DEPARTMENT OF HEALTH AND HUMAN SERVICES

National Institutes of Health
National Cancer Institute; Closed Meetings

Pursuant to section 10(d) of the Federal Advisory Committee Act, as amended (5 U.S.C. App.), notice is hereby given of the following meetings.

The meetings will be closed to the public in accordance with the provisions set forth in sections 552b(c)(4) and 552b(c)(6), Title 5 U.S.C., as amended. The grant applications/contract proposals and the discussions could disclose confidential trade secrets or commercial property such as patentable material, and personal information concerning individuals associated with the grant applications/contract proposals the disclosure of which would constitute a clearly unwarranted invasion of personal privacy.

Name of Committee: National Cancer Institute Special Emphasis Panel; Tools To Probe DNA Repair and Damage Signaling Networks.

Date: June 6, 2012.

Time: 11:00 a.m. to 12:00 p.m.

Agenda: To review and evaluate contract proposals.

Place: National Institutes of Health, 6116 Executive Boulevard, Rockville, MD 20852, (Telephone Conference Call).

Contact Person: David G. Ransom, Ph.D., Scientific Review Officer, Research Programs Review Branch, Division of Extramural Activities, National Cancer Institute, NIH, 6116 Executive Blvd., Room 8133, Bethesda, MD 20892–8328, 301–493–4757, david.ransom@nih.gov.

This notice is being published less than 15 days prior to the meeting due to scheduling conflicts.

Name of Committee: National Cancer Institute Special Emphasis Panel; Cancer Prevention Research Small Grant Program (R03).

Date: June 28, 2012.

Time: 8:00 a.m. to 6:00 p.m.

Agenda: To review and evaluate grant applications.

Place: Bethesda North Marriott Hotel Conference & Center, 5701 Marinelli Road, North Bethesda, MD.

Contact Person: Clifford W Schweinfest, Ph.D., Scientific Review Officer, Special Review and Logistics Branch, Division of Extramural Activities, National Cancer Institute, NIH, 6116 Executive Blvd., Room 8050a, Bethesda, MD 20892–8329, 301–402–9415, schweinfestcw@mail.nih.gov.

Information is also available on the Institute’s/Center’s home page: http://deainfo.nci.nih.gov/advisory/sep/sep.htm, where an agenda and any additional information for the meeting will be posted when available.

[Catalogue of Federal Domestic Assistance Program Nos. 93.392, Cancer Construction; 93.393, Cancer Cause and Prevention Research; 93.394, Cancer Detection and Diagnosis Research; 93.395, Cancer Treatment Research; 93.396, Cancer Biology Research; 93.397, Cancer Centers Support; 93.398, Cancer Research Manpower; 93.399, Cancer Control, National Institutes of Health, HHS]

Dated: May 16, 2012.

Jennifer S. Spaeth, Director, Office of Federal Advisory Committee Policy.

BILLING CODE 4140–01–P

DEPARTMENT OF HOMELAND SECURITY

Office of the Secretary
[Docket No. DHS–2012–0019]


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 and expand an existing Department of Homeland Security system of records notice titled, U.S. Customs and Border Protection, DHS/CBP–006—Automated Targeting System (ATS) 72 FR 43650, August 6, 2007. The Department of Homeland Security (DHS) and U.S. Customs and Border Protection (CBP) have designed ATS to efficiently perform risk assessments on information pertaining to international travelers and import and export shipments attempting to enter or leave the United States. ATS uses a rule-managed technology that facilitates the targeting of high-risk travelers and cargo.

DHS/CBP is publishing this System of Records Notice (SORN) to update ATS and to update and expand the categories of individuals, categories of records, routine uses, access provisions, and sources of data stored in ATS.

Elsewhere in the Federal Register, the Department of Homeland Security is concurrently issuing a Notice of Proposed Rulemaking exempting this system of records from certain provisions of the Privacy Act. This updated and expanded system will be included in the Department of Homeland Security’s inventory of record systems.

DATES: Submit comments on or before June 21, 2012. This system will be effective June 21, 2012.

ADDRESSES: You may submit comments, identified by docket number DHS–2012–0019 by one of the following methods:


Fax: 703–483–2999.

Mail: Mary Ellen Callahan, Chief Privacy Officer, Privacy Office, Department of Homeland Security, Washington, DC 20528.

