EXEMPTIONS CLAIMED FOR THE SYSTEM:

The Secretary of Homeland Security has exempted this system from the following provisions of the Privacy Act, subject to the limitation set forth in (c)(3); (d); (e)(1), (e)(4)(G), (e)(4)(H), (e)(4)(I); and (f) of the Privacy Act pursuant to 5 U.S.C. 552a(k)(1), (k)(2), and (k)(5) of the Privacy Act.


Mary Ellen Callahan,
Chief Privacy Officer, Department of Homeland Security.

[FR Doc. 2010–2206 Filed 2–2–10; 8:45 am]
BILLING CODE 9110–98–P

DEPARTMENT OF HOMELAND SECURITY

Office of the Secretary

[Docket No. DHS–2009–0043]

Privacy Act of 1974; Department of Homeland Security/ALL—025 Law Enforcement Authority in Support of the Protection of Property Owned, Occupied, or Secured by the Department of Homeland Security System of Records

AGENCY: Privacy Office; DHS.

ACTION: Notice of Privacy Act system of records.

SUMMARY: In accordance with the Privacy Act of 1974 the Department of Homeland Security proposes to update Department of Homeland Security/ALL—025 Law Enforcement Authority in Support of the Protection of Property Owned, Occupied, or Secured by the Department of Homeland Security System of Records to include record systems within the Federal Protective Service. The purpose of this system is to maintain and record the results of law enforcement activities in support of the protection of property owned, occupied, or secured by the Department of Homeland Security and its components, including the Federal Protective Service, and individuals maintaining a presence or access to such property. Categories of individuals, categories of records, and the routine uses of this system have been reviewed and updated to better reflect the Department’s law enforcement records associated with the protection of property owned, occupied, or secured by the Department of Homeland Security. The activities performed by the Department in the protection of property owned, occupied, or secured by the Department of Homeland Security often overlap with other security-related activities. Accordingly, data within the categories of individuals, categories of records, and routine uses may have similarities with other security-related systems of records, but each system is distinct based on its purpose.

Exclusion is made to perimeters and facilities secured by the U.S. Secret Service pursuant to 18 U.S.C. 3056 and 3056A and are not included under this system of records. Records pertaining to perimeters and facilities secured by the U.S. Secret Service, other than those records subject to the Presidential Records Act, are covered under Department of Homeland Security/ALL—025 Law Enforcement Authority in Support of the Protection of Property Owned, Occupied, or Secured by the Department of Homeland Security System of Records. This updated system will be effective March 5, 2010.

The purpose of this system is to maintain and record the results of law enforcement activities in support of the protection of property owned, occupied, or secured by DHS. The results are also used to pursue criminal prosecutions or civil penalty actions against individuals or entities suspected of offenses that may have been committed against property owned, occupied, or secured by DHS or persons on these premises; and to assess acceptability of Departmental, other United States Government personnel, contract security officer personnel, and other contractors who work in DHS facilities for assignment to or retention in sensitive positions consistent with the interest of national security and protection of DHS facilities. The Department’s authority for this collection is primarily 5 U.S.C. 301; the Homeland Security Act, codified in Title 6 of the U.S. Code; 40 U.S.C. 1315; 44 U.S.C. 3101; and Executive Order (EO) 9397; EO 10450; EO 12968, 5 CFR 731; 5 CFR 732; 5 CFR 736; 32 CFR 147; and DCID 6/4. This system will collect individuals’ personal information when the Department uses its law enforcement authority at facilities that DHS owns, occupies, or secures. Efforts have been made to safeguard records in accordance with applicable rules and policies, including all applicable DHS automated systems security and access policies. Strict controls have been imposed to minimize the risk of compromising information being stored. Access to the computer system containing the records in this system is limited to those individuals who have a need to know the information for the performance of their official duties and who have appropriate clearances or

FOR FURTHER INFORMATION CONTACT: For general questions and privacy issues please contact: Mary Ellen Callahan (703–235–0780), Chief Privacy Officer, Privacy Office, Department of Homeland Security, Washington, DC 20528.
permissions. The routine uses posted are unchanged from the previous publishing and are consistent with the purpose for collection. A review of this system is being conducted to determine if the system of records collects information under the Paperwork Reduction Act. Categories of individuals, categories of records, and the routine uses of this system have been reviewed and updated to better reflect the Department’s law enforcement records associated with the protection of property owned, occupied, or secured by DHS. Specifically, the Privacy Office updated the purpose to include law enforcement activities in support of the protection of property secured by DHS and its components, including FPS.

