

	Number of distinct respondents	Number of responses per respondent	Average 3-year burden per response (hours)	Total burden (hours)
<b>Summary of Annualized Burden Estimates for 3 Years</b>				
Caregivers .....	5,922	1.13	2.08	13,954
Youth .....	3,553	1.19	1.00	4,220
Provider/Administrators .....	648	.542	1.90	669
<b>Total Summary .....</b>	<b>10,123</b>	<b>.....</b>	<b>.....</b>	<b>18,844</b>
<b>Total Annual Average Summary .....</b>	<b>3,374</b>	<b>.....</b>	<b>.....</b>	<b>6,281</b>

<sup>1</sup> An average of 24 stakeholders in up to 27 grantee sites will complete the System of Care Assessment interview. These stakeholders will include site administrative staff, providers, agency representatives, family representatives, youth and youth coordinators.

<sup>2</sup> Assuming the average annual income across all types of staff/service providers/administrators is \$40,000, the wage rate was estimated using the following formula: \$40,000 (annual income)/2080 (hours worked per year) = \$19.25 (dollars per hour).

<sup>3</sup> Number of respondents across 27 grantees. Average based on a 5 percent attrition rate at each data collection point. These data are collected as part of the grantees' routine intake processes. Hence, burden is calculated only for the subset of the Cross-Sectional Descriptive Study sample that also participates in the Child and Family Outcome Study.

<sup>4</sup> Given that 65 percent of the families in the Phase III evaluation sample fall at or below the 2005 DHHS National Poverty Level of \$19,350 (based on family of four), the wage rate was estimated using the following formula: \$19,350 (annual family income)/2080 (hours worked per year) = 9.30 (dollars per hour).

<sup>5</sup> Average number of responses per respondent based on 6 data collection points for children recruited in year 3, 4 for children recruited in year 4, 2 for children recruited in year 5 (of grantee funding).

<sup>6</sup> Estimated number of caregivers with children over age 5, based on Phase IV preliminary needs-assessment that 95 percent of children served will be over age 5.

<sup>7</sup> Estimated number of caregivers with children under age 12, based on Phase IV preliminary needs-assessment that 40 percent of children served will be under age 12.

<sup>8</sup> Based on Phase III finding that approximately 60 percent of the children in the evaluation were 11 years old or older.

<sup>9</sup> Based on the Federal minimum wage rate of \$5.15 per hour.

<sup>10</sup> Respondents only complete Service Experience Study measures at follow-up points. Average number of follow-up responses per respondent based on 6 follow-up data collection points for children recruited in year 3, 4 for children recruited in year 4, and 2 for children recruited in year 5 (of grantee funding).

<sup>11</sup> Assuming the average annual income across all types of staff/service providers is \$31,200, the wage rate was estimated using the following formula: \$31,200 (annual income)/2080 (hours worked per year) = \$15.00 (dollars per hour).

<sup>12</sup> 25 respondents will be caregiver and 75 respondents will be administrators/providers.

Written comments and recommendations concerning the proposed information collection should be sent May 7, 2007 to: SAMHSA Desk Officer, Human Resources and Housing Branch, Office of Management and Budget, New Executive Office Building, Room 10235, Washington, DC 20503; due to potential delays in OMB's receipt and processing of mail sent through the U.S. Postal Service, respondents are encouraged to submit comments by fax to: 202-395-6974.

Dated: April 3, 2007

**Elaine Parry,**

*Acting Director, Office of Program Services.*

[FR Doc. E7-6481 Filed 4-5-07; 8:45 am]

**BILLING CODE 4162-20-P**

**DEPARTMENT OF HOMELAND SECURITY**

**Office of the Secretary**

[Docket Number DHS 2006-0082]

**Privacy Act; Biometric Storage System of Records**

**AGENCY:** Privacy Office, Department of Homeland Security.

**ACTION:** Notice of Privacy Act system of records.

**SUMMARY:** Pursuant to the Privacy Act of 1974, the Department of Homeland Security, U.S. Citizenship and Immigration Services, proposes to add a new system of records to the Department's inventory, entitled Biometric Storage System. This new system will replace the following existing legacy systems, the Image Storage and Retrieval System (ISRS), 64 FR 18052, and portions of the Biometric Benefit Support System (BBSS).

