DRAFT CBP/TSA May 22, 2003: Do not disseminate without the express prior written approval of the CBP, Office of Chief Counsel, (202) 927-6900 and TSA-ONRA, (240) 568-5665.

UNDERTAKINGS OF
THE UNITED STATES BUREAU OF CUSTOMS AND BORDER PROTECTION
AND
THE UNITED STATES TRANSPORTATION SECURITY ADMINISTRATION

In support of the plan of the European Commission (EC) to exercise the powers conferred on it by Article 25(6) of Directive 95/46/EC (the Directive) and to adopt a decision recognizing the United States Bureau of Customs and Border Protection (CBP) and the Transportation Security Administration (TSA) as providing adequate protection for the purposes of air carrier and Global Distribution System (GDS) transfers of Passenger[1] Name Record (PNR) data which may fall within the scope of the Directive, CBP and TSA undertake as follows:

Legal Authority to Obtain PNR[2]

1) The Bureau of Customs and Border Protection (CBP): by legal statute (title 49, United States Code, section 44909(c)(3)) and its implementing (interim) regulations (title 19, Code of Federal Regulations, section 122.49b), each air carrier operating passenger flights in foreign air transportation to or from the United States, must provide CBP (formerly, the U.S. Customs Service) with electronic access to PNR data to the extent it is collected and contained in the air carrier's automated reservation/departure control systems ("reservation systems");

2) The Transportation Security Administration (TSA): by legal statute, the Aviation and Transportation Security Act of 2001 (ATSA), TSA is required to evaluate all passengers before they board an aircraft using a computer assisted passenger prescreening system. 49 U.S.C. § 44903(j)(2)(A). ATSA gives TSA broad authority to issue regulations or orders necessary to carry out its screening and security functions. 49 U.S.C. §§ 114(1), 40113(a). TSA intends to exercise this authority by requiring air carriers and GDSs to provide TSA access to the passenger information needed by TSA to conduct passenger prescreening;

Use of PNR Data by CBP and TSA

3) Most data elements contained in PNR data can be obtained by CBP upon examining a data subject's airline ticket and other travel documents pursuant to its normal border control authority, but the ability to receive this data electronically will significantly enhance CBP's ability to facilitate *bona fide* travel and conduct efficient and effective advance risk assessment of passengers;

4) Information required by TSA to carry out its passenger screening function must be obtained well before the boarding of the aircraft. Electronic access to PNR information will enable TSA to obtain the required passenger information in a timely fashion to ensure the safety of all passengers. 49 U.S.C. §§ 114(l), 44905(b);

---

[1] For the purposes of these Undertakings, the terms "passenger" and "passengers" shall include crew members.

[2] See Attachment "A" hereof for copies of pertinent legal authorities.

5) PNR data is used by CBP strictly for preventing and combating terrorism and serious criminal offenses, with the principal purpose of facilitating CBP's mission to protect the borders through threat analysis to identify and interdict persons who have committed or may potentially commit a terrorist act. TSA will use PNR data for the limited purpose of detecting known and previously unknown persons with terrorist connections who are attempting to fly on commercial air transportation into, out of, through or within the United States. Use of PNR data for these purposes permits the agencies to focus their resources on high risk concerns, thereby facilitating and safeguarding *bona fide* travel;

Data Requirements

6) Data elements which CBP and TSA require (or will require) are listed herein at Attachment "B". (Such identified elements are hereinafter referred to as "PNR" for purposes of these Undertakings);

7) CBP and TSA will consult with the EC regarding revision of the required PNR data elements (Attachment "B"), prior to effecting any such revision, if the agencies become aware of additional PNR fields that airlines or GDSs may add to their systems whichwould significantly enhance the agencies' abilities to conduct passenger risk assessments or if circumstances indicate that a previously non-required PNR field will be needed to fulfill the limited purposes referred to in paragraph 5 of these Undertakings.

Treatment of "Sensitive" Data

8) CBP and TSA are committed to filtering sensitive data (i.e. personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and the processing of data concerning health or sex life of the individual) from the PNR on their own initiative and with the least possible delay, but are willing to also discuss development and implementation of such filters by the air carriers and GDSs;

9) Until such filters can be implemented (either by the air carriers or by CBP and TSA), TSA represents that it does not and will not use sensitive data in its automated pre-screening process (CAPPS II) and CBP represents that it does not and will not use such data to identify potential subjects for CBP border examination. With respect to sensitive PNR data that has been transferred by air carriers to CBP, should it become necessary for CBP to use such sensitive data for purposes of preventing and combating terrorism and serious criminal offenses, any such use will be subject to specific approval procedures, involving the U.S. Deputy Commissioner of CBP, in consultation with the DHS Chief Privacy Officer. Should the U.S. Deputy Commissioner of CBP authorize access to sensitive PNR data, the DHS Chief Privacy Officer will notify the EC regarding the fact that sensitive PNR data was accessed, and the general reasons for the access;[3]

[3] See paragraph 13 of these Undertakings for discussion of retention of sensitive PNR data.

Methods of Accessing PNR Data

10) Both CBP and TSA are components of the Directorate of Border and Transportation Security (BTS) within the Department of Homeland Security (DHS). In the interest of streamlining access to PNR data by these agencies, and to minimize any burden placed upon the air carriers and GDSs which must comply with these overlapping PNR access requirements, CBP and TSA intend to access PNR data from airline reservation and departure control systems ("reservation systems"), and GDSs,[4] through a single electronic portal. The standards for system security through the single portal will at all times equal or exceed the security standards as represented herein;

a) With regard to the PNR data which CBP accesses (or receives) directly from the air carrier's reservation systems for purposes of identifying potential subjects for border examination, CBP personnel will only access (or receive) and use PNR data concerning persons whose travel includes a flight into, out of, or through the United States;

b) With regard to the PNR data which TSA accesses (or receives) directly from the air carrier's reservation systems and the Global Distribution Systems (GDS), or through CBP, for purposes of conducting security pre-screening of air passengers, TSA will only access (or receive) and use PNR data concerning persons whose travel includes a flight into, out of, through or within the United States;

11) CBP or TSA will “pull” passenger information from air carriers and GDSs until such time as air carriers and GDSs are able to implement a system to “push” the data to CBP or TSA.

12) CBP or TSA will pull PNR data associated with a particular flight no earlier than 72 hours prior to the departure of that flight, and will re-check the systems no more than three (3) times between the initial pull and the flight's departure to or from (and in the case of CBP, arrival in) the United States, to identify any changes in the information. In the event that the air carriers and GDSs obtain the ability to "push" PNR data, CBP and TSA would need to receive the data 72 hours prior to departure of the flight, provided that changes to the PNR data which are made between that point and the time of the flight’s arrival in or departure from the U.S., are also pushed to CBP or TSA.[5] In the unusual event that CBP obtains advance information that person(s) of specific concern may be travelling on a flight to, from or through the U.S., CBP may pull (or request a particular push) of PNR data prior to 72 hours before departure of the flight to ensure

[4] Unlike CBP, TSA has the authority to obtain PNR data regarding flights "within" the United States and also has the authority to obtain PNR data from the GDSs for persons whose travel includes a flight into, out of, through or within the United States. 49 U.S.C. § 44901. Except for persons charged with maintaining and auditing the CBP computer systems, CBP personnel would be blocked under any single portal system from direct access to data that is outside the scope of its authority.

[5] In the event that the air carriers and GDSs agree to push the PNR data to CBP and TSA, the agencies will engage in discussions with the air carriers and GDSs regarding the possibility of pushing PNR data at periodic intervals between 72 hours before departure of the flight and the flight’s arrival in or departure from the United States. CBP and TSA seek to utilize a method of pushing the necessary PNR data that meets the agencies’ needs for effective risk assessment, while minimizing the economic impact upon air carriers and GDSs.

proper enforcement action may be taken when essential to prevent or combat a terrorist act or serious criminal offense. To the extent practicable, in such instances where PNR data must be accessed by CBP prior to 72 hours before the departure of the flight, CBP will utilize customary law enforcement channels;

Storage of PNR Data

13) Subject to the approval of the National Archives and Records Administration (44 U.S.C. 2101, et seq.), CBP will limit on-line access to PNR data to authorized CBP users[6] for a period of seven (7) days, after which the number of officers authorized to access the PNR data will be even further limited for a period of 7 (seven) years.[7] After seven (7) years, PNR data that has not been manually accessed during that period of time, will be destroyed. PNR data which has been manually accessed during the initial seven (7) year period will be transferred by CBP to a deleted record file,[8] where it will remain for a period of eight (8) years before it is destroyed. This schedule, however, would not apply to PNR data which is linked to a specific enforcement record (such data would remain accessible until the enforcement record is archived). In the case of TSA, PNR data will be retained in its computer system for purposes of identity authentication for seven (7) years after completion of travel. During this time, on-line access to PNR data will be restricted to a limited number of TSA employees assigned to the CAPPS II project, who have a specific need to know.

CBP and TSA Computer System Security

14) Authorized CBP personnel obtain access to PNR through the closed CBP intranet system which is encrypted end-to-end and the connection is controlled by the Customs Data Center. PNR data stored in the CBP database is limited to "read only" access by authorized personnel, meaning that the substance of the data may be programmatically reformatted, but will not be substantively altered in any manner by CBP once accessed from an air carrier's reservation system;

15) PNR data in TSA databases, as a general rule, will not be accessed at all by TSA employees, with all authentication and risk assessment being done by computer. Other than possibly adding an encrypted risk assessment score to PNR data, TSA will not modify or alter passenger information;

---

[6] These authorized CBP users would include employees assigned to analytical units in the field offices, as well as employees assigned to the National Targeting Center. As indicated previously, persons charged with maintaining, developing or auditing the CBP database will also have access to such data for those limited purposes during the initial (seven) 7 day period following access.

