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 magnetic disc, tape, digital media, and CD–ROM.

RETRIEVABILITY:

Data may be retrieved by an individual's name, date of birth, and social security number.

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 the 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 permission.

RETENTION AND DISPOSAL:

Records are destroyed after three years, in accordance with National Archives and Records Administration General Records Schedule 1, Item 36.

SYSTEM MANAGER AND ADDRESS:

For Headquarters of DHS, the System Manager is the Director of Departmental Disclosure, Department of Homeland Security, Washington, DC 20528. For components of DHS, the System Manager can be found at *http://www.dhs.gov/foia* under ''contacts.''

NOTIFICATION PROCEDURE:

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, 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 Director, Disclosure and FOIA, *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,
- 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:

Information originates from personnel who submit to drug and alcohol testing, DHS and its components and offices, and testing and treatment facilities.

EXEMPTIONS CLAIMED FOR THE SYSTEM:

None.

Dated: October 22, 2008.

Hugo Teufel III,

Chief Privacy Officer, Department of Homeland Security.

[FR Doc. E8–25971 Filed 10–30–08; 8:45 am]

BILLING CODE 4410–10–P

DEPARTMENT OF HOMELAND SECURITY

Office of the Secretary

Published Privacy Impact Assessments on the Web

AGENCY: Privacy Office, DHS.

ACTION: Notice of Publication of Privacy Impact Assessments.

SUMMARY: The Privacy Office of the Department of Homeland Security is making available eleven (11) Privacy Impact Assessments on various programs and systems in the Department. These assessments were approved and published on the Privacy Office's Web site between April 1, 2008 and June 30, 2008.

DATES: The Privacy Impact Assessments will be available on the DHS Web site until December 30, 2008, after which they may be obtained by contacting the DHS Privacy Office (contact information below).

FOR FURTHER INFORMATION CONTACT: Hugo Teufel III, Chief Privacy Officer, Department of Homeland Security, Mail Stop 0550, Washington, DC 20528, or e-mail: *pia@dhs.gov*.

SUPPLEMENTARY INFORMATION: April 1, 2008 and June 30, 2008, the Chief Privacy Officer of the Department of Homeland Security (DHS) approved and published eleven (11) Privacy Impact Assessments (PIAs) on the DHS Privacy Office Web site, *http://www.dhs.gov/privacy*, under the link for ''Privacy Impact Assessments.'' Below is a short summary of each of those systems, including the DHS component responsible for the system, the name of system, and the date on which the PIA was approved. Additional information can be found on the Web site or by contacting the Privacy Office.

System: Law Enforcement Information Data Base/Pathfinder.

Component: United States Coast Guard.

Date of approval: March 31, 2008.

The United States Coast Guard (USCG), a component of the Department of Homeland Security, established the Law Enforcement Information Data Base (LEIDB)/Pathfinder. LEIDB/Pathfinder archives text messages prepared by individuals engaged in Coast Guard law enforcement, counterterrorism, maritime security, maritime safety and other Coast Guard missions enabling intelligence analysis of field reporting. USCG conducted this PIA because the LEIDB/Pathfinder system collects and uses personally identifiable information (PII).

System: Maritime Awareness Global Network.

Component: United States Coast Guard.

Date of approval: April 11, 2008.

USCG developed the Maritime Awareness Global Network (MAGNET) system. MAGNET uses information relating to vessels and activities within

the maritime environment to accomplish the USCG's missions in the areas of Maritime Safety, Maritime Security, Maritime Mobility, National Defense, and Protection of Natural Resources. MAGNET is a new system that will replace the existing integrated intelligence sharing system known as the Joint Maritime Information Element Support System. This PIA was completed because MAGNET will process PII.

System: United States Visitor and Immigrant Status Indicator Technology (US–VISIT) Program In conjunction with the Notice of Proposed Rulemaking on the Collection of Alien Biometric Data upon Exit from the United States at Air and Sea Ports of Departure.

Component: United States Visitor and Immigrant Status Indicator Technology.

Date of approval: April 22, 2008.

The US–VISIT Program has been implemented in phases with each phase adding additional capabilities, locations of implementation, or subject populations. US–VISIT published this PIA in conjunction with the Notice of Proposed Rulemaking on Collection of Alien Biometric Data upon Exit from the United States at Air and Sea Ports of Departure. A revised PIA will be issued in conjunction with the Final Rule on Collection of Alien Biometric Data upon Exit from the United States at Air and Sea Ports of Departure.

System: Group Violent Intent Modeling (GVIM) Program.

Component: Science and Technology.

Date of approval: April 25, 2008.