**DATES:** The established system of records will be effective May 7, 2007 unless comments are received that result in a contrary determination.

**ADDRESSES:** You may submit comments, identified by Docket Number DHS 2006-0082 by one of the following methods:

- *Federal e-Rulemaking Portal:* <http://www.regulations.gov>. Follow the instructions for submitting comments.
- Fax: 1-866-466-5370.
- Mail: Hugo Teufel III, Chief Privacy Officer, Department of Homeland Security, Washington, DC 20528.

**FOR FURTHER INFORMATION CONTACT:** For system related questions please contact:

Phyllis Howard, Branch Chief of Application Support for Office of Field Operations, U.S. Citizenship and Immigration Services, Department of Homeland Security, 20 Massachusetts Avenue, NW., Washington, DC 20529. For privacy issues please contact: Hugo Teufel III, Chief Privacy Officer, Privacy Office, U.S. Department of Homeland Security, Washington, DC 20528.

**SUPPLEMENTARY INFORMATION:** The Department of Homeland Security (DHS), U.S. Citizenship and Immigration Services (USCIS) has been tasked by Congress with processing all immigration benefit applications and petitions. Many applications, petitions, and other benefits (hereinafter referred to as "applications") require that fingerprints and other biometrics be captured in order to conduct background checks, to verify the applicant's, petitioner's, or beneficiary's (hereinafter referred to as "applicants") identity, and to produce benefit cards with biometrics and documents. In order to fulfill its statutory mandate, USCIS is establishing a new system of records that will consolidate all biometrics collected by USCIS into one centralized system. This new system of

records is called the Biometric Storage System (BSS).

### I. USCIS Biometric Storage

Implemented as a part of a USCIS enterprise-wide "Transformation Program," BSS will help transition the agency's data management practices to a paperless, more centralized, and unique identity driven methodology. BSS will become the centralized repository for all biometric data captured by USCIS from applicants filing immigration applications. This new system will eventually replace existing legacy systems, including the Image Storage and Retrieval System (ISRS), 64 FR 18052, and portions of the Biometric Benefit Support System (BBSS).

USCIS captures biometric data from applicants to facilitate three key operational functions: (1) Conducting fingerprint-based background checks; (2) verifying an applicant's identity; and (3) producing benefit cards/documents. Currently, USCIS does not have a centralized, long-term storage program for fingerprint biometrics. Accordingly, applicants are sometimes required to return to an USCIS Application Support Center (ASC) to provide fingerprints again during the case adjudication process. BSS will store the biometric information, thereby decreasing the need to provide multiple sets of biometric data.

Further, BSS will consolidate storage of information from multiple, separate systems into a centralized database, allowing for greater control, security, and management of the data. BSS also will provide increased functionality over current systems, and improved communication between government databases and personnel, facilitating more efficient processing of applications. This furthers USCIS's goals of reducing immigration benefit and petition case backlog, and improving the process for vetting and resolving applications for immigration benefits.

#### *a. Fingerprint-Based Background Checks*

Under BSS, biometric and associated biographic information will be collected from the applicant in order to conduct fingerprint-based background checks through the Federal Bureau of Investigation (FBI) and United States Visitor and Immigrant Status Indicator Technology (US-VISIT).

Fingerprints will be taken electronically at an USCIS ASC or from hard copy fingerprint cards (FD-258) that are submitted for those applicants who are unable to go to an ASC. These

fingerprints, along with other biometric and limited biographical data collected from the applicant, will be assembled into a National Institute of Standard and Technology (NIST) approved Electronic Fingerprint Transmission Specification (EFTS) file and transferred to BSS from the ASCs. BSS will then submit the 10-print fingerprints and limited biographic information to, and receive results from, the FBI's Integrated Automated Fingerprint Identification System (IAFIS). The FBI fingerprint check is a search of the FBI's Criminal Master File, which will identify applicants and petitioners who have arrest records. The fingerprint check responses received from the FBI are interpreted as "classifiable" or "unclassifiable," and that classification is stored in BSS. A classifiable fingerprint set denotes that the FBI was able to utilize the fingerprints in the course of their matching processes. An unclassifiable fingerprint set denotes that the FBI was unable to utilize the fingerprints in the course of their matching processes. If applicable, the FBI Identification Record, which details an applicant's criminal history, will be transmitted by BSS to USCIS's Background Check Service (BCS), 71 FR 70414, for storage and not retained in BSS.

