

administering or enforcing the law, national security, immigration, or intelligence, where consistent with a DHS mission-related function as determined by DHS.

B. To appropriate Federal, state, local, tribal, foreign, or international government agencies charged with national security, law enforcement, immigration, intelligence, or other DHS mission-related functions in connection with the hiring or retention by such an agency of an employee, the issuance of a security clearance, the reporting of an investigation of such an employee, the letting of a contract, or the issuance of a license, grant, loan, or other benefit by the requesting agency.

C. To an actual or potential party or to his or her attorney for the purpose of negotiation or discussion on such matters as settlement of the case or matter, or discovery proceedings.

D. 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.

E. To the National Archives and Records Administration or other Federal government agencies pursuant to records management inspections being conducted under the authority of 44 U.S.C. Sections 2904 and 2906.

F. To individuals who are obligors or representatives of obligors of bonds posted.

G. To contractors, grantees, experts, consultants, students, 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.

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

**STORAGE:**

Information can be stored in case file folders, cabinets, safes, or a variety of electronic or computer databases and storage media.

**RETRIEVABILITY:**

Records may be retrieved by biometrics or select personal identifiers.

**SAFEGUARDS:**

The system is protected through multi-layer security mechanisms. The protective strategies are physical, technical, administrative, and environmental in nature, and 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 with National Archives and Records Administration (NARA):

Records that are stored in an individual's file will be purged according to the retention and disposition guidelines that relate to the individual's file (DHS/ICE/USCIS001A).

Testing and training data will be purged when the data is no longer required. Electronic records for which the statute of limitations has expired for all criminal violations or that are older than 75 years will be purged. Fingerprint cards, created for the purpose of entering records in the database, will be destroyed after data entry. Work Measurement Reports and Statistical Reports will be maintained within the guidelines set forth in NCI-95-78-5/2 and NCI-85-78-1/2 respectively.

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

System Manager, IDENT Program Management Office, US-VISIT Program, U.S. Department of Homeland Security, Washington, DC 20528, USA.

**NOTIFICATION PROCEDURE:**

To determine whether this system contains records relating to you, write to the US-VISIT Privacy Officer, US-VISIT Program, U.S. Department of Homeland Security, 245 Murray Lane, SW., Washington, DC 20528, USA.

**RECORD ACCESS PROCEDURES:**

The major part of this system is exempted from this requirement pursuant to 5 U.S.C. 552a(j)(2) and (k)(2). A determination as to the granting or denial of access shall be made at the time a request is received. Requests for access to records in this system must be in writing, and should be addressed to the US-VISIT Privacy Officer as noted above. Such request may be submitted either by mail or in person. The envelope and letter shall be clearly marked "Privacy Officer—Redress Request." To identify a record, the record subject should provide his or her full name, date and place of birth; if appropriate, the date and place of entry into or departure from the United States; verification of identity by submitting a copy of fingerprints if appropriate (in accordance with 8 CFR 103.21(b) and/or pursuant to 28 U.S.C.

1746, make a dated statement under penalty of perjury as a substitute for notarization), and any other identifying information that may be of assistance in locating the record. The requestor shall also provide a return address for transmitting the records to be released.

**CONTESTING RECORD PROCEDURES:**

The major part of this system is exempted from this requirement pursuant to 5 U.S.C. 552a(j)(2) and (k)(2). A determination as to the granting or denial of a request shall be made at the time a request is received. An individual desiring to request amendment of records maintained in this system should direct his or her request to the System Manager noted above or the appropriate FOIA/PA Officer. The request should state clearly what information is being contested, the reasons for contesting it, and the proposed amendment to the information.

**RECORD SOURCE CATEGORIES:**

Basic information contained in this system is supplied by individuals covered by this system, and other Federal, state, local, tribal, or foreign governments; private citizens; and public and private organizations.

**EXEMPTIONS CLAIMED FOR THE SYSTEM:**

The Secretary of Homeland Security has exempted this system from 5 U.S.C. 552a(c)(3) and (4); (d); (e)(1), (e)(2), (e)(3), (e)(4)(G), (e)(4)(H), (e)(5) and (e)(8); (f)(2) through (5); and (g) pursuant to 5 U.S.C. 552a(j)(2). In addition, the Secretary of Homeland Security has exempted portions of this system from 5 U.S.C. 552a(c)(3), (d), (e)(1), (e)(4)(G), and (e)(4)(H) pursuant to 5 U.S.C. 552a(k)(2). These exemptions apply only to the extent that records in the system are subject to exemption pursuant to 5 U.S.C. 552a(j)(2) and (k)(2).