This PIA describes the research and development objectives of DHS Science and Technology (S&T) Directorate's Human Factors Division Group Violent Intent Modeling (GVIM) project. The goal of GVIM is to determine whether including social and behavioral theories and concepts from established research in a software tool that is used to analyze group behaviors and motivations will improve the ability of analysts to identify indicators that could predict group violence. The project will develop a social and behaviorally based framework of theories and concepts that includes modeling and simulation tools to improve the efficiency and accuracy of intelligence analysts examining the likelihood of a group choosing violence to achieve its goals. This PIA is necessary because PII will be collected as part of the research and development effort.

System: Web Time and Attendance System.

Component: Department Wide.

Date of approval: May 1, 2008.

The DHS Office of the Chief Human Capital Officer procured a commercial off the shelf application and customized it to meet DHS standard requirements. This system is designed to implement an enterprise system that can efficiently automate the timesheet collection process and provide robust reporting features and a labor distribution capability. This PIA was conducted because WebTA utilizes PII.

System: Einstein 2.

Component: National Protection and Programs Directorate.

Date of approval: May 19, 2008.

This PIA is for an updated version of the EINSTEIN System. EINSTEIN is a computer network intrusion detection system (IDS) used to help protect federal executive agency information technology enterprises. EINSTEIN 2 will incorporate network intrusion detection technology capable of alerting the United States Computer Emergency Readiness Team (US–CERT) to the presence of malicious or potentially harmful computer network activity in federal executive agencies' network traffic. This network intrusion detection technology uses a set of pre-defined signatures based upon known malicious network traffic. The signatures are based upon malicious computer code and are not based upon PII. Nor is the IDS programmed specifically to collect or locate PII. While the IDS will collect some PII that is directly related to malicious code being transmitted to the federal networks, its main focus is to identify the malicious code and protect federal networks, not to collect PII.

System: Tactical Information Sharing System Update.

Component: Transportation Security Administration.

Date of approval: June 1, 2008.

The Transportation Security Administration (TSA) operates the Transportation Information Sharing System (TISS). TISS receives, assesses, and distributes intelligence information related to transportation security to Federal Air Marshals and other Federal, State, and local law enforcement. This PIA is being updated to reflect more clearly that TISS applies to all transportation modes, not just aviation modes as might have been assumed because the system involves Federal Air Marshals.

System: Security Threat Assessment for Airport Badge and Credential Holders.

Component: Transportation Security Administration.

Date of approval: June 2, 2008.

TSA is updating the PIA for the Security Threat Assessment (STA) for Airport Badge and Credential Holders to reflect an expansion of the covered population to include certain holders of airport approved badges, and to reflect the use of US–VISIT's Automated Biometrics Identification System (IDENT) database as part of the STA process, including enrollment of fingerprints in that database for recurring checks. This PIA is an updated and amended version of the PIA originally published by TSA on June 15, 2004, and subsequently amended on August 19, 2005 and on December 20, 2006. The requirements addressed in the previous PIAs are still in effect, including the requirement to conduct name-based STAs on all individuals seeking or holding airport identification badges or credentials and the requirement to conduct fingerprint-based criminal history record checks along with name-based checks on individuals seeking access to the Security Identification Display Area (SIDA) or Sterile Area of an airport.

System: Electronic System for Travel Authorization.

Component: Customs and Border Protection.

Date of approval: June 3, 2008.

CBP issued an Interim Final Rule to create regulations governing the submission of Electronic System for Travel Authorization (ESTA) data, a new system of records notice, and an associated PIA. The ESTA regulations will govern the collection and use of PII in determining the eligibility to travel of persons seeking to enter the United States under the Visa Waiver Program (VWP) by air or sea. The regulations will require nationals of VWP countries seeking to enter the United States by air or sea carriers to submit PII to an electronic system, ESTA, prior to travel. ESTA will run the applicant's information against various databases to determine whether there is a law enforcement or security reason to deem that a prospective traveler is ineligible to travel to the United States under the VWP. The ESTA system will serve to modernize and strengthen the security of the VWP as mandated by the ''Implementing Recommendations of the 9/11 Commission Act of 2007'' (9/11 Act), by providing automated vetting of travelers from VWP countries.

System: Critical Infrastructure Change Detection (CICD).

Component: Science and Technology.

Date of approval: June 19, 2008.

The Critical Infrastructure Change Detection (CICD) program is a DHS S&T research program that is examining novel technical approaches to provide wide area surveillance and change detection capabilities to protect the Nation's critical infrastructure. S&T

proposes to test a high resolution, 360 degree field-of-view video system that will accommodate multiple simultaneous users and also have change detection and tracking capabilities. A PIA is being conducted because the system demonstration will be performed in a public area of New York City and will involve capturing images of persons and textual information in the public space.

