

agencies. This regulation provides detailed guidance for contractors doing business with acquisition offices within the Department of Homeland Security (DHS) to implement the FAR. FAR Part 33.103, Protests, Disputes, and Appeals prescribe policies and procedures for filing protests and for processing contract disputes and appeals. DHS will not be asking for anything outside of what is already required in the FAR. Should anything outside the FAR arise, DHS will submit a request for Office of Management and Budget (OMB) approval. The information being collected will be obtained from contractors as part of their submissions whenever they file a bid protest with the Department's Components. The information will be used by DHS officials in deciding how the protest should be resolved. Failure to collect this information would result in delayed resolution of agency protests.

According to FPDS, the number of protest has increased each year over the past two years in annual respondent and burden hours. This increase in current protest activity is not the result of a deliberate program change, but from a new estimate of actions that are not controllable by the Federal government. Although, the number of protest has increased, there has not been any change in the information being collected.

The Office of Management and Budget is particularly interested in comments which:

1. Evaluate whether the proposed collection of information is necessary for the proper performance of the functions of the agency, including whether the information will have practical utility;
2. Evaluate the accuracy of the agency's estimate of the burden of the proposed collection of information, including the validity of the methodology and assumptions used;
3. Enhance the quality, utility, and clarity of the information to be collected; and
4. Minimize the burden of the collection of information on those who are to respond, including through the use of appropriate automated, electronic, mechanical, or other technological collection techniques or other forms of information technology, e.g., permitting electronic submissions of responses.

#### Analysis

*Agency:* Office of Chief Procurement Officer, Acquisition Policy and Legislation Office, DHS.

*Title:* Regulation on Agency Protests.  
*OMB Number:* 1600-0004.

*Frequency:* Annually.

*Affected Public:* Private Sector.

*Number of Respondents:* 75.

*Estimated Time per Respondent:* 2 hours.

*Total Burden Hours:* 150.

*Total Burden Cost (capital/startup):* \$4,104.00.

Dated: November 2, 2010.

**Richard Spires,**

*Chief Information Officer.*

[FR Doc. 2010-28574 Filed 11-12-10; 8:45 am]

**BILLING CODE 9110-9B-P**

## DEPARTMENT OF HOMELAND SECURITY

### Office of the Secretary

[Docket No. DHS-2010-0052]

#### Privacy Act of 1974; Department of Homeland Security Office of Operations Coordination and Planning—003 Operations Collection, Planning, Coordination, Reporting, Analysis, and Fusion 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 is giving notice that it proposes to establish a new Department of Homeland Security system of records titled, "Department of Homeland Security Office of Operations Coordination and Planning—003 Operations Collection, Planning, Coordination, Reporting, Analysis, and Fusion System of Records." This system of records will allow the Department of Homeland Security Office of Operations Coordination and Planning, including the National Operations Center, to collect, plan, coordinate, report, analyze, and fuse information related to all-threats and all-hazards, law enforcement activities, intelligence activities, man-made disasters and acts of terrorism, natural disasters, and other information collected or received from federal, state, local, tribal, and territorial agencies and organizations; foreign governments and international organizations; domestic security and emergency management officials; and private sector entities or individuals into the Department.

Some of the records in this system are in part transferred from the Department of Homeland Security/Information Analysis and Infrastructure Protection—001 Homeland Security Operations Center Database system of records, April

15, 2005, with the overall intent of narrowing the focus of these records to the specific purpose outlined in this system of records notice. It is the Department's intent, after all records are transferred into this and other system of records, to retire the Department of Homeland Security/Information Analysis and Infrastructure Protection—001 Homeland Security Operations Center Database system of records.

Additionally, the Department of Homeland Security is issuing a Notice of Proposed Rulemaking concurrent with this system of records elsewhere in the **Federal Register**. This newly established system will be included in the Department of Homeland Security's inventory of record systems.

**DATES:** Submit comments on or before December 15, 2010. This new system will be effective December 15, 2010.

**ADDRESSES:** You may submit comments, identified by docket number DHS-2010-0052 by one of the following methods:

- *Federal e-Rulemaking Portal:* <http://www.regulations.gov>. Follow the instructions for submitting comments.
- *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: Michael Page (202-357-7626), Privacy Point of Contact, Office of Operations Coordination and Planning, Department of Homeland Security, Washington, DC 20528. For privacy issues please contact: Mary Ellen Callahan (703-235-0780), Chief Privacy Officer, Privacy Office, Department of Homeland Security, Washington, DC 20528.

#### SUPPLEMENTARY INFORMATION:

##### I. Background

In accordance with the Privacy Act of 1974, 5 U.S.C. 552a, the Department of Homeland Security (DHS) Office of Operations Coordination and Planning (OPS), including the National Operations Center (NOC), proposes to establish a new DHS system of records titled, "DHS/OPS—003 Operations Collection, Planning, Coordination,

Reporting, Analysis, and Fusion System of Records.”