[7] After the seven (7) day period following initial access to the particular PNR data, on-line access by CBP will be limited to employees assigned to the National Targeting Center. See also footnote 6 regarding access for maintenance, development and auditing of the computer system.

[8] Although the PNR record is not technically deleted when it is transferred to the Deleted Record File, it is stored as raw data (not a readily searchable form and, therefore, of no use for "traditional" law enforcement investigations) and is only available to authorized personnel in the Office of Internal Affairs for CBP (and in some cases the Office of the Inspector General in connection with audits) and personnel responsible for maintaining the database in CBP's Office of Information Technology, on a "need to know" basis.

16) No other foreign, federal, state or local agency has direct electronic access to PNR data through CBP or TSA databases (including through the Integrated Border Information System (IBIS));

17) Details regarding access to information in CBP databases (such as who, where, when (date and time) and any revisions to the data) are automatically recorded and routinely audited by the Office of Internal Affairs to prevent unauthorized use of the system. The CAPPS II database and system are subject to real time auditing; accordingly, when a TSA employee accesses the system, the access account, as well as time of access and changes made to system parameters, will be automatically noted. Access by either agency or its employees through the single portal would be controlled in the same manner;

18) Only certain CBP and TSA officers, employees or information technology contractors[9] (under CBP or TSA supervision) who have successfully completed a background investigation, have an active, password-protected account in the CBP or CAPPS II computer systems, and have a recognized official purpose for reviewing PNR data, may access PNR data;

19) CBP officers, employees and contractors are required to complete security and data privacy training, including passage of a test, on a biennial basis. TSA officers, employees and contractors are required to complete security and data privacy training on an annual basis. CBP and CAPPS II system auditing is used to monitor and ensure compliance with all privacy and data security requirements.

20) Unauthorized access by CBP and TSA personnel to air carrier reservation systems or the CBP or TSA computerized systems which store PNR is subject to strict disciplinary action (which may include termination of employment) and may result in criminal sanctions being imposed (fines, imprisonment of up to one year, or both) (see title 18, United States Code, section 1030);

21) CBP policy and regulations also provide for stringent disciplinary action (which may include termination of employment) to be taken against any CBP employee who discloses information from CBP's computerized systems without official authorization (title 19, Code of Federal Regulations, section 103.34). TSA employment standards provide that any TSA employee, who without authorization obtains access to or discloses information from TSA computerized systems, is subject to strict disciplinary action (which may include termination of employment).[10]

22) Criminal penalties (including fines, imprisonment of up to one year, or both) may be assessed against any officer or employee of the United States for disclosing PNR data obtained in the course of his employment, where such disclosure is not authorized by law (see title 18, United States Code, sections 641, 1030, 1905);

[9] Access by "contractors" to any PNR data contained in the CBP or TSA computer systems would be confined to persons under contract with either agency to assist in the maintenance or development of that agency's computer system.

[10] TSA employment standards referenced here are pending final approval by TSA.

DRAFT CBP/TSA May 22, 2003: Do not disseminate without the express prior written approval of the CBP, Office of Chief Counsel, (202) 927-6900 and TSA-ONRA, (240) 568-5665.

CBP and TSA Treatment and Protection of PNR Data

23) CBP and TSA treat PNR information regarding persons of any nationality or country of residence as law enforcement sensitive, confidential personal information of the data subject, and confidential commercial information of the air carrier or GDS, and, therefore, would not make disclosures of such data to the public, except as provided in these Undertakings;

24) Public disclosure of PNR data is generally governed by the Freedom of Information Act (FOIA) (title 5, United States Code, section 552) which permits any person (regardless of nationality or country of residence) access to a U.S. federal agency's records, except to the extent such records (or a portion thereof) are protected from public disclosure by an applicable exemption under the FOIA. Among its exemptions, the FOIA permits an agency to withhold a record (or a portion thereof) from disclosure where the information is confidential commercial information, where disclosure of the information would constitute a clearly unwarranted invasion of personal privacy, or where the information is compiled for law enforcement purposes, to the extent that disclosure may reasonably be expected to constitute an unwarranted invasion of personal privacy (title 5, United States Code, sections 552(b)(4), (6), (7)(C));

25) CBP regulations (title 19, Code of Federal Regulations, section 103.12), which govern the processing of requests for information (such as PNR data) pursuant to the FOIA, specifically provide that (subject to certain limited exceptions in the case of requests by the data subject) the disclosure requirements of the FOIA are not applicable to CBP records relating to (1) confidential commercial information, (2) material involving personal privacy where the disclosure would constitute a clearly unwarranted invasion of personal privacy; and (3) information compiled for law enforcement purposes, where disclosure could reasonably be expected to constitute an unwarranted invasion of personal privacy.[11] In processing requests under the FOIA, TSA would as a matter of policy withhold information on the same grounds as CBP;

26) CBP and TSA will take the position in connection with any administrative or judicial proceeding arising out of a FOIA request for PNR information accessed from air carriers or GDSs, that such records are exempt from disclosure under the FOIA;

Transfer of PNR Data to Other Government Authorities

27) With the exception of transfers between CBP and TSA (which jointly make representations herein in support of the European Commission Decision and have independent legal authority to collect PNR data), Department of Homeland Security (DHS) components will be treated as "third agencies", subject to the same rules and conditions for sharing of PNR data as other government authorities outside DHS;

28) CBP or TSA, in its discretion, will only provide PNR data to other government authorities with counter-terrorism or law enforcement functions, on a case-by-case basis,

[11] CBP (and TSA) would invoke these exemptions uniformly, without regard to the nationality or country of residence of the subject of the data.

for purposes of preventing and combating terrorism or other serious criminal offenses. (Authorities with whom CBP or TSA may share such data shall hereinafter be referred to as the "Designated Authorities");

29) For purposes of regulating the dissemination of PNR data which may be shared with other Designated Authorities, CBP or TSA, as applicable, is considered the "owner" of the data and such Designated Authorities are obligated by the express terms of disclosure to (1) use the PNR data only for the purposes set forth in paragraph 28 or 34 herein, as applicable (2) ensure the orderly disposal of PNR information that has been received, consistent with the Designated Authority's record retention procedures, and (3) obtain the "owner" agency's express authorization for any further dissemination. Failure to respect the conditions for transfer may be investigated and reported by the DHS Chief Privacy Officer and may make the Designated Authority ineligible to receive subsequent transfers of PNR from CBP and TSA;

30) Persons employed by such Designated Authorities who without appropriate authorization disclose PNR data, may be liable for criminal sanctions (title 18, United States Code, sections 641, 1030, 1905);

31) Each disclosure of PNR data by CBP and TSA will be conditioned upon the receiving agency's treatment of this data as confidential commercial information and law enforcement sensitive, confidential personal information of the data subject, as identified in paragraphs 24 and 25 hereof, which should be treated as exempt from disclosure under the Freedom of Information Act (5 U.S.C. 552). Further, the recipient agency will be advised that further disclosure of such information is not permitted without the express prior approval of CBP or TSA, as appropriate. CBP and TSA will not authorize any further transfer of PNR data for purposes other than those identified in paragraphs 28, 34 or 35 herein;

32) CBP and TSA will judiciously exercise their discretion to transfer PNR data for the stated purposes. CBP and TSA will first determine if the reason for disclosing the PNR data to another Designated Authority fits within the stated purpose (see paragraph 28 herein). If so, CBP or TSA will determine whether that Designated Authority is responsible for preventing, investigating or prosecuting the violations of, or enforcing or implementing, a statute or regulation related to that purpose, where CBP or TSA is aware of an indication of a violation or potential violation of law. The merits of disclosure will need to be reviewed in light of all the circumstances presented;

33) Additionally, before sensitive PNR data may be transferred by CBP to other Designated Authorities, such transfer must be necessary to the purposes identified in paragraphs 28 or 34, and will be subject to specific approval procedures outlined in paragraph 9 of these Undertakings;

34) No statement herein shall impede the use or disclosure of PNR data to relevant government authorities, where such disclosure is necessary for the protection of the vital interests of the data subject or of other persons, in particular as regards significant health risks. Disclosures for these purposes will be subject to the same conditions for transfers set forth in paragraphs 29-31 and 33 of these Undertakings;

35) No statement in these Undertakings shall impede the use or disclosure of PNR data in any criminal judicial proceedings or as otherwise required by law. CBP and TSA will advise the EC regarding the passage of any U.S. legislation which materially affects the statements made in these Undertakings;

Notice, Access and Opportunities for Redress for PNR Data Subjects

36) CBP and TSA will provide information to the traveling public regarding the PNR requirement and the issues associated with its use (i.e., general information regarding the authority under which the data is collected, the purpose for the collection, protection of the data, data sharing, the identity of the responsible official, procedures available for redress and contact information for persons with questions or concerns, etc., for posting on CBP and TSA website(s), in travel pamphlets, etc.);

37) Requests by the data subject (also known as "first party requesters") to receive a copy of PNR data contained in CBP or TSA databases regarding the data subject are processed under the Freedom of Information Act (FOIA).[12] In the case of a first-party request, the fact that CBP and TSA otherwise consider PNR data to be confidential personal information of the data subject and confidential commercial information of the air carrier will not be used by CBP or TSA as a basis under FOIA for withholding PNR data from the data subject;

38) In certain exceptional circumstances, CBP and TSA may exercise their authority under FOIA to deny or postpone disclosure of all (or, more likely, part) of the PNR record to a first party requester, pursuant to title 5, United States Code, section 552(b) (e.g., if disclosure under FOIA "could reasonably be expected to interfere with enforcement proceedings" or "would disclose techniques and procedures for law enforcement investigations...[which] could reasonably be expected to risk circumvention of the law"). Under FOIA, any requester has the authority to administratively and judicially challenge the agency's decision to withhold information (see 5 U.S.C. 552(a)(4)(B); 19 CFR 103.7-103.9; 6 CFR 5.9);

39) CBP and TSA will undertake to rectify[13] data at the request of passengers and crewmembers, air carriers or EU data protection authorities (to the extent specifically authorized by the data subject), where CBP or TSA determines that such data is contained in their respective database and a correction is justified and properly supported. CBP and TSA will inform any Designated Authority which has received such PNR data of any material rectification of that PNR data;

[12] The procedures for requesting information from CBP and TSA pursuant to the FOIA are explained in title 19, Code of Federal Regulations, Part 103, subpart A, and title 6, Code of Federal Regulations, Part 5, respectively.

