Federal Register: May 18, 2004 (Volume 69, Number 96)
Rules and Regulations
Page 28066-28086

==========

DEPARTMENT OF TRANSPORTATION

Office of the Secretary of Transportation

49 CFR Part 15

DEPARTMENT OF HOMELAND SECURITY

Transportation Security Administration

49 CFR Part 1520

[Docket No. TSA-2003-15569; Amendment No. 1520-1]
RIN 1652-AA08

Protection of Sensitive Security Information

AGENCY: Transportation Security Administration (TSA), DHS, and Office of the Secretary of Transportation (OST), DOT.

ACTION: Interim final rule; request for comments.

SUMMARY: TSA is revising its regulation governing the protection of sensitive security information (SSI) in order to protect the confidentiality of maritime security measures adopted under the U.S. Coast Guard's regulations, published on October 22, 2003, implementing the Maritime Transportation Security Act (MTSA) and other activities related to port and maritime security. SSI is information that TSA has determined must be protected from improper disclosure in order to ensure transportation security. TSA's SSI regulation establishes certain requirements for the handling and dissemination of SSI, including restrictions on disclosure and civil penalties for violations of those restrictions. Currently, the SSI regulation applies primarily to information related to aviation security. Airlines, airports, and others operating in civil aviation are required to limit access to this information to those personnel who need it to carry out their security functions.

Under MTSA, Congress directed the Coast Guard to issue regulations requiring maritime facility and vessel operators to develop security plans detailing the types of security measures they will implement under varying threat conditions. In order to meet statutory deadlines for implementation of these plans, the Coast Guard issued a series of final rules on October 22, 2003, requiring facility and vessel operators to submit security plans to the Coast Guard for approval. In order to protect the security of the facilities and vessels that prepare security plans, it is necessary to ensure that the plans and related security information are subject to limitations on their

disclosure. Therefore, TSA is issuing an interim final rule expanding the scope of its SSI regulation so that it covers security plans and other information about security measures required by the Coast Guard's MTSA regulations. The Coast Guard also will supplement the MTSA regulations by exercising its longstanding authority under the Ports and Waterways Safety Act and the Magnuson Act. Sensitive information related to maritime security collected pursuant to these authorities should likewise be protected from public disclosure.

In connection with this revision to the regulations, TSA is requiring employees, contractors, grantees, and agents of DHS and DOT to follow the same requirements governing protection of SSI as those in the transportation sector who are subject to the regulation. This change will provide clear standards for those persons employed by and acting on behalf of DHS and DOT regarding the obligation to safeguard SSI.

The interim rule also makes clarifying changes to existing provisions of the SSI regulation governing aviation security.

The Office of the Secretary of Transportation (OST) is issuing this rule jointly with TSA to implement DOT's parallel authority to protect SSI. In

[[Page 28067]]

order to promote the efficiency and effectiveness of the regulation as well as ease of compliance, TSA and OST are adopting identical regulatory standards governing SSI.

DATES: This rule is effective June 17, 2004. Comments must be received by July 19, 2004.

ADDRESSES: You may submit comments, identified by the TSA docket number to this rulemaking, using any one of the following methods:

Comments Filed Electronically: You may submit comments through the docket Web site at http://dms.dot.gov. Please be aware that anyone is able to search the electronic form of all comments received into any of our dockets by the name of the individual submitting the comment (or signing the comment, if submitted on behalf of an association, business, labor union, etc.). You may review the applicable Privacy Act Statement published in the Federal Register on April 11, 2000 (65 FR 19477), or you may visit http://dms.dot.gov.

You also may submit comments through the Federal eRulemaking portal at http://www.regulations.gov.

Comments Submitted by Mail, Fax, or In Person: Address or deliver your written, signed comments to the Docket Management System, U.S. Department of Transportation, Room Plaza 401, 400 Seventh Street, SW., Washington, DC 20590-0001; fax: 202-493-2251.

Comments that include trade secrets, confidential commercial or financial information, or sensitive security information (SSI) should not be submitted to the public regulatory docket. Please submit such comments separately from other comments on the rule. Comments containing trade secrets, confidential commercial or financial information, or SSI should be appropriately marked as containing such information and submitted by mail to Ann Hunt, Office of Aviation Operations Litigation Support & Special Activities Staff, TSA-7, Transportation Security Administration Headquarters, 601 S. 12th

Street, Arlington, VA 22202.

Reviewing Comments in the Docket: You may review the public docket containing comments in person in the Dockets Office between 9 a.m. and 5 p.m., Monday through Friday, except Federal holidays. The Dockets Office is located on the plaza level of the NASSIF Building at the Department of Transportation address above. Also, you may review public dockets on the Internet at http://dms.dot.gov.

See SUPPLEMENTARY INFORMATION for format and other information about comment submissions.

FOR FURTHER INFORMATION CONTACT: For questions on 49 CFR part 15: Robert Ross, Office of the General Counsel, Department of Transportation, Washington, DC 20590; e-mail: Bob.Ross@ost.dot.gov, telephone: (202) 366-9156.

For questions on 49 CFR part 1520: Ann Hunt, Director, Aviation Operations Litigation Support & Special Activities Staff, TSA-7, Transportation Security Administration , 601 South 12th Street, Arlington, VA 22202-4220; e-mail: Ann.Hunt@dhs.gov, telephone: (571) 227-2278.

SUPPLEMENTARY INFORMATION:

Comments Invited

Interested persons are invited to participate in this rulemaking by submitting written data, views, or arguments. We also invite comments relating to the economic, environmental, energy, or federalism impacts that might result from adopting this amendment. The most helpful comments will reference a specific portion of the rule, explain the reason for any recommended change, and include supporting data. See ADDRESSES above for information on how to submit comments.

Comments that include trade secrets, confidential commercial or financial information, or SSI should not be submitted to the public regulatory docket. Please submit such comments separately from other comments on the rule. Comments containing this type of information should be appropriately marked and submitted to the address specified in the ADDRESSES section. Upon receipt of such comments, TSA will not place the comments in the public docket and will handle them in accordance with applicable safeguards and restrictions on access. TSA will hold them in a separate file to which the public does not have access, and place a note in the public docket that TSA has received such materials from the commenter. If TSA receives a request to examine or copy this information, TSA would treat it as any other request under the Freedom of Information Act (FOIA) (5 U.S.C. 552) and the Department of Homeland Security's FOIA regulation found in 6 CFR part 5.

With each comment, please include your name and address, identify the docket number at the beginning of your comments, and give the reason for each comment. The most helpful comments reference a specific portion of the proposal, explain the reason for any recommended change, and include supporting data. You may submit comments and material electronically, in person, by mail, or fax as provided under ADDRESSES, but please submit your comments and material by only one means. If you submit comments by mail or delivery, submit them in two copies, in an unbound format, no larger than 8.5 by 11 inches, suitable for copying and electronic filing.

If you want TSA to acknowledge receipt of your comments on this

rulemaking, include with your comments a self-addressed, stamped postcard on which the docket number appears. We will stamp the date on the postcard and mail it to you.

Except for comments containing confidential information and SSI, we will file in the docket all comments we receive, as well as a report summarizing each substantive public contact with TSA personnel concerning this rulemaking. The docket is available for public inspection before and after the comment closing date.

We will consider all comments we receive on or before the closing date for comments. We will consider comments filed late to the extent practicable. We may change these rules in light of the comments we receive.

Availability of Interim Final Rule

You can get an electronic copy using the Internet by--

(1) Searching the Department of Transportation's electronic Docket Management System (DMS) Web page (http://dms.dot.gov/search);

(2) Accessing the Government Printing Office's Web page at http://

http://www.access.gpo.gov/su_docs/aces/aces140.html; or

(3) Visiting TSA's Law and Policy Web page at http://www.tsa.dot.gov/public/index.jsp
.

In addition, copies are available by writing or calling the individual in the FOR FURTHER INFORMATION CONTACT section. Make sure to identify the docket number of this rulemaking.

Small Entity Inquiries

The Small Business Regulatory Enforcement Fairness Act (SBREFA) of 1996 requires an agency to comply with small entity requests for information and advice about compliance with statutes and regulations within the agency's jurisdiction. Any small entity that has a question regarding this document may contact persons listed in FOR FURTHER INFORMATION CONTACT for information. You can get further information regarding SBREFA on the Small Business Administration's Web page at http://www.sba.gov/advo/laws/law_lib.html.

[[Page 28068]]

Abbreviations of Terms Used in This Document

ATSA--Aviation and Transportation Security Act
CII--Critical Infrastructure Information
DHS--Department of Homeland Security
DOT--Department of Transportation
FAA--Federal Aviation Administration
FOIA--Freedom of Information Act
HSA--Homeland Security Act of 2002
MTSA--Maritime Transportation Security Act of 2002
SSI--Sensitive Security Information
TSA--Transportation Security Administration

Statutory and Regulatory Background

The Aviation and Transportation Security Act

Following the terrorist attacks on the United States on September 11, 2001, Congress passed the Aviation and Transportation Security Act (ATSA) on November 19, 2001, Public Law 107-71, which established TSA. ATSA established TSA within DOT, operating under the direction of the Under Secretary of Transportation for Security (Under Secretary).

ATSA transferred the responsibility for civil aviation security from the Federal Aviation Administration (FAA) to TSA. 49 U.S.C. 114(d). Among the statutory authorities previously administered by FAA that ATSA transferred to TSA's purview was the authority in 49 U.S.C. 40119 (section 40119), governing the protection of certain information related to transportation security.

Prior to ATSA, section 40119 authorized the Administrator of FAA to prescribe regulations prohibiting disclosure of information obtained or developed in carrying out security or in research and development activities carried out under various FAA authorities, if the FAA Administrator determined by regulation that disclosing the information would: (1) Be an unwarranted invasion of personal privacy; (2) reveal a trade secret or privileged or confidential commercial or financial information; or (3) be detrimental to the safety of passengers in air transportation.

FAA implemented this authority by regulation at 14 CFR part 191, which established a category of sensitive, but unclassified, information known as Sensitive Security Information (SSI), the unauthorized disclosure of which could compromise systems that protect aviation security. FAA's SSI regulation defined SSI in both general and specific terms. It identified specific types of records constituting SSI, such as airport and air carrier security programs, as well as general categories of SSI, such as information revealing specific details of aviation security measures. Consistent with the scope of FAA's regulatory authority over aviation, the universe of entities and individuals covered by the FAA's SSI regulation was limited to airport operators, air carriers, and other aviation-related entities and personnel.

Section 101(e) of ATSA amended the FAA's SSI authority in section 40119(b) by transferring its administration to the Under Secretary and by deleting the word ``air'' modifying ``transportation,'' thereby expanding the scope of section 40119 to cover information in all modes of transportation. On February 22, 2002, TSA published a final rule transferring the bulk of FAA's aviation security regulations to TSA, including FAA's SSI regulation, which now is codified at 49 CFR part 1520, and is administered by TSA (67 FR 8340, 8351).

