applicable laws, rules and policies, including the DHS Information Technology Security Program Handbook. All records are protected from unauthorized access through appropriate administrative, physical, and technical safeguards. These safeguards include restricting access to authorized personnel who have a need-to-know, and using locks and password protection identification features. OIG file areas are locked after normal duty hours and facilities are protected from the outside by security personnel.

RETENTION AND DISPOSAL:

Records are retained and disposed of in accordance with the National Archives and Records Administration General Records Schedule 1, Item 29, Transmittal No. 12 (July 2004). Files may be retained for up to five years. For requests that result in litigation, the files related to that litigation will be retained for three years after final court adjudication.

SYSTEM MANAGER(S) AND ADDRESSES:

The System Managers are System Manager/OIG Office of Technology and System Manager/OIG Office of Audits, 1120 Vermont Avenue, NW., Washington, DC 20528.

NOTIFICATION PROCEDURES:

To determine whether this system contains records relating to you, write to the System Manager identified above.

RECORD ACCESS PROCEDURES:

A request for access to records in this system may be made by writing to the System Manager identified above, in conformance with 6 CFR part 5, subpart B, which provides the rules for requesting access to Privacy Act records maintained by DHS agencies.

CONTESTING RECORD PROCEDURES:

Same as ''Record Access Procedures,'' above.

RECORD SOURCE CATEGORIES:

Information contained in this system is obtained from OIG auditors and government and non-government entities conducting continuing professional education courses and conferences.

EXEMPTIONS CLAIMED FOR THE SYSTEM:

None.

Dated: April 7, 2005.

Nuala O'Connor Kelly,

Chief Privacy Officer, Department of Homeland Security.

[FR Doc. 05–7703 Filed 4–15–05; 8:45 am]

BILLING CODE 4410–10–P

DEPARTMENT OF HOMELAND SECURITY

Office of the Secretary

[DHS2005–0028]

Privacy Act of 1974; Systems of Records: Homeland Security Operations Center Database

AGENCY: Privacy Office, Department of Homeland Security.

ACTION: Notice of Privacy Act systems of records.

SUMMARY: In accordance with the Privacy Act of 1974, the Department of Homeland Security is giving notice that it proposes to add a new system of records to its inventory of record systems, the Homeland Security Operations Center Database.

DATES: Comments must be received on or before May 18, 2005.

ADDRESSES: You may submit comments, identified by Docket Number DHS–2004-xxxx, by *one* of the following methods:

- EPA Federal Partner EDOCKET Web site: *http://www.epa.gov/feddocket.* Follow instructions for submitting comments on the Web site.
- Federal eRulemaking Portal: *http://www.regulations.gov.* Follow the instructions for submitting comments.
- Fax: (202) 772–5036 (This is not a toll-free number).
- Mail: Sandy Ford Page, Director, Disclosure Officer, Office of the Chief Of Staff, Office of the Under Secretary for Information Analysis and Infrastructure Protection, Department of Homeland Security, Washington, DC 20528; Nuala O'Connor Kelly, Chief Privacy Officer, Department of Homeland Security, 245 Murray Lane, Building 410, Washington, DC 20528.
- Hand Delivery / Courier: Nuala O'Connor Kelly, DHS Chief Privacy Officer, 245 Murray Lane, Building 410, Washington, DC 20528.

Instructions: All submissions received must include the agency name and docket number for this notice. All comments received will be posted without change to *http://www.epa.gov/feddocket,* including any personal information provided. For detailed instructions on submitting comments and additional information on the rulemaking process, see the ''Public Participation'' heading of the **SUPPLEMENTARY INFORMATION** section of this document.

Docket: For access to the docket to read background documents or comments received, go to *http://www.epa.gov/feddocket.* You may also access the Federal eRulemaking Portal at *http://www.regulations.gov.*

FOR FURTHER INFORMATION CONTACT: Sandy Ford Page, Director, Disclosure Office, Office of the Chief of Staff, Office of the Under Secretary for Information Analysis and Infrastructure Protection, Department of Homeland Security, Washington, DC by telephone (202) 282–8522 or facsimile (202) 282–9069; Nuala O'Connor Kelly, Chief Privacy Officer, Department of Homeland Security, Washington, DC 20528 by telephone (202) 772–9848 or facsimile (202) 772–5036.

SUPPLEMENTARY INFORMATION: The Department of Homeland Security (DHS) is composed of five directorates. The mission of the Directorate for Information Analysis and Infrastructure Protection (IAIP) is to help deter, prevent, and mitigate acts of terrorism by assessing vulnerabilities in the context of changing threats. Within IAIP, the Homeland Security Operations Center (HSOC) serves as the technological platform to receive threat information, integrate it and disseminate it in order to support the following activities of IAIP:

a. Maintaining domestic situational awareness;

b. Facilitating homeland security information sharing and operational coordination with other operations centers to include incident management;

c. Monitoring threats and assisting in dissemination of homeland security threat warnings, advisory bulletins, and other information pertinent to national incident management;

d. Providing general situational awareness and support to, and acting upon, requests for information generated by the Interagency Incident Management Group; and

e. Facilitating domestic incident awareness, prevention, deterrence, and response and recovery activities, as well as direction to DHS components.