[13] By "rectify", CBP and TSA wish to make clear that they will not be authorized to revise the data within the PNR record that they access from the air carriers or GDSs. Rather, a separate record linked to the PNR record will be created to note that the data was determined to be inaccurate and the proper correction. In the case of CBP, the agency will annotate the passenger's secondary examination record to reflect that certain data in the PNR may be or is inaccurate.

DRAFT CBP/TSA May 22, 2003: Do not disseminate without the express prior written approval of the CBP, Office of Chief Counsel, (202) 927-6900 and TSA-ONRA, (240) 568-5665.

a) Requests for rectification directed to CBP may be made to its Office of Field Operations in Washington, D.C.;

b) Requests for rectification by TSA may be made through a TSA ombudsman or passenger advocate who will be appointed to address any questions or concerns raised by CAPPS II;

40) Complaints by individuals about the handling of their PNR data may be made, either directly or via the relevant Data Protection Authority (to the extent specifically authorized by the data subject), as follows:

a) complaints directed to CBP may be made to its Office of Field Operations in Washington, D.C.;

b) complaints directed to TSA may be made through a TSA ombudsman or passenger advocate who will be appointed to address any questions or concerns raised by CAPPS II;

In the event that a complaint cannot be resolved by CBP and TSA, the complaint may be directed to the DHS Chief Privacy Officer, who will review the situation and endeavor to resolve the complaint. The DHS Chief Privacy Officer will include in her report to Congress issues regarding the number, the substance and the resolution of complaints regarding the handling of personal data, such as PNR.[14]

Compliance Issues

41) CBP, TSA and the European Commission (EC) will consult with each other on a regular basis concerning compliance with the Undertakings, consistent with US law and practice. Such discussions would include the results of any audits or other findings regarding, in particular, sharing of PNR data with Designated Authorities and personnel access to PNR information in CBP and TSA databases. Audits concerning CBP and TSA access to and use of PNR data which may be conducted by the DHS Chief Privacy Officer,[15] the DHS Office of the Inspector General (OIG), or the General Accounting Office (GAO), would be available to the EC and any other interested person, to the extent they are made public;

42) CBP and TSA will issue regulations, directives or other policy documents incorporating the statements herein, to ensure compliance with these Undertakings by CBP and TSA officers, employees and contractors. As indicated herein, failure of CBP and TSA officers, employees and contractors to abide by their agency's policies incorporated therein may result in strict disciplinary measures being taken, and criminal sanctions, as applicable;

[14] Pursuant to section 222 of the Homeland Security Act of 2002 (Public Law 107-296, dated November 25, 2002), the Privacy Officer for DHS is charged with conducting a "privacy impact assessment" of proposed rules of the Department on "on the privacy of personal information, including the type of personal information collected and the number of people affected" and must report to Congress on an annual basis regarding the "activities of the Department that affect privacy...."

[15] See footnote 14, discussing the reporting mandates of the DHS Chief Privacy Officer.

Reciprocity

43) In the event that the European Union decides to adopt an airline passenger identification system similar to that of the U.S. Government, which requires all air carriers and GDSs to provide European authorities with access to PNR data for persons whose current travel itinerary includes a flight to, from, through or within the European Union, CBP and TSA would encourage U.S.-based airlines to cooperate.

Attachment "A"
U.S. Legal Authorities

49 USCS § 44909 (2003)

§ 44909. Passenger manifests

(a) Air carrier requirements.
(1) Not later than March 16, 1991, the Secretary of Transportation shall require each air carrier to provide a passenger manifest for a flight to an appropriate representative of the Secretary of State--
(A) not later than one hour after that carrier is notified of an aviation disaster outside the United States involving that flight; or
(B) if it is not technologically feasible or reasonable to comply with clause (A) of this paragraph, then as expeditiously as possible, but not later than 3 hours after the carrier is so notified.
(2) The passenger manifest should include the following information:
(A) the full name of each passenger.
(B) the passport number of each passenger, if required for travel.
(C) the name and telephone number of a contact for each passenger.
(3) In carrying out this subsection, the Secretary of Transportation shall consider the necessity and feasibility of requiring air carriers to collect passenger manifest information as a condition for passengers boarding a flight of the carrier.

(b) Foreign air carrier requirements. The Secretary of Transportation shall consider imposing a requirement on foreign air carriers comparable to that imposed on air carriers under subsection (a)(1) and (2) of this section.

(c) Flights in foreign air transportation to the United States.
(1) In general. Not later than 60 days after the date of enactment of the Aviation and Transportation Security Act [enacted Nov. 19, 2001], each air carrier and foreign air carrier operating a passenger flight in foreign air transportation to the United States shall provide to the Commissioner of Customs by electronic transmission a passenger and crew manifest containing the information specified in paragraph (2). Carriers may use the advanced passenger information system established under section 431 of the Tariff Act of 1930 *(19 U.S.C. 1431)* to provide the information required by the preceding sentence.
(2) Information. A passenger and crew manifest for a flight required under paragraph (1) shall contain the following information:
(A) The full name of each passenger and crew member.
(B) The date of birth and citizenship of each passenger and crew member.
(C) The sex of each passenger and crew member.
(D) The passport number and country of issuance of each passenger and crew member if required for travel.
(E) The United States visa number or resident alien card number of each passenger and crew member, as applicable.
(F) Such other information as the Under Secretary, in consultation with the Commissioner of Customs, determines is reasonably necessary to ensure aviation safety.

(3) Passenger name records. The carriers shall make passenger name record information available to the Customs Service upon request.

(4) Transmission of manifest. Subject to paragraph (5), a passenger and crew manifest required for a flight under paragraph (1) shall be transmitted to the Customs Service in advance of the aircraft landing in the United States in such manner, time, and form as the Customs Service prescribes.

(5) Transmission of manifests to other Federal agencies. Upon request, information provided to the Under Secretary or the Customs Service under this subsection may be shared with other Federal agencies for the purpose of protecting national security.

HISTORY: (July 5, 1994, P.L. 103-272, § 1(e), 108 Stat. 1211.) (As amended April 5, 2000, P.L. 106-181, Title VII, § 718, 114 Stat. 163; Nov. 19, 2001, P.L. 107-71, Title I, § 115, 115 Stat. 623.)

DRAFT CBP/TSA May 22, 2003: Do not disseminate without the express prior written approval of the CBP, Office of Chief Counsel, (202) 927-6900 and TSA-ONRA, (240) 568-5665.

19 CFR 122.49b

§ 122.49b Passenger Name Record (PNR) information.

(a) General requirement. Each air carrier, foreign and domestic, operating a passenger flight in foreign air transportation to or from the United States, including flights to the United States where the passengers have already been pre-inspected or pre-cleared at the foreign location for admission to the U.S., must, upon request, provide Customs with electronic access to certain Passenger Name Record (PNR) information, as defined and described in paragraph (b) of this section. In order to readily provide Customs with such access to requested PNR information, each air carrier must ensure that its electronic reservation/departure control systems correctly interface with the U.S. Customs Data Center, Customs Headquarters, as prescribed in paragraph (c)(1) of this section.

(b) PNR information defined; PNR information that Customs may request.

(1) PNR information defined. Passenger Name Record (PNR) information refers to reservation information contained in an air carrier's electronic reservation system and/or departure control system that sets forth the identity and travel plans of each passenger or group of passengers included under the same reservation record with respect to any flight covered by paragraph (a) of this section.

(2) PNR data that Customs may request. The air carrier, upon request, must provide Customs with electronic access to any and all PNR data elements relating to the identity and travel plans of a passenger concerning any flight under paragraph (a) of this section, to the extent that the carrier in fact possesses the requested data elements in its reservation system and/or departure control system. There is no requirement that the carrier collect any PNR information under this paragraph, that the carrier does not otherwise collect on its own and maintain in its electronic reservation/departure control systems.

(c) Required carrier system interface with Customs Data Center to facilitate Customs retrieval of requested PNR data. (1) Carrier requirements for interface with Customs. Within the time specified in paragraph (c)(2) of this section, each air carrier must fully and effectively interface its electronic reservation/departure control systems with the U.S. Customs Data Center, Customs Headquarters, in order to facilitate Customs ability to retrieve needed Passenger Name Record data from these electronic systems. To effect this interface between the air carrier's electronic reservation/departure control systems and the Customs Data Center, the carrier must:

(i) Provide Customs with an electronic connection to its reservation system and/or departure control system. (This connection can be provided directly to the Customs Data Center, Customs Headquarters, or through a third party vendor that has such a connection to Customs.);

(ii) Provide Customs with the necessary airline reservation/departure control systems' commands that will enable Customs to:

(A) Connect to the carrier's reservation/departure control systems;

(B) Obtain the carrier's schedules of flights;

(C) Obtain the carrier's passenger flight lists; and

(D) Obtain data for all passengers listed for a specific flight; and

(iii) Provide technical assistance to Customs as required for the continued full and effective interface of the carrier's electronic reservation/departure control systems with the Customs Data Center, in order to ensure the proper response from the carrier's systems to requests for data that are made by Customs.