Instructions: All submissions received must include the agency name and docket number for this rulemaking. All comments received will be posted without change to http://www.regulations.gov, including any personal information provided.

Docket: For access to the docket to read background documents or comments received go to http://www.regulations.gov.

FOR FURTHER INFORMATION CONTACT: For general questions please contact: Laurence E. Castelli (202–325–0280), CBP Privacy Officer, Office of

SUPPLEMENTARY INFORMATION:

I. Background


This SORN is being updated and expanded to inform the public about changes to the Automated Targeting System (ATS) categories of individuals, categories of records, routine uses, access provisions, and sources of data. DHS/CBP is updating and expanding the categories of individuals, categories of records, and sources of records stored in ATS because it has certain data that it must ingest for performance purposes. The Privacy Impact Assessment (PIA), which DHS will publish on its Web site (http://www.dhs.gov/privacy) concurrently with the publication of this SORN in the Federal Register, provides a full discussion of the functional capabilities of ATS and its modules. DHS and CBP have previously exempted portions of ATS from the notification, access, amendment, and public accounting provisions of the Privacy Act because it is a law enforcement system. DHS and CBP, however, will consider each request for access to records maintained in ATS to determine whether or not information may be released. DHS and CBP further note that despite the exemption taken on this system of records they are providing access and amendment to passenger name records (PNR) collected by CBP pursuant to its statutory authority, 49 U.S.C. 44909, as implemented by 19 CFR 122.49d, for CBP uses, as well as for security, public law enforcement, and other official purposes.

ATS provides the following basic functionalities to support CBP in identifying individuals and cargo that need additional review across the different means or modes of travel to and from the United States:

Comparison: ATS compares information on travelers and cargo coming into and going out of the country against law enforcement and intelligence databases to identify individuals and cargo requiring additional scrutiny. For example, ATS compares information on individuals (identified as passengers, travelers, crewmembers, or persons appearing on documents supporting the movement of cargo) trying to enter the country or trying to enter merchandise into the country against the Terrorist Screening Database (TSDB), which ATS ingests from the DHS Watchlist Service (WLS), and outstanding warrants and warrants.

• Rules: ATS compares existing information on individuals and cargo entering and exiting the country with patterns identified as requiring additional scrutiny. The patterns are based on CBP officer experience, analysis of trends of suspicious activity, and raw intelligence corroborating those trends. For example, ATS might compare information on cargo entering the country against a set of scenario-based targeting rules that indicate a particular type of fish rarely is imported from a given country.

• Federated Query: ATS allows users to search data across many different databases and correlate it across the various systems to provide a person centric view of all data responsive to a query about the person’s identity from the selected databases.

In order to do the above, ATS pulls data from many different source systems. In some instances ATS is the official record for the information, while in other instances ATS ingests and maintains the information as a copy or provides a pointer to the information in the underlying system. Below is a summary:

• Official Record: ATS maintains the official record for Passenger Name Records (PNR) collected by CBP pursuant to its statutory authority, 49 U.S.C. 44909, as implemented by 19 CFR 122.49d, for Importer Security Filing (10+2 documentation) information, which provides advanced information about cargo and related persons and entities for risk assessment and targeting purposes; for results of Cargo Enforcement Exams; for the combination of license plate, Department of Motor Vehicle (DMV) registration data and biographical data associated with a border crossing; for law enforcement and/or intelligence data, reports, and projects developed by CBP analysts that may include public source and/or classified information; and information obtained through memoranda of understanding or other arrangements where the information is relevant to the border security mission of the Department.

• Ingestion of Data: ATS maintains copies of key elements of certain CBP databases in order to minimize the processing time for searches on the operational systems and to act as a backup for certain operational systems, including, but not limited to:

Automated Commercial Environment (ACE), Automated Commercial System (ACS), Automated Export System (AES), Advance Passenger Information System (APIS), Border Crossing Information (BCI), Consular Electronic Application Center (CEAC), Enforcement Integrated Database (EID)(which includes the Enforcement Case Tracking System (ENFORGE)), Electronic System for Travel Authorization (ESTA), Global Enrollment System (GES), Non-Immigrant Information System (NIIS), historical National Security Entry-Exit Registration System (NSEE-RS), Seized Asset and Case Tracking System (SEACATS), U.S. Immigration and Customs Enforcement (ICE) Student Exchange and Visitor Information System (SEVIS), Social Security Administration (SSA) Death Master File, TECS, Terrorist Screening Database (TSDB) through the DHS Watchlist Service (WLS), and WebIDENT. If additional data is ingested and that additional data does not require amendment of the categories of individuals or categories of records in this SORN, the PIA for ATS will be updated to reflect that information. The updated PIA can be found at www.dhs.gov/privacy.

