(b) Potential threats or significant security concerns encompass incidents, suspicious activities, and threat information including, but not limited to, the categories of reportable events listed in appendix A to this part.

(c) Information reported must include the following, as available and applicable:

(1) The name of the reporting individual and contact information, including a telephone number or email address.

(2) The affected freight or passenger train, transit vehicle, motor vehicle, station, terminal, rail hazardous materials facility, or other facility or infrastructure, including identifying information and current location.

(3) Scheduled origination and termination locations for the affected freight or passenger train, transit vehicle, or motor vehicle–including departure and destination city and route.

(4) Description of the threat, incident, or activity, including who has been notified and what action has been taken.

(5) The names, other available biographical data, and/or descriptions (including vehicle or license plate information) of individuals or motor vehicles known or suspected to be involved in the threat, incident, or activity.

(6) The source of any threat information.

[85 FR 16499, Mar. 23, 2020, as amended at 86 FR 23632, May 4, 2021]

Subpart D—Security Threat Assessments

§ 1570.301 Fraudulent use or manufacture; responsibilities of persons.

(a) No person may use or attempt to use a credential, security threat assessment, access control medium, or identification medium issued or conducted under this subchapter that was issued or conducted for another person.

(b) No person may make, produce, use or attempt to use a false or fraudulently created access control medium, identification medium or security threat assessment issued or conducted under this subchapter.

(c) No person may tamper or interfere with, compromise, modify, attempt to circumvent, or circumvent TWIC access control procedures.

(d) No person may cause or attempt to cause another person to violate paragraphs (a) through (c) of this section.

§ 1570.303 Inspection of credential.

(a) Each person who has been issued or possesses a TWIC must present the TWIC for inspection upon a request from TSA, the Coast Guard, or other authorized DHS representative; an authorized representative of the National Transportation Safety Board; or a Federal, State, or local law enforcement officer.

(b) Each person who has been issued or who possesses a TWIC must allow his or her TWIC to be read by a reader and must submit his or her reference biometric, such as a fingerprint, and any other required information, such as a PIN, to the reader, upon a request from TSA, the Coast Guard, other authorized DHS representative; or a Federal, State, or local law enforcement officer.

§ 1570.305 False statements regarding security background checks by public transportation agency or railroad carrier.

(a) *Scope.* This section implements sections 1414(e) (6 U.S.C. 1143) and 1522(e) (6 U.S.C. 1170) of the ''Implementing Recommendations of the 9/11 Commission Act of 2007,'' Public Law 110–53 (121 Stat. 266, Aug. 3, 2007).

(b) *Definitions.* In addition to the terms in §§ 1500.3, 1500.5, and 1503.202 of subchapter A and § 1570.3 of subchapter D of this chapter, the following term applies to this part:

Security background check means reviewing the following for the purpose of identifying individuals who may pose a threat to transportation security, national security, or of terrorism:

(i) Relevant criminal history databases.

(ii) In the case of an alien (as defined in sec. 101 of the Immigration and Nationality Act (8 U.S.C. 1101(a)(3)), the relevant databases to determine the status of the alien under the immigration laws of the United States.