(2) Time within which carrier must interface with Customs Data Center to facilitate Customs access to requested PNR data. Any air carrier which has not taken steps to fully and effectively interface its electronic reservation/departure control systems with the Customs Data Center must do so, as prescribed in paragraphs (c)(1)(i)-(c)(1)(iii) of this section, within 30 days from the date that Customs contacts the carrier and requests that the carrier effect such an interface. After being contacted by Customs, if an air carrier determines it needs more than 30 days to properly interface its automated database with the Customs Data Center, it may apply in writing to the Assistant Commissioner, Office of Field Operations (OFO) for an extension. Following receipt of the application, the Assistant Commissioner, OFO, may, in writing, allow the carrier an extension of this period for good cause shown. The Assistant Commissioner's decision as to whether and/or to what extent to grant such an extension is within the sole discretion of the Assistant Commissioner and is final.

(d) Sharing of PNR information with other Federal agencies. Passenger Name Record information as described in paragraph (b)(2) of this section that is made available to Customs electronically may, upon request, be shared with other Federal agencies for the purpose of protecting national security *(49 U.S.C. 44909*(c)(5). Customs may also share such data as otherwise authorized by law.

HISTORY: [T.D. 02-33, *67 FR 42710, 42712,* June 25, 2002]

AUTHORITY: AUTHORITY NOTE APPLICABLE TO ENTIRE PART:

5 U.S.C. 301; 19 U.S.C. 58b, 66, 1431, 1433, 1436, 1448, 1459, 1590, 1594, 1623, 1624, 1644, 1644a.

§ 122.49a also issued under *49 U.S.C. 1431* and *49 U.S.C. 44909*(c).

§ 122.49b also issued under *49 U.S.C. 44909*(c).

NOTES: [EFFECTIVE DATE NOTE: *67 FR 42710, 42712,* June 25, 2002, added this section, effective June 25, 2002.]

DRAFT CBP/TSA May 22, 2003: Do not disseminate without the express prior written approval of the CBP, Office of Chief Counsel, (202) 927-6900 and TSA-ONRA, (240) 568-5665.

49 USCS § 114 (2003)

§ 114. Transportation Security Administration

(a) In general. The Transportation Security Administration shall be an administration of the Department of Transportation.

(b) Under Secretary.
(1) Appointment. The head of the Administration shall be the Under Secretary of Transportation for Security. The Under Secretary shall be appointed by the President, by and with the advice and consent of the Senate.
(2) Qualifications. The Under Secretary must--
(A) be a citizen of the United States; and
(B) have experience in a field directly related to transportation or security.
(3) Term. The term of office of an individual appointed as the Under Secretary shall be 5 years.

(c) Limitation on ownership of stocks and bonds. The Under Secretary may not own stock in or bonds of a transportation or security enterprise or an enterprise that makes equipment that could be used for security purposes.

(d) Functions. The Under Secretary shall be responsible for security in all modes of transportation, including--
(1) carrying out chapter 449 [*49 USCS § § 44901* et seq.], relating to civil aviation security, and related research and development activities; and
(2) security responsibilities over other modes of transportation that are exercised by the Department of Transportation.

(e) Screening operations. The Under Secretary shall--
(1) be responsible for day-to-day Federal security screening operations for passenger air transportation and intrastate air transportation under sections 44901 and 44935;
(2) develop standards for the hiring and retention of security screening personnel;
(3) train and test security screening personnel; and
(4) be responsible for hiring and training personnel to provide security screening at all airports in the United States where screening is required under section 44901, in consultation with the Secretary of Transportation and the heads of other appropriate Federal agencies and departments.

(f) Additional duties and powers. In addition to carrying out the functions specified in subsections (d) and (e), the Under Secretary shall--
(1) receive, assess, and distribute intelligence information related to transportation security;
(2) assess threats to transportation;
(3) develop policies, strategies, and plans for dealing with threats to transportation security;
(4) make other plans related to transportation security, including coordinating countermeasures with appropriate departments, agencies, and instrumentalities of the United States Government;

(5) serve as the primary liaison for transportation security to the intelligence and law enforcement communities;

(6) on a day-to-day basis, manage and provide operational guidance to the field security resources of the Administration, including Federal Security Managers as provided by section 44933;

(7) enforce security-related regulations and requirements;

(8) identify and undertake research and development activities necessary to enhance transportation security;

(9) inspect, maintain, and test security facilities, equipment, and systems;

(10) ensure the adequacy of security measures for the transportation of cargo;

(11) oversee the implementation, and ensure the adequacy, of security measures at airports and other transportation facilities;

(12) require background checks for airport security screening personnel, individuals with access to secure areas of airports, and other transportation security personnel;

(13) work in conjunction with the Administrator of the Federal Aviation Administration with respect to any actions or activities that may affect aviation safety or air carrier operations;

(14) work with the International Civil Aviation Organization and appropriate aeronautic authorities of foreign governments under section 44907 to address security concerns on passenger flights by foreign air carriers in foreign air transportation; and

(15) carry out such other duties, and exercise such other powers, relating to transportation security as the Under Secretary considers appropriate, to the extent authorized by law.

(g) National emergency responsibilities.

(1) In general. Subject to the direction and control of the Secretary, the Under Secretary, during a national emergency, shall have the following responsibilities:

(A) To coordinate domestic transportation, including aviation, rail, and other surface transportation, and maritime transportation (including port security).

(B) To coordinate and oversee the transportation-related responsibilities of other departments and agencies of the Federal Government other than the Department of Defense and the military departments.

(C) To coordinate and provide notice to other departments and agencies of the Federal Government, and appropriate agencies of State and local governments, including departments and agencies for transportation, law enforcement, and border control, about threats to transportation.

(D) To carry out such other duties, and exercise such other powers, relating to transportation during a national emergency as the Secretary shall prescribe.

(2) Authority of other departments and agencies. The authority of the Under Secretary under this subsection shall not supersede the authority of any other department or agency of the Federal Government under law with respect to transportation or transportation-related matters, whether or not during a national emergency.

(3) Circumstances. The Secretary shall prescribe the circumstances constituting a national emergency for purposes of this subsection.

(h) Management of security information. In consultation with the Transportation Security Oversight Board, the Under Secretary shall--

(1) enter into memoranda of understanding with Federal agencies or other entities to share or otherwise cross-check as necessary data on individuals identified on Federal agency databases who may pose a risk to transportation or national security;

(2) establish procedures for notifying the Administrator of the Federal Aviation Administration, appropriate State and local law enforcement officials, and airport or airline security officers of the identity of individuals known to pose, or suspected of posing, a risk of air piracy or terrorism or a threat to airline or passenger safety;

(3) in consultation with other appropriate Federal agencies and air carriers, establish policies and procedures requiring air carriers--

(A) to use information from government agencies to identify individuals on passenger lists who may be a threat to civil aviation or national security; and

(B) if such an individual is identified, notify appropriate law enforcement agencies, prevent the individual from boarding an aircraft, or take other appropriate action with respect to that individual; and

(4) consider requiring passenger air carriers to share passenger lists with appropriate Federal agencies for the purpose of identifying individuals who may pose a threat to aviation safety or national security.

(i) View of NTSB. In taking any action under this section that could affect safety, the Under Secretary shall give great weight to the timely views of the National Transportation Safety Board.

(j) Acquisitions.

(1) In general. The Under Secretary is authorized--

(A) to acquire (by purchase, lease, condemnation, or otherwise) such real property, or any interest therein, within and outside the continental United States, as the Under Secretary considers necessary;

(B) to acquire (by purchase, lease, condemnation, or otherwise) and to construct, repair, operate, and maintain such personal property (including office space and patents), or any interest therein, within and outside the continental United States, as the Under Secretary considers necessary;

(C) to lease to others such real and personal property and to provide by contract or otherwise for necessary facilities for the welfare of its employees and to acquire, maintain, and operate equipment for these facilities;

(D) to acquire services, including such personal services as the Secretary determines necessary, and to acquire (by purchase, lease, condemnation, or otherwise) and to construct, repair, operate, and maintain research and testing sites and facilities; and

(E) in cooperation with the Administrator of the Federal Aviation Administration, to utilize the research and development facilities of the Federal Aviation Administration.

(2) Title. Title to any property or interest therein acquired pursuant to this subsection shall be held by the Government of the United States.

(k) Transfers of funds. The Under Secretary is authorized to accept transfers of unobligated balances and unexpended balances of funds appropriated to other Federal agencies (as such term is defined in section 551(1) of title 5) to carry out functions transferred, on or after the date of enactment of the Aviation and Transportation Security Act, by law to the Under Secretary.

(l) Regulations.

(1) In general. The Under Secretary is authorized to issue, rescind, and revise such regulations as are necessary to carry out the functions of the Administration.

(2) Emergency procedures.

(A) In general. Notwithstanding any other provision of law or executive order (including an executive order requiring a cost-benefit analysis), if the Under Secretary determines that a regulation or security directive must be issued immediately in order to protect transportation security, the Under Secretary shall issue the regulation or security directive without providing notice or an opportunity for comment and without prior approval of the Secretary.