BSS will also submit the 10-print fingerprints, photograph, and limited biographic information to, and receive results from, US-VISIT/IDENT 71 FR 42651. The US-VISIT/IDENT fingerprint check is a search of US-VISIT's entire fingerprint database, which will identify applicants and petitioners who have entered or exited the country previously, as well as those for whom warrants and warrants may be outstanding, or who otherwise may be the subjects of ongoing law enforcement or investigative activity. This information, referred to as the US-VISIT/IDENT information file, will be transmitted by BSS to USCIS's BCS for storage and not retained in BSS. The US-VISIT/IDENT check will also return a unique enumerator for any currently enrolled 10-print fingerprints. The unique enumerator is based on and assigned to an applicant's unique fingerprint biometric signature. If US-VISIT/IDENT does not find a match, the system will enroll the 10-print fingerprints, generate a unique enumerator, and return that number to BSS.

The results of these fingerprint checks will be used to make eligibility determinations, which will result in the approval or denial of a benefit. If fraudulent or criminal activity is detected as a result of the fingerprint

check, information may be referred to appropriate law enforcement agencies including Immigration and Customs Enforcement (ICE), Customs and Border Protection (CBP), FBI, or other federal, state, local, tribal, foreign, or international law enforcement agencies.

#### *b. Card Production Information in BSS*

USCIS issues cards to individuals who have been granted immigration benefits such as Permanent Resident Cards and Border Crossing Cards. BSS will store information regarding benefit card and document production, including but not limited to photographs, signatures, press-prints (one fingerprint image, typically the index finger), and card production status.

BSS also will interface with the National Card Production System II / Integrated Card Production System (NPS II/ICPS) and the Computer-Linked Application Information System 3 (CLAIMS 3) 62 FR 64132 system of records. Specifically, BSS and NPS II/ICPS will share data linked with benefit cards and documents, including but not limited to: Card serial number; receipt number; production site; production date; class of admission; type of benefit card or document; and expiration date. BSS and CLAIMS 3 will share data related to benefit case adjudication, including the case status and card production status.

#### *c. Collection and Use of Information in BSS*

The data collected in BSS during the background check process provides USCIS with information about an applicant or petitioner that may have national security or public safety implications, or which may contain indicia of fraud. Collection and use of this information will enable DHS to take action to prevent potentially undesirable and often dangerous people from staying in this country, thereby supporting two primary missions of DHS: (1) Preventing terrorist attacks within the United States and reducing America's vulnerability to terrorism; and (2) facilitating the adjudication of lawful benefit applications.

All information to be stored in BSS is currently collected as part of the established USCIS application/petition process. The requested data is required to verify the applicant's identity and eligibility for the benefit being sought. ICE, CBP, and the Department of State (DoS) also will have read-only access to the BSS through a web-based user interface. This interface will allow the stated users to access and view biometric and limited biographic

information for identity verification purposes.

Consistent with DHS's information sharing mission, information collected and stored in the BSS may be provided by USCIS to appropriate federal, state, local, tribal or foreign governmental agencies or multi-lateral government organizations where DHS determines that sharing the information will assist in the enforcement of civil or criminal laws.

As mentioned previously, US-VISIT/IDENT will also receive a copy of the applicant's 10-print fingerprints, photograph, and limited biographic information. The information stored in US-VISIT/IDENT, including information received from BSS, 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 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 and the US-VISIT/IDENT system of records notice (71 FR 42651).

## II. The 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 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 an individual or by some identifying number, symbol, or other particular assigned to an individual.

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 to make agency recordkeeping practices transparent, to notify individuals reading the uses to which personally identifiable information is put, and to assist the individual to more easily find such files within the agency.

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

## DHS/USCIS-2006-0082

### SYSTEM NAME:

DHS/USCIS—003 Biometric Storage System (BSS)

### SECURITY CLASSIFICATION:

Sensitive; Unclassified.

### SYSTEM LOCATION:

The primary BSS system is located at a Department of Homeland Security (DHS) approved data center in the Washington, DC, metropolitan area. Backups are maintained offsite. BSS will be accessible worldwide from all USCIS field offices, service centers, and application support centers in the DHS Network.

### CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM:

All individuals who are applying for benefits and/or who are petitioning on behalf of individuals applying or petitioning for benefits pursuant to the Immigration and Nationality Act. 8 U.S.C. 1101 *et seq.*

### CATEGORIES OF RECORDS IN THE SYSTEM:

BSS maintains three general categories of records: (a) Applicant and Petitioner Biometric information; (b) Applicant and Petitioner Biographic Identification information; and (c) Card Production information.

A. *Applicant and Petitioner Biometric information* contains data necessary to perform a fingerprint-based background check through the FBI and US-VISIT/IDENT fingerprint check services, as well as data for verifying an applicant's identity and card production. This data may include: 10-print fingerprint images; photographs; signatures; transaction control numbers associated with FBI fingerprint checks; receipt numbers; date/time of submission; physical description of subject; and a reason for the submission of the application (i.e., a USCIS Form Code). This category also covers the applicants' US-VISIT/IDENT assigned enumerator. The unique enumerator is based on and assigned to an applicant's unique fingerprint biometric signature. If US-VISIT/IDENT does not find a match, the system will enroll the 10-print fingerprints, generate a unique enumerator, and return it to BSS. Lastly, this category covers logs associated with the requests of background checks, which may include requesting location and requesting person.

B. *Applicant and Petitioner Biographic Identification information* includes basic biographic information associated with each applicant or petitioner, including but not limited to: Name; date of birth; country of birth;

address; employment status; aliases; application type; height; weight; eye color; gender; hair color; and race. The applicant and petitioner information also includes uniquely identifiable numbers, including but not limited to: Alien Registration Number; Z-number; Receipt Number; Social Security Number; and Armed Forces Identification Number. This information would be obtained from multiple sources, including from the applicant at the time the fingerprints are taken, as well as from the applicant's preexisting case file.

C. *Card Production information* encompasses data received from and sent to NPS II/ICPS and CLAIMS 3. This data may include identifying transactional information (i.e., transaction control number), biographical information used for card production, card production status, benefit card/document type, and class of admission.

### AUTHORITY FOR MAINTENANCE OF THE SYSTEM:

8 U.S.C. 1103 *et seq.*

### PURPOSE(S):

BSS is a single centralized system that stores all biometric and associated biographic data that USCIS collects. Biometric data and associated biographic data are used by USCIS to conduct background checks, facilitate card production, and accurately identify applicants. Currently, no system exists that centrally manages all of this data. BSS will replace the following existing legacy systems, the Image Storage and Retrieval System, 64 FR 180526, and portions of the Biometric Benefit Support System (BBSS). BBSS is a legacy system that transfers biometric data from USCIS to the FBI to conduct fingerprint-based background checks. BBSS does not store the 10-print fingerprint images. ISRS is a legacy system that stores a limited amount of information related to an applicant's 10-print fingerprint images and card production information. BSS also will add new functionality so the collection of biometric data for USCIS applications may become centrally managed.

US-VISIT/IDENT will also receive a copy of the applicant's 10-print fingerprints, photograph, and limited biographic information. Consistent with DHS's information sharing mission, information stored in US-VISIT/IDENT, including information received from BSS, 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 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.

**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 United States Department of Justice (including United States Attorney offices) or other federal agency conducting litigation or in proceedings before any court, adjudicative or administrative body, or to the court 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; (2) any employee of DHS in his or her official capacity; (3) any employee of DHS in his or her individual capacity where DOJ or DHS has agreed to represent said employee; or (4) the United States or any agency thereof;

B. 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.

C. To the Department of State in the processing of petitions or applications for benefits under the Immigration and Nationality Act, and all other immigration and nationality laws including treaties and reciprocal agreements;

D. 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.

E. To contractors, 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 a DHS mission function related to this system of records, in compliance with the Privacy Act of 1974, as amended.

F. To appropriate federal, state, local, tribal, 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, license, or treaty where DHS determines that the information would assist in the enforcement of civil or criminal laws;

G. To federal and foreign government intelligence or counterterrorism agencies when DHS reasonably believes there to be a threat or potential threat to national or international security for which the information may be useful in countering the threat or potential threat, when DHS reasonably believes such use is to assist in anti-terrorism efforts, and disclosure is appropriate to the proper performance of the official duties of the person making the disclosure;

H. To employers participating in the Basic Pilot Verification Program or any successor program thereof, in order to verify the employment eligibility of all newly hired employees in the United States.