The Homeland Security Act

On November 25, 2002, the President signed into law the Homeland Security Act of 2002 (HSA), Pub. L. 107-296, which transferred TSA to the newly established DHS. In connection with that transfer, the HSA transferred TSA's SSI authority under 49 U.S.C. 40119 to 49 U.S.C. 114(s), and amended section 40119 to vest similar SSI authority in the Secretary of DOT. New 49 U.S.C. 114(s) provides:

``(s) NONDISCLOSURE OF SECURITY ACTIVITIES--(1) IN GENERAL--Notwithstanding section 552 of title 5, the Under Secretary shall

prescribe regulations prohibiting the disclosure of information obtained or developed in carrying out security under authority of the Aviation and Transportation Security Act (Public Law 107-71) or under chapter 449 of this title if the Under Secretary decides that disclosing the information would--(A) Be an unwarranted invasion of personal privacy; (B) reveal a trade secret or privileged or confidential commercial or financial information; or (C) be detrimental to the security of transportation.''

The SSI authority of the Secretary of DOT is set forth in amended 49 U.S.C. 40119(b)(1), as follows:

``Notwithstanding section 552 of title 5, and the establishment of a Department of Homeland Security, the Secretary of Transportation shall prescribe regulations prohibiting disclosure of information obtained or developed in ensuring security under this title if the Secretary of Transportation decides disclosing the information would--(A) Be an unwarranted invasion of personal privacy; (B) reveal a trade secret or privileged or confidential commercial or financial information; or (C) be detrimental to transportation safety.''

In both sections, Congress made an important change to the previous statutory language that broadens the scopes of the SSI authority of both the Under Secretary and the Secretary of DOT. Specifically, Congress changed the phrase ``detrimental to the safety of passengers in transportation'' (emphasis added) to ``detrimental to the security of transportation'' and ``detrimental to transportation safety,'' respectively. Therefore, the HSA amendments clarified that the SSI authority is not limited to passenger modes of transportation. It covers all transportation activities, including non-passenger modes such as air and maritime cargo, trucking and freight transport, and pipelines.

In conjunction with the transfer of TSA to DHS, the Under Secretary has adopted the new title of Administrator. Consequently, in the remainder of this document, the Under Secretary is referred to as the Administrator or the TSA Administrator.

The Maritime Transportation Security Act

On November 25, 2002, the President signed into law the MTSA, which established a new framework for maritime security, to be administered largely by the Secretary of DHS, including through TSA, the Coast Guard, and the Bureau of Customs and Border Protection, along with the Maritime Administration of the DOT. Primary elements of this framework are national, area, port, and facility and vessel security plans to be approved or required by DHS. Specifically, under the MTSA the Secretary of DHS must prepare a National Maritime Transportation Security Plan, which, in turn, will identify areas of the country for which DHS will adopt Area Maritime Security Plans. Section 70103 of MTSA also directs the Secretary of DHS to prescribe regulations requiring certain classes of vessels and maritime facilities to adopt plans for deterring a transportation security incident. 46 U.S.C. 70103(a).

The Coast Guard issued final rules on October 22, 2003, that require vessel and maritime facility operators to prepare security plans for Coast Guard approval. See 68 FR 60448. Currently these types of documents are not subject to the disclosure limitations of TSA's SSI regulation, nor are maritime facility and vessel operators subject to

the regulation's requirements to protect these documents from unauthorized access or disclosure.

With the establishment of new Federal security standards for maritime transportation comes an immediate

need to expand the existing legal protections governing SSI so that those who will have access to sensitive information related to maritime security must safeguard it from improper disclosure. While the MTSA provides broad limitations on public disclosure of the information related to maritime security requirements (see 46 U.S.C. 70103), it does not establish binding requirements for owners and operators of maritime transportation facilities and vessels to safeguard the information from disclosure. As previously mentioned, the Coast Guard also will exercise other authorities to enhance maritime security. Without such a legal framework to protect security information, there is an increased risk that newly adopted security measures will be defeated through their unregulated dissemination.

In addition, the absence of such regulatory protections has inhibited TSA and the Coast Guard from disseminating threat information to those who need to act on it in the maritime transportation mode. TSA regularly disseminates Information Circulars to airlines and airports detailing current threat information related to aviation security. The Coast Guard disseminates threat information evaluation reports in coordination with the Directorate of Informational Analysis and Infrastructure Protection to the maritime industry. The Coast Guard also issues guidance related to maritime security through Navigation and Vessel Inspection Circulars and similar documents. In order to continue to disseminate relevant threat information to maritime transportation operators, there must be requirements in place that the information be protected by those who receive it. Therefore, there is an immediate need to expand the existing regulatory framework governing information related to aviation security to cover information related to security of maritime transportation.

Critical Infrastructure Information Act of 2002

The Critical Infrastructure Information Act of 2002 (CII Act), enacted as Subtitle B of title II of the HSA, establishes new requirements for the Federal Government's handling of information related to the nation's critical infrastructure, known as ``critical infrastructure information,'' or ``CII'', that is voluntarily submitted by the private sector to the Federal Government. The CII Act generally prohibits Federal agencies from disclosing such information, except within the Federal Government and to State and local governments in order to protect critical infrastructure.

In practice, the situations in which information constitutes both SSI and CII may be limited. For the most part, information that is SSI is created by TSA or the Coast Guard or is required to be submitted to TSA, the Coast Guard, or another part of the Federal Government, such as DOT. As further discussed below, SSI includes security programs and procedures of airport, aircraft, vessel, and maritime facility operators; procedures that TSA uses to perform security screening of airline passengers and baggage; and information detailing vulnerabilities in transportation systems or facilities. SSI is created by airports and aircraft operators and other regulated parties,

pursuant to regulatory requirements. TSA and the Coast Guard also create SSI, such as screening procedures and certain non-public security directives issued to regulated parties. The SSI regulation prohibits regulated parties from disseminating SSI, except to those employees, contractors, or agents who have a need to know the information in order to carry out security duties.

Therefore, information constituting SSI generally is not voluntarily submitted to the government, which is required for CII designation. In addition, SSI relates to both critical and non-critical infrastructure assets. There may be cases, however, where the owner or operator of a critical transportation asset voluntarily submits information, such as a vulnerability assessment, to TSA or the Coast Guard. If that information were to be designated by DHS as CII, it would be governed by the requirements for handling of CII, rather than by the SSI regulation.

Another key difference between SSI and CII is the extent to which a Federal employee may disclose such information. Under the SSI regulation, TSA may disclose SSI to persons with a need to know in order to ensure transportation security. This includes persons both within and outside the Federal Government. The CII Act, however, generally prohibits disclosure of properly designated CII outside the Federal Government. Thus, the interim final rule clarifies that in cases where information is both SSI and CII, the receipt, maintenance, or disclosure of such information by a Federal agency or employee is governed by the CII Act and any implementing regulations, not by the interim final rule.

Summary of the Interim Final Rule

In this interim final rule, TSA is revising its SSI regulation to expand the existing regulatory framework governing information related to aviation security to cover information related to security in maritime transportation, consistent with the security framework required by the Coast Guard's regulations implementing the MTSA. In making this change, TSA is revising part 1520 in its entirety. The Section-by Section Analysis describes the relationship between each section of the current SSI regulation and the regulation as revised by the interim final rule. While the interim final rule largely incorporates the substance of the provisions of the current SSI regulation, it streamlines and consolidates some of the current provisions and expands on some current provisions in order to provide additional clarity.

As discussed above in the Statutory and Regulatory Background section, the HSA vested parallel SSI authority in the Secretary of DOT under 49 U.S.C. 40119. Because the HSA transferred the SSI regulation to TSA, however, there currently is no regulation implementing the DOT authority under section 40119. In order to implement that authority, DOT is issuing this interim final rule jointly with TSA. In order to promote the efficiency and effectiveness of the regulation as well as ease of compliance, TSA and DOT are adopting identical regulatory standards governing SSI. The DOT regulation will appear in 49 CFR part 15.

Section-by-Section Analysis

The following is a section-by-section analysis of the provisions of the interim final rule. For ease of reference, the section-by-section

analysis discusses the sections of 49 CFR part 1520, but the discussion is applicable to parallel sections in new part 15 of title 49 CFR.

Section 1520.1--Scope

Section 1520.1(a) of the SSI regulation currently provides that part 1520 governs the release by TSA and other persons of records and information obtained or developed during security or research and development activities. Current Sec. 1520.1(c) and (d) provide that TSA's authority regarding SSI may be further delegated within TSA, and that TSA exercises authority to withhold or disclose SSI in consultation with the heads of the DOT administrations in cases where those administrations hold SSI.

Section 1520.1 of the interim final rule adds new language to clarify that part 1520 governs the maintenance, safeguarding, and disclosure of records and information that TSA has determined to be SSI, but does not apply to classified national security information or to sensitive unclassified

[[Page 28070]]

information that is not SSI, but nonetheless may be exempted from public disclosure under the Freedom of Information Act (FOIA). This section also makes clear that, in the case of information that has been designated as CII under section 214 of the Homeland Security Act, the receipt, maintenance, or disclosure of such information by a Federal agency or employee is governed by section 214 and any implementing regulations, not by part 1520.

The interim final rule eliminates unnecessary language in current Sec. 1520.1(d) regarding the disclosure of SSI held by DOT administrations.

Section 1520.3--Terms Used in This Part

The interim final rule modifies and expands the list of definitions now in Sec. 1520.1(b) of the SSI regulation in order to clarify the regulation and expand its scope to maritime security matters. Section 1520.1(b) currently defines the terms ``record'' and ``vulnerability assessment''. ``Record'' currently is defined as ``any writing, drawing, map, tape, film, photograph, or other means by which information is preserved, irrespective of format.'' ``Vulnerability assessment'' now is defined as ``any examination of a transportation system, vehicle, or facility to determine its vulnerability to unlawful interference.'' The interim final rule revises these definitions and adds definitions of several new terms.

Section 1520.3 of the interim final rule modifies the definition of ``record'' to include any draft, proposed, or recommended change to any record. This is not a substantive change. It merely incorporates the substance of Sec. 1520.7(l) of the current SSI regulation, which provides that SSI includes any draft, proposed, or recommended change to information and records that constitute SSI.

A record subject to the SSI regulation is not necessarily a Federal record under the Federal Records Act (5 U.S.C. 105). Therefore, for purposes of compliance with the requirements to destroy SSI under Sec. 1520.19 (which is discussed below in the Section-by-Section Analysis), a Federal agency should make a separate determination as to whether a record containing SSI is a record for purposes of the Federal Records

Act, which may override the destruction requirements of Sec. 1520.19.

