

to carry out any aviation or maritime 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 or a secure or restricted area of a maritime facility, port area, or vessel or;

(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 or maritime infrastructure asset information.* Any list identifying systems or assets, whether physical or virtual, so vital to the aviation or maritime transportation system 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 or maritime transportation security activities, where such research is approved, accepted, funded, recommended, or directed by the 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 49 U.S.C. 40119. Upon the request of another Federal agency, TSA or the Secretary of DOT may designate as SSI information not otherwise described in this section.

(c) *Loss of SSI designation.* TSA or the Coast Guard may determine in writing that information or records described in paragraph (b) of this section do not constitute SSI because they no longer meet the criteria set forth in paragraph (a) of this section.

§ 1520.7 Covered persons.

Persons subject to the requirements of part 1520 are:

(a) Each airport operator and aircraft operator subject to the requirements of Subchapter C of this title.

(b) Each indirect air carrier, as defined in 49 CFR 1540.5.

(c) Each owner, charterer, or operator of a vessel, including foreign vessel owners, charterers, and operators,

required to have a security plan under Federal or International law.

(d) Each owner or operator of a maritime facility required to have a security plan under the Maritime Transportation Security Act, (Pub.L. 107-295), 46 U.S.C. 70101 *et seq.*, 33 CFR part 6, or 33 U.S.C. 1221 *et seq.*

(e) Each person performing the function of a computer reservation system or global distribution system for airline passenger information.

(f) Each person participating in a national or area security committee established under 46 U.S.C. 70112, or a port security committee.

(g) Each industry trade association that represents covered persons and has entered into a non-disclosure agreement with the DHS or DOT.

(h) DHS and DOT.

(i) Each person conducting research and development activities that relate to aviation or maritime transportation security and are approved, accepted, funded, recommended, or directed by DHS or DOT.

(j) Each person who has access to SSI, as specified in §1520.11.

(k) Each person employed by, contracted to, or acting for a covered person, including a grantee of DHS or DOT, and including a person formerly in such position.

(l) Each person for which a vulnerability assessment has been directed, created, held, funded, or approved by the DOT, DHS, or that has prepared a vulnerability assessment that will be provided to DOT or DHS in support of a Federal security program.

(m) Each person receiving SSI under §1520.15(d) or (e).

§ 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 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 other-

wise 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

(2) Inform the sender of the record that the record must be marked as specified in §1520.13.

(c) *Duty to report unauthorized disclosure.* When a covered person becomes aware that SSI has been released to unauthorized persons, the covered person must promptly inform TSA or the applicable DOT or DHS component or agency.

(d) *Additional Requirements for Critical Infrastructure Information.* In the case of information that is both SSI and has been designated as critical infrastructure information under section 214 of the Homeland Security Act, any covered person who is a Federal employee in possession of such information must comply with the disclosure restrictions and other requirements applicable to such information under section 214 and any implementing regulations.

§ 1520.11 Persons with a need to know.

(a) *In general.* A person has a need to know SSI in each of the following circumstances:

(1) When the person requires access to specific SSI to carry out aviation or maritime transportation security activities approved, accepted, funded, recommended, or directed by DHS or DOT.

(2) When the person is in training to carry out aviation or maritime transportation security activities approved, accepted, funded, recommended, or directed by DHS or DOT.

(3) When the information is necessary for the person to supervise or otherwise manage individuals carrying out aviation or maritime transportation security activities approved, accepted, funded, recommended, or directed by the DHS or DOT.