I. 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.

J. To appropriate agencies, entities, and persons when: (1) It is suspected or confirmed that the security or confidentiality of information in the system of records has been compromised; (2) USCIS 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 USCIS or another agency or entity) that rely upon the compromised information; and (3) the disclosure is made to such agencies, entities, and persons when reasonably necessary to assist in connection with USCIS's efforts to respond to the suspected or confirmed compromise and prevent, minimize, or remedy such harm.

**DISCLOSURE TO CONSUMER REPORTING AGENCIES:**

None.

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

**STORAGE:**

Records in the system will be stored in a central computer database.

**RETRIEVABILITY:**

A combination of the following BSS data elements may be used to initiate a query in order to retrieve data from the BSS User Interface: An individual's Alien Registration Number; name; date of birth; receipt number; and unique enumerator.

**SAFEGUARDS:**

Information in this system is safeguarded in accordance with applicable laws and policies, including the DHS information technology security policies and the Federal Information Security Management Act (FISMA). 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, using locks, and password protection features. The system is also protected through a multi-layer security approach. The protective strategies are physical, technical, administrative and environmental in nature, which provide access control to sensitive data, physical access control to DHS facilities, confidentiality of communications, authentication of sending parties, and personnel screening to ensure that all personnel with access to data are screened through background investigations commensurate with the level of access required to perform their duties.

**RETENTION AND DISPOSAL:**

The following proposal for retention and disposal is pending approval by the National Archives and Records Administration. Records are stored and retained in the BSS Repository for seventy-five (75) years, from the date of last action on the file. BSS is utilizing ISRS' retention schedule as a model. Biometric-based background checks are conducted on individuals and/or petitioners from the age of fourteen (14) and up. The 75-year retention rate comes from the length of time USCIS may interact with a customer. Further, retaining the data for this period of time will enable USCIS to fight identity fraud and misappropriation of benefits.

**SYSTEM MANAGER(S) AND ADDRESS:**

Branch Chief of Application Support for Office of Field Operations, U.S. Citizenship and Immigration Services, Department of Homeland Security, 20 Massachusetts Avenue, NW., Washington, DC 20529.

**NOTIFICATION PROCEDURE:**

To determine whether this system contains records relating to you, write the USCIS Freedom of Information Act/Privacy Act officer. Mail requests to: U.S. Citizenship and Immigration Services, National Records Center, FOIA/PA Office, P.O. Box 648010, Lee's Summit, MO 64064-8010.

**RECORD ACCESS PROCEDURES:**

Follow "Notification procedures" above.

**CONTESTING RECORD PROCEDURES:**

Redress procedures are established and operated by the program through which the data was originally collected. In the case of redress requests for DHS organizations, if an individual is not satisfied with the response, an individual can appeal his or her case to the DHS Chief Privacy Officer, who will conduct a review and provide final adjudication on the matter.

**RECORD SOURCE CATEGORIES:**

Information contained in this system of records is obtained from other USCIS Systems of Records; including, CLAIMS3, NPS II/ICPS, and electronic live scan devices located at ASCs. Information contained in the system is also obtained from the Federal Bureau of Investigation, and the United States Visitor and Immigrant Status Indicator Technology. All information contained in BSS is derived from the above systems.

**EXEMPTIONS CLAIMED FOR THE SYSTEM:**

None.

Dated: March 28, 2007.

**Hugo Teufel III,**

Chief Privacy Officer.

[FR Doc. 07-1643 Filed 4-5-07; 8:45 am]

BILLING CODE 4410-10-P

**DEPARTMENT OF HOMELAND SECURITY****National Communications System**

[Docket No. NCS-2007-0002]

**National Security Telecommunications Advisory Committee**

**AGENCY:** National Communications System, DHS.

**ACTION:** Notice of Partially Closed Advisory Committee Meeting.

**SUMMARY:** The President's National Security Telecommunications Advisory Committee (NSTAC) will meet in a partially closed session.

