Date: October 15, 2010.
Time: 11 a.m. to 3 p.m.
Agenda: To review and evaluate grant applications.
Place: JW Marriott San Francisco Union Square, 500 Post Street corner of Post and Mason, San Francisco, CA 94102.
Contact Person: John C. Pugh, PhD, Scientific Review Officer, Center for Scientific Review, National Institutes of Health, 6701 Rockledge Drive, Room 3114, MSC 7808, Bethesda, MD 20892, (301) 435–2398, *pughjohn@csr.nih.gov.*

(Catalogue of Federal Domestic Assistance Program Nos. 93.306, Comparative Medicine; 93.333, Clinical Research, 93.306, 93.333, 93.337, 93.393–93.396, 93.837–93.844, 93.846–93.878, 93.892, 93.893, National Institutes of Health, HHS)

Dated: September 1, 2010.

Jennifer S. Spaeth,

Director, Office of Federal Advisory Committee Policy.

[FR Doc. 2010–22316 Filed 9–7–10; 8:45 am]

BILLING CODE 4140–01–P

DEPARTMENT OF HEALTH AND HUMAN SERVICES

National Institutes of Health

National Heart, Lung, and Blood Institute; Notice of Closed Meeting

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 meeting.

The meeting 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 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 contract proposals, the disclosure of which would constitute a clearly unwarranted invasion of personal privacy.

Name of Committee: National Heart, Lung, and Blood Institute Special Emphasis Panel; Maintenance of the NHLBI Biologic Specimen Repository.
Date: September 22, 2010.
Time: 10 a.m. to 2 p.m.
Agenda: To review and evaluate contract proposals.
Place: National Institutes of Health, 6701 Rockledge Drive, Bethesda, MD 20892, (Telephone Conference Call).
Contact Person: William J. Johnson, PhD, Scientific Review Officer, Review Branch/DERA, National Heart, Lung, and Blood Institute, 6701 Rockledge Drive, Room 7178, Bethesda, MD 20892–7924, 301–435–0725, *johnsonwj@nhlbi.nih.gov.*

(Catalogue of Federal Domestic Assistance Program Nos. 93.233, National Center for Sleep Disorders Research; 93.837, Heart and Vascular Diseases Research; 93.838, Lung Diseases Research; 93.839, Blood Diseases and Resources Research, National Institutes of Health, HHS)

Dated: September 1, 2010.

Jennifer S. Spaeth,

Director, Office of Federal Advisory Committee Policy.

[FR Doc. 2010–22314 Filed 9–7–10; 8:45 am]

BILLING CODE 4140–01–P

DEPARTMENT OF HEALTH AND HUMAN SERVICES

National Institutes of Health

National Eye Institute; Notice of Meeting

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

The meeting will be open to the public as indicated below, with attendance limited to space available. Individuals who plan to attend and need special assistance, such as sign language interpretation or other reasonable accommodations, should notify the Contact Person listed below in advance of the meeting.

The meeting 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 and/or 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 and/or contract proposals, the disclosure of which would constitute a clearly unwarranted invasion of personal privacy.

Name of Committee: National Advisory Eye Council.
Date: October 21, 2010.
Open: 8:30 a.m. to 12 p.m.
Agenda: Following opening remarks by the Director, NEI, there will be presentations by the staff of the Institute and discussions concerning Institute programs.
Place: Melrose Hotel, 2430 Pennsylvania Ave., NW., Washington, DC 20037.
Closed 1 p.m. to Adjournment.
Agenda: To review and evaluate grant applications.
Place: Melrose Hotel, 2430 Pennsylvania Ave., NW., Washington, DC 20037.
Contact Person: Andrew P. Mariani, PhD, Executive Secretary, National Advisory Eye Council, National Eye Institute, National Institutes of Health, 301–451–2020, *amp@nei.nih.gov.*

Any person interested may file written comments with the committee by forwarding the statement to the Contact Person listed on this notice. The statement should include the name, address, telephone number and when applicable, the business or professional affiliation of the interested person.

Information is also available on the Institute's/Center's home page: *http://www.nei.nih.gov,* where an agenda and any additional information will be posted when available.

(Catalogue of Federal Domestic Assistance Program Nos. 93.867, Vision Research, National Institutes of Health, HHS)

Dated: September 1, 2010.