Section 1520.3 of the interim final rule revises the definition of ``vulnerability assessment'' to include expressly the examination of any transportation-related automated system or network to determine its vulnerability to unlawful interference. The revised definition also makes clear that a vulnerability assessment includes any recommended actions to address security concerns.

Section 1520.3 of the interim final rule adds the following new definitions. Under the interim final rule, the term ``Administrator'' means the Under Secretary of Transportation for Security referred to in 49 U.S.C. 114(b), or his or her designee. As discussed previously, this reflects the Under Secretary's decision to adopt the title of Administrator in connection with the transfer of TSA to DHS.

As further discussed below, the interim final rule introduces the concept of a ``covered person'' for purposes of the SSI regulation in order to clarify the universe of entities and individuals that are subject to the regulation's requirements. Although the list of ``covered persons'' is set forth in Sec. 1520.7 of the interim final rule, TSA is adding a definition of the term ``covered person'' to Sec. 1520.3 in order to provide additional clarity. ``Covered person'' is defined as any organization, entity, individual, or other person described in Sec. 1520.7. In the case of an individual, a ``covered person'' includes any individual applying for employment in a position that would be a covered person, or in training for such a position, regardless of whether that individual is receiving a wage, salary, or other form of payment. The definition includes individual applicants and trainees because individuals acting in those capacities may receive or have access to SSI before they are hired or accepted into a permanent position that otherwise would involve access to SSI. ``Covered person'' includes a person applying for certification or other form of approval that, if granted, would make the person a covered person. Persons applying for a certification or approval that would make them covered persons may have access to SSI as part of the application process, and therefore must be subject to a regulatory obligation to protect it from unauthorized disclosure. The reference to applicants and trainees in the definition of ``covered person'' carries forward in substance Sec. 1520.5(f) of the current SSI regulation.

Section 1520.3 adds a definition of ``DHS'', which means any directorate, bureau, or other component within DHS, including the Coast Guard. Under some circumstances, the Coast Guard may be temporarily transferred to the Department of the Navy and will operate as a service with the Navy. See 14 U.S.C. 3. Nonetheless, the SSI regulation would continue to apply to information held or distributed by the Coast Guard.

Section 1520.3 also includes a number of new definitions that have been added in order to clarify terms currently used in the SSI regulation, such as ``security program'', ``security contingency plan'', ``security screening'', and ``threat image projection system''. In addition to explaining the meaning of these terms, the definitions make clear that they apply in the context of maritime transportation.

Section 1520.5--Sensitive Security Information

Section 1520.3(b) of the SSI regulation currently sets forth the general criteria under which TSA determines whether information is SSI. It authorizes TSA to prohibit the disclosure of information developed in the conduct of security or research and development activities if,

in TSA's judgment, the disclosure of such information would: (1) Constitute an unwarranted invasion of privacy; (2) reveal trade secrets or confidential information obtained from any person; or (3) be detrimental to the safety of persons traveling in transportation. Section 1520.5(a) of the interim final rule carries forward and updates this provision to reflect changes to TSA's SSI authority made by the HSA, discussed above.

Section 1520.5(b) of the interim final rule incorporates the provisions of current Sec. 1520.7 of the SSI regulation that define the types of information that constitute SSI. In large part, Sec. 1520.5(b) carries forward categories of information or records that constitute SSI under the current regulation, while expanding their description to make clear that they now encompass information related to the security of maritime transportation and are not limited to the security of passengers.

Section 1520.5(b) of the interim final rule carries forward in substance the introductory text of Sec. 1520.7 of the current regulation, which provides that the specific information described in that section is SSI, ``except as otherwise provided in writing by the Under Secretary as necessary in the interest of safety of persons in transportation * * *'' This exception serves two functions. First, some SSI documents contain information that is released to the public. TSA may issue press releases or otherwise make this information available to the public where TSA determines in writing that such a release is appropriate. Second, TSA may publicly release some SSI to help achieve compliance with security requirements. For instance, as part of its security rules, TSA requires airlines to ask passengers for identification at check-in. Although this requirement is

[[Page 28071]]

part of a security procedure that is SSI, TSA has released this information to the public in order to facilitate the secure and efficient processing of passengers when they arrive at an airport. In this type of situation, TSA must determine whether releasing certain portions of security procedures will improve transportation security to a greater extent than maintaining the confidentiality of the procedure. See 62 FR 13471 (Mar. 21, 1997, preamble to 1997 amendments to SSI regulation).

Sections 1520.5(b)(1) through (5) of the interim final rule, which cover security programs and contingency plans, Security Directives, Information Circulars, performance specifications, and vulnerability assessments, carry forward in substance the current provisions of Sec. Sec. 1520.7(a) through (e), (g), and (r).

For instance, Sec. 1520.5(b)(1) carries forward the provisions relating to security programs and contingency plans from current Sec. 1520.7(a) and (d), but expands those provisions to cover national and area security plans and security incident response plans established under the MTSA, as well as vessel and facility security plans required or directed under Federal law. See 46 U.S.C. 70103, 70104.

Section 1520.5(b)(3) of the interim final rule modifies the reference to Information Circulars to include any notice issued by DHS or DOT regarding a threat to aviation or maritime transportation. Information Circulars are documents that TSA distributes to entities in the transportation sector that detail information of security concern. The interim final rule clarifies that SSI includes not only Information Circulars issued to entities within the aviation sector, but also any

circular, guidance, or notice regarding threats to aviation or maritime transportation that DHS or DOT may issue to a covered person.\1\ For instance, the interim final rule covers Navigation or Vessel Inspection Circulars issued by the Coast Guard related to maritime security, and similar issuances of DOT.

\1\ Information Circulars were primarily used by the FAA (and are now used by TSA) to pass information of security concern to airport and aircraft operators.

The interim final rule carries forward in substance the current reference to vulnerability assessments now in Sec. 1520.7(r) of the SSI regulation. The revised provision would apply to vulnerability assessments created at the initiative of a covered person, but which the covered person intends to provide to DOT or DHS in support of a Federal security program.

Section 1520.5(b)(6) of the interim final rule modifies the reference now in Sec. 1520.7(h) of the SSI regulation to inspections and investigations of regulatory violations. The interim final rule expands the current provision so that it applies in the context of maritime transportation. The interim final rule also retains, in large part, the language now in the SSI regulation detailing the specific types of investigative information related to the aviation sector that constitutes SSI.

Section 1520.5(b)(7) of the interim final rule carries forward and incorporates the reference in Sec. 1520.7(i) of the SSI regulation to information concerning threats against transportation. The revised language includes threats against cyber infrastructure in order to make clear that information on threats to transportation includes threats to computer systems. The provision also is revised to clarify that it applies to threat information held by any Federal agency, not just TSA, as well as sources and methods used to gather or develop such information.

Section 1520.5(b)(8) of the interim final rule incorporates Sec. 1520.7(j) of the SSI regulation, which defines as SSI the specific details of aviation security measures applied by TSA or another entity, including details of the deployment and operations of Federal Air Marshals. The interim final rule expands this provision to cover specific details of transportation security measures applied in maritime transportation and includes security measures and protocols recommended by the Federal government. It also now includes information concerning the deployments, numbers, and operations of Coast Guard personnel engaged in maritime security duties and Federal Flight Deck Officers. This section covers the details of deployments, numbers, and operations of Federal Air Marshals only to the extent that such information is not national security classified information.

Section 1520.5(b)(9) of the interim final rule consolidates and expands the references now in Sec. 1520.7(m) through (q) of the SSI regulation to information about security screening. Section 1520.5(b)(9)(i) adds a new provision stating that SSI includes 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 pursuant to any aviation or maritime transportation security requirements of Federal law. This language is intended to clarify that aviation or maritime security screening procedures carried out not only by TSA, but also by other Federal or State government entities, or by private entities, such as operators of private air charter operations under TSA regulations, constitute SSI.

Section 1520.5(b)(9)(ii) adds a new provision clarifying that SSI includes information and sources of information used by a passenger or property screening program or system, including an automated screening system. This is intended to cover information used by a computerized passenger screening system, including lists of individuals identified as threats to transportation or national security.

Section 1520.5(b)(10) of the interim final rule adds a new provision clarifying that training materials detailing any aviation or maritime security measures required or recommended by DHS or DOT are SSI. These types of materials contain descriptions of screening equipment, particular screening methods, or security measures or countermeasures that a terrorist or other criminal could use to determine how to defeat security systems or procedures.

Section 1520.5(b)(11) of the interim final rule adds a new provision intended to safeguard lists of information about the identities of individuals who hold certain positions with aviation or maritime security responsibilities. It covers lists of information that would identify individuals as persons: (1) With unescorted access to secure or restricted areas of an airport or maritime facility, port area, or vessel; (2) acting as security screening personnel employed by or under contract to the Federal government pursuant to aviation or maritime transportation security requirements of Federal law, when aggregated by airport; and (3) acting as Federal Air Marshals, certain Coast Guard personnel engaged in maritime security duties. This section also covers names, whether or not part of a list, of current, former, and applicants to be Federal Flight Deck Officers. These types of individuals may be targeted by terrorists or other criminals to obtain their security identification cards or credentials or to obtain SSI, such as screening procedures or security training methods. Thus, information that personally identifies these individuals must be protected.

Section 1520.5(b)(12) of the interim final rule designates as SSI certain lists of critical aviation or maritime infrastructure assets prepared by Federal, State, or local government

agencies. Specifically, this provision covers any list identifying systems, facilities, or other assets, whether physical or virtual, so vital to the transportation system that the incapacity or destruction of such assets would have a debilitating impact on transportation security. This information constitutes SSI, however, only if it is either prepared by DHS or DOT or is prepared by a State or local agency and is submitted to DHS or DOT.

In the course of developing security measures for their transportation systems, State and local governments create lists of critical transportation systems, facilities, or other assets that may be vulnerable to attack. The compilation of these lists does not necessarily involve vulnerability assessments of each asset on the list. Therefore, the lists may not be protected as vulnerability

assessments under Sec. 1520.5(b)(5) of the interim final rule. Nonetheless, such lists should be SSI because their release to the public would increase the risk of attack on critical transportation assets. It would be impractical, however, to designate all lists of critical aviation and maritime transportation assets prepared by State or local governments as SSI. Therefore, the interim final rule establishes a clear standard to determine when such lists are covered. A list of critical aviation or maritime transportation infrastructure assets created by a State or local agency must be submitted to DHS or DOT in order to be SSI. Once submitted, the list constitutes SSI both in the hands of DHS or DOT and in the hands of the State or local agency that prepared it. Lists of such assets created by DHS or DOT also constitute SSI under this provision of the interim final rule.

