL. Acceptable forms of TWIC[®] validation using either the VCCL or the CCL are presented in B.1. and B.2. below.

1. **Visual Canceled Card List (VCCL):** Validation checks against the VCCL require States to view the printed 8-digit CIN located on the bottom left-hand corner of the back of a TWIC[®]. VCCL checks may be performed manually by downloading daily the VCCL.xls worksheet and searching it for the CIN presented by an applicant. If the State does not identify a match or result in its search, the card is not expired (see above), and visual inspection of the card does not indicate tampering or alteration, the TWIC[®] may be considered to be valid.

The VCCL checks may be performed electronically by downloading daily the VCCL to an electronic card reader or leveraging validation solutions developed by TSA or another entity (where available). For example, the TWIC[®] Advanced Digital Visual Inspection Solution for Revocation (ADVISR[™]) mobile application, developed for TSA, is available on Android[™] and iOS operating systems via the Google[®] Play Store[™] and Apple[®] App Store[®], respectively. Using the mobile application (where available), States can enter or scan the CIN from a TWIC[®] and input the card's expiration date to determine if the TWIC[®] is canceled and listed on the VCCL. For more information on validation solutions, please contact TWIC-Technology@tsa.dhs.gov.

2. **Canceled Card List (CCL):** Validation checks against the CCL require States to access the card's FASC-N, which is not printed visibly on the card. CCL checks may be performed electronically by downloading daily the CCL onto an electronic smart card reader. Once downloaded to a qualified reader, States can use the reader to access a TWIC[®] FASC-N and determine that it is not listed on the CCL.

C. Identity Verification

Identity verification is a critical component of TWIC[®] security. The State must ensure the individual presenting the TWIC[®] to the State is the same person to whom the TWIC[®] was issued. This verification can be performed by visually comparing the facial photograph on the front of the TWIC[®] to the applicant presenting the credential.

For more information on electronically authenticating and validating the TWIC[®] beyond the acceptable methods listed above, please contact TSA at TWIC-Technology@tsa.dhs.gov.

APPENDIX B

TWIC® VALIDATION GUIDE

Transportation Worker Identification Credential

Design Comparison

In 2018, TSA discontinued issuance of the "2007 Design." While the "2007 Design" is no longer issued, TWIC® is a 5-year credential. The "2007 Design" will remain valid until 2023.

2007 Design



2018 Design



For more information on the TWIC card, please contact TSA at: twic.issue@tsa.dhs.gov.

v1.3 October 2019

2007 Design



Transportation Worker Identification Credential

TWIC® Authentication Features

Card Design Front

The TWIC card maintains several visible (i.e., overt) design features to promote secure use of the credential.

1. Photograph: Full frontal facial photograph of the card holder.
2. Credential Expiration Date: Year, Month, Day (YYYYMMDD).
3. Card Holder's Full Name: last name, first name, and abbreviated middle name (first initial followed by period) in capital letters.
4. Color Shifting Ink: TWIC text and registered trademark symbol color shifts between red-gold (T, I) and green-purple (W, C, ®) dependent on lighting conditions when viewed from different angles.

TWIC authentication guidance provided in this document does not supersede facility or vessel physical security requirements established by the U.S. Coast Guard, designated maritime authority, owner, and/or operator. Please contact your entity's security office for more information.

For more information on the TWIC card, please contact TSA at: twic.issue@tsa.dhs.gov.

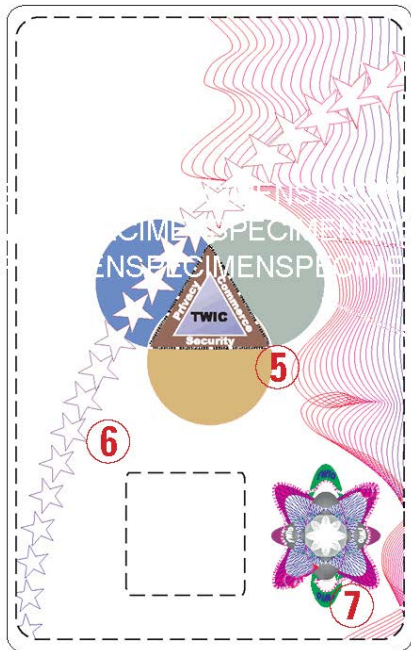
v1.3 October 2019

2007 Design

Transportation Worker Identification Credential

TWIC® Authentication Features

Laminate Card Design Front



- 5. Kinetic Image: "TWIC" centered within triangle image with words, "Privacy," "Commerce," and "Security."
- 6. Kinetic Image: Star images cascading from top right to bottom left of card front.
- 7. Kinetic Image: Four (4) overlapping oval images, including "TWIC" text within oval borders.