(B) Review by Transportation Security Oversight Board. Any regulation or security directive issued under this paragraph shall be subject to review by the Transportation Security Oversight Board established under section 115. Any regulation or security directive issued under this paragraph shall remain effective for a period not to exceed 90 days unless ratified or disapproved by the Board or rescinded by the Under Secretary.

(3) Factors to consider. In determining whether to issue, rescind, or revise a regulation under this section, the Under Secretary shall consider, as a factor in the final determination, whether the costs of the regulation are excessive in relation to the enhancement of security the regulation will provide. The Under Secretary may waive requirements for an analysis that estimates the number of lives that will be saved by the regulation and the monetary value of such lives if the Under Secretary determines that it is not feasible to make such an estimate.

(4) Airworthiness objections by FAA.

(A) In general. The Under Secretary shall not take an aviation security action under this title if the Administrator of the Federal Aviation Administration notifies the Under Secretary that the action could adversely affect the airworthiness of an aircraft.

(B) Review by Secretary. Notwithstanding subparagraph (A), the Under Secretary may take such an action, after receiving a notification concerning the action from the Administrator under subparagraph (A), if the Secretary of Transportation subsequently approves the action.

(m) Personnel and services; cooperation by Under Secretary.

(1) Authority of under secretary. In carrying out the functions of the Administration, the Under Secretary shall have the same authority as is provided to the Administrator of the Federal Aviation Administration under subsections (l) and (m) of section 106.

(2) Authority of agency heads. The head of a Federal agency shall have the same authority to provide services, supplies, equipment, personnel, and facilities to the Under Secretary as the head has to provide services, supplies, equipment, personnel, and facilities to the Administrator of the Federal Aviation Administration under section 106(m).

(n) Personnel management system. The personnel management system established by the Administrator of the Federal Aviation Administration under section 40122 shall apply to employees of the Transportation Security Administration, or, subject to the requirements of such section, the Under Secretary may make such modifications to the personnel management system with respect to such employees as the Under Secretary considers appropriate, such as adopting aspects of other personnel systems of the Department of Transportation.

(o) Acquisition management system. The acquisition management system established by the Administrator of the Federal Aviation Administration under section 40110 shall apply to acquisitions of equipment, supplies, and materials by the Transportation Security Administration, or, subject to the requirements of such section, the Under Secretary may make such modifications to the acquisition management system with respect to such acquisitions of equipment, supplies, and materials as the Under Secretary considers appropriate, such as adopting aspects of other acquisition management systems of the Department of Transportation.

(p) Authority of Inspector General. The Transportation Security Administration shall be subject to the Inspector General Act of 1978 (5 U.S.C. App.) and other laws relating to the authority of the Inspector General of the Department of Transportation.

(q) Law enforcement powers.

(1) In general. The Under Secretary may designate an employee of the Transportation Security Administration or other Federal agency to serve as a law enforcement officer.

(2) Powers. While engaged in official duties of the Administration as required to fulfill the responsibilities under this section, a law enforcement officer designated under paragraph (1) may--

(A) carry a firearm;

(B) make an arrest without a warrant for any offense against the United States committed in the presence of the officer, or for any felony cognizable under the laws of the United States if the officer has probable cause to believe that the person to be arrested has committed or is committing the felony; and

(C) seek and execute warrants for arrest or seizure of evidence issued under the authority of the United States upon probable cause that a violation has been committed.

(3) Guidelines on exercise of authority. The authority provided by this subsection shall be exercised in accordance with guidelines prescribed by the Under Secretary, in consultation with the Attorney General of the United States, and shall include adherence to the Attorney General's policy on use of deadly force.

(4) Revocation or suspension of authority. The powers authorized by this subsection may be rescinded or suspended should the Attorney General determine that the Under Secretary has not complied with the guidelines prescribed in paragraph (3) and conveys the determination in writing to the Secretary of Transportation and the Under Secretary.

(r) Authority to exempt. The Under Secretary may grant an exemption from a regulation prescribed in carrying out this section if the Under Secretary determines that the exemption is in the public interest.

(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 [*49 USCS § § 44901* et seq.] 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.

(2) Availability of information to Congress. Paragraph (1) does not authorize information to be withheld from a committee of Congress authorized to have the information.

(3) Limitation on transferability of duties. Except as otherwise provided by law, the Under Secretary may not transfer a duty or power under this subsection to another department, agency, or instrumentality of the United States.

HISTORY: (Added Nov. 19, 2001, P.L. 107-71, Title I, § 101(a), 115 Stat. 597; Nov. 25, 2002, P.L. 107-296, Title XVI, § 1601(b), Title XVII, § 1707, 116 Stat. 2312, 2318; Feb. 20, 2003, P.L. 108-7, Div I, Title III, § 351(d), 117 Stat. 420.)

49 USCS § 44903 (2003)

§ 44903. Air transportation security

(a) Definition. In this section, "law enforcement personnel" means individuals--
(1) authorized to carry and use firearms;
(2) vested with the degree of the police power of arrest the Under Secretary of Transportation for Security considers necessary to carry out this section; and
(3) identifiable by appropriate indicia of authority.

(b) Protection against violence and piracy. The Under Secretary shall prescribe regulations to protect passengers and property on an aircraft operating in air transportation or intrastate air transportation against an act of criminal violence or aircraft piracy. When prescribing a regulation under this subsection, the Under Secretary shall--
(1) consult with the Secretary of Transportation, the Attorney General, the heads of other departments, agencies, and instrumentalities of the United States Government, and State and local authorities;
(2) consider whether a proposed regulation is consistent with--
(A) protecting passengers; and
(B) the public interest in promoting air transportation and intrastate air transportation;
(3) to the maximum extent practicable, require a uniform procedure for searching and detaining passengers and property to ensure--
(A) their safety; and
(B) courteous and efficient treatment by an air carrier, an agent or employee of an air carrier, and Government, State, and local law enforcement personnel carrying out this section; and
(4) consider the extent to which a proposed regulation will carry out this section.

(c) Security programs.
(1) The Under Secretary shall prescribe regulations under subsection (b) of this section that require each operator of an airport regularly serving an air carrier holding a certificate issued by the Secretary of Transportation to establish an air transportation security program that provides a law enforcement presence and capability at each of those airports that is adequate to ensure the safety of passengers. The regulations shall authorize the operator to use the services of qualified State, local, and private law enforcement personnel. When the Under Secretary decides, after being notified by an operator in the form the Under Secretary prescribes, that not enough qualified State, local, and private law enforcement personnel are available to carry out subsection (b), the Under Secretary may authorize the operator to use, on a reimbursable basis, personnel employed by the Under Secretary, or by another department, agency, or instrumentality of the Government with the consent of the head of the department, agency, or instrumentality, to supplement State, local, and private law enforcement personnel. When deciding whether additional personnel are needed, the Under Secretary shall consider the number of passengers boarded at the airport, the extent of anticipated risk of criminal violence or aircraft piracy at the airport or to the air carrier aircraft operations at the airport, and the availability of qualified State or local law enforcement personnel at the airport.

(2) (A) The Under Secretary may approve a security program of an airport operator, or an amendment in an existing program, that incorporates a security program of an airport tenant (except an air carrier separately complying with part 108 or 129 of title 14, Code of Federal Regulations) having access to a secured area of the airport, if the program or amendment incorporates--

(i) the measures the tenant will use, within the tenant's leased areas or areas designated for the tenant's exclusive use under an agreement with the airport operator, to carry out the security requirements imposed by the Under Secretary on the airport operator under the access control system requirements of section 107.14 of title 14, Code of Federal Regulations, or under other requirements of part 107 of title 14; and

(ii) the methods the airport operator will use to monitor and audit the tenant's compliance with the security requirements and provides that the tenant will be required to pay monetary penalties to the airport operator if the tenant fails to carry out a security requirement under a contractual provision or requirement imposed by the airport operator.

(B) If the Under Secretary approves a program or amendment described in subparagraph (A) of this paragraph, the airport operator may not be found to be in violation of a requirement of this subsection or subsection (b) of this section when the airport operator demonstrates that the tenant or an employee, permittee, or invitee of the tenant is responsible for the violation and that the airport operator has complied with all measures in its security program for securing compliance with its security program by the tenant.

(C) Maximum use of chemical and biological weapon detection equipment. The Secretary of Transportation may require airports to maximize the use of technology and equipment that is designed to detect or neutralize potential chemical or biological weapons.

(3) Pilot programs. The Administrator [Under Secretary] shall establish pilot programs in no fewer than 20 airports to test and evaluate new and emerging technology for providing access control and other security protections for closed or secure areas of the airports. Such technology may include biometric or other technology that ensures only authorized access to secure areas.

(d) Authorizing individuals to carry firearms and make arrests. With the approval of the Attorney General and the Secretary of State, the Secretary of Transportation may authorize an individual who carries out air transportation security duties--

(1) to carry firearms; and

(2) to make arrests without warrant for an offense against the United States committed in the presence of the individual or for a felony under the laws of the United States, if the individual reasonably believes the individual to be arrested has committed or is committing a felony.

(e) Exclusive responsibility over passenger safety. The Under Secretary has the exclusive responsibility to direct law enforcement activity related to the safety of passengers on an aircraft involved in an offense under section 46502 of this title from the moment all external doors of the aircraft are closed following boarding until those doors are opened to allow passengers to leave the aircraft. When requested by the Under Secretary, other departments, agencies, and instrumentalities of the Government shall provide assistance necessary to carry out this subsection.

(f) Government and industry consortia. The Under Secretary may establish at airports such consortia of government and aviation industry representatives as the Under Secretary may designate to provide advice on matters related to aviation security and safety. Such consortia shall not be considered Federal advisory committees for purposes of the Federal Advisory Committee Act (5 U.S.C. App.).