Section 1520.5(b)(13) of the interim final rule designates as SSI any information involving the security of operational or administrative data systems that have been identified by DOT or DHS as critical to aviation or maritime transportation safety or security. This would include automated information security procedures and systems, vulnerability information concerning such systems, and security inspections. This addition is necessary to protect electronic data systems from cyberspace attacks.

As discussed previously, 49 U.S.C. 114(s)(1)(B) authorizes TSA to prescribe regulations restricting the disclosure of information that would ``reveal a trade secret or privileged or confidential commercial of financial information.'' TSA is adding a new provision to the SSI regulation that clarifies this authority.

In carrying out transportation security responsibilities, TSA procures security-related products and services, such as explosive detection equipment, risk-assessment systems, and security personnel services. TSA obtains these products and services through solicitations of proposals under a procurement process, through grants and cooperative agreements, and through other types of transactions. In addition, TSA receives unsolicited proposals offering security products and services. In many cases, materials submitted to TSA in the course of these transactions include details of existing or proposed transportation security measures, the disclosure of which would compromise the effectiveness of those measures. These materials also include trade secrets and other confidential commercial or financial information that the submitter would not disclose to the public. The Coast Guard and agencies within DOT such as the Research and Special Programs Administration, the Federal Railroad Administration, and the Federal Transit Administration also may obtain this type of information in the course of grant and procurement processes.

While this type of information is to some extent exempt from disclosure under FOIA, TSA is clarifying its independent authority under 49 U.S.C. 114(s)(1)(B) to protect this information as it relates to transportation security.

Section 1520.5(b)(14)(i) of the interim final rule designates as SSI proposals received by DHS or DOT, and negotiations arising therefrom, to perform work pursuant to a grant, contract, cooperative agreement, or other transaction, to the extent that the subject matter of the proposal relates to specific aviation or maritime transportation security measures. Section 1520.5(b)(14)(ii) covers 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. Section 1520.5(b)(14)(iii) covers 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, where the source of the information does not customarily disclose it to the public.

Section 1520.5(b)(15) of the interim final rule adds language clarifying the types of research and development information covered by the SSI regulation.

Section 1520.5(b)(16) carries forward in substance Sec. 1520.7(k) of the current SSI regulation, which provides that TSA may determine, on a case-by-case basis, that information or records not expressly listed in the SSI regulation are nonetheless subject to the non-disclosure requirements of the regulation. The interim final rule also adds language to cover the Secretary of DOT acting pursuant to the authority in 49 U.S.C. 40119.

Section 1520.5(c) adds a new provision clarifying that TSA may determine that certain information or records are not SSI even though they otherwise appear to be covered by one of the categories in Sec. 1520.5(b)(1) through (16). For example, this situation may arise in the case of a Security Directive containing security measures that become obsolete. Normally, the passage of time or the updating of security procedures or measures does not affect the SSI status of superseded security procedures. In most cases, key elements of the superseded procedures are carried forward or otherwise reflected in new procedures. In addition, where TSA rescinds a Security Directive because the particular threat it addresses has receded, TSA may reinstitute the security measures described in the directive to address threats that may arise in the future. Therefore, improper disclosure of the superseded or rescinded procedures would continue to be detrimental to transportation security. In some cases, however, security information that at one time was SSI is no longer in use, current procedures are not derived from that information, and TSA does not expect the information to have security implications in the future. Therefore, its disclosure would not be detrimental to transportation security, and it no longer meets the statutory criteria for designation as SSI. In cases where records or information no longer meet the statutory criteria, Sec. 1520.5(c) makes clear that TSA may determine that the information is no longer SSI.

Section 1520.7--Covered Persons

The interim final rule incorporates and revises the current provisions of the SSI regulation in Sec. 1520.5(a) that define the universe of entities and individuals that are subject to the regulation's requirements. Section 1520.5(a) currently covers: (1) Airport operators; (2) aircraft operators; (3) foreign air carriers; (4) indirect air carriers; (5) persons who received SSI as part of a legal enforcement action; (6) persons for whom a vulnerability assessment had been authorized, approved, or funded by DOT; and (7) persons employed by,

contracted to, or acting for any of the persons listed above.

The interim final rule adds references to various entities and individuals in maritime transportation, such as maritime vessel owners, charterers, and operators; owners and operators of maritime facilities; and persons participating in national or area security committees

established under the MTSA. In addition, rail operators, commuter authorities, pipeline operators, and other operators of transportation facilities may be covered persons if they are required by the Coast Guard to have a security plan.

Section 1520.7(e) of the interim final rule adds a provision clarifying that the SSI rule applies to persons performing the function of a computer reservation system (CRS) or global distribution system (GDS) for airline passenger information. CRSs and GDSs maintain electronic reservation systems used by aircraft operators. While these persons currently are covered by the SSI regulation under Sec. 1520.5(a)(1) because they are contracted to or acting for aircraft operators, the interim final rule is intended to clarify that CRSs and GDSs that have SSI in connection with passenger screening must protect that information in accordance with the SSI regulation. For instance, a CRS or GDS may have SSI related to the operation of the Computer Assisted Passenger Prescreening System.

Section 1520.7(g) of the interim final rule codifies TSA's current practice of sharing SSI with selected individuals working on behalf of trade associations pursuant to non-disclosure agreements.

Sections 1520.7(h) and (k) of the interim final rule expand the coverage of the SSI regulation to DHS, DOT, and their employees, contractors, grantees, and agents. These individuals currently are not covered by the SSI regulation, although in practice they may be required to take the same steps as covered persons to safeguard SSI, pursuant to agency order or other rule or by agreement. In addition, Federal employees are subject to general requirements governing the disclosure of information under FOIA and agency regulations. In many cases, however, the only consequence of improper disclosure of SSI for a Federal employee is the potential for disciplinary action.

In the interest of transportation security, employees of DHS and DOT, which are the departments that administer the SSI authority, should be required to follow the requirements of the SSI regulation to the same extent as other covered persons. Similarly, these employees should be subject to the same consequences for improper disclosure of SSI as regulated parties. Under Sec. 1520.7(k), contractors, grantees, and agents of DHS and DOT also are covered by the interim final rule. Therefore, Federal employees and persons performing contracts with, or who obtain SSI in connection with grants from, DHS or DOT are subject to civil penalties for non-compliance with part 1520.

As further discussed below, the SSI regulation permits disclosures of SSI to those persons who have a need to know. This is currently expressed in Sec. 1520.5(b) of the SSI regulation, which describes those categories of persons deemed to have a need to know. The interim final rule revises this provision in a new Sec. 1520.11. Section 1520.7(j) of the interim final rule adds a corresponding provision clarifying that individuals or entities who have a need to know, as described in new Sec. 1520.11, are covered persons and must comply with the requirements of the SSI regulation.

In some cases, an entity that is a covered person may be owned by a State or local government, and individuals covered by the regulation may be State or local employees. This is currently the case under part 1520, which applies to State or local airport operators and, therefore, to airport employees who may be State or local government employees and to other State or local employees carrying out security functions at an airport. For instance, the SSI regulation applies to airport police acting on behalf of the airport operator in fulfilling the airport operator's duty to provide law enforcement support under TSA's

regulations.

Similarly, under the interim final rule, some individuals who are covered persons may be State or local employees if they are employed by a transportation facility or operator that is a State or local government entity, such as a covered maritime facility. The interim final rule, however, does not cover State or local employees who are not employed by or acting for a covered entity. For instance, the interim final rule does not apply generally to State and local emergency response workers or law enforcement officers. There may be situations, however, where these types of individuals need access to SSI in order to prevent or respond to a transportation security incident. Therefore, TSA is considering whether to include additional State and local entities, such as emergency services providers and their employees, as covered persons. TSA requests comment on this issue.

Section 1520.9--Restrictions on the Disclosure of SSI

Section 1520.9 of the interim final rule incorporates the provisions of current Sec. 1520.5(a) and (c) of the SSI regulations. Section 1520.5(a) of the SSI regulation currently requires covered persons to restrict disclosure of and access to SSI to persons with a need to know and to refer requests by other persons for SSI to TSA or the applicable DOT administration. Section 1520.5(c) currently requires that when SSI is released to unauthorized persons, covered persons or individuals with knowledge of the release must inform DOT.

Section 1520.9 of the interim final rule adds new provisions specifying restrictions on the disclosure of SSI. Paragraph (a) requires all covered persons to restrict disclosure of and access to SSI to covered persons with a need to know and to refer requests for SSI by other persons to TSA or the applicable agency within DOT or DHS. These requirements are the same as the requirements in the current Sec. 1520.5(a), except for the reference to DHS.

Section 1520.9(a) of the interim final rule also requires covered persons to mark SSI as specified in Sec. 1520.13 of the interim final rule and to dispose of SSI as specified in Sec. 1520.19 of the interim final rule. These are new requirements. The marking requirement will ensure that persons handling records containing SSI are aware of the sensitive nature of the information in the records, the restrictions on release of the information, and the consequences of unauthorized release. The disposal requirement will ensure that copies and drafts of records containing SSI that are no longer needed are destroyed promptly.

Section 1520.9(b) of the interim final rule requires a covered person who receives a record containing SSI that is not marked as specified in Sec. 1520.13 to mark the record properly and inform the sender of the record that the record must be marked as specified in Sec. 1520.13 of the interim final rule. These requirements ensure that records containing SSI that inadvertently have been left unmarked are marked with the SSI notice and treated accordingly.

Section 1520.9(c) of the interim final rule requires that 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 agency. This requirement is currently contained in Sec. 1520.5(c) of the SSI regulation.

Section 1520.9(d) adds a provision clarifying that in the case of information that is both SSI and has been designated as CII 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.

While the interim final rule establishes a broad category of covered persons, as a practical matter many persons who fall within the coverage of the rule may not have possession of SSI and therefore would not be affected by the requirements of Sec. 1520.9.

Section 1520.11--Persons With a Need To Know

Currently, Sec. 1520.5(b) of the current SSI regulation specifies when a person has a need to know SSI. Under that section, a person has a need to know in each of the following circumstances: (1) When the person needs the SSI to carry out DOT-approved, accepted, or directed security duties; (2) when the person is in training to carry out DOT-approved, accepted, or directed security duties; (3) when the SSI is necessary for the person to supervise or manage persons carrying out DOT-approved, accepted, or directed security duties; (4) when the person needs the SSI to advise other covered persons regarding any DOT security-related requirements; and (5) when the person needs the SSI to represent covered persons in connection with any judicial or administrative proceeding regarding certain requirements. Section 1520.5(b) also currently specifies that for some specific SSI, TSA can make a finding that only specific persons or classes of persons have a need to know.