Privacy Impact Assessments (PIAs) have been conducted and are on file for the (1) Personnel Security Activities Management System; (2) Integrated Security Management System; (3) DHS Access Gate System; (4) Automated Continuing Evaluation System (ACES) Pilot; (5) Personal Identity Verification System; (6) Federal Protective Service Information Support Tracking System (FISTTS) Contract Suitability Module; (7) Federal Protective Service Dispatch Incident Records Management Systems; and (8) Livewave CCTV System along with other related component specific PIAs and can be found at http://www.dhs.gov/privacy.

Consistent with DHS’s information sharing mission, information stored in the DHS/ALL—025 Law Enforcement Authority in Support of the Protection of Property Owned, Occupied, or Secured by DHS System of Records may be shared with other DHS components, as well as appropriate federal, state, local, tribal, foreign, or international government agencies. This sharing will only take place after DHS determines that the receiving component or agency has a need to know the information to carry out national security, law enforcement, immigration, intelligence, or other functions consistent with the routine uses set forth in this system of records notice.

Exclusion is made to perimeters and facilities secured by the U.S. Secret Service pursuant to 18 U.S.C. 3056 and 3056A and are not included under this system of records. Records pertaining to perimeters and facilities secured by the U.S. Secret Service, other than those records subject to the Presidential Records Act, are covered under Department of Homeland Security/U.S. Secret Service—004 Protection Information System of Records (73 FR 77733, December 19, 2008).

There will be no change to the Privacy Act exemptions currently in place for this system of records and therefore remain in effect. This system will be included in DHS’s inventory of record systems.

II. Privacy Act

The Privacy Act embodies fair information principles in a statutory framework governing the means by which the United States Government collects, maintains, uses and disseminates individual’s records. The Privacy Act applies to information that is maintained in a “system of records.” A “system of records” is a group of any records under the control of an agency from which information is stored and retrieved by the name of the individual or by some identifying number such as property address, mailing address, or symbol assigned to the individual. In the Privacy Act, an individual is defined to encompass United States citizens and lawful permanent residents. DHS extends administrative Privacy Act protections to all individuals where information is maintained on both U.S. citizens, lawful permanent residents, and visitors. Individuals may request their own records that are maintained in a system of records in the possession of agencies under the control of DHS by complying with DHS Privacy Act regulations, 6 CFR 5.21.

The Privacy Act requires each agency to publish in the Federal Register a description denoting the type and character of each system of records that the agency maintains, and the routine uses that are contained in each system in order to make agency record keeping practices transparent, to notify individuals regarding the uses of their records, and to assist individuals to more easily find such files within the agency. Below is a description of DHS/ALL—025 Law Enforcement Authorities in Support of the Protection of Property Owned, Occupied, or Secured by DHS Security Systems of Records.

In accordance with 5 U.S.C. 552(a), DHS has provided a report of this new system of records to the Office of Management and Budget (OMB) and to Congress.

SYSTEM OF RECORDS:
DHS/ALL—025

SYSTEM NAME:

SECURITY CLASSIFICATION:
Unclassified, sensitive, for official use only, and classified.

SYSTEM LOCATION:
Records are maintained at several Headquarters locations and component offices of DHS, in both Washington, DC and field locations.

CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM:
Categories of individuals covered by this system include any person or entity involved in, or suspected of being involved in, criminal acts against the buildings, grounds, and property that are owned, occupied, or secured by DHS or against persons who are in or on such buildings, grounds, or property. This includes, but is not limited to: any agency, instrumentality, or wholly owned or mixed-ownership corporation thereof, and persons on the property; Departmental, other United States Government personnel, contract security officer personnel, and other contractors who work in federal facilities; and property located in or outside of the United States; and individuals who are involved in or suspected to be involved in such criminal acts, who provide information that is relevant to the investigation, such as victims and witnesses, and who report such crimes or acts. Also included in this system of records are the travel records of current, former, or retired Departmental personnel who travelled outside the United States while employed by DHS; applicants, appointees, and nominees of the Department; and contractors and consultants who have or have had access to DHS facilities and/or classified national security information.

CATEGORIES OF RECORDS IN THE SYSTEM:
Categories of records in the system may include but are not limited to the following:
• Individual’s or entity’s name;
• Digital photograph;
• Date of birth, place of birth, and age;
• Social security number;
• Duty/work address and telephone number;
• Alias;
• Race and ethnicity;
• Citizenship;
• Fingerprints;
• Sex;
• Marital status;
• Identifying marks such as tattoos, scars, etc;
• Height and weight;
• Eye and hair color;
• Biometric data;
• Home address, telephone number, and other contact information;
• Driver’s license information and citations issued;
• Vehicle information;
• Date, location, nature and details of the incident/offense;
• Alcohol, drugs and/or weapons involvement;
• Bias against any particular group;
• Confinement information to include location of correctional facility;
• Gang/cult affiliation if applicable;
• Records of possible espionage, foreign intelligence service elicitation activities, and other investigative support to criminal investigations to include source control documentation and regional information;
• Data on individuals to include: victims, witnesses, complainants, offenders, and suspects;
• Records of possible espionage, foreign intelligence service elicitation activities, and terrorist collection efforts directed at the Department or its staff, contractors or visitors;
• Records of close coordination with the intelligence and law enforcement community;
• Records relating to the management and operation of DHS special security programs, including but not limited to:
  o Requests for access to sensitive compartmented information (SCI);
  o Foreign travel; and
  o Foreign contact registries for individuals with SCI access;
• Records relating to the management and operation of the DHS security program, including but not limited to:
  o Inquiries relating to suspected security violation(s);
  o Recommended remedial actions for possible security violation(s);
  o Reports of investigation regarding security violations;
  o Statements of individuals;
  o Affidavits;
  o Correspondence; and
  o Other documentation pertaining to investigative or analytical efforts by DHS to identify threats to the Department’s personnel, property, facilities, and information: intelligence reports and database results relating to DHS personnel applicants or candidates for DHS employment or a DHS contract, or other individuals interacting or having contact with DHS personnel or contractors; foreign contact registries for individuals; or unsolicited communications with DHS personnel or contractors that raise a security concern; and
  o Other documents obtained from applicants for employment or contract positions and documents obtained during a background investigation or re-investigation including medical and financial data.

AUTHORITY FOR MAINTENANCE OF THE SYSTEM:

PURPOSE(S):
The purpose of this system is to maintain and record the results of law enforcement activities in support of the protection of property owned, occupied, or secured by DHS and its components, including FPS, and individuals maintaining a presence or access to such property. It will also be used to pursue criminal prosecution or civil penalty action against individuals or entities suspected of offenses that may have been committed against property owned, occupied, or secured by DHS or persons on the property; and to assess Departmental, contract security officer personnel, and other contractors who work in such facilities, acceptability for assignment to or retention in sensitive positions consistent with the interest of national security and the protection of these facilities.