Jennifer Spaeth,

Director, Office of Federal Advisory, Committee Policy.

[FR Doc. 2010–22312 Filed 9–7–10; 8:45 am]

BILLING CODE 4140–01–P

DEPARTMENT OF HOMELAND SECURITY

Office of the Secretary

[Docket No. DHS–2010–0067]

Privacy Act of 1974; United States Citizenship and Immigration Services—012 Citizenship and Immigration Data Repository System of Records

AGENCY: Privacy Office, DHS.

ACTION: Notice of Privacy Act system of records.

SUMMARY: In accordance with the Privacy Act of 1974, the Department of Homeland Security proposes to establish a new Department of Homeland Security system of records notice titled, "DHS U.S. Citizenship and Immigration Services 012 Citizenship and Immigration Data Repository System of Records." Citizenship and Immigration Data Repository is a mirror copy of USCIS's major immigrant and non-immigrant benefits databases combined into a single user interface and presented in an updated, searchable format on the classified network. This system takes existing USCIS data and recompiles them into a system for the following three purposes: (1) Vetting USCIS application information for indications of possible immigration fraud and national security concerns, (2) detecting possible fraud and misuse of immigration information or position by USCIS employees, for personal gain or by coercion, and (3) to respond to requests for information (RFIs) from the DHS Office of Intelligence and Analysis (I&A) and/or the Federal intelligence and law enforcement community members that are based on classified criteria. The Department of Homeland Security is issuing a Notice of Proposed

Rulemaking concurrent with this system of records elsewhere in the **Federal Register** because certain information in the system may be classified or relevant to a law enforcement investigation. This newly established system will be included in the Department of Homeland Security's inventory of record systems.

DATES: Submit comments on or before October 8, 2010. This new system will be effective October 8, 2010.

ADDRESSES: You may submit comments, identified by docket number DHS–2010–0067 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: Donald K. Hawkins (202–272–8000), Privacy Officer, U.S. Citizenship and Immigration Services, 20 Massachusetts Avenue, NW., Washington, DC 20529. For privacy issues please contact: Mary Ellen Callahan (703–235–0780), Chief Privacy Officer, Privacy Office, U.S. Department of Homeland Security, Washington, DC 20528.

SUPPLEMENTARY INFORMATION:

I. Background

USCIS collects personally identifiable information (PII) directly from and about immigrants and nonimmigrants through applications and petitions for the purposes of adjudicating and bestowing immigration benefits. USCIS maintains a number of systems to facilitate these purposes including: The Computer Linked Application Information Management System (CLAIMS 3), CLAIMS 4, the Refugees, Asylum, and Parole System (RAPS), Asylum Pre-screen System (APSS), Re-engineered Naturalization Application Casework System (RNACS), Central Index System (CIS) and the Fraud Detection and National Security Data System (FDNS–DS). As part of the adjudication process, USCIS personnel engage in a number of steps to ensure that an individual is eligible for a requested benefit. One of these steps is the performance of background checks to make certain that an individual is not attempting to obtain the requested benefit by fraudulent means, has not committed a crime involving moral turpitude, and/or does not pose a public safety threat or a threat to national security.

USCIS developed CIDR, hosted on DHS classified networks, in order to make information from these USCIS systems available to authorized USCIS personnel for the purposes of: (1) Vetting USCIS application information for indications of possible immigration fraud and national security concerns, (2) detecting possible fraud and misuse of immigration information or position by USCIS employees, for personal gain or by coercion, and (3) responding to requests for information (RFIs) from the DHS Office of Intelligence and Analysis (I&A) and/or Federal intelligence and law enforcement community members that are based on classified criteria. CIDR enables authorized USCIS users to more efficiently search multiple USCIS systems from a single entry point, the results of which will be retained in CIDR. CIDR's placement on DHS classified networks allows USCIS to securely conduct searches based on classified parameters and searches based on possible fraud and national security concerns.