TWIC authentication guidance provided in this document does not supersede facility or vessel physical security requirements established by the U.S. Coast Guard, designated maritime authority, owner, and/or operator. Please contact your entity's security office for more information.
 For more information on the TWIC card, please contact TSA at: twic.issue@tsa.dhs.gov.

v1.3 October 2019

2007 Design

Transportation Worker Identification Credential

TWIC® Authentication Features

Card Design Back

- 8. Section 499, Title 18 Notice
- 9. Return Address
- 10. Card Identification Number

TWIC authentication guidance provided in this document does not supersede facility or vessel physical security requirements established by the U.S. Coast Guard, designated maritime authority, owner, and/or operator. Please contact your entity's security office for more information.
 For more information on the TWIC card, please contact TSA at: twic.issue@tsa.dhs.gov.



v1.3 October 2019

2018 Design



Transportation Worker Identification Credential

TWIC® Authentication Features

The TWIC card maintains several overt (i.e., overt) design features to promote secure use of the credential.

1. Frontal facial photograph of the card holder.
2. Credential Expiration Date: Color-coded background that will update on annual basis.
3. Card Holder's Full Name: last name, first name, and abbreviated middle name (first initial followed by period) in capital letters.
4. Color Shifting Ink: TWIC text and Propeller design color shift between red, gold, and green (depending on lighting conditions) when viewed from different angles.
5. Facility: Card Identification Number (CIN) and Anchor design embossed on the card's laminate. (The CIN is an 8 digit number that can be validated to the CIN printed on the rear of the card, bottom left.)
6. Kinetic image: Rope design color changes when viewed from different angles. (Laminate)
7. Shaped Lenses/Images: Star designs partially covering photograph with color changes when viewed from different angles. (Laminate)

TWIC authentication guidance provided in this document does not supersede facility or vessel physical security requirements established by the U.S. Coast Guard, designated maritime authority, owner, and/or operator. Please contact your entity's security office for more information.

For more information on the TWIC card, please contact TSA at twic.issue@tsa.dhs.gov.

v1.3 October 2019

2018 Design



Transportation Worker Identification Credential

TWIC® Authentication Features

Card Design Front

The TWIC card maintains several visible (i.e., overt) design features to promote secure use of the credential.

1. Photograph: Full frontal facial photograph of the card holder.
2. Credential Expiration Date: Colored-coded background that will update on annual basis.

2018	2019	2020	2021	2022	2023	2024
2025	2026	2027	2028	2029	2030	2031
3. Card Holder's Full Name: last name, first name, and abbreviated middle name (first initial followed by period) in capital letters.
4. Color Shifting Ink: TWIC text and Propeller design color shifts between red, gold, and green (dependent on lighting conditions) when viewed from different angles.
5. Facility: Card Identification Number (CIN) and Anchor design embossed on the card's laminate. (The CIN is an 8 digit number that can be validated to the CIN printed on the rear of the card.)

TWIC authentication guidance provided in this document does not supersede facility or vessel physical security requirements established by the U.S. Coast Guard, designated maritime authority, owner, and/or operator. Please contact your entity's security office for more information.

For more information on the TWIC card, please contact TSA at twic.issue@tsa.dhs.gov.

v1.3 October 2019

2018 Design



Transportation Worker Identification Credential

TWIC® Authentication Features

Laminate Card Design Front

- 6. Kinetic Image: "Rope design color changes when viewed from different angles.
Shaped Lenses/Images: Star designs partially covering
- 7. photograph with color changes when viewed from different angles.

TWIC authentication guidance provided in this document does not supersede facility or vessel physical security requirements established by the U.S. Coast Guard, designated maritime authority, owner, and/or operator. Please contact your entity's security office for more information.
For more information on the TWIC card, please contact TSA at twic.issue@tsa.dhs.gov.

v1.3 October 2019

2018 Design

Transportation Worker Identification Credential

TWIC® Authentication Features

Card Design Back

- 8. Section 499, Title 18 Notice
 - 9. Return Address
 - 10. Card Identification Number
- TWIC authentication guidance provided in this document does not supersede facility or vessel physical security requirements established by the U.S. Coast Guard, designated maritime authority, owner, and/or operator. Please contact your entity's security office for more information.
For more information on the TWIC card, please contact TSA at twic.issue@tsa.dhs.gov.



v1.3 October 2019