• Pointer System: ATS accesses and uses additional databases without ingesting the data, including, but not limited to: CBP Border Patrol Enforcement Tracking System (BPETS), Department of State Consular Consolidated Database (CCD), commercial data aggregators, CBP’s Enterprise Geospatial Information Services (eGIS), DHS/USVISIT IDENT, National Law Enforcement Telecommunications System (Nlets), DOJ’s National Crime Information Center (NCIC), the results of queries in the FBI’s Interstate Identification Index (III), and the National Insurance Crime Bureau’s (NICB’s) private database of stolen vehicles. If additional data is ingested and that additional data does not require amendment of the categories of individuals or categories of records in this SORN, the PIA for ATS will be updated to reflect that information. The updated PIA can be found at www.dhs.gov/privacy.

DHS/CBP has reorganized the ATS routine uses to provide greater uniformity across DHS systems. Consistent with DHS’s information sharing mission, information stored in
ATS 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 recipient has a need to know the information to carry out functions consistent with the routine uses set forth in this SORN.

DHS has exempted the system from the notification, access, amendment, and certain accounting provisions of the Privacy Act of 1974 because of the law enforcement nature of ATS. Despite the exemptions taken under the Privacy Act of records, CBP and DHS are not exempting the following records from the access and amendment provisions of the Privacy Act: passenger name records (PNR) collected by CBP pursuant to its statutory authority, 49 U.S.C. 44909, as implemented by 19 CFR 122.49, Importer Security Filing (10+2 documentation) information, and any records that were ingested by ATS where the source system of records already provides access and/or amendment under the Privacy Act. A traveler may obtain access to his or her PNR and request amendment as appropriate, but records concerning the targeting rules, the responses to rules, case events, law enforcement and/or intelligence data, reports, projects developed by CBP that may include public source and/or classified information, information obtained through memorandum of understanding or other arrangements because the information is relevant to the border security mission of the Department, or records exempted from access by the system from which ATS ingested or accessed the information, will not be accessible to the individual.

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 individuals’ 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 for which information is retrieved by the name of an individual or by some identifying number, symbol, or other identifying particular assigned to the individual. In the Privacy Act, an individual is defined to encompass United States citizens and lawful permanent residents. As a matter of policy (Privacy Policy Guidance Memorandum 2007-1, most recently updated January 7, 2009), DHS extends administrative Privacy Act protections to all persons, regardless of citizenship, where a system of records maintains information on U.S. citizens, lawful permanent residents, and visitors. Individuals may request access to their own records that are maintained in a system of records in the possession or under the control of DHS by complying with DHS Privacy Act regulations, 6 CFR Part 5.

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 to which their records are put, and to assist individuals with more easily finding such files within the agency. Below is the description of the U.S. Customs and Border Protection DHS/CBP–006 Automated Targeting System system of records.

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

System of Records

DHS/CBP–006.

SYSTEM NAME:

U.S. Customs and Border Protection Automated Targeting System.

SECURITY CLASSIFICATION:

Unclassified, sensitive, classified.

SYSTEM LOCATION:

Records are maintained at the CBP Headquarters in Washington, DC, and can be accessed from field offices and from locations abroad where ATS users are stationed.

CATegories of Records in the System:

ATS contains various types of data to support its targeting missions, incorporating information germane to the identification of individuals, including, but not limited to:

- Name
- Addresses (home, work, and/or destination, as appropriate)
- Telephone and fax numbers
- Tax ID number (e.g., Employer Identification Number (EIN) or Social Security Number (SSN), where available)
- Date and place of birth
- Gender
- Nationality
- Country of Residence
- Citizenship
- Alias
- Physical characteristics, including biometrics where available (e.g., height, weight, race, eye and hair color, scars, tattoos, marks, fingerprints)
- Familial relationships and other contact information
- Property information
- Occupation and employment information
- Biographical and biometric information from or associated with online immigrant and non-immigrant visa applications, including (as available):
  - U.S. sponsor’s name, address, and phone number
  - U.S. contact name, address, and phone number