There are occasions when USICS receives RFIs from members of the Intelligence Community (IC) and Law Enforcement (LE) that are classified. In order to assist with classified investigatory leads and respond to I&A's requests, USCIS must conduct searches whose parameters are classified on an unclassified data sets. To facilitate a more efficient and secure environment in which to conduct these queries and to store their results, DHS determined that creating mirror copies of its unclassified data sets on the classified side would be the most appropriate solution. CIDR provides the capability to properly conduct and protect classified searches and maintain detailed audit trails of search activities and results. Copying unclassified data from the unclassified systems to a classified site does not render this information classified, only the search parameters and their results. CIDR will enable USCIS personnel to perform searches of its non classified data sets in a classified environment, ensuring that the integrity of the classified RFI process is maintained. Based on the results of the searches performed in CIDR, USCIS will produce a response to the RFI, which will include the content of the RFI, information from CIDR that is responsive to the RFI, and any necessary explanations to provide proper context and interpretations of the information provided. These responses will contain PII when de-identified or statistical data cannot satisfy the RFI. These responses will be produced by USCIS personnel as separate electronic documents and sent to I&A in the same manner that the RFI was received; usually via e-mail over the classified e-mail network.

USCIS is proposing to exempt classified information in CIDR from disclosure to a requestor to preserve the integrity of ongoing counterterrorism, intelligence, or other homeland security activities, pursuant to the Privacy Act. 5 U.S.C. 552a(k)(1) and (2).

Consistent with DHS's information sharing mission, information stored in CIDR may be shared with other DHS components, as well as appropriate Federal, State, local, Tribal, foreign, or international governmental agencies. This sharing will only take place after DHS determines that the receiving component or agency has a need to know the information to carry out national security, law enforcement, immigration, intelligence, or other functions consistent with the routine uses set forth in this system of records notice.

In accordance with the Privacy Act of 1974 the Department of Homeland Security proposes to establish a new Department of Homeland Security (DHS) system of records notice, titled DHS U.S. Citizenship and Immigration Services 012—Citizenship and Immigration Data Repository (CIDR).

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 as 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 recordkeeping practices transparent, to notify individuals regarding the uses of their records, and to assist individuals to more easily find such files within the agency. Below is the description of the USCIS 012 CIDR 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/USCIS—012

SYSTEM NAME:

United States Citizenship and Immigration Services—012 Citizenship and Immigration Data Repository.

SECURITY CLASSIFICATION:

Unclassified and classified.

SYSTEM LOCATION:

Records are maintained at the USCIS Headquarters in Washington, DC.

CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM:

Categories of individuals covered by this system include: Persons who have filed (for themselves or on the behalf of others) applications or petitions for immigration benefits under the Immigration and Nationality Act, as amended, and/or who have submitted fee payments or received refunds from such applications or petitions; current, former and potential (*e.g.,* fiancé) family members of applicants/petitioners; persons who complete immigration forms for applicants and petitioners (*e.g.,* attorneys, form preparers); and name of applicant's employer. Additionally, CIDR will maintain information on USCIS personnel who have used the underlying USCIS systems included in CIDR.

CATEGORIES OF RECORDS IN THE SYSTEM:

Categories of records in this system include:

- Individual's name;
- Social Security Number (if applicable);
- A-Number (if applicable);
- Addresses;
- Telephone numbers;
- Birth and death information;
- Citizenship or nationality;
- Immigration status;
- Marital and family status;
- Personal characteristics (*e.g.,* height and weight);
- Records regarding tax payment and financial matters;
- Records regarding employment;
- Medical records;
- Military and Selective Service records;
- Records regarding organization membership or affiliation;
- DHS issued card serial numbers;
- Records regarding criminal history and other background check information;
- Case processing information, such as date applications were filed or received by USCIS; application/petition status, location of record, FOIA/PA or other control number when applicable;
- Fee receipt data;
- Records of searches, analyses, correspondence, and outputs generated by USCIS personnel in response to a classified request for USCIS immigrant and non-immigrant data; and
- System audit logs.

AUTHORITY FOR MAINTENANCE OF THE SYSTEM:

Authority for maintaining this system is in § 101 and 103 of the Immigration and Nationality Act, as amended (8 U.S.C. 1101 and 1103), and the regulations issued pursuant thereto; § 451 of the Homeland Security Act of 2002 (Pub. L. 107–296); E.O. 12958; E.O. 13356; E.O. 13388; and E.O. 12333.

PURPOSE(S):

The purpose of this system is (1) vetting USCIS application information for indications of possible immigration fraud and national security concerns, (2) detecting possible fraud and misuse of immigration information or position by USCIS employees, for personal gain or by coercion, and (3) to respond to RFIs from the DHS I&A and/or the Federal intelligence and law enforcement community members that are based on classified criteria.