ROUTINE USES OF RECORDS MAINTAINED IN THE SYSTEM, INCLUDING CATEGORIES OF USERS AND THE PURPOSES OF SUCH USES:
In addition to those disclosures generally permitted under 5 U.S.C. 552a(b) of the Privacy Act, all or a portion of the records of information contained in this system may be disclosed outside DHS as a routine use pursuant to 5 U.S.C. 552a(b)(3) as follows:
A. To the Department of Justice (including United States Attorney Offices) or other federal agency conducting litigation or in proceedings before any court, adjudicative or administrative body when it is necessary to the litigation and one of the following is a party to the litigation or has an interest in such litigation:
1. DHS or any component thereof;
2. any employee of DHS in his/her official capacity;
3. any employee of DHS in his/her individual capacity where DOJ or DHS has agreed to represent the employee; or
4. the United States or any agency thereof, is a party to the litigation or has an interest in such litigation, and DHS determines that the records are both relevant and necessary to the litigation and the use of such records is compatible with the purpose for which DHS collected the records.
B. To a congressional office from the record of an individual in response to a written inquiry from that congressional office made at the written request of the individual to whom the record pertains.
C. To the National Archives and Records Administration or other federal government agencies pursuant to records management inspections being conducted under the authority of 44 U.S.C. 2904 and 2906.
D. To an agency, organization, or individual for the purpose of performing audit or oversight operations as authorized by law, but only such information as is necessary and relevant to such audit or oversight function.
E. To appropriate agencies, entities, and persons when:
1. DHS suspects or has confirmed that the security or confidentiality of information in the system of records has been compromised;
2. The Department has determined that as a result of the suspected or confirmed compromise there is a risk of harm to economic or property interests, identity theft or fraud, or harm to the security or integrity of this system or other systems or programs (whether maintained by DHS or another agency or entity) or harm to the individual who relies upon the compromised information; and
3. The disclosure made to such agencies, entities, and persons is reasonably necessary to assist in connection with DHS’s efforts to respond to the suspected or confirmed compromise and prevent, minimize, or remedy such harm.
F. To contractors and their agents, grantees, experts, consultants, and others performing or working on a contract, service, grant, cooperative agreement, or other assignment for DHS, when necessary to accomplish an agency function related to this system of records. Individuals provided information under this routine use are subject to the same Privacy Act requirements and limitations on disclosure as are applicable to DHS officers and employees.
G. To an appropriate federal, state, tribal, local, international, or foreign law enforcement agency or other appropriate authority charged with investigating or prosecuting a violation or enforcing or implementing a law, rule, regulation, or order, where a record, either on its face or in conjunction with other information, indicates a violation or potential violation of law, which includes criminal, civil, or regulatory violations and such disclosure is proper and consistent with the official duties of the person making the disclosure.

H. To an appropriate federal, state, local, tribal, foreign, or international agency or contract provider, if the information is relevant and necessary to a requesting agency’s decision concerning the hiring or retention of an individual, or issuance of a security clearance, license, contract, grant, or other benefit, or if the information is relevant and necessary to a DHS decision concerning the hiring or retention of an employee or contractor, the issuance of a security clearance, the reporting of an investigation of an employee or contractor, the letting of a contract, or the issuance of a license, grant or other benefit and disclosure is appropriate to the proper performance of the official duties of the person making the request.

I. To a court, magistrate, or administrative tribunal in the course of presenting evidence, including disclosures to opposing counsel or witnesses in the course of civil discovery, litigation, or settlement negotiations or in connection with criminal law proceedings or pursuant to the order of a court of competent jurisdiction in response to a subpoena from a court of competent jurisdiction.

J. To third parties during the course of a law enforcement investigation to the extent necessary to obtain information pertinent to the investigation, provided disclosure is appropriate to the proper performance of the official duties of the officer making the disclosure.

K. To a federal, state, local agency, or other appropriate entities or individuals, or through established liaison channels to selected foreign governments, in order to provide intelligence, counterintelligence, or other information for the purposes of intelligence, counterintelligence, or antiterrorism activities authorized by United States law, Executive Order, or any other applicable national security directive.

L. To a public or professional licensing organization when such information indicates, either by itself or in combination with other information, a violation or potential violation of professional standards, or reflects on the moral, educational, or professional qualifications of an individual who is licensed or who is seeking to become licensed.