I. Persons who may pose a threat to the United States.

CATegories of Individuals Covered by the System:

ATS handles information relating to the following individuals:

A. Persons, including operators, crew, and passengers, who seek to, or do in fact, enter, exit, or transit through the United States or through other locations where CBP maintains an enforcement or operational presence by land, air, or sea.
B. Crew members traveling on commercial aircraft that fly over the United States.
C. Persons who engage in any form of trade or other commercial transaction related to the importation or exportation of merchandise, including those required to submit an Importer Security Filing.
D. Persons who are employed in any capacity related to the transit of merchandise intended to cross the United States border.
E. Persons who serve as booking agents, brokers, or other persons who provide information on behalf of persons seeking to enter, exit, or transit through the United States, or on behalf of persons seeking to import, export or ship merchandise through the United States.
F. Owners of vehicles that cross the border.
G. Persons whose data was received by the Department as the result of memoranda of understanding or other information sharing agreement or arrangement because the information is relevant to the border security mission of the Department.
H. Persons who were identified in a narrative report, prepared by an officer or agent, as being related to or associated with other persons who are alleged to be involved in, who are suspected of, or who have been arrested for violations of the laws enforced or administered by DHS.
I. Persons who may pose a threat to the United States.
• Passenger Name Record (PNR):  
   1. PNR record locator code  
   2. Date of reservation/issue of ticket  
   3. Date(s) of intended travel  
   4. Name(s)  
   5. Available frequent flier and benefit information (i.e., free tickets, upgrades)  
   6. Other names on PNR, including number of travelers on PNR  
   7. All available contact information (including originator of reservation)  
   8. All available payment/billing information (e.g., credit card number)  
   9. Travel itinerary for specific PNR  
  10. Travel agency/travel agent  
  11. Code share information (e.g., when one air carrier sells seats on another air carrier’s flight)  
  12. Split/divided information (e.g., when one PNR contains a reference to another PNR)  
  13. Travel status of passenger (including confirmations and check-in status)  
  14. Ticketing information, including ticket number, one way tickets and Automated Ticket Fare Quote (ATFQ) fields  
  15. Baggage information  
  16. Seat information, including seat number  
  17. General remarks including Other Service Indicated (OSI), Special Service Indicated (SSI) and Supplemental Service Request (SSR) information  
  18. Any collected APIS information (e.g., Advance Passenger Information (API)) that is initially captured by an air carrier within its PNR, such as passport number, date of birth and gender  

Note: Not all air carriers maintain the same sets of information for PNR, and a particular individual’s PNR likely will not include information for all possible categories. In addition, PNR does not routinely include information that could directly indicate the racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, health, or sex life of the individual. To the extent PNR does include terms that reveal such personal matters, DHS employs an automated system that filters certain of these terms and only uses this information in exceptional circumstances where the life of an individual could be imperiled or seriously impaired.

The system contains information collected for the importation or exportation of cargo and/or property, including:  
- Bill of Lading  
- Commodity type  
- License number and license country for Office of Defense Trade Controls registrants  
- Inspection and examination results  

The system contains information for Joint Automated Targeting System (JATS) and/or classified information obtained by users/analysts for reference or incorporation into the report or project.

PORTIVE PURPOSES FOR PNR IN ATS: PNR may be used:  
(1) To prevent, detect, investigate, and prosecute:  
   a. Terrorist offenses and related crimes, including  

AUTHORITY FOR MAINTENANCE OF THE SYSTEM:  
i. Conduct that—
  1. involves a violent act or an act
dangerous to human life, property, or
infrastructure; and
  2. appears to be intended to—
    a. intimidate or coerce a civilian
population;
    b. influence the policy of a
government by intimidation or coercion;
or
    c. affect the conduct of a government
by mass destruction, assassination,
kidnapping, or hostage-taking.
ii. Activities constituting an offense
within the scope of and as defined in
applicable international conventions
and protocols relating to terrorism;
iii. Providing or collecting funds, by
any means, directly or indirectly, with
the intention that they should be used
or in the knowledge that they are to be
used, in full or in part, in order to carry
out any of the acts described in
subparagraphs (i) or (ii);
iv. Attempting to commit any of the
acts described in subparagraphs (i), (ii),
or (iii);
v. Participating as an accomplice in
the commission of any of the acts
described in subparagraphs (i), (ii), or
(iii);
vi. Organizing or directing others to
commit any of the acts described in
subparagraphs (i), (ii), or (iii);