(g) Improvement of secured-area access control.

(1) Enforcement.

(A) Under Secretary to publish sanctions. The Under Secretary shall publish in the Federal Register a list of sanctions for use as guidelines in the discipline of employees for infractions of airport access control requirements. The guidelines shall incorporate a progressive disciplinary approach that relates proposed sanctions to the severity or recurring nature of the infraction and shall include measures such as remedial training, suspension from security-related duties, suspension from all duties without pay, and termination of employment.

(B) Use of sanctions. Each airport operator, air carrier, and security screening company shall include the list of sanctions published by the Under Secretary in its security program. The security program shall include a process for taking prompt disciplinary action against an employee who commits an infraction of airport access control requirements.

(2) Improvements. The Under Secretary shall--

(A) work with airport operators and air carriers to implement and strengthen existing controls to eliminate airport access control weaknesses;

(B) require airport operators and air carriers to develop and implement comprehensive and recurring training programs that teach employees their roles in airport security, the importance of their participation, how their performance will be evaluated, and what action will be taken if they fail to perform;

(C) require airport operators and air carriers to develop and implement programs that foster and reward compliance with airport access control requirements and discourage and penalize noncompliance in accordance with guidelines issued by the Under Secretary to measure employee compliance;

(D) on an ongoing basis, assess and test for compliance with access control requirements, report annually findings of the assessments, and assess the effectiveness of penalties in ensuring compliance with security procedures and take any other appropriate enforcement actions when noncompliance is found;

(E) improve and better administer the Under Secretary's security database to ensure its efficiency, reliability, and usefulness for identification of systemic problems and allocation of resources;

(F) improve the execution of the Under Secretary's quality control program; and

(G) work with airport operators to strengthen access control points in secured areas (including air traffic control operations areas, maintenance areas, crew lounges, baggage handling areas, concessions, and catering delivery areas) to ensure the security of passengers and aircraft and consider the deployment of biometric or similar technologies that identify individuals based on unique personal characteristics.

(h) Improved airport perimeter access security.

(1) In general. The Under Secretary, in consultation with the airport operator and law enforcement authorities, may order the deployment of such personnel at any secure area of the airport as necessary to counter the risk of criminal violence, the risk of aircraft piracy at the airport, the risk to air carrier aircraft operations at the airport, or to meet national security concerns.

(2) Security of aircraft and ground access to secure areas. In determining where to deploy such personnel, the Under Secretary shall consider the physical security needs of air traffic control facilities, parked aircraft, aircraft servicing equipment, aircraft supplies (including fuel), automobile parking facilities within airport perimeters or adjacent to secured facilities, and access and transition areas at airports served by other means of ground or water transportation.

(3) Deployment of Federal law enforcement personnel. The Secretary may enter into a memorandum of understanding or other agreement with the Attorney General or the head of any other appropriate Federal law enforcement agency to deploy Federal law enforcement personnel at an airport in order to meet aviation safety and security concerns.

(4) Airport perimeter screening. The Under Secretary--

(A) shall require, as soon as practicable after the date of enactment of this subsection, screening or inspection of all individuals, goods, property, vehicles, and other equipment before entry into a secured area of an airport in the United States described in section 44903(c);

(B) shall prescribe specific requirements for such screening and inspection that will assure at least the same level of protection as will result from screening of passengers and their baggage;

(C) shall establish procedures to ensure the safety and integrity of--

(i) all persons providing services with respect to aircraft providing passenger air transportation or intrastate air transportation and facilities of such persons at an airport in the United States described in section 44903(c);

(ii) all supplies, including catering and passenger amenities, placed aboard such aircraft, including the sealing of supplies to ensure easy visual detection of tampering; and

(iii) all persons providing such supplies and facilities of such persons;

(D) shall require vendors having direct access to the airfield and aircraft to develop security programs; and

(E) may provide for the use of biometric or other technology that positively verifies the identity of each employee and law enforcement officer who enters a secure area of an airport.

(i) Authority to arm flight deck crew with less-than-lethal weapons.

(1) In general. If the Under Secretary, after receiving the recommendations of the National Institute of Justice, determines, with the approval of the Attorney General and the Secretary of State, that it is appropriate and necessary and would effectively serve the public interest in avoiding air piracy, the Under Secretary may authorize members of the flight deck crew on any aircraft providing air transportation or intrastate air transportation to carry a less-than-lethal weapon while the aircraft is engaged in providing such transportation.

(2) Usage. If the Under Secretary grants authority under paragraph (1) for flight deck crew members to carry a less-than-lethal weapon while engaged in providing air transportation or intrastate air transportation, the Under Secretary shall--

(A) prescribe rules requiring that any such crew member be trained in the proper use of the weapon; and

(B) prescribe guidelines setting forth the circumstances under which such weapons may be used.

(3) Request of air carriers to use less-than-lethal weapons. If, after the date of enactment of this paragraph [enacted Nov. 25, 2002], the Under Secretary receives a request from an air carrier for authorization to allow pilots of the air carrier to carry less-than-lethal weapons, the Under Secretary shall respond to that request within 90 days.

(j) Short-term assessment and deployment of emerging security technologies and procedures.

(1) In general. The Under Secretary of Transportation for Security shall recommend to airport operators, within 6 months after the date of enactment of the Aviation and Transportation Security Act [enacted Nov. 19, 2001], commercially available measures or procedures to prevent access to secure airport areas by unauthorized persons. As part of the 6-month assessment, the Under Secretary for Transportation Security shall--

(A) review the effectiveness of biometrics systems currently in use at several United States airports, including San Francisco International;

(B) review the effectiveness of increased surveillance at access points;

(C) review the effectiveness of card- or keypad-based access systems;

(D) review the effectiveness of airport emergency exit systems and determine whether those that lead to secure areas of the airport should be monitored or how breaches can be swiftly responded to; and

(E) specifically target the elimination of the "piggy-backing" phenomenon, where another person follows an authorized person through the access point.

The 6-month assessment shall include a 12-month deployment strategy for currently available technology at all category X airports, as defined in the Federal Aviation Administration approved air carrier security programs required under part 108 of title 14, Code of Federal Regulations. Not later than 18 months after the date of enactment of this Act, the Secretary of Transportation shall conduct a review of reductions in unauthorized access at these airports.

(2) Computer-Assisted Passenger Prescreening System.

(A) In general. The Secretary of Transportation shall ensure that the Computer-Assisted Passenger Prescreening System, or any successor system--

(i) is used to evaluate all passengers before they board an aircraft; and

(ii) includes procedures to ensure that individuals selected by the system and their carry-on and checked baggage are adequately screened.

(B) Modifications. The Secretary of Transportation may modify any requirement under the Computer-Assisted Passenger Prescreening System for flights that originate and terminate within the same State, if the Secretary determines that--

(i) the State has extraordinary air transportation needs or concerns due to its isolation and dependence on air transportation; and

(ii) the routine characteristics of passengers, given the nature of the market, regularly triggers primary selectee status.

(k) Limitation on liability for acts to thwart criminal violence or aircraft piracy. An individual shall not be liable for damages in any action brought in a Federal or State court arising out of the acts of the individual in attempting to thwart an act of criminal violence or piracy on an aircraft if that individual reasonably believed that such an act of criminal violence or piracy was occurring or was about to occur.

HISTORY: (July 5, 1994, P.L. 103-272, § 1(e), 108 Stat. 1205.) (As amended April 5, 2000, P.L. 106-181, Title VII, § 717, 114 Stat. 163; Nov. 22, 2000, P.L. 106-528, § § 4, 6, 114 Stat. 2520, 2521; Nov. 19, 2001, P.L. 107-71, Title I, § § 101(f)(7)-(9), 106(a), (c), (d), 120, 126(b), 136, 144, 115 Stat. 603, 608, 609, 610, 629, 632, 636, 644; Nov. 25, 2002, P.L. 107-296, Title XIV, § § 1405, 1406, 116 Stat. 2307.)

49 USCS § 40113 (2003)

§ 40113. Administrative

(a) General authority. The Secretary of Transportation (or the Under Secretary of Transportation for Security with respect to security duties and powers designated to be carried out by the Under Secretary or the Administrator of the Federal Aviation Administration with respect to aviation safety duties and powers designated to be carried out by the Administrator) may take action the Secretary, Under Secretary, or Administrator, as appropriate, considers necessary to carry out this part [*49 USCS § § 40101* et seq.], including conducting investigations, prescribing regulations, standards, and procedures, and issuing orders.

(b) Hazardous material. In carrying out this part [*49 USCS § § 40101* et seq.], the Secretary has the same authority to regulate the transportation of hazardous material by air that the Secretary has under section 5103 of this title. However, this subsection does not prohibit or regulate the transportation of a firearm (as defined in section 232 of title 18) or ammunition for a firearm, when transported by an individual for personal use.

(c) Governmental assistance. The Secretary (or the Administrator of the Federal Aviation Administration with respect to aviation safety duties and powers designated to be carried out by the Administrator) may use the assistance of the Administrator of the National Aeronautics and Space Administration and any research or technical department, agency, or instrumentality of the United States Government on matters related to aircraft fuel and oil, and to the design, material, workmanship, construction, performance, maintenance, and operation of aircraft, aircraft engines, propellers, appliances, and air navigation facilities. Each department, agency, and instrumentality may conduct scientific and technical research, investigations, and tests necessary to assist the Secretary or Administrator of the Federal Aviation Administration in carrying out this part [*49 USCS § § 40101* et seq.]. This part [*49 USCS § § 40101* et seq.] does not authorize duplicating laboratory research activities of a department, agency, or instrumentality.