M. To the news media and the public, with the approval of the Chief Privacy Officer in consultation with counsel, when there exists a legitimate public interest in the disclosure of the information or when disclosure is necessary to preserve confidence in the integrity of DHS or is necessary to demonstrate the accountability of DHS’s officers, employees, or individuals covered by the system, except to the extent it is determined that release of the specific information in the context of a particular case would constitute an unwarranted invasion of personal privacy.

DISCLOSURE TO CONSUMER REPORTING AGENCIES:

None.

POLICIES AND PRACTICES FOR STORING, RETRIEVING, ACCESSING, RETAINING, AND DISPOSING OF RECORDS IN THE SYSTEM:

STORAGE:

Records in this system are stored electronically or on paper in secure facilities in a locked drawer behind a locked door. The records are stored on servers, magnetic disc, tape, digital media, and CD-ROM.

RETRIEVABILITY:

Records may be retrieved by individual name, social security number, or other personal information identified listed in “Categories of Records,” if applicable.

SAFEGUARDS:

Records in this system are safeguarded in accordance with applicable rules and policies, including all applicable DHS automated systems security and access policies. Strict controls have been imposed to minimize risk of compromising the information that is being stored. Access to the computer system containing the records in this system is limited to those individuals who have a need to know the information for the performance of their official duties and who have appropriate clearances or permissions.

RETENTION AND DISPOSAL:

Records are pending National Archives and Records Administration approval. DHS has proposed the following retention schedule: Records are maintained for 20 years after the end of the fiscal year in which the case was closed and are then destroyed. No records will be destroyed until the retention schedule is approved.

SYSTEM MANAGER AND ADDRESS:


NOTIFICATION PROCEDURE:

The Secretary of Homeland Security has exempted this system from the notification, access, and amendment procedures of the Privacy Act because it is a law enforcement system. However, DHS will consider individual requests to determine whether or not information may be released. Thus, individuals seeking notification of and access to any record contained in this system of records, or seeking to contest its content, may submit a request in writing to the Headquarters or component’s FOIA Officer, whose contact information can be found at http://www.dhs.gov/foia under “contacts.” If an individual believes more than one component maintains Privacy Act records concerning him or her the individual may submit the request to the Chief Privacy Officer and Chief Freedom of Information Act Officer, Department of Homeland Security, 245 Murray Drive, SW., Building 410, STOP–0550, Washington, DC 20528.

When seeking records about yourself from this system of records or any other Departmental system of records your request must conform with the Privacy Act regulations set forth in 6 CFR Part 5. You must first verify your identity, meaning that you must provide your full name, current address and date and place of birth. You must sign your request, and your signature must either be notarized or submitted under 28 U.S.C. 1746, a law that permits statements to be made under penalty of perjury as a substitute for notarization. While no specific form is required, you may obtain forms for this purpose from the Chief Privacy Officer and Chief Freedom of Information Act Officer, http://www.dhs.gov or 1–866–431–0486. In addition you should provide the following:

• An explanation of why you believe the Department would have information on you;

• Identify which component(s) of the Department you believe may have the information about you;

• Specify when you believe the records would have been created;
- Provide any other information that will help the FOIA staff determine which DHS component agency may have responsive records; and
- If your request is seeking records pertaining to another living individual, you must include a statement from that individual certifying his/her agreement for you to access his/her records.

Without this bulleted information the component(s) may not be able to conduct an effective search, and your request may be denied due to lack of specificity or lack of compliance with applicable regulations.

RECORD ACCESS PROCEDURES:
See “Notification procedure” above.

CONTESTING RECORD PROCEDURES:
See “Notification procedure” above.

RECORD SOURCE CATEGORIES:
Records are generated from sources contacted during investigations, state and local law enforcement, and federal departments and agencies.

EXEMPTIONSclaimed for the system:
The Secretary of Homeland Security has exempted this system from the following provisions of the Privacy Act, subject to the limitation set forth in (c)(3); (d); (e)(1), (e)(4)(G), (e)(4)(H), (e)(4)(I); and (f) of the Privacy Act pursuant to 5 U.S.C. 552a (k)(1), (k)(2), and (k)(5) of the Privacy Act.

