§ 1520.5 Sensitive security information.

(a) In general. In accordance with 49 U.S.C. 114(a), SSI is information obtained or developed in the conduct of security activities, including research and development, the disclosure of which TSA has determined would—

(1) Constitute an unwarranted invasion of privacy (including, but not limited to, information contained in any personnel, medical, or similar file);

(2) Reveal trade secrets or privileged or confidential information obtained from any person; or

(3) Be detrimental to the security of transportation.

(b) Information constituting SSI. Except as otherwise provided in writing by TSA in the interest of public safety or in furtherance of transportation security, the following information, and records containing such information, constitute SSI:

(1) Security programs and contingency plans. Any security program or security contingency plan issued, established, required, received, or approved by DOT or DHS, including any comments, instructions, or implementing guidance, including—

(i) Any aircraft operator, airport operator, fixed base operator, or air cargo security program, or security contingency plan under this chapter;

(ii) Any vessel, maritime facility, or port area security plan required or directed under Federal law;

(iii) Any national or area security plan prepared under 46 U.S.C. 70103; and


(2) Security Directives. Any Security Directive or order—

(i) Issued by TSA under 49 CFR 1542.303, 1544.305, 1548.19, or other authority;

(ii) Issued by the Coast Guard under the Maritime Transportation Security Act, 33 CFR part 6, or 33 U.S.C. 1221 et seq. related to maritime security; or

(iii) Any comments, instructions, and implementing guidance pertaining thereto.

(3) Information Circulars. Any notice issued by DHS or DOT regarding a threat to aviation or maritime transportation, including any—

(i) Information circular issued by TSA under 49 CFR 1542.303, 1544.305, 1548.19, or other authority; and

(ii) Navigation or Vessel Inspection Circular issued by the Coast Guard related to maritime security.

(4) Performance specifications. Any performance specification and any description of a test object or test procedure, for—

(i) Any device used by the Federal Government or any other person pursuant to any aviation or maritime transportation security requirements of Federal law for the detection of any person, and any weapon, explosive, incendiary, or destructive device, item, or substance; and

(ii) Any communications equipment used by the Federal government or any other person in carrying out or complying with any aviation or maritime transportation security requirements of Federal law.

(5) Vulnerability assessments. Any vulnerability assessment directed, created, held, funded, or approved by the DOT, DHS, or that will be provided to DOT or DHS in support of a Federal security program.

(6) Security inspection or investigative information. (i) Details of any security inspection or investigation of an alleged violation of aviation, maritime, or rail transportation security requirements of Federal law that could reveal a security vulnerability, including the identity of the Federal special agent or other Federal employee who conducted the inspection or audit.

(ii) In the case of inspections or investigations performed by TSA, this includes the following information as to events that occurred within 12 months of the date of release of the information: the name of the airport where a violation occurred, the airport identifier in the case number, a description of the violation, the regulation allegedly violated, and the identity of any aircraft operator in connection with specific locations or specific security procedures. Such information will be released after the relevant 12-month period, except that TSA will not release the specific gate or other location on an airport where an event occurred, regardless of the amount of time that has passed since its occurrence. During the period within 12 months of the date of release of the information, TSA may release summaries of an aircraft operator’s, but not an airport operator’s, total security violations in a specified time range without identifying specific violations or locations. Summaries may include total enforcement actions, total proposed civil penalty amounts, number of cases opened, number of cases referred to TSA or FAA counsel for legal enforcement action, and number of cases closed.

(7) Threat information. Any information held by the Federal government concerning threats against transportation or transportation systems and sources and methods used to gather or develop threat information, including threats against cyber infrastructure.

(8) Security measures. Specific details of aviation, maritime, or rail transportation security measures, both operational and technical, whether applied directly by the Federal government or another person, including—

(i) Security measures or protocols recommended by the Federal government;

(ii) Information concerning the deployments, numbers, and operations of Coast Guard personnel engaged in maritime security duties and Federal Air Marshals, to the extent it is not classified national security information; and

(iii) Information concerning the deployments and operations of Federal Flight Deck Officers, and numbers of Federal Flight Deck Officers aggregated by aircraft operator.

(iv) Any armed security officer procedures issued by TSA under 49 CFR part 1562.