(d) Indemnification. The Under Secretary of Transportation for Security or the Administrator of the Federal Aviation Administration may indemnify an officer or employee of the Transportation Security Administration or Federal Aviation Administration, as the case may be, against a claim or judgment arising out of an act that the Under Secretary or Administrator, as the case may be, decides was committed within the scope of the official duties of the officer or employee.

(e) Assistance to foreign aviation authorities.

(1) Safety-related training and operational services. The Administrator may provide safety-related training and operational services to foreign aviation authorities with or without reimbursement, if the Administrator determines that providing such services promotes aviation safety. To the extent practicable, air travel reimbursed under this subsection shall be conducted on United States air carriers.

(2) Reimbursement sought. The Administrator shall actively seek reimbursement for services provided under this subsection from foreign aviation authorities capable of providing such reimbursement.

(3) Crediting appropriations. Funds received by the Administrator pursuant to this section shall be credited to the appropriation from which the expenses were incurred in providing such services.

(4) Reporting. Not later than December 31, 1995, and annually thereafter, the Administrator shall transmit to Congress a list of the foreign aviation authorities to which the Administrator provided services under this subsection in the preceding fiscal year. Such list shall specify the dollar value of such services and any reimbursement received for such services.

(f) Application of certain regulations to Alaska. In amending title 14, Code of Federal Regulations, in a manner affecting intrastate aviation in Alaska, the Administrator of the Federal Aviation Administration shall consider the extent to which Alaska is not served by transportation modes other than aviation, and shall establish such regulatory distinctions as the Administrator considers appropriate.

HISTORY: (July 5, 1994, P.L. 103-272, § 1(e), 108 Stat. 1110; Aug. 23, 1994, P.L. 103-305, Title II, § 202, 108 Stat. 1582.) (As amended April 5, 2000, P.L. 106-181, Title I, Subtitle C, § 156(a), 114 Stat. 89; Nov. 19, 2001, P.L. 107-71, Title I, § 140(c), 115 Stat. 641.)

49 USCS § 44903 (2003)

§ 44903. Air transportation security

(a) Definition. In this section, "law enforcement personnel" means individuals--
(1) authorized to carry and use firearms;
(2) vested with the degree of the police power of arrest the Under Secretary of Transportation for Security considers necessary to carry out this section; and
(3) identifiable by appropriate indicia of authority.

(b) Protection against violence and piracy. The Under Secretary shall prescribe regulations to protect passengers and property on an aircraft operating in air transportation or intrastate air transportation against an act of criminal violence or aircraft piracy. When prescribing a regulation under this subsection, the Under Secretary shall--
(1) consult with the Secretary of Transportation, the Attorney General, the heads of other departments, agencies, and instrumentalities of the United States Government, and State and local authorities;
(2) consider whether a proposed regulation is consistent with--
(A) protecting passengers; and
(B) the public interest in promoting air transportation and intrastate air transportation;
(3) to the maximum extent practicable, require a uniform procedure for searching and detaining passengers and property to ensure--
(A) their safety; and
(B) courteous and efficient treatment by an air carrier, an agent or employee of an air carrier, and Government, State, and local law enforcement personnel carrying out this section; and
(4) consider the extent to which a proposed regulation will carry out this section.

(c) Security programs.
(1) The Under Secretary shall prescribe regulations under subsection (b) of this section that require each operator of an airport regularly serving an air carrier holding a certificate issued by the Secretary of Transportation to establish an air transportation security program that provides a law enforcement presence and capability at each of those airports that is adequate to ensure the safety of passengers. The regulations shall authorize the operator to use the services of qualified State, local, and private law enforcement personnel. When the Under Secretary decides, after being notified by an operator in the form the Under Secretary prescribes, that not enough qualified State, local, and private law enforcement personnel are available to carry out subsection (b), the Under Secretary may authorize the operator to use, on a reimbursable basis, personnel employed by the Under Secretary, or by another department, agency, or instrumentality of the Government with the consent of the head of the department, agency, or instrumentality, to supplement State, local, and private law enforcement personnel. When deciding whether additional personnel are needed, the Under Secretary shall consider the number of passengers boarded at the airport, the extent of anticipated risk of criminal violence or aircraft piracy at the airport or to the air carrier aircraft operations at the airport, and the availability of qualified State or local law enforcement personnel at the airport.

(2) (A) The Under Secretary may approve a security program of an airport operator, or an amendment in an existing program, that incorporates a security program of an airport tenant (except an air carrier separately complying with part 108 or 129 of title 14, Code of Federal Regulations) having access to a secured area of the airport, if the program or amendment incorporates--

(i) the measures the tenant will use, within the tenant's leased areas or areas designated for the tenant's exclusive use under an agreement with the airport operator, to carry out the security requirements imposed by the Under Secretary on the airport operator under the access control system requirements of section 107.14 of title 14, Code of Federal Regulations, or under other requirements of part 107 of title 14; and

(ii) the methods the airport operator will use to monitor and audit the tenant's compliance with the security requirements and provides that the tenant will be required to pay monetary penalties to the airport operator if the tenant fails to carry out a security requirement under a contractual provision or requirement imposed by the airport operator.

(B) If the Under Secretary approves a program or amendment described in subparagraph (A) of this paragraph, the airport operator may not be found to be in violation of a requirement of this subsection or subsection (b) of this section when the airport operator demonstrates that the tenant or an employee, permittee, or invitee of the tenant is responsible for the violation and that the airport operator has complied with all measures in its security program for securing compliance with its security program by the tenant.

(C) Maximum use of chemical and biological weapon detection equipment. The Secretary of Transportation may require airports to maximize the use of technology and equipment that is designed to detect or neutralize potential chemical or biological weapons.

(3) Pilot programs. The Administrator [Under Secretary] shall establish pilot programs in no fewer than 20 airports to test and evaluate new and emerging technology for providing access control and other security protections for closed or secure areas of the airports. Such technology may include biometric or other technology that ensures only authorized access to secure areas.

(d) Authorizing individuals to carry firearms and make arrests. With the approval of the Attorney General and the Secretary of State, the Secretary of Transportation may authorize an individual who carries out air transportation security duties--

(1) to carry firearms; and

(2) to make arrests without warrant for an offense against the United States committed in the presence of the individual or for a felony under the laws of the United States, if the individual reasonably believes the individual to be arrested has committed or is committing a felony.

(e) Exclusive responsibility over passenger safety. The Under Secretary has the exclusive responsibility to direct law enforcement activity related to the safety of passengers on an aircraft involved in an offense under section 46502 of this title from the moment all external doors of the aircraft are closed following boarding until those doors are opened to allow passengers to leave the aircraft. When requested by the Under Secretary, other departments, agencies, and instrumentalities of the Government shall provide assistance necessary to carry out this subsection.

(f) Government and industry consortia. The Under Secretary may establish at airports such consortia of government and aviation industry representatives as the Under Secretary may designate to provide advice on matters related to aviation security and safety. Such consortia shall not be considered Federal advisory committees for purposes of the Federal Advisory Committee Act (5 U.S.C. App.).

(g) Improvement of secured-area access control.

(1) Enforcement.

(A) Under Secretary to publish sanctions. The Under Secretary shall publish in the Federal Register a list of sanctions for use as guidelines in the discipline of employees for infractions of airport access control requirements. The guidelines shall incorporate a progressive disciplinary approach that relates proposed sanctions to the severity or recurring nature of the infraction and shall include measures such as remedial training, suspension from security-related duties, suspension from all duties without pay, and termination of employment.

(B) Use of sanctions. Each airport operator, air carrier, and security screening company shall include the list of sanctions published by the Under Secretary in its security program. The security program shall include a process for taking prompt disciplinary action against an employee who commits an infraction of airport access control requirements.

(2) Improvements. The Under Secretary shall--

(A) work with airport operators and air carriers to implement and strengthen existing controls to eliminate airport access control weaknesses;

(B) require airport operators and air carriers to develop and implement comprehensive and recurring training programs that teach employees their roles in airport security, the importance of their participation, how their performance will be evaluated, and what action will be taken if they fail to perform;

(C) require airport operators and air carriers to develop and implement programs that foster and reward compliance with airport access control requirements and discourage and penalize noncompliance in accordance with guidelines issued by the Under Secretary to measure employee compliance;

(D) on an ongoing basis, assess and test for compliance with access control requirements, report annually findings of the assessments, and assess the effectiveness of penalties in ensuring compliance with security procedures and take any other appropriate enforcement actions when noncompliance is found;

(E) improve and better administer the Under Secretary's security database to ensure its efficiency, reliability, and usefulness for identification of systemic problems and allocation of resources;

(F) improve the execution of the Under Secretary's quality control program; and

(G) work with airport operators to strengthen access control points in secured areas (including air traffic control operations areas, maintenance areas, crew lounges, baggage handling areas, concessions, and catering delivery areas) to ensure the security of passengers and aircraft and consider the deployment of biometric or similar technologies that identify individuals based on unique personal characteristics.

(h) Improved airport perimeter access security.

(1) In general. The Under Secretary, in consultation with the airport operator and law enforcement authorities, may order the deployment of such personnel at any secure area of the airport as necessary to counter the risk of criminal violence, the risk of aircraft piracy at the airport, the risk to air carrier aircraft operations at the airport, or to meet national security concerns.

(2) Security of aircraft and ground access to secure areas. In determining where to deploy such personnel, the Under Secretary shall consider the physical security needs of air traffic control facilities, parked aircraft, aircraft servicing equipment, aircraft supplies (including fuel), automobile parking facilities within airport perimeters or adjacent to secured facilities, and access and transition areas at airports served by other means of ground or water transportation.