Mary Ellen Callahan,
Chief Privacy Officer, Department of Homeland Security.

[FR Doc. 2010–2207 Filed 2–2–10; 8:45 am]
BILLING CODE 9111–14–P

DEPARTMENT OF HOMELAND SECURITY

U.S. Customs and Border Protection

Notice of Issuance of Final Determination Concerning a Certain Alternator


ACTION: Notice of final determination.

SUMMARY: This document provides notice that U.S. Customs and Border Protection (“CBP”) has issued a final determination concerning the country of origin of a certain alternator. Based upon the facts presented, CBP has concluded in the final determination that the U.S. is the country of origin of the alternator for purposes of U.S. government procurement.

DATE: The final determination was issued on January 21, 2010. A copy of the final determination is attached. Any party-at-interest, as defined in 19 CFR 177.22(d), may seek judicial review of this final determination within 30 days of publication in the Federal Register.

FOR FURTHER INFORMATION CONTACT: Elif Eroglu, Valuation and Special Programs Branch: (202) 325–0277.

SUPPLEMENTARY INFORMATION: Notice is hereby given that on January 21, 2010, pursuant to subpart B of part 177, Customs Regulations (19 CFR part 177, subpart B), CBP issued a final determination concerning the country of origin of the alternator which may be offered to the U.S. Government under an undesignated government procurement contract. This final determination, in HQ H075667, was issued at the request of Ecoair Corp., pursuant to procedures set forth at 19 CFR part 177, subpart B, which implements Title III of the Trade Agreements Act of 1979, as amended (19 U.S.C. 2511–18). In the final determination, CBP has concluded that, based upon the facts presented, the alternator, assembled in the U.S. from parts made in China and the U.S., is substantially transformed in the U.S., such that the U.S. is the country of origin of the finished article for purposes of U.S. government procurement.

Section 177.29, Customs Regulations (19 CFR 177.29), provides that notice of final determinations shall be published in the Federal Register within 60 days of the date the final determination is issued. Section 177.30, Customs Regulations (19 CFR 177.30), provides that any party-at-interest, as defined in 19 CFR 177.22(d), may seek judicial review of a final determination within 30 days of publication of such determination in the Federal Register.


Sandra L. Bell,
Executive Director, Regulations and Rulings, Office of International Trade.

Attachment

H075667

January 21, 2010

OT:RR:CTF:VS H075667 EE

CATEGORY: Marking

Mr. Peter S. Knudsen, Jr.
Ecoair Corp.
Four Industrial Circle
Hamden, CT 06517–3152

RE: U.S. Government Procurement;
Title III, Trade Agreements Act of 1979 (19 U.S.C. § 2511); Subpart B, Part 177, CBP Regulations; Country of Origin; Eco-Tech Heavy Duty Alternator

Dear Mr. Knudsen: This is in response to your correspondence of October 31, 2009, in which you requested a final determination on behalf of Ecoair Corp. (“Ecoair”), pursuant to subpart B of part 177, Customs and Border Protection (“CBP”) Regulations (19 C.F.R. § 177.21 et seq.). Under the pertinent regulations, which implement Title III of the Trade Agreements Act of 1979, as amended (19 U.S.C. § 2511 et seq.), CBP issues country of origin advisory rulings and final determinations as to whether an article is or would be a product of a designated country or instrumentality for the purpose of granting waivers of certain “Buy American” restrictions in U.S. law or practice for products offered for sale to the U.S. Government.

This final determination concerns the country of origin of the Eco-Tech Heavy Duty Alternator. We note that Ecoair is a party-at-interest within the meaning of 19 C.F.R. § 177.22(d)[1] and is entitled to request this final determination.

FACTS:
You describe the pertinent facts as follows. Eco-Tech Alternators operate in diesel powered military boats, fire trucks, ambulances, utility trucks, school shuttles, party buses, and commercial fishing boats; all applications where significant operating time is spent at idle and where electric power needs are independent of the