Section 1520.11(a) of the interim final rule maintains those five ``need to know'' categories with the following modifications. The phrase ``DOT-approved, accepted, or directed security duties'' in the first three categories is changed to ``aviation or maritime transportation security activities approved, accepted, funded, recommended, or directed by DHS or DOT.'' The fourth category is revised to read: ``when the person needs the information to provide technical or legal advice to a covered person regarding aviation or maritime transportation security requirements of Federal law.''

Section 1520.11(b) of the interim final rule adds new provisions describing when Federal employees and contractors have a need to know SSI. Section 1520.11(b)(1) provides that a Federal employee has a need to know SSI if access to the information is necessary for performance of the employee's official duties. Section 1520.11(b)(2) provides that a person acting in the performance of a contract with the Federal government has a need to know SSI if access to the information is necessary to performance of the contract.

Section 1520.11(c) adds a new provision permitting TSA or the Coast Guard to make an individual's access to SSI contingent upon completion of a security background check and the imposition of requirements or procedures for safeguarding SSI. The purpose of this change is to give TSA and the Coast Guard discretion to apply stricter safeguards in protecting SSI of a more sensitive nature or in ensuring that individuals who receive SSI do not pose a security threat or have a history of making improper disclosures of SSI.

Section 1520.11(d) of the interim final rule carries forward in substance Sec. 1520.5(b) of the current SSI regulation, providing that DHS or DOT may determine that for some types of SSI only specific

persons or classes of persons have a need to know.

Section 1520.13--Marking SSI

Currently, part 1520 does not contain any specific requirement to mark records as SSI. Marking of records, however, is an important means of protecting SSI from unauthorized disclosure. Therefore, Sec. 1520.13 of the interim final rule adds a new requirement specifying the marking requirements for records containing SSI. Records must be marked with both a protective marking and a distribution limitation statement. The protective marking reads ``SENSITIVE SECURITY INFORMATION''. The distribution limitation statement reads:

WARNING: This record contains Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a ``need to know'', as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 U.S.C. 552 and 49 CFR parts 15 and 1520.

Paper records must have the protective marking on the top and the distribution limitation statement on the bottom of: (1) The outside of any front and back cover, including a binder cover or folder; (2) any title page; and (3) each page of the document. Non-paper records must be marked clearly and conspicuously with the protective marking and distribution limitation statement, such that the viewer is reasonably likely to see or hear them when obtaining access to the contents of the record.

These marking requirements will ensure that persons handling records containing SSI are aware of the sensitive nature of the information contained in the records, the restrictions on release of the information, and the consequences of unauthorized release. As is the case under the current SSI regulation, however, records containing SSI that are not so marked are nonetheless subject to the requirements of the SSI regulation.

Section 1520.15--SSI Disclosed by TSA or the Coast Guard

Section 1520.3 of the current SSI regulation describes records and information that TSA withholds in response to a FOIA or other request for SSI. Section 1520.3(a) provides that notwithstanding FOIA or other laws, TSA does not release SSI to the public or make it available for public inspection or copying, with two exceptions.

First, under the current SSI regulation, if a record contains both information that is SSI and information that is not SSI, the latter information, on a proper FOIA request, is provided for public inspection and copying. However, if it is impractical to redact the requested information from the record, the entire record is withheld.

Second, after initiation of legal enforcement action, if the alleged violator or designated representative requests it, the TSA Chief Counsel, or designee, can provide copies of portions of the enforcement investigative report (EIR), including SSI. Such information is provided only to the alleged violator or designated representative and is not released under FOIA. Whenever such information is provided,

the Chief Counsel, or designee, currently is required to advise the alleged violator or designated representative that the documents are provided for the sole purpose of providing information necessary to respond to the allegations, and that SSI contained in the records provided must be maintained in a confidential manner to prevent compromising civil aviation security.

Section 1520.15 of the interim final rule carries forward provisions in the current SSI regulation stating that records containing SSI are exempt from disclosure under FOIA, and adds appropriate references to the Coast Guard. Section 1520.15 also makes clear, however, that records containing SSI are exempt from disclosure under

[[Page 28075]]

the Privacy Act (5 U.S.C. 552a), and other laws.

Under FOIA, Federal agencies are prohibited from disclosing to the public any record that is specifically exempted from disclosure by statute, where ``such statute (1) requires that the matters be withheld from the public in such a manner as to leave no discretion on the issue, or (2) establishes particular criteria for withholding or refers to particular types of matters to be withheld.'' See 5 U.S.C. 552(b)(3).

TSA's authority under 49 U.S.C. 114(s) constitutes a statute establishing ``particular criteria for withholding or refer[ing] to particular types of matters to be withheld.'' As discussed above, 49 U.S.C. 114(s) requires TSA to promulgate regulations prohibiting disclosure of information obtained or developed in carrying out security where disclosure would: (1) Be an unwarranted invasion of personal privacy; (2) reveal a trade secret or privileged or confidential commercial or financial information; or (3) be detrimental to the security of transportation. TSA's regulation at 49 CFR part 1520 implements this statutory requirement. Consequently, records containing SSI are exempt from disclosure under FOIA, to the extent disclosure is prohibited by 49 CFR part 1520. Moreover, this exemption applies regardless of whether the records are held by TSA, another component of DHS, or another Federal agency.

Section 1520.15 provides for several exceptions to the general rule against disclosure of SSI by TSA or the Coast Guard. The first exception is substantively the same as the first exception of current Sec. 1520.3. It provides that if a record contains both SSI and information that is not SSI, the record, on a proper FOIA or Privacy Act request, will be disclosed with the SSI redacted from the record, provided the record is not otherwise exempt from disclosure under FOIA or the Privacy Act.

The second exception applies to disclosure of SSI to a committee of Congress authorized to have the information as provided in 49 U.S.C. 114(s)(2), or to the General Accounting Office.

The third exception carries forward the existing procedures that provide fair access to SSI for respondents in enforcement proceedings, while ensuring that such access is balanced against security concerns raised by disclosing the information to individuals and entities that do not have a need to know the information. Specifically, Sec. 1520.15(d) of the interim final rule provides that in cases where TSA or the Coast Guard determines that a respondent needs access to SSI in order to prepare a response to allegations contained in a legal enforcement action document, the agency may provide the SSI to the

respondent, and may make the release contingent upon the respondent and the respondent's counsel completing a security background check. If the respondent or his counsel fails to satisfy the background check, TSA or the Coast Guard may limit or deny access to the SSI. If TSA or the Coast Guard releases SSI, the recipients become covered persons under the SSI regulation and must protect the SSI accordingly.

Section 1520.15(e) adds a new provision that makes express TSA's authority to determine on a case-by-case basis that a person who is not otherwise within the general categories of persons with a need to know SSI under Sec. 1520.11(a) has a need for access to SSI, and that granting access, subject to such safeguards as TSA may prescribe, will not be detrimental to transportation security. For instance, persons who are grantees or contractors of Federal agencies other than DHS or DOT may have a need to know SSI in order to carry out functions related to aviation or maritime transportation security. Section 1520.15(f) and (g) of the interim final rule makes clear that when TSA or the Coast Guard discloses SSI to a respondent or his counsel for use in responding to allegations contained in a legal enforcement action document, and when TSA makes a conditional disclosure under 1520.15(e), the recipients of the SSI become covered persons under the SSI regulation, and the disclosure is not a public release of information under FOIA.

Section 1520.15(h) makes clear that disclosure of information that is both SSI and has been designated as critical infrastructure information under section 214 of the Homeland Security Act is governed solely by the requirements of section 214 and any implementing regulations. As discussed above, a Federal agency or employee generally may not disclose information designated as CII under the CII Act, except within the Federal Government and to State and local governments in order to protect critical infrastructure.

Section 1520.17--Consequences of Unauthorized Disclosure of SSI

Section 1520.17 of the interim final rule specifies that the unauthorized disclosure of SSI is grounds for a civil penalty and other enforcement or corrective action by DOT or DHS, including appropriate personnel actions for Federal employees. This provision is currently contained in Sec. 1520.5(d) of the SSI regulation. Corrective action may include issuance of an order requiring retrieval of SSI to remedy unauthorized disclosure or an order to cease future unauthorized disclosure.

Section 1520.19--Destruction of SSI

Section 1520.19 of the interim final rule specifies the requirements for the destruction of SSI. Currently, part 1520 does not contain destruction requirements. However, such requirements are necessary to ensure that copies and drafts of records containing SSI that are no longer needed are destroyed promptly.

The interim final rule provides that DHS and DOT destroy SSI when no longer needed to carry out their functions. This requirement is subject to the requirements of the Federal Records Act (5 U.S.C. 105), including the duty to preserve records.

Other covered persons are required to destroy SSI completely to preclude recognition or reconstruction of the information when they no longer need the information to carry out transportation security measures, with one exception. A State or local government agency is not

required to destroy information that it is required to preserve under State or local law.

Good Cause for Immediate Adoption

TSA and OST are issuing this final rule without prior notice and opportunity for comment pursuant to the authority under section 4(a) of the Administrative Procedure Act (APA) (5 U.S.C. 553(b)). This provision allows an agency to issue a final rule without notice and opportunity for comment when the agency for good cause finds that notice and comment procedures are ``impracticable, unnecessary or contrary to the public interest.''

In response to the terrorist attacks of September 11, 2001, Congress enacted a series of statutes intended to strengthen homeland security, including the security of the transportation system. On November 19, 2001, the President signed into law ATSA, which established sweeping new security requirements for commercial air passenger transportation and assigned to TSA the responsibility for security in all modes of transportation. (Pub. L. 107-71). Over the past 24 months, TSA worked to meet congressional deadlines established in ATSA for the deployment of a Federal workforce to screen passengers and baggage in air transportation. On November 25, 2002, the President signed into law MTSA (Pub. L. 107-295), which established a new framework for maritime security, to

be implemented through national, regional, and facility- and vessel-specific security plans. On November 25, 2002, the President also signed into law HSA, which consolidated the components of the Federal Government responsible for security of the homeland into a single department. (Pub. L. 107-296).

TSA, the Coast Guard, and other components of DHS are working together to implement the maritime security measures required by MTSA under an expedited deadline established by Congress. These new transportation security measures have created an immediate need for the expansion of the existing legal protections governing SSI to include entities and individuals operating in maritime transportation. Under the MTSA, Congress directed DHS to issue interim rules as soon as practicable to implement the new security requirements for maritime facilities and vessels. (See 46 U.S.C. 70117). The Coast Guard issued final rules on October 22, 2003, that require vessel and maritime facility operators to prepare security plans. MTSA requires protection of these plans from public disclosure. (See 46 U.S.C. 70103(d)).