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 functions.

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 a Federal, State, or local agency, or other appropriate entity or individual, or through established liaison channels to selected foreign governments, in order to provide intelligence, counterintelligence, or other information for the purposes of intelligence, counterintelligence, or antiterrorism activities authorized by U.S. law, Executive Order, or other applicable national security directive.

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:

Records may be retrieved by an individual's name, other identifiers, attributes, benefits application and case status data, address, associates, and any other data associated with an individual maintained by USCIS in source systems. Additionally, records may be retrieved by the output of USCIS's search, analysis, and response to classified requests for USCIS data.

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:

CIDR does not retain the replicated data sets from the underlying USCIS data systems, to include CLAIMS 3, CLAIMS 4, RAPS, APSS, RNACS, and CIS and the associated audit trails of DHS personnel using the systems, as covered by the DHS/ALL–004—General Information Technology Access Account Records System (GITAARS). The data supplied by these systems are retained by those systems in accordance with their own retention schedules. CIDR simply mirrors these data sets. Information will be removed from CIDR after it has been removed in the source system. CIDR retains a record of the classified search request, the results of the request, and a log of these activities for five years. These are maintained for a minimum of five years in accordance with DCID 6/3. Classified data will be maintained for the period of time required by the originating classification authority.

SYSTEM MANAGER AND ADDRESS:

Chief, Technology Coordination Division Office of Security and Integrity, USCIS, 111 Massachusetts Avenue, NW., Washington, DC 20529.

NOTIFICATION PROCEDURE:

DHS is exempting the records from general access provisions, pursuant to 5 U.S.C. 552a(k)(1) and (2). Each request for information within CIDR will be reviewed to determine whether or not the record within CIDR meets the requirements of the exemptions and, as appropriate, to disclose information that does not meet the requirements. This does not prevent the individual from gaining access to his records in the source systems noted below. Persons may seek access to records maintained in the source systems that feed into CIDR, currently CLAIMS 3, and in future releases, CLAIMS 4, RAPS, APSS, RNACS, and CIS.

USCIS treats all requests for amendment of information in a system of records as Privacy Act amendment requests. Any individual seeking to access information maintained in CLAIMS 3, CLAIMS 4, RAPS, APSS, RNACS, and CIS and associated systems should direct his or her request to the USCIS FOIA/Privacy Act (PA) Officer at USCIS FOIA/PA, 70 Kimball Avenue, South Burlington, Vermont 05403–6813 (Human resources and procurement records) or USCIS National Records Center (NRC), P.O. Box 648010, Lee's Summit, MO 64064–8010 (all other USCIS records). The process for requesting records can be found at 6 CFR 5.21. Requests for records amendments may also be submitted to the service center where the application was originally submitted. The request should clearly state the information that is being contested, the reasons for contesting it, and the proposed amendment to the information. If USCIS intends to use information that is not contained in the application or supporting documentation (*e.g.,* criminal history received from law enforcement), it will provide formal notice to the applicant and provide them an opportunity to refute the information prior to rendering a final decision regarding the application. This provides yet another mechanism for erroneous information to be corrected.

Requests for access to records in this system must be in writing. Such requests may be submitted by mail or in person. If a request for access is made by mail, the envelope and letter must be clearly marked "Privacy Access Request" to ensure proper and expeditious processing. The requester should provide his or her full name, date and place of birth, and verification of identity (full name, current address, and date and place of birth) in accordance with DHS regulations governing Privacy Act requests (found at 6 CFR 5.21), and any other identifying information that may be of assistance in locating the record.

When seeking records from this system of records or any other USCIS system of records, the requestor must conform with the Privacy Act regulations set forth in 6 CFR part 5. You must first verify your identity by providing 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 or perjury as a substitute for notarization. While no specific form is required, you may obtain forms for this purpose from the Director, Disclosure and FOIA, *http://www.dhs.gov* or 1–866–431–0486. In addition you should provide the following:

- An explanation of why you believe the Department would have information on you,
- Specify when you believe the records would have been created,
- 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, USCIS will 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 of records is obtained from the following systems of records:

USCIS Systems:

• Benefits Information System DHS–USCIS–007, September 29, 2008, 73 FR 56596, which corresponds to the following USCIS databases:

○ Computer Linked Adjudication Information Management System (CLAIMS 3, case tracking for all benefits except refugee status, asylum, and naturalizations.)