(9) Security screening information. The following information regarding security screening under aviation or maritime transportation security requirements of Federal law:

(i) Any procedures, including selection criteria and any comments, instructions, and implementing guidance pertaining thereto, for screening of persons, accessible property, checked baggage, U.S. mail, stores, and cargo, that is conducted by the Federal government or any other authorized person.

(ii) Information and sources of information used by a passenger or property
screening program or system, including an automated screening system.

(iii) Detailed information about the locations at which particular screening methods or equipment are used, only if determined by TSA to be SSI.

(iv) Any security screener test and scores of such tests.

(v) Performance or testing data from security equipment or screening systems.

(vi) Any electronic image shown on any screening equipment monitor, including threat images and descriptions of threat images for threat image projection systems.

(10) Security training materials. Records created or obtained for the purpose of training persons employed by, contracted with, or acting for the Federal government or another person to carry out aviation, maritime, or rail transportation security measures required or recommended by DHS or DOT.

(11) Identifying information of certain transportation security personnel.

(i) Lists of the names or other identifying information that identify persons as—

(A) Having unescorted access to a secure area of an airport, a rail secure area, or a secure or restricted area of a maritime facility, port area, or vessel;

(B) Holding a position as a security screener employed by or under contract with the Federal government pursuant to aviation or maritime transportation security requirements of Federal law, where such lists are aggregated by airport;

(C) Holding a position with the Coast Guard responsible for conducting vulnerability assessments, security boardings, or engaged in operations to enforce maritime security requirements or conduct force protection;

(D) Holding a position as a Federal Air Marshal; or

(ii) The name or other identifying information that identifies a person as a current, former, or applicant for Federal Flight Deck Officer.

(12) Critical aviation, maritime, or rail infrastructure asset information. Any list identifying systems or assets, whether physical or virtual, so vital to the aviation, maritime, or rail transportation system (including rail hazardous materials shippers and rail hazardous materials receivers) that the incapacity or destruction of such assets would have a debilitating impact on transportation security, if the list is—

(i) Prepared by DHS or DOT; or

(ii) Prepared by a State or local government agency and submitted by the agency to DHS or DOT.

(13) Systems security information. Any information involving the security of operational or administrative data systems operated by the Federal government that have been identified by the DOT or DHS as critical to aviation or maritime transportation safety or security, including automated information security procedures and systems, security inspections, and vulnerability information concerning those systems.

(14) Confidential business information.

(i) Solicited or unsolicited proposals received by DHS or DOT, and negotiations arising therefrom, to perform work pursuant to a grant, contract, cooperative agreement, or other transaction, but only to the extent that the subject matter of the proposal relates to aviation or maritime transportation security measures;

(ii) Trade secret information, including information required or requested by regulation or Security Directive, obtained by DHS or DOT in carrying out aviation or maritime transportation security responsibilities; and

(iii) Commercial or financial information, including information required or requested by regulation or Security Directive, obtained by DHS or DOT in carrying out aviation or maritime transportation security responsibilities, but only if the source of the information does not customarily disclose it to the public.

(15) Research and development. Information obtained or developed in the conduct of research related to aviation, maritime, or rail transportation security activities, where such research is approved, accepted, funded, recommended, or directed by DHS or DOT, including research results.

(16) Other information. Any information not otherwise described in this section that TSA determines is SSI under 49 U.S.C. 114(s) or that the Secretary of DOT determines is SSI under
Transportation Security Administration, DHS

§ 1520.9 Restrictions on the disclosure of SSI.

(a) Duty to protect information. A covered person must—
(1) Take reasonable steps to safeguard SSI in that person’s possession or control from unauthorized disclosure. When a person is not in physical possession of SSI, the person must store it in a secure container, such as a locked desk or file cabinet or in a locked room.

(2) Disclose, or otherwise provide access to, SSI only to covered persons who have a need to know, unless otherwise authorized in writing by TSA, the Coast Guard, or the Secretary of DOT.

(3) Refer requests by other persons for SSI to TSA or the applicable component or agency within DOT or DHS.

(4) Mark SSI as specified in §1520.13.

(5) Dispose of SSI as specified in §1520.19.

(b) Unmarked SSI. If a covered person receives a record containing SSI that is not marked as specified in §1520.13, the covered person must—
(1) Mark the record as specified in §1520.13; and