Currently, these types of documents are not subject to the disclosure limitations of TSA's SSI regulation, nor are the maritime facility or vessel operators subject to the regulation's requirements. Therefore, there currently is no legal framework for the protection of this type of information to prevent it from falling into the hands of those who may seek to do harm to the transportation system. Requirements for the protection of this information, including security measures adopted by operators on their own initiative, must be put in place now so that the information remains useful in carrying out security. Without a legal framework limiting the disclosure of security measures undertaken by maritime facility and vessel operators, there is an increased risk that those measures will become known by individuals who seek to disrupt transportation or use them to perpetrate attacks on

the U.S. In short, if the security plans and other security measures called for by Congress under the MTSA are not subject to the SSI regulation, there is a greater likelihood that those plans and measures may be defeated through their disclosure.

The existing SSI regulation currently provides the necessary information protection requirements in the case of individuals and entities operating in the aviation sector. The absence of such protections in other transportation sectors, however, has inhibited TSA from disseminating threat information to those in maritime transportation who need to act on it. In addition, it has inhibited maritime transportation operators from sharing their security plans with TSA.

As TSA and the Coast Guard begin to issue standards and required security measures and countermeasures to entities and individuals in maritime transportation pursuant to the MTSA and other applicable authorities, there must be a legal framework in place to ensure that those in possession of that information safeguard it from disclosure. The issuance of these security measures is imminent, and in some cases is already underway. Moreover, even before security measures are put in place, TSA and the Coast Guard have a need to provide security vulnerability and threat information to these entities that must be protected from disclosure.

For the foregoing reasons, there is a compelling need to expand the scope of the SSI rule to maritime transportation through the immediate issuance of a regulatory change to 49 CFR part 1520 and the establishment of parallel requirements implementing the authority of DOT under 49 U.S.C. 40119. In light of the need to protect the efficacy of maritime transportation security measures, it would be contrary to the public interest to delay the issuance of this regulatory change until after a public comment period. This action is necessary to prevent an imminent hazard to maritime transportation facilities and vessels, as well as persons and property within the United States.

Although there is good cause to forgo prior notice and comment procedures in issuing this rule, TSA and DOT are requesting public comments on all aspects of the rule. If, based upon information provided in public comments, TSA and DOT determine that changes to the rule are necessary to address transportation security more effectively, or in a less burdensome but equally effective manner, the agencies will not hesitate to make such changes.

Paperwork Reduction Act

The Paperwork Reduction Act of 1995 (44 U.S.C. 3507(d)) requires consideration of the impact of paperwork and other information collection burdens imposed on the public. TSA and DOT have determined that there are no new information collection requirements associated with this rule.

As protection provided by the Paperwork Reduction Act, as amended, an agency may not conduct or sponsor, and a person is not required to respond to, a collection of information unless it displays a currently valid Office of Management and Budget (OMB) control number.

Regulatory Impact Analyses

Changes to Federal regulations must undergo several economic analyses. First, Executive Order 12866, Regulatory Planning and Review

(58 FR 51735, October 4, 1993), directs each Federal agency to propose or adopt a regulation only upon a reasoned determination that the benefits of the intended regulation justify its costs. Second, the Regulatory Flexibility Act of 1980 (5 U.S.C. 601-612) requires agencies to analyze the economic impact of regulatory changes on small entities. Third, under the Trade Agreement Act of 1979, agencies must assess the effect of regulatory changes on international trade. Fourth, the Unfunded Mandates Reform Act of 1995 (2 U.S.C. 1531-1538) requires agencies to prepare a written assessment of the costs, benefits, and other effects of proposed or final rules that include a Federal mandate likely to result in the expenditure by State, local, or tribal governments, in the aggregate, or by the private sector, of $100 million or more annually (adjusted for inflation.)

Executive Order 12866 Assessment

Executive Order 12866 (58 FR 51735, October 4, 1993), provides for making determinations whether a regulatory action is ``significant'' and therefore subject to Office of Management and Budget (OMB) review and to the requirements of the Executive Order.

TSA and DOT have determined that this action is a significant regulatory action within the meaning of Executive Order 12866 because there is significant public interest in security issues since the events of September 11, 2001.

TSA has performed an analysis of the expected costs of this interim final rule. The interim final rule affects entities in the maritime transportation sector, including maritime facility and vessel owners and operators. The interim final rule requires that, when an affected person receives SSI, the person must take appropriate action to safeguard its contents and to destroy it when it is no longer needed. The interim final rule does not require the use of safes or enhanced security equipment or the use of a crosscut shredder. Rather, the interim final rule requires only that an affected person restrict disclosure of, and access to, the protected information to those with a need to know, and destroy such information when it is no longer needed. Under the rule, a locked drawer or cabinet is an acceptable

[[Page 28077]]

means of complying with the requirement to secure SSI, and a normal paper shredder or manual destruction are acceptable means of destroying SSI documents.

Costs

TSA believes that affected entities will incur minimal costs from complying with the interim final rule because, in practice, affected entities already have systems in place for securing sensitive commercial, trade secret, or personnel information, which are appropriate for safeguarding SSI. For instance, a normal filing cabinet with a lock may be used to safeguard SSI, and a normal paper shredder or manual destruction may be used to destroy SSI. Moreover, TSA does not expect compliance with the interim final rule will require affected entities to increase existing capacity to secure SSI. Accordingly, the agency estimates that there will be minimal costs associated with safeguarding SSI.

The agency has estimated the following costs for placing the

required protective marking and distribution limitation statement on records containing SSI.

For an electronic document, a person can place the required markings on each page with a few keystrokes. The agency estimates that there will be no costs associated with this action.

For a document that is already printed, a person can use a rubber stamp for the required markings. Such stamps can be custom ordered and last several years. For the protective marking, the agency estimates that the cost of a rubber stamp is from $9.90 (for a stamp 5 inches wide by \1/4\ inch high) to $10.25 (for a stamp 4\1/4\ inches wide by \1/4\ inch high). For the distribution limitation statement, the agency estimates that the cost of a rubber stamp is from $16.25 (for a stamp 6 inches wide by 1 inch high) to $33.25 (for a stamp 5\1/2\ inches wide by 2\1/2\ inches high). A single ink pad can be used for both stamps. A typical ink pad costs approximately $15.60. A two-ounce bottle of ink for the ink pad costs about $3.75.

For other types of record, such as maps, photos, DVDs, CD-ROMs, and diskettes, a person can use a label for the required markings. Labels typically cost from $7.87 (for 840 multipurpose labels) to $22.65 (for 225 diskette inkjet labels) to $34.92 (for 30 DVC/CD-ROM labels). These labels can be pre-printed with the required markings, or the affected person can print the required markings on an as-aves\rules.xmlneeded basis.

The interim final rule does not require a specific method for destroying SSI. Thus, a person may use any method of destruction, so long as it precludes recognition or reconstruction of the SSI. TSA believes that most affected entities already have the capability to destroy SSI in accordance with the requirements in this interim final rule. Thus, the agency estimates that there will be no costs associated with these destruction requirements.

Accordingly, TSA believes that the costs associated with this interim final rule are minimal.

Benefits

The primary benefit of the interim final rule will be the potential disruption of terrorist attacks on the aviation and maritime transportation sectors by ensuring that persons operating in those sectors protect SSI. TSA currently provides SSI, including threat information, security directives, and information circulars, to aircraft operators, airport operators, and other persons in the aviation sector that have a need to know, and to act upon, information about security concerns related to civil aviation. Some of these persons also produce information that is treated as SSI, such as airport security programs.

Prior to providing SSI to entities in maritime transportation, and to ensure that any information these entities produce that would be treated as SSI is safeguarded, TSA must ensure that those entities are under a legal obligation to protect the SSI from disclosure. Absent such an obligation, recipients and producers of SSI are not subject to the requirements in this rule to protect such information, which may undermine the effectiveness of security measures in preventing terrorist attacks. Therefore, TSA is amending the SSI regulation by adding entities in maritime transportation to the list of persons subject to the regulation.

TSA notes that the unauthorized disclosure of SSI can have a detrimental effect on the ability to thwart terrorist and other

criminal activities in the transportation sector. TSA also notes that the disclosure of some types of SSI that are restricted by this interim final rule, such as security training programs, security screening information, and vulnerability assessments, could aid the planning of a terrorist attack or other criminal activities.

The effectiveness of providing information of security concern to persons in maritime transportation, and of security measures developed by those persons, depends on strictly limiting access to the information to those persons who have a need to know. Given the minimal cost associated with this interim final rule and the potential benefits of preventing attacks on the transportation sector, TSA believes that this interim final rule will be cost beneficial.

Regulatory Flexibility Act Assessment

Pursuant to the Regulatory Flexibility Act (5 U.S.C. 601 et seq., as amended by the Small Business Regulatory Enforcement Fairness Act (SBREFA) of 1996), an agency is required to prepare and make available a regulatory flexibility analysis that describes the effect of the rule on small entities (i.e., small businesses, small organizations, and small governmental jurisdictions). Because good cause exists for issuing this regulation as an interim final rule, no regulatory flexibility analysis is required.

Although a regulatory flexibility analysis is not required, consideration was given to the effect of this interim final rule under the Regulatory Flexibility Act. As discussed above in the section on Executive Order 12866, this interim final rule will result in minimal costs to entities in the maritime transportation sector. Based on this analysis, TSA and DOT certify that this interim final rule will not have a significant economic impact on a substantial number of small entities.

Trade Impact Assessment

The Trade Agreement Act of 1979 prohibits Federal agencies from engaging in any standards or related activities that create unnecessary obstacles to the foreign commerce of the United States. Legitimate domestic objectives, such as safety and security, are not considered unnecessary obstacles. The Act also requires consideration of international standards and, where appropriate, that they be the basis for U.S. standards. TSA has assessed the potential effect of this amendment, and has determined that it will impose the same costs on domestic and international entities, and thus will have a neutral trade impact.

Unfunded Mandates Reform Act Assessment

Section 202 of the Unfunded Mandates Reform Act of 1995 (UMRA) requires Federal agencies to prepare a written assessment of the costs, benefits, and other effects of proposed or final rules that include a Federal mandate likely to result in the expenditure by State, local, or tribal governments, in the aggregate, or by the private sector, of more than $100 million in any one year (adjusted for inflation with base year of 1995). Before promulgating a rule for which a written statement is needed,

section 205 of the UMRA generally requires an agency to identify and consider a reasonable number of regulatory alternatives and adopt the least costly, most cost-effective, or least burdensome alternative that achieves the objective of the rule. The provisions of section 205 do not apply when they are inconsistent with applicable law. Moreover, section 205 allows an agency to adopt an alternative other than the least costly, most cost-effective, or least burdensome alternative if the agency publishes with the final rule an explanation why that alternative was not adopted.

This interim final rule will not result in the expenditure by State, local, or tribal governments, in the aggregate, or by the private sector, of more than $100 million annually. As discussed above in the section on Executive Order 12866, this interim final rule will result in minimal costs to entities in the transportation sector.