System: Department of Homeland Security General Contact List.

Component: DHS Wide.

Date of approval: June 30, 2008.

Many Department of Homeland Security operations and projects collect a minimal amount of contact information in order to distribute information and perform various other administrative tasks. Department Headquarters conducted this privacy impact assessment because contact lists contain PII. The Department added the following systems to this PIA:

- Science and Technology Cyber Security Research and Development Center Web Site,
- U.S. Coast Guard Proceedings magazine online subscription request form,
- Federal Emergency Management Agency National Fire Academy Long-Term Evaluation,
- Federal Emergency Management Agency Port Security Grant Program,
- National Protection and Programs Directorate Telecommunications Service Priority (TSP) Web.

Dated: October 21, 2008.

Hugo Teufel III,

Chief Privacy Officer, Department of Homeland Security.

[FR Doc. E8–25962 Filed 10–30–08; 8:45 am]

BILLING CODE 4410–10–P

DEPARTMENT OF HOMELAND SECURITY

U.S. Customs and Border Protection

Notice of Issuance of Final Determination Concerning Walkers

AGENCY: U.S. Customs and Border Protection, Department of Homeland Security.

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 certain walkers which may be offered to the United States Government under a government procurement contract. Based upon the facts presented, in the final determination CBP concluded that Hong Kong is the country of origin of the walkers for purposes of U.S. Government procurement.

DATES: The final determination was issued on October 22, 2008. 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 December 1, 2008.

FOR FURTHER INFORMATION CONTACT: Gerry O'Brien, Valuation and Special Programs Branch, Regulations and Rulings, Office of International Trade (202–572–8792).

SUPPLEMENTARY INFORMATION: Notice is hereby given that on October 22, 2008, 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 certain walkers which may be offered to the United States Government under a government procurement contract. This final determination, in HQ H033839, was issued at the request of Drive Medical Design and Manufacturing under 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 concluded that, based upon the facts presented, certain articles will be substantially transformed in Hong Kong. Therefore, CBP found that Hong Kong is the country of origin of the finished articles 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, CBP 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**.

Dated: October 22, 2008.

Sandra L. Bell,

Executive Director, Office of Regulations and Rulings, Office of International Trade.

Attachment

HQ H033839

October 22, 2008

MAR–2–05 OT:RR:CTF:VS H033839 GOB

Category: Marking. Beth C. Ring, Esq., Sandler, Travis & Rosenberg, P.A., 551 Fifth Avenue, New York, NY 10176.

Re: U.S. Government Procurement; Title III, Trade Agreements Act of 1979 (19 U.S.C. 2511); Subpart B, Part 177, CBP Regulations; Walkers

Dear Ms. Ring: This is in response to your letter of July 18, 2008, requesting a final determination on behalf of Drive Medical Design and Manufacturing (''Drive Medical''), pursuant to subpart B of Part 177, Customs and Border Protection (''CBP'') Regulations (19 CFR 177.21 *et seq.*). You made a supplemental submission on September 29, 2008. 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 certain walkers. We note that Drive Medical is a party-at-interest within the meaning of 19 CFR 177.22(d)(1) and is entitled to request this final determination.

Facts

You describe the pertinent facts as follows. Drive Medical will assemble the walkers at a facility in Hong Kong. You state that the two ''U'' frame side pieces will be manufactured in Hong Kong. All of the other parts will be manufactured in China. The parts consist of the following:

- two ''U'' frame side pieces
- two release pins
- two springs
- four brass pins
- four stainless steel wire springs
- four crossbars
- one ''H'' frame
- four silencer caps
- four rubber tips
- two composite plastic hand grips
- two plastic push buttons
- an assortment of steel screws and nuts

You describe the manufacturing process as follows:

- The side frame is fitted with a handle grip using high pressure air to seat the handle in the proper position, The handle grip is heated prior to this process for better malleability.
- The top cross brace is secured to the side frame using a stainless steel star nut applied with an air screwdriver with a predetermined torque setting. This process is carried out on both front and back of the side frame and on both the left and right side.
- The side frames are placed through the ends of the center ''H'' frame. During this process a silencer ring is placed on the bottom tubes of the ''H'' frame, and an internal spacer is wrapped on the inside of the top of the ''H'' frame to reduce ''wobble.''
- A rivet with plastic guide is now mounted under the ''H'' frame directly to the side frame on both sides. These rivets hold the ''H'' frame in place.
- The lower side ''U'' frame support is now riveted to the side frame, front and back, on both sides of the walker.
- Release pins are dropped into both sides of the ''H'' frame to create the folding