This system of records will allow DHS/OPS, including the NOC, to collect, plan, coordinate, report, analyze, and fuse information related to all-threats and all-hazards, law enforcement activities, intelligence activities, man-made disasters and acts of terrorism, natural disasters, and other information collected or received from federal, state, local, tribal, and territorial agencies and organizations; foreign governments and international organizations; domestic security and emergency management officials; and private sector entities or individuals into the Department.

OPS serves as a joint operations coordination and planning capability at the strategic level to support internal DHS operational decision making, DHS leadership, and participation in interagency operations. OPS integrates DHS and interagency planning and operations coordination in order to prevent, protect, and respond to and recover from all-threats and all-hazards, man-made disasters and acts of terrorism, and natural disasters.

The NOC serves as the nation’s homeland security center for information sharing and domestic incident management, dramatically increasing coordination between federal, state, local, tribal, and territorial agencies and organizations; foreign governments and international organizations; domestic security and emergency management officials; and private sector entities or individuals. The NOC collects and fuses information from a variety of sources everyday to help deter, detect, and prevent terrorist acts as well as to prepare for, respond to, and recover from all-threats and all-hazards, man-made disasters and acts of terrorism, and natural disasters. Operating 24 hours a day, seven days a week, 365 days a year, the NOC provides real-time situational awareness and monitoring of the homeland, coordinates incidents and response activities, and, in conjunction with other DHS components, issues advisories and bulletins concerning threats to homeland security, including natural disasters, as well as specific protective measures. Information on domestic incident management is shared with state Fusion Centers and Emergency Operations Centers (EOC) at all levels through Watch Officer Desks located in the NOC.

The purpose of this system is to:

1. *Collect, plan, coordinate, and analyze* all-threats and all-hazards, law enforcement activities, intelligence activities, man-made disasters and acts

of terrorism, natural disasters, and other information collected or received from Federal, State, local, tribal, and territorial agencies and organizations; foreign governments and international organizations; domestic security and emergency management officials; and private sector entities or individuals; and

2. *Report, integrate, and fuse* such information throughout DHS in order to share information, increase coordination, identify and assess the nature and scope of information and understand risks in light of potential or actual vulnerabilities to the homeland; and help deter, detect, and prevent terrorist acts as well as to prepare for, respond to, and recover from all-threats and all-hazards, man-made disasters and acts of terrorism, and natural disasters.

DHS is authorized to implement this program primarily through 5 U.S.C. 301, 552, 552a; 44 U.S.C. 3101; 6 U.S.C. 121; §§ 201 and 514 of the Homeland Security Act of 2002, as amended; § 520 of the Post Katrina Emergency Management Reform Act; 44 U.S.C. 3101; Executive Order (E.O.) 12958; E.O. 9397; E.O. 12333; E.O. 13356; E.O. 13388; and Homeland Security Presidential Directive 5. This system has an effect on individual privacy that is balanced by the need to collect, plan, coordinate, report, analyze, and fuse homeland security information coming into and going out of OPS, including the NOC. Routine uses contained in this notice include sharing with the Department of Justice (DOJ) for legal advice and representation; to a congressional office at the request of an individual; to the National Archives and Records Administration (NARA) for records management; to contractors in support of their contract assignment to DHS; to appropriate Federal, State, tribal, local, international, foreign agency, or other appropriate entity including the privacy sector in their role aiding OPS in their mission; to agencies, organizations or individuals for the purpose of audit; to agencies, entities, or persons during a security or information compromise or breach; to an agency, organization, or individual when there could potentially be a risk of harm to an individual; and to the news media in the interest of the public. A review of this system is being conducted to determine if the system of records collects information under the Paperwork Reduction Act (PRA).

Consistent with DHS’s information sharing mission, information contained in the DHS/OPS—003 Collection, Planning, Coordination, Reporting, Analysis, and Fusion System of Records

may be shared with other DHS components, as well as appropriate Federal, State, local, tribal, territorial, foreign, or international government agencies. This sharing will only take place after DHS determines that the receiving component or agency has a verifiable 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.

The information within this system that meets the functional standard of the National Suspicious Activity Reporting Initiative will be placed into the DHS/ALL—031 Information Sharing Environment Suspicious Activity Reporting Initiative (September 10, 2010, 75 FR 55335).

DHS is issuing a Notice of Proposed Rulemaking concurrent with this system of records elsewhere in the **Federal Register**. This newly established system will be included in DHS’ 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 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, DHS extends administrative Privacy Act protections to all individuals where systems of records maintain 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 their records are put, and to assist individuals to more easily find such files within the

agency. Below is the description of the DHS/OPS—003 Collection, Planning, Coordination, Reporting, Analysis, and Fusion 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/OPS—003

##### SYSTEM NAME:

DHS/OPS—003 Collection, Planning, Coordination, Reporting, Analysis, and Fusion System of Records.