Executive Order 13132 (Federalism)

TSA has analyzed this rule under the principles and criteria of Executive Order 13132, Federalism. We determined that this action would not have a substantial direct effect on the States, on the relationship between the national government and the States, or on the distribution of power and responsibilities among the various levels of government. Therefore, we determined that this rule does not have federalism implications.

Environmental Analysis

TSA has reviewed this action for purposes of the National Environmental Policy Act of 1969 (NEPA) (42 U.S.C. 4321-4347) and has determined that this action will not have a significant effect on the human environment.

Energy Impact

The energy impact of this rule has been assessed in accordance with the Energy Policy and Conservation Act (EPCA), Public Law 94-163, as amended (42 U.S.C. 6362). We have determined that this rulemaking is not a major regulatory action under the provisions of the EPCA.

List of Subjects

49 CFR Part 15

Air carriers, Aircraft, Airports, Maritime carriers, Reporting and recordkeeping requirements, Security measures, Vessels.

49 CFR Part 1520

Air carriers, Aircraft, Airports, Maritime carriers, Reporting and recordkeeping requirements, Security measures, Vessels.

Department of Transportation

Office of the Secretary of Transportation

49 CFR Subtitle A

0
For the reasons stated in the preamble, the Department of Transportation amends subtitle A of title 49, Code of Federal Regulations, by adding a new part 15 to read as follows:

PART 15--PROTECTION OF SENSITIVE SECURITY INFORMATION

Authority: 49 U.S.C. 40119.

Sec. 15.1 Scope.

(a) Applicability. This part governs the maintenance, safeguarding, and disclosure of records and information that the Secretary of DOT has determined to be Sensitive Security Information, as defined in Sec. 15.5. This part does not apply to the maintenance, safeguarding, or disclosure of classified national security information, as defined by Executive Order 12968, or to other sensitive unclassified information that is not SSI, but that nonetheless may be exempt from public disclosure under the Freedom of Information Act. In addition, in the case of information that has been designated as critical infrastructure information under section 214 of the Homeland Security Act, the receipt, maintenance, or disclosure of such information by a Federal agency or employee is governed by section 214 and any implementing regulations, not by this part.

(b) Delegation. The authority of the Secretary under this part may be further delegated within DOT.

Sec. 15.3 Terms used in this part.

In addition to the terms in Sec. 15.3 of this chapter, the following terms apply in this part:

Administrator means the Under Secretary of Transportation for Security referred to in 49 U.S.C. 114(b), or his or her designee.

Coast Guard means the United States Coast Guard.

Covered person means any organization, entity, individual, or other person described in Sec. 15.7. In the case of an individual, covered person includes any individual applying for employment in a position that would be a covered person, or in training for such a position, regardless of whether that individual is receiving a wage, salary, or other form of payment. Covered person includes a person applying for certification or other form of approval that, if granted, would make the person a covered person described in Sec. 15.7.

DHS means the Department of Homeland Security and any directorate, bureau, or other component within the Department of Homeland Security, including the United States Coast Guard.

DOT means the Department of Transportation and any operating administration, entity, or office within the Department of Transportation, including the Saint Lawrence Seaway Development Corporation and the Bureau of Transportation Statistics.

Federal Flight Deck Officer means a pilot participating in the Federal Flight Deck Officer Program under 49 U.S.C. 44921 and implementing regulations.

Maritime facility means any facility as defined in 33 CFR part 101.

Record includes any means by which information is preserved, irrespective of format, including a book, paper, drawing, map, recording, tape, film, photograph, machine-readable material, and any information stored in an electronic format. The term record also includes any draft, proposed, or recommended change to any record.

Security contingency plan means a plan detailing response procedures to address a transportation security incident, threat assessment, or specific threat against transportation, including details of preparation, response, mitigation, recovery, and reconstitution procedures, continuity of government, continuity of transportation operations, and crisis management.

Security program means a program or plan and any amendments developed for the security of the following, including any comments, instructions, or implementing guidance:

(1) An airport, aircraft, or aviation cargo operation;

(2) A maritime facility, vessel, or port area; or

(3) A transportation-related automated system or network for information processing, control, and communications.

Security screening means evaluating a person or property to determine whether either poses a threat to security.

SSI means sensitive security information, as described in Sec. 15.5.

Threat image projection system means an evaluation tool that involves periodic presentation of fictional threat images to operators and is used in connection with x-ray or explosives detection systems equipment.

TSA means the Transportation Security Administration.

Vulnerability assessment means any review, audit, or other examination of the security of a transportation infrastructure asset; airport; maritime facility, port area, vessel, aircraft, train, commercial motor vehicle, or pipeline, or a transportation-related automated system or network, to determine its vulnerability to unlawful interference, whether during the conception, planning, design, construction, operation, or decommissioning phase. A vulnerability assessment may include proposed, recommended, or directed actions or countermeasures to address security concerns.

Sec. 15.5 Sensitive security information.

(a) In general. In accordance with 49 U.S.C. 40119(b)(1), SSI is information obtained or developed in the conduct of security activities, including research and development, the disclosure of which

the Secretary of DOT 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 transportation safety.

(b) Information constituting SSI. Except as otherwise provided in writing by the Secretary of DOT 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--

(i) Any aircraft operator or airport operator 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

(iv) Any security incident response plan established under 46 U.S.C. 70104.

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

(i) Issued by TSA under 49 CFR 1542.303, 1544.305, 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 or 1544.305, 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 weapon, explosive, incendiary, or destructive device 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 or maritime 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 or maritime 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.

(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 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, the Secretary of DOT may designate as SSI information not otherwise described in this section.

(c) Loss of SSI designation. The Secretary of DOT 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.

Sec. 15.7 Covered persons.

Persons subject to the requirements of part 15 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 Sec. 15.11.

(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 Sec. 1520.15(d) or (e).

Sec. 15.9 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 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 Sec. 15.13.

(5) Dispose of SSI as specified in Sec. 15.19.

(b) Unmarked SSI. If a covered person receives a record containing SSI that is not marked as specified in Sec. 1520.13, the covered person must--

(1) Mark the record as specified in Sec. 15.13; and

(2) Inform the sender of the record that the record must be marked as specified in Sec. 15.13.

(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.

Sec. 15.11 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.

(4) When the person needs the information to provide technical or legal advice to a covered person regarding aviation or maritime transportation security requirements of Federal law.

(5) When the person needs the information to represent a covered person in connection with any judicial or administrative proceeding regarding those requirements.

(b) Federal employees, contractors, and grantees. (1) A Federal employee has a need to know SSI if access to the information is necessary for performance of the employee's official duties.

(2) A person acting in the performance of a contract with or grant from DHS or DOT has a need to know SSI if access to the information is necessary to performance of the contract or grant.

(c) Background check. The Secretary of DOT may make an individual's access to the SSI contingent upon satisfactory completion of a security background check and the imposition of procedures and requirements for safeguarding SSI that are satisfactory to the Secretary.

(d) Need to know further limited by the DHS or DOT. For some specific SSI, DHS or DOT may make a finding that only specific persons

or classes of persons have a need to know.

Sec. 15.13 Marking SSI.

(a) Marking of paper records. In the case of paper records containing SSI, a covered person must mark the record by placing the protective marking conspicuously on the top, and the distribution limitation statement on the bottom, of--

(1) The outside of any front and back cover, including a binder cover or folder, if the document has a front and back cover;

(2) Any title page; and

(3) Each page of the document.

(b) Protective marking. The protective marking is: SENSITIVE SECURITY INFORMATION.

(c) Distribution limitation statement. The distribution limitation statement is:

WARNING: This record contains Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a ``need to know'', as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 U.S.C. 552 and 49 CFR parts 15 and 1520.

(d) Other types of records. In the case of non-paper records that contain SSI, including motion picture films, videotape recordings, audio recording, and electronic and magnetic records, a covered person must clearly and conspicuously mark the records with the protective marking and the distribution limitation statement such that the viewer or listener is reasonably likely to see or hear them when obtaining access to the contents of the record.

Sec. 15.15 SSI disclosed by DOT.

(a) In general. Except as otherwise provided in this section, and notwithstanding the Freedom of Information Act (5 U.S.C. 552), the Privacy Act (5 U.S.C. 552a), and other laws, records containing SSI are not available for public inspection or copying, nor does DOT release such records to persons without a need to know.

(b) Disclosure under the Freedom of Information Act and the Privacy Act. If a record contains both SSI and information that is not SSI, DOT, on a proper Freedom of Information Act or Privacy Act request, may disclose the record with the SSI redacted, provided the record is not otherwise exempt from disclosure under the Freedom of Information Act or Privacy Act.

(c) Disclosures to committees of Congress and the General Accounting Office. Nothing in this part precludes DOT from disclosing SSI to a committee of Congress authorized to have the information or to the Comptroller General, or to any authorized representative of the Comptroller General.

(d) Disclosure in enforcement proceedings. (1) In general. The

Secretary of DOT may provide SSI to a person in the context of an administrative enforcement proceeding when, in the sole discretion of the Secretary, access to the SSI is necessary for the person to prepare a response to allegations contained in a legal enforcement action document issued by DOT.

(2) Security background check. Prior to providing SSI to a person under paragraph (d)(1) of this section, the Secretary of DOT may require the individual or, in the case of an entity, the individuals representing the entity, and their counsel, to undergo and satisfy, in the judgment of the Secretary of DOT, a security background check.

(e) Other conditional disclosure. The Secretary of DOT may authorize a conditional disclosure of specific records or information that constitute SSI upon the written determination by the Secretary that disclosure of such records or information, subject to such limitations and restrictions as the Secretary may prescribe, would not be detrimental to transportation safety.

(f) Obligation to protect information. When an individual receives SSI pursuant to paragraph (d) or (e) of this section that individual becomes a covered person under Sec. 15.7 and is subject to the obligations of a covered person under this part.

(g) No release under FOIA. When DOT discloses SSI pursuant to paragraphs (b) through (e) of this section, DOT makes the disclosure for the sole purpose described in that paragraph. Such disclosure is not a public release of information under the Freedom of Information Act.

(h) Disclosure of Critical Infrastructure Information. Disclosure of information that is both SSI and has been designated as critical infrastructure information under section 214 of the Homeland Security Act is governed solely by the requirements of section 214 and any implementing regulations.

[[Page 28082]]

Sec. 15.17 Consequences of unauthorized disclosure of SSI.

Violation of this part is grounds for a civil penalty and other enforcement or corrective action by DOT, and appropriate personnel actions for Federal employees. Corrective action may include issuance of an order requiring retrieval of SSI to remedy unauthorized disclosure or an order to cease future unauthorized disclosure.

Sec. 15.19 Destruction of SSI.