A crime is considered as transnational
in nature in particular if:
  i. It is committed in more than one
country;
  ii. It is committed in one country but
a substantial part of its preparation,
planning, direction or control takes
place in another country;
  iii. It is committed in one country but
involves an organized criminal group
that engages in criminal activities in
more than one country;
  iv. It is committed in one country but
has substantial effects in another
country; or
  v. It is committed in one country and
the offender is in or intends to travel to
another country;
  2. on a case-by-case basis where
necessary in view of a serious threat and
for the protection of vital interests of
any individual or if ordered by a court;
  3. to identify persons who would be
subject to closer questioning or
examination upon arrival to or
departure from the United States or who
may require further examination.
  4. for domestic law enforcement,
judicial powers, or proceedings, where
violations of law or indications thereof
are detected in the course of the use and
processing of PNR.

PURPOSES OF ATS (EXCEPT FOR
PNR):

ATS uses all other data for purposes
listed above as well as below:
(a) To perform targeting of individuals
who may pose a risk to border security
or public safety, may be a terrorist or
suspected terrorist, or may otherwise be
engaged in activity in violation of U.S.
law;
(b) To perform a risk-based
assessment of conveyances and cargo to
focus CBP’s resources for inspection and
examination and enhance CBP’s ability
to identify potential violations of U.S.
law, possible terrorist threats, and other
threats to border security; and
(c) To otherwise assist in the
enforcement of the laws enforced or
administered by DHS, including those
related to counterterrorism.

ROUTINE USES OF RECORDS MAINTAINED
IN THE SYSTEM, INCLUDING CATEGORIES OF USERS
AND THE PURPOSES OF SUCH USES:

Information ingested into this system
from another source system is to be
distributed consistent with the published
system of records notice for the
source system and will continue to be
governed by the routine uses for that
source system. The routine uses below apply
only to records that are maintained as
official records in ATS (i.e., records
which are maintained in ATS that are
not covered by other originating systems
of record, including: PNR; Importer
Security Filings; Cargo Enforcement
Exams; the combination of license plate,
Department of Motor Vehicle (DMV)
registration data and biographical data
associated with a border crossing; law
enforcement and/or intelligence data,
reports, and projects developed by
CSBP analysts that may include public
source information and/or classified
information; and information obtained
through memoranda of understanding or
other arrangements because the
information is relevant to the border
security mission of the Department).

With respect to PNR, DHS only
discloses information to those
authorities who intend to use the
information consistent with the
purposes identified above, and have
sufficient capability to protect and
safeguard the information. In addition to
disclosures generally permitted
under 5 U.S.C. 552(a)(b) of the Privacy
Act, all or a portion of the records or
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 or relevant 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.
B. To a congressional office from the
record of an individual in response to
an inquiry from that congressional office
made pursuant to a written Privacy Act
waiver at the request of the individual to
whom the record pertains.
C. To the National Archives and
Records Administration or General
Services Administration pursuant to
records management inspections being
conducted under the authority of
44 U.S.C. 2904 and 2906.
D. To an agency or organization 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. DHS has determined that as a result
of the suspected or confirmed
compromise there is a risk of harm to
economic or property interests, of
identity theft or fraud, or of harm to the
security or integrity of this system or of
harm to other systems or programs
(which maintained by DHS or another
agency or entity) or harm to the
individuals that rely 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 the
federal government 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 appropriate federal, state, tribal, local, or foreign governmental agencies or multilateral governmental organizations responsible for investigating or prosecuting the violations of, or for enforcing or implementing, a statute, rule, regulation, order, or license, where CBP believes the information would assist enforcement of applicable civil or criminal laws;

H. To federal and foreign government intelligence or counterterrorism agencies or components where DHS becomes aware of an indication of a threat or potential threat to national or international security, or to assist in anti-terrorism efforts;

I. To an organization or person in either the public or private sector, either foreign or domestic, where there is a reason to believe that the recipient is or could become the target of a particular terrorist activity or conspiracy, or where the information is relevant to the protection of life, property, or other vital interests of a person;

J. To appropriate federal, state, local, tribal, or foreign governmental agencies or multilateral governmental organizations for the purpose of protecting the vital interests of a data subject or other persons, including to assist such agencies or organizations in preventing exposure to or transmission of a communicable or quarantinable disease or to combat other significant public health threats; appropriate notice will be provided of any identified health threat or risk;