DHS is establishing a new system of records under the Privacy Act (5 U.S.C. 552a), which will be maintained in the IAIP Directorate, the Homeland Security Operations Center Database. 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 personally identifiable information. 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 retrieved by the name of the individual or by some

identifying number, symbol, or other identifying particular assigned to the individual. Individuals may request 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 that each agency publish in the **Federal Register** a description denoting the type and character of each system of records in order to make agency recordkeeping practices transparent, to notify individuals about the use to which personally identifiable information is put, and to assist the individual to more easily find files within the agency.

This system of records notice describes the HSOC database within IAIP. The information in the HSOC database includes intelligence information and other information received from agencies and components of the Federal Government, foreign governments, organizations or entities, international organizations, state and local government agencies (including law enforcement agencies), and private sector entities, as well as information provided by individuals, regardless of the medium used to submit the information or the agency to which it was submitted. This system also contains: information regarding persons on watch lists with possible links to terrorism; the results of intelligence analysis and reporting; ongoing law enforcement investigative information, information systems security analysis and reporting; historical law enforcement information, operational and administrative records; financial information; and public-source data such as that contained in media reports and commercial databases as appropriate to identify and assess the nature and scope of terrorist threats to the homeland, detect and identify threats of terrorism against the United States, and understand such threats in light of actual and potential vulnerabilities of the homeland. Data about the providers of information, including the means of transmission of the data is also retained.

IAIP will use the information in the HSOC database to access, receive, and analyze law enforcement information, intelligence information, and other information and to integrate such information in order to identify and assess the nature and scope of terrorist or other threats to the homeland.

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

DHS/IAIP–001

SYSTEM NAME:

Homeland Security Operations Center Database

SECURITY CLASSIFICATION:

Classified; sensitive

SYSTEM LOCATION:

Records are maintained at the Homeland Security Operations Center, Office of the Undersecretary for Information Analysis and Infrastructure Protection, Department of Homeland Security, Washington, DC 20528.

CATEGORY OF INDIVIDUALS COVERED BY THE SYSTEM:

Individuals who have been linked in any manner to potential terrorism, to other domestic incidents with homeland security implications, or whose behavior arouses reasonable suspicion of possible terrorist activity; individuals who are the subject of information pertaining to terrorism and/or homeland security; individuals who offer information pertaining to terrorism and/or homeland security; individuals who request assistance or information; or individuals who make inquiries concerning possible terrorist activity. The system will also contain information about individuals who are or have been associated with DHS homeland security operations or with DHS administrative operations.

CATEGORIES OF RECORDS IN THE SYSTEM:

Intelligence information obtained from agencies and components of the Federal Government, foreign governments, organizations or entities, international organizations, state and local government agencies (including law enforcement agencies), and private sector entities; information provided by individuals, regardless of the medium used to submit the information; information obtained from the Terrorist Screening Center or on terrorist watch lists about individuals known or reasonably suspected to be engaged in conduct constituting, preparing for, aiding, or relating to terrorism; results of intelligence analysis and reporting; ongoing law enforcement investigative information; information systems security analysis and reporting; historical law enforcement information; operational and administrative records; financial information; and public source data such as that contained in media reports and commercial databases. Data about the providers of information, including the means of transmission of the data, will also be retained.

AUTHORITY FOR MAINTENANCE OF THE SYSTEM:

5 U.S.C. 301, 552, 552a; Section 201 of the Homeland Security Act of 2002, Pub. L. 107–296, 116 Stat. 2145 (Nov. 25, 2002), as amended (6 U.S.C. 121); 44 U.S.C. 3101; E.O. 12958; E.O. 9397.

PURPOSE(S):

This record system is maintained to collect, access, and analyze law enforcement information, intelligence information, and other information from agencies of the Federal Government, foreign governments, international organizations, state and local government agencies (including law enforcement agencies), and private sector entities or individuals; and to integrate such information in order to: detect, identify and assess the nature and scope of terrorist or other threats to the United States; and understand such threats in light of actual and potential vulnerabilities of the homeland.

ROUTINE USES OF RECORDS MAINTAINED IN THE SYSTEM:

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 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. If the record, on its face or in conjunction with other information, indicates a violation or potential violation of any law, regulation, rule, order, or contract, the record may be disclosed to the appropriate entity, whether federal, state, local, joint, tribal, foreign, or international, that is charged with the responsibility of investigating, prosecuting and/or enforcing such law, regulations, rule, order or contract.

B. To a Federal, state, local, joint, tribal, foreign, international or other public agency or organization, or to any person or entity in either the public or private sector, domestic or foreign, where such disclosure may promote assist or otherwise serve homeland or national security interests.

C. To an organization or individual in either the public or private sector, where there is a reason to believe that the recipient is or could become the target of a particular terrorist activity or conspiracy, to the extent the information is relevant to the protection of life or property.

D. To recipients under circumstances and procedures as are mandated by Federal statute, treaty, or international agreement.