##### SECURITY CLASSIFICATION:

Unclassified, For Official Use Only, Law Enforcement Sensitive, and Classified.

##### SYSTEM LOCATION:

Records are maintained at the Department of Homeland Security (DHS) Office of Operations Coordination and Planning (OPS) National Operations Center (NOC) Headquarters in Washington, DC and field locations.

##### CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM:

Categories of individuals covered by the system may include:

- Federal, State, local, tribal, and territorial officials; foreign government and international officials; domestic security and emergency management officials; and private sector individuals who request assistance from, provide information to, are the subject of, or participate with the Department in activities related to all-threats and all-hazards, man-made disasters and acts of terrorism, and natural disasters;
- Individuals who request assistance from the Department related to all-threats and all-hazards, man-made disasters and acts of terrorism, and natural disasters;
- Individuals who provide information to the Department related to all-threats and all-hazards, man-made disasters and acts of terrorism, and natural disasters, including Suspicious Activity Reports (SARs);
- Individuals who are the subject of, or are linked in any manner to, all-threats and all-hazards, man-made disasters and acts of terrorism, and natural disasters with Departmental implications;
- Individuals participating with, involved in, or the subject of domestic security or law enforcement operations, with Departmental implications, where activity is planned or has taken place;
- Individuals participating with or involved in emergency management and

first responder operations, with Departmental implications, and where activity is planned or has taken place;

- Individuals involved in natural disasters where activity is planned or has taken place;
- Individuals derived from intelligence information of interest to the Department;
- Individuals who make inquiries concerning all-threats and all-hazards, man-made disasters and acts of terrorism, and natural disasters;
- Individuals who are or have been associated with DHS operations.

##### CATEGORIES OF RECORDS IN THE SYSTEM:

Categories of records in the system may include:

- Full name;
- Date and place of birth;
- Social Security Number (Many state, local, tribal, territorial, domestic security, emergency management, and private sector individuals, organizations and agencies collect/use SSN's as an identifier and may be shared with the Department);
- Citizenship;
- Contact information including phone numbers and email addresses;
- Address;
- Physical description including height, weight, eye and hair color;
- Distinguishing marks including scars, marks, and tattoos;
- Automobile registration information;
- Watch list information;
- Medical records;
- Financial information;
- Results of intelligence analysis and reporting;
- Ongoing law enforcement investigative information;
- Historical law enforcement information;
- Information systems security analysis and reporting;
- Public source data including commercial databases, media, newspapers, and broadcast transcripts;
- Intelligence information including links to terrorism, law enforcement and any criminal and/or incident activity, and the date information is submitted;
- Intelligence and law enforcement information obtained from federal, state, local, tribal, and territorial agencies and organizations, foreign governments and international organizations; law enforcement, domestic security and emergency management officials; and private sector entities or individuals;
- Information provided by individuals, regardless of the medium, used to submit the information;
- Information obtained from the Federal Bureau of Investigation's (FBI)

Terrorist Screening Center (TSC), or on terrorist watchlists, about individuals known or reasonably suspected to be engaged in conduct constituting, preparing for, aiding, or relating to terrorism;

- Data about the providers of information, including the means of transmission of the data; (e.g. where it is determined that maintaining the identity of the source of investigative lead information may be necessary to provide an indicator of the reliability and validity of the data provided and to support follow-on investigative purposes relevant and necessary to a legitimate law enforcement or homeland security matter, such data may likely warrant retention. Absent such a need, no information on the provider of the information would be maintained)
- Scope of terrorist, law enforcement, or natural threats to the homeland;
- National disaster threat and activity information;
- The date and time national disaster information is submitted, and the name of the contributing/submitted individual or agency;
- Limited data concerning the providers of information, including the means of transmission of the data may also be retained where necessary. Such information on other than criminal suspects or subjects is accepted and maintained only to the extent that the information provides descriptive matters relevant to a criminal subject or organization and has been deemed factually accurate and relevant to ongoing homeland security situational awareness and monitoring efforts.
- Name of the contributing or submitting agency, organization, or individual.

##### AUTHORITY FOR MAINTENANCE OF THE SYSTEM:

5 U.S.C. 301, 552, 552a; 44 U.S.C. 3101; 6 U.S.C. § 121; §§ 201 and 514 of the Homeland Security Act of 2002, as amended; § 520 of the Post Katrina Emergency Management Reform Act; 44 U.S.C. 3101; Executive Order (E.O.) 12958; E.O. 9397; E.O. 12333; E.O. 13356; E.O. 13388; and Homeland Security Presidential Directive 5.