K. 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 response to a subpoena, or in connection with criminal law proceedings;

L. 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 in the proper performance of the official duties of the officer making the disclosure;

M. To appropriate federal, state, local, tribal, or foreign governmental agencies or multilateral governmental organizations where CBP is aware of a need to utilize relevant data for purposes of testing new technology and systems designed to enhance ATS;

N. 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, RETRIEVAL, 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:

Records may be retrieved by any of the data elements described in “Categories of Records,” including by name or personal identifier from an electronic database.

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 permissions.

RETENTION AND DISPOSAL:

Official Records in this system (Passenger Name Records (PNR); Importer Security Filings (10+2 documentation); results of Cargo Enforcement Exams; the combination of license plate, Department of Motor Vehicle registration data, and biographical data associated with a border crossing; law enforcement and/or intelligence data, reports, and projects developed by CBP analysts that may include public source information and/or classified information; and information obtained through memoranda of understanding or other arrangements because the information is relevant to the border security mission of the Department will be retained and disposed of in accordance with a records schedule approved by the National Archives and Records Administration on April 12, 2008. ATS collects information directly, ingests information from various systems, and accesses other systems without ingesting the data. To the extent information is ingested from other systems, data is retained in ATS in accordance with the record retention requirements of those systems, or the retention period for ATS, whichever is shortest. The retention period for the official records maintained in ATS will not exceed fifteen years, after which time the records will be deleted, except as noted below. The retention period for PNR will be subject to the following further access restrictions: ATS users with PNR access will have access to PNR in an active database for up to five years, during which time the PNR will be depersonalized following the first six months retention. After this initial five-year retention, the PNR data will be transferred to a dormant database for a period of up to ten years. PNR data in dormant status will be subject to additional controls including the requirement of obtaining access approval from a senior DHS official designated by the Secretary of Homeland Security. Furthermore, PNR in the dormant database may only be repersonalized in connection with a law enforcement operation and only in response to an identifiable case, threat, or risk. Such limited access and use for older PNR strikes a reasonable balance between protecting this information and allowing CBP to continue to identify potential high-risk travelers. Notwithstanding the foregoing, information maintained only in ATS that is linked to active law enforcement lookout records, CBP matches to enforcement activities, and/or investigations or cases (i.e., specific and credible threats; flights, individuals, and routes of concern; or other defined sets of circumstances) will remain accessible for the life of the law enforcement matter to support that activity and other enforcement activities that may become related. The justification for a fifteen-year retention period for the official records is based on CBP’s law enforcement and security functions at the border. This retention period is based on CBP’s
historical encounters with suspected terrorists and other criminals, as well as the broader expertise of the law enforcement and intelligence communities. It is well known, for example, that potential terrorists may make multiple visits to the United States in advance of performing an attack. It is over the course of time and multiple visits that a potential risk becomes clear. Travel records, including historical records, are essential in assisting CBP Officers with their risk-based assessment of travel indicators and identifying potential links between known and previously unidentified terrorist facilitators. Analyzing these records for these purposes allows CBP to continue to effectively identify suspect travel patterns and irregularities.

**SYSTEM MANAGER AND ADDRESS:**

Executive Director, Automation and Targeting Division, Office of Intelligence and Investigative Liaison, U.S. Customs and Border Protection, and Director, Targeting and Analysis, Systems Program Office, Office of Information and Technology, U.S. Customs and Border Protection, both of whom are located at 1300 Pennsylvania Avenue NW., Washington, DC 20229.

**NOTIFICATION PROCEDURE:**

The Secretary of Homeland Security has exempted this system from the notification, access, amendment, and certain accounting procedures of the Privacy Act because it is a law enforcement system. These exemptions also apply to the extent that information in this system of records is recompiled or is created from information contained in other systems of records with appropriate exemptions in place. To the extent that a record is exempted in a source system, the exemption will continue to apply. Despite the exemptions taken on this system of records, CBP and DHS are not exempting the following records from the access and amendment provisions of the Privacy Act: passenger name records (PNR) collected by CBP pursuant to its statutory authority, 49 U.S.C. 44909, as implemented by 19 CFR 122.49d; Importer Security Filing (10+2 documentation) information; and any records that were ingested by ATS where the source system of records already provides access and/or amendment under the Privacy Act. Individuals seeking notification of and access to records contained in this system of records, or seeking to contest its content, may submit a request in writing to the Headquarters or CBP 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–0655, Washington, DC 20528.