(3) Deployment of Federal law enforcement personnel. The Secretary may enter into a memorandum of understanding or other agreement with the Attorney General or the head of any other appropriate Federal law enforcement agency to deploy Federal law enforcement personnel at an airport in order to meet aviation safety and security concerns.

(4) Airport perimeter screening. The Under Secretary--

(A) shall require, as soon as practicable after the date of enactment of this subsection, screening or inspection of all individuals, goods, property, vehicles, and other equipment before entry into a secured area of an airport in the United States described in section 44903(c);

(B) shall prescribe specific requirements for such screening and inspection that will assure at least the same level of protection as will result from screening of passengers and their baggage;

(C) shall establish procedures to ensure the safety and integrity of--

(i) all persons providing services with respect to aircraft providing passenger air transportation or intrastate air transportation and facilities of such persons at an airport in the United States described in section 44903(c);

(ii) all supplies, including catering and passenger amenities, placed aboard such aircraft, including the sealing of supplies to ensure easy visual detection of tampering; and

(iii) all persons providing such supplies and facilities of such persons;

(D) shall require vendors having direct access to the airfield and aircraft to develop security programs; and

(E) may provide for the use of biometric or other technology that positively verifies the identity of each employee and law enforcement officer who enters a secure area of an airport.

(i) Authority to arm flight deck crew with less-than-lethal weapons.

(1) In general. If the Under Secretary, after receiving the recommendations of the National Institute of Justice, determines, with the approval of the Attorney General and the Secretary of State, that it is appropriate and necessary and would effectively serve the public interest in avoiding air piracy, the Under Secretary may authorize members of the flight deck crew on any aircraft providing air transportation or intrastate air transportation to carry a less-than-lethal weapon while the aircraft is engaged in providing such transportation.

(2) Usage. If the Under Secretary grants authority under paragraph (1) for flight deck crew members to carry a less-than-lethal weapon while engaged in providing air transportation or intrastate air transportation, the Under Secretary shall--

(A) prescribe rules requiring that any such crew member be trained in the proper use of the weapon; and

(B) prescribe guidelines setting forth the circumstances under which such weapons may be used.

(3) Request of air carriers to use less-than-lethal weapons. If, after the date of enactment of this paragraph [enacted Nov. 25, 2002], the Under Secretary receives a request from an air carrier for authorization to allow pilots of the air carrier to carry less-than-lethal weapons, the Under Secretary shall respond to that request within 90 days.

(j) Short-term assessment and deployment of emerging security technologies and procedures.

(1) In general. The Under Secretary of Transportation for Security shall recommend to airport operators, within 6 months after the date of enactment of the Aviation and Transportation Security Act [enacted Nov. 19, 2001], commercially available measures or procedures to prevent access to secure airport areas by unauthorized persons. As part of the 6-month assessment, the Under Secretary for Transportation Security shall--

(A) review the effectiveness of biometrics systems currently in use at several United States airports, including San Francisco International;

(B) review the effectiveness of increased surveillance at access points;

(C) review the effectiveness of card- or keypad-based access systems;

(D) review the effectiveness of airport emergency exit systems and determine whether those that lead to secure areas of the airport should be monitored or how breaches can be swiftly responded to; and

(E) specifically target the elimination of the "piggy-backing" phenomenon, where another person follows an authorized person through the access point.

The 6-month assessment shall include a 12-month deployment strategy for currently available technology at all category X airports, as defined in the Federal Aviation Administration approved air carrier security programs required under part 108 of title 14, Code of Federal Regulations. Not later than 18 months after the date of enactment of this Act, the Secretary of Transportation shall conduct a review of reductions in unauthorized access at these airports.

(2) Computer-Assisted Passenger Prescreening System.

(A) In general. The Secretary of Transportation shall ensure that the Computer-Assisted Passenger Prescreening System, or any successor system--

(i) is used to evaluate all passengers before they board an aircraft; and

(ii) includes procedures to ensure that individuals selected by the system and their carry-on and checked baggage are adequately screened.

(B) Modifications. The Secretary of Transportation may modify any requirement under the Computer-Assisted Passenger Prescreening System for flights that originate and terminate within the same State, if the Secretary determines that--

(i) the State has extraordinary air transportation needs or concerns due to its isolation and dependence on air transportation; and

(ii) the routine characteristics of passengers, given the nature of the market, regularly triggers primary selectee status.

(k) Limitation on liability for acts to thwart criminal violence or aircraft piracy. An individual shall not be liable for damages in any action brought in a Federal or State court arising out of the acts of the individual in attempting to thwart an act of criminal violence or piracy on an aircraft if that individual reasonably believed that such an act of criminal violence or piracy was occurring or was about to occur.

HISTORY: (July 5, 1994, P.L. 103-272, § 1(e), 108 Stat. 1205.) (As amended April 5, 2000, P.L. 106-181, Title VII, § 717, 114 Stat. 163; Nov. 22, 2000, P.L. 106-528, § § 4, 6, 114 Stat. 2520, 2521; Nov. 19, 2001, P.L. 107-71, Title I, § § 101(f)(7)-(9), 106(a), (c), (d), 120, 126(b), 136, 144, 115 Stat. 603, 608, 609, 610, 629, 632, 636, 644; Nov. 25, 2002, P.L. 107-296, Title XIV, § § 1405, 1406, 116 Stat. 2307.)

DRAFT CBP/TSA May 22, 2003: Do not disseminate without the express prior written approval of the CBP, Office of Chief Counsel, (202) 927-6900 and TSA-ONRA, (240) 568-5665.

49 USCS § 44905 (2003)

§ 44905. Information about threats to civil aviation

(a) Providing information. Under guidelines the Secretary of Transportation prescribes, an air carrier, airport operator, ticket agent, or individual employed by an air carrier, airport operator, or ticket agent, receiving information (except a communication directed by the United States Government) about a threat to civil aviation shall provide the information promptly to the Secretary.

(b) Flight cancellation. If a decision is made that a particular threat cannot be addressed in a way adequate to ensure, to the extent feasible, the safety of passengers and crew of a particular flight or series of flights, the Under Secretary of Transportation for Security shall cancel the flight or series of flights.

(c) Guidelines on public notice.

(1) The President shall develop guidelines for ensuring that public notice is provided in appropriate cases about threats to civil aviation. The guidelines shall identify officials responsible for--

(A) deciding, on a case-by-case basis, if public notice of a threat is in the best interest of the United States and the traveling public;

(B) ensuring that public notice is provided in a timely and effective way, including the use of a toll-free telephone number; and

(C) canceling the departure of a flight or series of flights under subsection (b) of this section.

(2) The guidelines shall provide for consideration of--

(A) the specificity of the threat;

(B) the credibility of intelligence information related to the threat;

(C) the ability to counter the threat effectively;

(D) the protection of intelligence information sources and methods;

(E) cancellation, by an air carrier or the Under Secretary, of a flight or series of flights instead of public notice;

(F) the ability of passengers and crew to take steps to reduce the risk to their safety after receiving public notice of a threat; and

(G) other factors the Under Secretary considers appropriate.

(d) Guidelines on notice to crews. The Under Secretary shall develop guidelines for ensuring that notice in appropriate cases of threats to the security of an air carrier flight is provided to the flight crew and cabin crew of that flight.

(e) Limitation on notice to selective travelers. Notice of a threat to civil aviation may be provided to selective potential travelers only if the threat applies only to those travelers.

(f) Restricting access to information. In cooperation with the departments, agencies, and instrumentalities of the Government that collect, receive, and analyze intelligence information related to aviation security, the Under Secretary shall develop procedures to minimize the number of individuals who have access to information about threats. However, a restriction on access to that information may be imposed only if the

restriction does not diminish the ability of the Government to carry out its duties and powers related to aviation security effectively, including providing notice to the public and flight and cabin crews under this section.

(g) Distribution of guidelines. The guidelines developed under this section shall be distributed for use by appropriate officials of the Department of Transportation, the Department of State, the Department of Justice, and air carriers.

HISTORY: (July 5, 1994, P.L. 103-272, § 1(e), 108 Stat. 1207.) (As amended Nov. 19, 2001, P.L. 107-71, Title I, § 101(f)(7), (9), 115 Stat. 603.)

DRAFT CBP/TSA May 22, 2003: Do not disseminate without the express prior written approval of the CBP, Office of Chief Counsel, (202) 927-6900 and TSA-ONRA, (240) 568-5665.

Attachment "B"

PNR Data Elements Required from Air Carriers and Global Distribution Systems (GDSs)

PNR record locator code
Date of reservation
Date(s) of intended travel
Name
Other names on PNR
Number of travelers on PNR
Seat information
Address
All forms of payment information
Billing address
Contact telephone numbers
All travel itinerary for specific PNR
Frequent flyer information (limited to miles flown and address(es))
Travel agency
Travel agent
Code share PNR information
Travel status of passenger
Split/Divided PNR information
Identifiers for free tickets
One-way tickets
Email address
Ticketing field information
ATFQ fields
General remarks
Ticket number
Seat number
Date of ticket issuance
Any collected APIS information
No show history
Number of bags
Bag tag numbers
Go show information
Number of bags on each segment
OSI information
SSI information
SSR information
Voluntary/involuntary upgrades
Received from information
All historical changes to the PNR

Attachment "B" (Continued)

TSA Additional PNR Requirements[16]

Traveler's full name
Date of birth
Complete home address
Home phone number

[16] TSA will require that air carriers collect and complete these particular fields.