(a) DOT. Subject to the requirements of the Federal Records Act (5 U.S.C. 105), including the duty to preserve records containing documentation of a Federal agency's policies, decisions, and essential transactions, DOT destroys SSI when no longer needed to carry out the agency's function.

(b) Other covered persons. (1) In general. A covered person must destroy SSI completely to preclude recognition or reconstruction of the information when the covered person no longer needs the SSI to carry out transportation security measures.

(2) Exception. Paragraph (b)(1) of this section does not require a State or local government agency to destroy information that the agency is required to preserve under State or local law.

Issued in Washington, DC, on May 6, 2004.
Norman Y. Mineta,
Secretary of Transportation.

Department of Homeland Security

Transportation Security Administration

49 CFR Chapter XII

0
For the reasons stated in the preamble, the Transportation Security Administration amends chapter XII of title 49, Code of Federal Regulations, by revising part 1520 to read as follows:

PART 1520--PROTECTION OF SENSITIVE SECURITY INFORMATION

Sec.

Authority: 46 U.S.C. 70102-70106, 70117; 49 U.S.C. 114, 40113, 44901-44907, 44913-44914, 44916-44918, 44935-44936, 44942, 46105.

Sec. 1520.1 Scope.

(a) Applicability. This part governs the maintenance, safeguarding, and disclosure of records and information that TSA has determined to be Sensitive Security Information, as defined in Sec. 1520.5. This part does not apply to the maintenance, safeguarding, or disclosure of classified national security information, as defined by Executive Order 12968, or to other sensitive unclassified information that is not SSI, but that nonetheless may be exempt from public disclosure under the Freedom of Information Act. In addition, in the case of information that has been designated as critical infrastructure information under section 214 of the Homeland Security Act, the receipt, maintenance, or disclosure of such information by a Federal agency or employee is governed by section 214 and any implementing regulations, not by this part.

(b) Delegation. The authority of TSA and the Coast Guard under this part may be further delegated within TSA and the Coast Guard, respectively.

Sec. 1520.3 Terms used in this part.

In addition to the terms in Sec. 1500.3 of this chapter, the following terms apply in this part:

Administrator means the Under Secretary of Transportation for Security referred to in 49 U.S.C. 114(b), or his or her designee.

Coast Guard means the United States Coast Guard.

Covered person means any organization, entity, individual, or other person described in Sec. 1520.7. In the case of an individual, covered person includes any individual applying for employment in a position that would be a covered person, or in training for such a position, regardless of whether that individual is receiving a wage, salary, or other form of payment. Covered person includes a person applying for certification or other form of approval that, if granted, would make the person a covered person described in Sec. 1520.7.

DHS means the Department of Homeland Security and any directorate, bureau, or other component within the Department of Homeland Security, including the United States Coast Guard.

DOT means the Department of Transportation and any operating administration, entity, or office within the Department of Transportation, including the Saint Lawrence Seaway Development Corporation and the Bureau of Transportation Statistics.

Federal Flight Deck Officer means a pilot participating in the Federal Flight Deck Officer Program under 49 U.S.C. 44921 and implementing regulations.

Maritime facility means any facility as defined in 33 CFR part 101.

Record includes any means by which information is preserved, irrespective of format, including a book, paper, drawing, map, recording, tape, film, photograph, machine-readable material, and any information stored in an electronic format. The term record also includes any draft, proposed, or recommended change to any record.

Security contingency plan means a plan detailing response procedures to address a transportation security incident, threat assessment, or specific threat against transportation, including details of preparation, response, mitigation, recovery, and reconstitution procedures, continuity of government, continuity of transportation operations, and crisis management.

Security program means a program or plan and any amendments, developed for the security of the following, including any comments, instructions, or implementing guidance:

(1) An airport, aircraft, or aviation cargo operation;

(2) A maritime facility, vessel, or port area; or

(3) A transportation-related automated system or network for information processing, control, and communications.

Security screening means evaluating a person or property to determine whether either poses a threat to security.

SSI means sensitive security information, as described in Sec. 1520.5.

Threat image projection system means an evaluation tool that involves periodic presentation of fictional threat images to operators and is used in connection with x-ray or explosives detection systems equipment.

TSA means the Transportation Security Administration.

Vulnerability assessment means any review, audit, or other examination of the security of a transportation infrastructure asset; airport; maritime facility, port area, vessel, aircraft, train, commercial motor vehicle, or pipeline, or a transportation-related automated system or network, to determine its vulnerability to unlawful interference, whether during the conception, planning, design, construction, operation, or decommissioning phase. A vulnerability assessment may include proposed, recommended, or directed actions or

countermeasures to address security concerns.

Sec. 1520.5 Sensitive security information.

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

[[Page 28083]]

(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--
(i) Any aircraft operator or airport operator 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
(iv) Any security incident response plan established under 46 U.S.C. 70104.
(2) Security Directives. Any Security Directive or order--
(i) Issued by TSA under 49 CFR 1542.303, 1544.305, 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, 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 weapon, explosive, incendiary, or destructive device 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 or maritime 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 or maritime 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.

(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 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.

Sec. 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 Sec. 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 Sec. 1520.15(d) or (e).

Sec. 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 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 Sec. 1520.13.

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

(b) Unmarked SSI. If a covered person receives a record containing SSI that is not marked as specified in Sec. 1520.13, the covered person must--

(1) Mark the record as specified in Sec. 1520.13; and

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

Sec. 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.

[[Page 28085]]

(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.

(4) When the person needs the information to provide technical or legal advice to a covered person regarding aviation or maritime transportation security requirements of Federal law.

(5) When the person needs the information to represent a covered person in connection with any judicial or administrative proceeding regarding those requirements.

(b) Federal employees, contractors, and grantees. (1) A Federal employee has a need to know SSI if access to the information is necessary for performance of the employee's official duties.

(2) A person acting in the performance of a contract with or grant from DHS or DOT has a need to know SSI if access to the information is necessary to performance of the contract or grant.

(c) Background check. TSA or Coast Guard may make an individual's access to the SSI contingent upon satisfactory completion of a security background check or other procedures and requirements for safeguarding SSI that are satisfactory to TSA or the Coast Guard.

(d) Need to know further limited by the DHS or DOT. For some specific SSI, DHS or DOT may make a finding that only specific persons or classes of persons have a need to know.

Sec. 1520.13 Marking SSI.

(a) Marking of paper records. In the case of paper records containing SSI, a covered person must mark the record by placing the protective marking conspicuously on the top, and the distribution limitation statement on the bottom, of--

(1) The outside of any front and back cover, including a binder cover or folder, if the document has a front and back cover;

(2) Any title page; and

(3) Each page of the document.

(b) Protective marking. The protective marking is: SENSITIVE SECURITY INFORMATION.

(c) Distribution limitation statement. The distribution limitation statement is:

WARNING: This record contains Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a ``need to know'', as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 U.S.C. 552 and 49 CFR parts 15 and 1520.

(d) Other types of records. In the case of non-paper records that contain SSI, including motion picture films, videotape recordings, audio recording, and electronic and magnetic records, a covered person must clearly and conspicuously mark the records with the protective marking and the distribution limitation statement such that the viewer or listener is reasonably likely to see or hear them when obtaining access to the contents of the record.

Sec. 1520.15 SSI disclosed by TSA or the Coast Guard.

(a) In general. Except as otherwise provided in this section, and notwithstanding the Freedom of Information Act (5 U.S.C. 552), the Privacy Act (5 U.S.C. 552a), and other laws, records containing SSI are not available for public inspection or copying, nor does TSA or the Coast Guard release such records to persons without a need to know.

(b) Disclosure under the Freedom of Information Act and the Privacy Act. If a record contains both SSI and information that is not SSI, TSA

or the Coast Guard, on a proper Freedom of Information Act or Privacy Act request, may disclose the record with the SSI redacted, provided the record is not otherwise exempt from disclosure under the Freedom of Information Act or Privacy Act.

(c) Disclosures to committees of Congress and the General Accounting Office. Nothing in this part precludes TSA or the Coast Guard from disclosing SSI to a committee of Congress authorized to have the information or to the Comptroller General, or to any authorized representative of the Comptroller General.

(d) Disclosure in enforcement proceedings. (1) In general. TSA or the Coast Guard may provide SSI to a person in the context of an administrative enforcement proceeding when, in the sole discretion of TSA or the Coast Guard, as appropriate, access to the SSI is necessary for the person to prepare a response to allegations contained in a legal enforcement action document issued by TSA or the Coast Guard.

(2) Security background check. Prior to providing SSI to a person under paragraph (d)(1) of this section, TSA or the Coast Guard may require the individual or, in the case of an entity, the individuals representing the entity, and their counsel, to undergo and satisfy, in the judgment of TSA or the Coast Guard, a security background check.

(e) Other conditional disclosure. TSA may authorize a conditional disclosure of specific records or information that constitute SSI upon the written determination by TSA that disclosure of such records or information, subject to such limitations and restrictions as TSA may prescribe, would not be detrimental to transportation security.

(f) Obligation to protect information. When an individual receives SSI pursuant to paragraph (d) or (e) of this section that individual becomes a covered person under Sec. 1520.7 and is subject to the obligations of a covered person under this part.

(g) No release under FOIA. When TSA discloses SSI pursuant to paragraphs (b) through (e) of this section, TSA makes the disclosure for the sole purpose described in that paragraph. Such disclosure is not a public release of information under the Freedom of Information Act.

(h) Disclosure of Critical Infrastructure Information. Disclosure of information that is both SSI and has been designated as critical infrastructure information under section 214 of the Homeland Security Act is governed solely by the requirements of section 214 and any implementing regulations.

Sec. 1520.17 Consequences of unauthorized disclosure of SSI.

Violation of this part is grounds for a civil penalty and other enforcement or corrective action by DHS, and appropriate personnel actions for Federal employees. Corrective action may include issuance of an order requiring retrieval of SSI to remedy unauthorized disclosure or an order to cease future unauthorized disclosure.

Sec. 1520.19 Destruction of SSI.

(a) DHS. Subject to the requirements of the Federal Records Act (5 U.S.C. 105), including the duty to preserve records containing documentation of a Federal agency's policies, decisions, and essential transactions, DHS destroys SSI when no longer needed to carry out the agency's function.

(b) Other covered persons. (1) In general. A covered person must destroy SSI completely to preclude recognition or reconstruction of the information when the covered person no longer needs the SSI to carry out transportation security measures.

(2) Exception. Paragraph (b)(1) of this section does not require a State or local government agency to destroy

information that the agency is required to preserve under State or local law.

Issued in Arlington, VA, on May 6, 2004.
David M. Stone,
Acting Administrator, Transportation Security Administration.
[FR Doc. 04-11142 Filed 5-17-04; 8:45 am]

BILLING CODE 4910-62-P