**RECORD ACCESS PROCEDURES:**

See “Notification procedure” above.

**CONTESTING RECORD PROCEDURES:**

See “Notification procedure” above.

**RECORD SOURCE CATEGORIES:**

Records are ingested from other DHS and federal systems, and from foreign governments (in accordance with the terms of international agreements and arrangements), including but not limited to ACE, ACS, AES, APIS, BCI, CEAC, (including Forms DS–160 and DS–260), ENFORCE, ESTA, GES, NIIS, NSEERS, SEACATS, SEVIS, TECS, TSDB–WLS, Social Security Administration’s Death Master File, and WebDENT. Additionally, PNR is obtained from travel reservation systems of commercial carriers. Information from Importer Security Filings is received from importers and ocean carriers. Records are accessed from BPETS, CCD, eGIS, NCIC, and Nlets. Also, the results of queries in the FBI’s Interstate Identification Index (III), the National Insurance Crime Bureau’s (NICB’s) private database of stolen vehicles, and commercial data aggregators are stored in ATS. Lastly, records are also developed from analysis created by users as a result of their use of the system.

**EXEMPTIONS CLAIMED FOR THE SYSTEM:**

Pursuant to 6 CFR Part 5, Appendix C, certain records and information in this system are exempt from 5 U.S.C. 552a(c)(3) and (4); (d)(1), (2), (3), and (4); (e)(1), (2), (3), (4)(C) through (I), (o)(5), and (8); (f), and (g) of the Privacy Act pursuant to 5 U.S.C. 552a(j)(2). Additionally, the Secretary of Homeland Security has exempted this system from the following provisions of the Privacy Act, pursuant to 5 U.S.C. 552a(k)(1) and (k)(2): 5 U.S.C. 552a(c)(3); (d)(1), (d)(2), (d)(3), and (d)(4); (e)(1), (o)(4)(G), (o)(4)(H), (o)(4)(I); and (f).

Despite the exemptions taken on this system of records, CBP and DHS are not exempting the following records from the access and amendment provisions of the Privacy Act: passenger name records (PNR) collected by CBP pursuant to its statutory authority, 49 U.S.C. 44909, as implemented by 19 CFR 122.49d; Importer Security Filing (10+2 documentation) information; and any records that were ingested by ATS where the source system of records already provides access and/or amendment under the Privacy Act. A traveler may obtain access to his or her PNR, but records concerning the targeting rules, the responses to rules, case events, law enforcement and/or intelligence data, reports, and projects developed by CBP analysts that may include public source information and/or classified information, information obtained through memorandum of understanding or other arrangements because the information is relevant to the border security mission of the Department, or records exempted from access by the system from which ATS
ingested or accessed the information will not be accessible to the individual.

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

[FR Doc. 2012–12396 Filed 5–21–12; 8:45 am]
BILLING CODE 9110–06–P

DEPARTMENT OF HOMELAND SECURITY

Coast Guard

[Docket No. USCG–2012–0456]

Merchant Marine Personnel Advisory Committee: Intercessional Meeting

AGENCY: Coast Guard, DHS.

ACTION: Notice of Federal Advisory Committee Working Group Meeting.

SUMMARY: A working group of the Merchant Marine Personnel Advisory Committee (MERPAC) will meet to discuss Task Statement 76, “Review of Performance Measures (Assessment Criteria);” and Task Statement 77, “Development of Performance Measures (Assessment Criteria).” This meeting will be open to the public.

DATES: The working group will meet from June 11th through June 15th, 2012, from 8 a.m. until 5 p.m. each day. Please note that the meeting may adjourn before June 15th if all business is finished. Written comments to be distributed to working group members and placed on MERPAC’s Web site are due by June 5th, 2012.

ADDRESSES: The working group will meet at the Seafarers Harry Lundeborg School of Seamanship, 45353 Saint Georges Ave., Piney Point, MD 20674.

For information on facilities or services for individuals with disabilities or to request special assistance, contact Mr. Howard Thompson at telephone number 301–994–0010 ext. 5463 as soon as possible.