##### PURPOSE(S):

The purpose of this system is to:

1. *Collect, plan, coordinate, and analyze* all-threats and all-hazards, law enforcement activities, intelligence activities, man-made disasters and acts of terrorism, natural disasters, and other information collected or received from Federal, State, local, tribal, and territorial agencies and organizations; foreign governments and international organizations; domestic security and

emergency management officials; and private sector entities or individuals; and

2. *Report, integrate, and fuse* such information throughout DHS in order to share information, increase coordination, identify and assess the nature and scope of said information and understand risks in light of potential or actual vulnerabilities to the homeland; and help deter, detect, and prevent terrorist acts as well as to prepare for, respond to, and recover from all-threats and all-hazards, man-made disasters and acts of terrorism, and natural disasters.

**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 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 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 an inquiry from that congressional office made at the 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 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 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 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.

I. To a Federal, State, tribal, local or foreign government agency or organization, or international organization, lawfully engaged in collecting law enforcement intelligence information, whether civil or criminal, or charged with investigating,

prosecuting, enforcing or implementing civil or criminal laws, related rules, regulations or orders, to enable these entities to carry out their law enforcement responsibilities, including the collection of law enforcement intelligence.

J. To Federal and foreign government intelligence or counterterrorism agencies or state, local, tribal or territorial components where DHS becomes aware of an indication of a threat or potential threat to national or international security.

K. To Federal and foreign government intelligence or counterterrorism agencies or state, local, tribal or territorial components where the information is or may be terrorism-related information and such use is to assist in anti-terrorism efforts.

L. 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.

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' 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 magnetic disc, tape, digital media, and CD-ROM.

**RETRIEVABILITY:**

Much of the data within this system does not pertain to an individual; rather, the information pertains to locations, geographic areas, facilities, and other things or objects not related to individuals. However, some personal information is captured. Personal data

may be retrieved by NOC tracker numbers, name, social security number and other identifiers listed under the Categories of Records Section. Most information is stored as free text and any word, phrase, or number is searchable.

#### 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:

OPS is working with the DHS Records Officer to develop a NARA approved retention schedule.

#### SYSTEM MANAGER AND ADDRESS:

Director, Office of Operations Coordination and Planning, National Operations Center, Department of Homeland Security, Washington, DC 20528.

#### NOTIFICATION PROCEDURE:

The Secretary of Homeland Security is proposing to exempt this system from the notification, access, and amendment procedures of the Privacy Act. However, DHS/OPS will consider individual requests to determine whether or not information may be released. 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 OPS FOIA Officer, whose contact information can be found at <http://www.dhs.gov/foia> under "contacts."

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:

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

#### 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 5 U.S.C. 552a(c)(3); (d); (e)(1), (e)(4)(G), (e)(4)(H), (e)(4)(I); and (f) pursuant to 5 U.S.C. 552a(k)(1), (k)(2), and (k)(3).

Dated: November 5, 2010.

**Mary Ellen Callahan,**

*Chief Privacy Officer, Department of Homeland Security.*

[FR Doc. 2010-28566 Filed 11-12-10; 8:45 am]

**BILLING CODE 9110-9A-P**

## DEPARTMENT OF HOMELAND SECURITY

### Office of the Secretary

[Docket No. DHS-2010-0086]

### Privacy Act of 1974; Department of Homeland Security National Protection and Programs Directorate—001 National Infrastructure Coordinating Center Records 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 is giving notice that it proposes to establish a new Department of Homeland Security system of records titled, "Department of Homeland Security National Protection and Programs Directorate—001 National Infrastructure Coordinating Center Records System of Records." This system of records will allow the Department of Homeland Security National Protection and Programs Directorate National Infrastructure Coordinating Center, an extension of the National Operations Center, to collect, plan, coordinate, report, analyze, and fuse infrastructure information related to all-threats and all-hazards, law enforcement activities, intelligence activities, man-made disasters and acts of terrorism, natural disasters, and other information collected or received from federal, state, local, tribal, and territorial agencies and organizations; foreign governments and international organizations; domestic security and emergency management officials; and private sector entities or individuals into the National Infrastructure Coordinating Center. Additionally, the Department of Homeland Security is issuing a Notice of Proposed Rulemaking concurrent with this system of records elsewhere in the Federal Register. This newly established system will be included in the Department of Homeland Security's inventory of record systems.

**DATES:** Submit comments on or before December 15, 2010. This new system will be effective December 15, 2010.

**ADDRESSES:** You may submit comments, identified by docket number DHS-2010-0086 by one of the following methods:

- *Federal e-Rulemaking Portal:* <http://www.regulations.gov>. Follow the instructions for submitting comments.
- *Fax:* 703-483-2999.
- *Mail:* Mary Ellen Callahan, Chief Privacy Officer, Privacy Office,