○ Computer Linked Adjudication Information Management System (CLAIMS 4, case tracking for naturalization benefits.)

○ Electronic Citizenship and Immigration Services Centralized Oracle Repository (eCISCOR).

○ Citizenship and Immigration Services Centralized Oracle Repository (CISCOR).

• Fraud Detection and National Security Data System (FDNS DS) DHS–USCIS–006, August 18, 2008, 73 FR 48231.

• Central Index System, (CIS) DHS–USCIS 001, January 16, 2007, 72 FR 1755.

• Asylum Information and Pre-Screening System, DHS–USCIS–010, January 5, 2010, 75 FR 409, which corresponds to the following USCIS databases:

○ The Refugees, Asylum, and Parole System (RAPS), a case management system that tracks applications for asylum pursuant to § 208 of the Immigration and Naturalization Act (INA) and applications for suspension of deportation or special rule cancellation of removal pursuant to Nicaraguan Adjustment and Central American Relief Act (NACARA) § 203 of the INA.

○ Asylum Pre-Screening System (APSS), a case management system that tracks the processing of "Credible Fear" and "Reasonable Fear" cases by Asylum staff.

DHS Intelligence and Analysis System:

• Enterprise Records System (ERS), DHS/IA–001, May 15, 2008, 73 FR 28128.

DHS-Wide:

• DHS/ALL–004—General Information Technology Access Account Records System (GITAARS), September 29, 2009, 74 FR 49882.

EXEMPTIONS CLAIMED FOR THE SYSTEM:

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

Mary Ellen Callahan,

Chief Privacy Officer, Department of Homeland Security.

[FR Doc. 2010–22306 Filed 9–7–10; 8:45 am]

BILLING CODE 9111–97–P

DEPARTMENT OF HOMELAND SECURITY

U.S. Citizenship and Immigration Services

[OMB Control No. 1615–0099]

Agency Information Collection Activities: Form I–914; Extension of an Existing Information Collection; Comment Request

ACTION: 60-Day Notice of Information Collection Under Review; Form I–914 and Supplements A and B, Application for T Nonimmigrant Status; Application for Immediate Family Member of T–1 Recipient; and Declaration of Law Enforcement Officer for Victim of Trafficking in Persons; OMB Control No. 1615–0099.

The Department of Homeland Security, U.S. Citizenship and Immigration Services (USCIS) will be submitting the following information collection request for review and clearance in accordance with the Paperwork Reduction Act of 1995. The information collection is published to obtain comments from the public and affected agencies. Comments are encouraged and will be accepted for sixty days until November 8, 2010.

During this 60 day period, USCIS will be evaluating whether to revise the Form I–914. Should USCIS decide to revise Form I–914 we will advise the public when we publish the 30-day notice in the **Federal Register** in accordance with the Paperwork Reduction Act. The public will then have 30 days to comment on any revisions to the Form I–914.

Written comments and/or suggestions regarding the item(s) contained in this notice, especially regarding the estimated public burden and associated response time, should be directed to the Department of Homeland Security (DHS), USCIS, Chief, Regulatory Products Division, 111 Massachusetts Avenue, NW., Washington, DC 20529–2210. Comments may also be submitted to DHS via facsimile to 202–272–8352 or via e-mail at *rfs.regs@dhs.gov*. When submitting comments by e-mail, please make sure to add OMB Control No. 1615–0099 in the subject box. Written comments and suggestions from the public and affected agencies concerning the collection of information should address one or more of the following four points:

(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 agencies 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 submission of responses.

Overview of This Information Collection

(1) *Type of Information Collection:* Extension of an existing information collection.

(2) *Title of the Form/Collection:* Application for T Nonimmigrant Status; Supplement A: Application for Immediate Family Member of T–1 Recipient; and Supplement B: Declaration of Law Enforcement Officer for Victim of Trafficking in Persons.

(3) *Agency form number, if any, and the applicable component of the Department of Homeland Security sponsoring the collection:* Form I–914; U.S. Citizenship and Immigration Services (USCIS).

(4) *Affected public who will be asked or required to respond, as well as a brief abstract: Primary:* Individuals or households. Form I–914 permits victims of severe forms of trafficking and their immediate family members to demonstrate that they qualify for temporary nonimmigrant status pursuant to the Victims of Trafficking