To facilitate public participation, we are inviting public comment on the issues to be considered by the working group, which are listed in the “Agenda” section below. Written comments must be submitted by Docket No. USCG–2012–0456 and may be submitted by one of the following methods:

• Federal eRulemaking Portal: http://www.regulations.gov. Follow the instructions for submitting comments (preferred method to avoid delays in processing).

• Fax: 202–372–1918.

• Mail: Docket Management Facility (M-30), U.S. Department of Transportation, West Building Ground Floor, Room W12–140, 1200 New Jersey Avenue SE., Washington, DC 20590–0001.

• Hand delivery: Same as mail address above, between 9 a.m. and 5 p.m., Monday through Friday, except Federal Holidays. The telephone number is 202–366–9329.

Instructions: All submissions received must include the words “Department of Homeland Security” and the docket number for this action. Comments received will be posted without alteration at http://www.regulations.gov, including any personal information provided. You may review a Privacy Act notice regarding our public dockets in the January 17, 2008, issue of the Federal Register (73 FR 3316).

Docket: For access to the docket to read documents or comments related to this notice, go to http://www.regulations.gov. This notice may be viewed in our online docket, USCG–2012–0456, at http://www.regulations.gov.

FOR FURTHER INFORMATION CONTACT: Mr. Rogers Henderson, Alternate Designated Federal Officer (ADFO), telephone 202–372–1408. If you have any questions on viewing or submitting material to the docket, call Renee V. Wright, Program Manager, Docket Operations, telephone 202–366–9826.

SUPPLEMENTARY INFORMATION: Notice of this meeting is given under the Federal Advisory Committee Act (FACA), 5 U.S.C. App. (Pub. L. 92–463).

MERPAC is an advisory committee established under the Secretary’s authority in section 871 of the Homeland Security Act of 2002, Title 6, United States Code, section 451, and chartered under the provisions of the FACA. The Committee acts solely in an advisory capacity to the Secretary of the Department of Homeland Security (DHS) through the Commandant of the Coast Guard and the Director of Commercial Regulations and Standards on matters relating to personnel in the U.S. merchant marine, including but not limited to training, qualifications, certification, documentation, and fitness standards. The Committee will advise, consult with, and make recommendations reflecting its independent judgment to the Secretary.

Agenda

June 11–15, 2012

The agenda for the June 11th–June 15th, 2012 working group meeting is as follows:

(1) Discuss, prepare, and review proposed recommendations for the full committee to consider concerning Task Statement 76, “Review of Performance Measures (Assessment Criteria),” and Task Statement 77, “Development of Performance Measures (Assessment Criteria).” Task Statements 76 and 77 can be used to assess mariner competencies listed in the International Convention on Standards of Training, Certification and Watchkeeping, 1978 as amended. The working group will specifically address performance measures (assessment criteria) for mariners seeking an endorsement as: Officer in Charge of a Navigational Watch and Master on ships of less than 500 Gross Tonnage as measured under the International Tonnage Convention (ITC) while engaged on near-coastal voyages; Able Seafarer—Deck; Chief Engineer Officer and Second Engineer Officer on ships powered by main propulsion machinery of 3,000 kW propulsion power or more; Chief Engineer Officer and Second Engineer Officer on ships powered by main propulsion machinery of between 750 kW and 3,000 kW propulsion power; Able Seafarer—Engine; Electro-Technical Officer; and Electro-Technical Rating;

(2) Public comment period (each day); and

(3) Adjournment of meeting.

Procedural: A copy of all meeting documentation is available at http://www.fido.gov/facadatabase or by contacting Rogers Henderson as indicated above. Once you have accessed the site’s main page, click on “Public Access;” at the next page highlight “2012” then click “Explore Data.” At the next page, click on “Department of Homeland Security;” Click on the MERPAC Committee page, click on the meetings tab and then the “View” button for the meeting dated June 11, 2012 to access the information for this meeting. Minutes will be available 90 days after this meeting. Both minutes and documents applicable for this meeting can also be found at an alternative site using the following web address: https://homeport.uscg.mil and use these key strokes: Missions; Port and Waterways; Safety Advisory Committees; MERPAC; and then use the event key. A public oral comment period will be held each day during the working group meeting. Speakers are requested to limit their comments to 3 minutes. Please note that the public oral comment period may end before the prescribed ending time of the meeting. Contact Rogers Henderson as indicated above to register as a speaker.