**DATES:** Thursday, April 26, 2007, from 1:15 p.m. until 5 p.m.

**ADDRESSES:** The meeting will take place at the U.S. Chamber of Commerce, 1615 H St., NW., Washington DC. For access to the meeting materials, contact Mr. William Fuller at (703) 235-5521 or by e-mail at [william.c.fuller@dhs.gov](mailto:william.c.fuller@dhs.gov) by 5 p.m. on Friday, April 20, 2007. If you desire to submit comments, they must be submitted by May 3, 2007. Comments must be identified by NCS-2007-0002 and may be submitted by one of the following methods:

- *Federal eRulemaking Portal:* <http://www.regulations.gov>. Follow the instructions for submitting comments.

- *E-mail:* [NSTAC1@dhs.gov](mailto:NSTAC1@dhs.gov). Include docket number in the subject line of the message.

- *Mail:* Office of the Manager, National Communications System (N5), Department of Homeland Security, CS&T/NCS/N5, 245 Murray Lane, Mail Stop 8510, Washington, DC 20528.

- *Fax:* 1-866-466-5370

*Instructions:* All submissions received must include the words "Department of Homeland Security" and NCS-2007-0002, the docket number for this action. Comments received will be posted without alteration at <http://www.regulations.gov>, including any personal information provided.

*Docket:* For access to the docket to read background documents or comments received by the NSTAC, go to <http://www.regulations.gov>.

**FOR FURTHER INFORMATION CONTACT:** Ms. Kiesha Gebreyes, Chief, Industry Operations Branch at (703) 235-5525, e-mail: [Kiesha.Gebreyes@dhs.gov](mailto:Kiesha.Gebreyes@dhs.gov) or write the Deputy Manager, National Communications System, Department of Homeland Security, IP/NCS/N5, 245 Murray Lane, Mail Stop 8510, Washington, DC 20528.

**SUPPLEMENTARY INFORMATION:** The NSTAC advises the President on issues and problems related to implementing national security and emergency preparedness telecommunications policy. Notice of this meeting is given under the Federal Advisory Committee Act (FACA), Public Law 92-463, as amended (5 U.S.C. App.1 *et seq.*).

At the upcoming meeting, between 1:15 p.m. and 2:15 p.m., the NSTAC will receive comments from government stakeholders, discuss the work of the Emergency Communications and Interoperability Task Force (ECITF), and discuss and vote on the International Task Force (ITF) Report. This portion of the meeting will be open to the public.

Between 2:30 p.m. and 5 p.m., the NSTAC will discuss Global Infrastructure Resiliency (GIR) and Cyber Security. This portion of the meeting will be closed to the public.

Persons with disabilities who require special assistance should indicate this when arranging access to the teleconference and are encouraged to identify anticipated special needs as early as possible.

*Basis for Closure:* The GIR and Cyber Security discussions will likely involve sensitive infrastructure information concerning system threats and explicit physical/cyber vulnerabilities related to current communications capabilities.

Public disclosure of such information would heighten awareness of potential vulnerabilities and increase the likelihood of exploitation by terrorists or other motivated adversaries. Pursuant to Section 10(d) of the Federal Advisory Committee Act, Public Law 92-463, as amended (5 U.S.C. App. 1 *et seq.*), the Department has determined that this discussion will concern matters which, if disclosed, would be likely to frustrate significantly the implementation of a proposed agency action. Accordingly, the relevant portion of this meeting will be closed to the public pursuant to the authority set forth in 5 U.S.C. 552b(c)(9)(B).

Dated: March 23, 2007.

**Sallie McDonald,**

Director, National Communications System.

[FR Doc. E7-6418 Filed 4-5-07; 8:45 am]

BILLING CODE 4410-10-P

**DEPARTMENT OF HOMELAND SECURITY****U.S. Citizenship and Immigration Services****Agency Information Collection Activities: Revision of an Existing Information Collection; Comment Request**

**ACTION:** 60-Day notice of information collection under review; Form I-817, Application for Family Unity Benefits; OMB Control No. 1615-0005.

The Department Homeland Security, U.S. Citizenship and Immigration Services has submitted 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 June 5, 2007.

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 Management Division, Clearance Officer, 111 Massachusetts Avenue, 3rd floor, Suite 3008, Washington, DC 20529. Comments may also be submitted to DHS via facsimile to 202-272-8352 or via e-mail at [rfs.regs@dhs.gov](mailto:rfs.regs@dhs.gov). When submitting comments by e-mail please make sure to add OMB Control No. 1615-0005 in the subject box.