E. To the news media or members of the general public in furtherance of a function related to homeland security as

determined by the system manager where disclosure could not reasonably be expected to constitute an unwarranted invasion of privacy.

F. To the Department of Justice or other federal agency conducting litigation or in proceedings before any court, adjudicative or administrative body, when: (a) DHS, or (b) any employee of DHS in his/her official capacity, or (c) any employee of DHS in his/her individual capacity where DOJ or DHS has agreed to represent the employee, or (d) the United States or any agency thereof, is a party to the litigation or has an interest in such litigation.

G. To a congressional office from the record of an individual in response to an inquiry from that congressional office made at the request of the individual to whom the record pertains.

H. 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. Sections 2904 and 2906.

I. To contractors, grantees, experts, consultants, volunteers, 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.

J. To an agency, organization, or individual for the purposes of performing authorized audit or oversight operations.

K. To a Federal, state, local, tribal, territorial, foreign, or international agency, if necessary to obtain information relevant to a Department of Homeland Security decision concerning the hiring or retention of an employee, the issuance of a security clearance, the reporting of an investigation of any employee, the letting of a contract, or the issuance of a license, grant, or other benefit.

L. To a Federal, state, local, tribal, territorial, foreign, or international agency, in response to its request, in connection with the hiring or retention of an employee, the issuance of a security clearance, the reporting of an investigation of an employee, the letting of a contract, or the issuance of a license, grant, or other benefit by the requesting agency, to the extent that the information is relevant and necessary to the requesting agency's decision on the matter.

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

STORAGE:

Records in this system are stored electronically at the HSOC in a secure facility. The records are stored on magnetic disc, tape, digital media, and CD-ROM, and may also be retained in hard copy format in secure folders.

RETRIEVABILITY:

Data may be retrieved by the individual's name or other identifier.

SAFEGUARDS:

Information in this system is safeguarded in accordance with applicable rules and policies, including any applicable IAIP and DHS automated systems security and access policies. Strict controls have been imposed to minimize the risks of compromising the information that is being stored. Access to the computer system containing the records in this system is limited to those individuals specifically authorized and granted access by DHS regulations, who hold appropriate security clearances, and who have a need to know the information in the performance of their official duties. The system also maintains a real-time auditing function of individuals who access the system. Classified information is appropriately stored in a secured facility, in secured databases and containers, and in accordance with other applicable requirements, including those pertaining to classified information. Access is limited to authorized personnel only.

RETENTION AND DISPOSAL:

IAIP is working with the National Archives and Records Administration to obtain approval of a records retention and disposal schedule to cover records in the HSOC database. IAIP has proposed a short retention schedule for these records.

SYSTEM MANAGER(S) AND ADDRESS:

Director, Disclosure Office, Office of the Chief of Staff, Office of the Undersecretary for Information Analysis and Infrastructure Protection, Department of Homeland Security, Washington, D.C. 20528.

NOTIFICATION PROCEDURES:

To determine whether this system contains records relating to you, write to the System Manager identified above.

RECORDS ACCESS PROCEDURES:

A request for access to records in this system may be made by writing to the System Manager, identified above, in conformance with 6 CFR Part 5, Subpart B, which provides the rules for requesting access to Privacy Act records maintained by DHS.

CONTESTING RECORD PROCEDURES:

Same as ''Record Access Procedures,'' above.

RECORD SOURCE CATEGORIES:

Information contained in this system is obtained from subject individuals, other agencies and organizations, both domestic and foreign, media, including periodicals, newspapers, and broadcast transcripts and public and classified reporting, privacy organizations and individuals, intelligence source documents, investigative reports, and correspondence.

EXEMPTIONS CLAIMED FOR THE SYSTEM:

Portions of this system are exempt under 5 U.S.C. 552a((j)(2), (k)(1), and (k)(2).

Dated: April 7, 2005.

Nuala O'Connor Kelly,

Chief Privacy Officer, Department of Homeland Security.

[FR Doc. 05–7704 Filed 4–15–05; 8:45 am]

BILLING CODE 4410–10–P

DEPARTMENT OF HOMELAND SECURITY

Coast Guard

[CGD08–05–020]

Houston/Galveston Navigation Safety Advisory Committee

AGENCY: Coast Guard, DHS.

ACTION: Notice of meetings.

SUMMARY: The Houston/Galveston Navigation Safety Advisory Committee (HOGANSAC) and its working groups will meet to discuss waterway improvements, aids to navigation, area projects impacting safety on the Houston Ship Channel, and various other navigation safety matters in the Galveston Bay area. All meetings will be open to the public.

DATES: The next meeting of HOGANSAC will be held on Tuesday, May 24, 2005 at 9 a.m. The meeting of the Committee's working groups will be held on Tuesday, May 10, 2005 at 9 a.m. The meetings may adjourn early if all business is finished. Members of the public may present written or oral statements at either meeting. Requests to make oral presentations or distribute written materials should reach the Coast Guard five (5) working days before the meeting at which the presentation will be made. Requests to have written materials distributed to each member of