Dated: July 19, 2006.

**Maureen Cooney,**

*Acting Chief Privacy Officer.*

[FR Doc. E6-11995 Filed 7-26-06; 8:45 am]

**BILLING CODE 4410-10-P**

**DEPARTMENT OF HOMELAND SECURITY**

**Publication and Release of the National Response Plan**

**AGENCY:** Department of Homeland Security.

**ACTION:** Notice.

**SUMMARY:** This Notice informs the public that the Department of Homeland

Security (DHS) has developed and published a Notice of Change to the National Response Plan, that is now available to the public.

**Authority:** Homeland Security Act of 2002, Public Law 107-296; Homeland Security Presidential Directive—5, *Management of Domestic Incidents*.

**FOR FURTHER INFORMATION CONTACT:** Ms. Tina Gabbrielli, National Preparedness Task Force, DHS, Washington, DC 20528, 202-282-9810 or [NPTF-CP@dhs.gov](mailto:NPTF-CP@dhs.gov); Mr. Paul Schwartz, Interagency Response Planning, DHS, Federal Emergency Management Agency, Washington, DC 20472, 202-646-7653 or [paul.k.schwartz@dhs.gov](mailto:paul.k.schwartz@dhs.gov).

**SUPPLEMENTARY INFORMATION:** In December 2004, the Department of Homeland Security (DHS) published the National Response Plan (NRP). The NRP, using the comprehensive framework of the National Incident Management System (NIMS), establishes a comprehensive, national, all-hazards approach to domestic incident management across a spectrum of activities including prevention, preparedness, response, and recovery. It provides the structure and mechanisms for the coordination of Federal support to State, local, and tribal incident managers and for exercising direct Federal authorities and responsibilities. The NRP is applicable to all Federal departments and agencies that may be requested to provide assistance or conduct operations in the context of actual or potential domestic incidents requiring a coordinated Federal response.

As of April 14, 2005, the NRP superseded the Initial National Response Plan, Federal Response Plan, U.S. Government Interagency Domestic Terrorism Concept of Operations Plan, and Federal Radiological Emergency Response Plan, and all Federal departments and agencies were required to fully implement the NRP.

Based on lessons learned during Hurricane Katrina, DHS reviewed recommendations applicable to the execution of the NRP and worked with the White House Homeland Security Council (HSC) to identify and amend select sections of the NRP. A Notice of Change, which was limited in scope to those actions requiring immediate clarification or modification in order to ensure future effective and coordinated Federal responses, was subsequently developed by DHS and approved by the HSC Domestic Readiness Group. A full scale review of the NRP will commence at a later date.

The Notice of Change to the NRP became effective on May 25, 2006.

When providing support under the NRP, Federal departments and agencies are required to conform to any modifications to the processes or structures identified in the Notice of Change.

This Notice informs the public of the release and availability of the National Response Plan Notice of Change. The Notice of Change is available on the Department of Homeland Security's Web site at <http://www.dhs.gov/nationalresponseplan>.

**George W. Foresman,**

*Under Secretary for Preparedness,  
Department of Homeland Security.*

**R. David Paulison,**

*Under Secretary for Federal Emergency  
Management, Department of Homeland  
Security.*

[FR Doc. E6-11998 Filed 7-26-06; 8:45 am]

**BILLING CODE 9110-09-P**

## DEPARTMENT OF HOMELAND SECURITY

### United States Visitor and Immigrant Status Indicator Technology Program

#### Processing Additional Aliens Privacy Impact Assessment

**AGENCY:** Privacy Office, Office of the Secretary, DHS.

**ACTION:** Notice of availability of a Privacy Impact Assessment.

**SUMMARY:** The Department of Homeland Security has updated and is making available its United States Visitor and Immigrant Status Indicator Technology Program (US-VISIT) Privacy Impact Assessment (PIA) to discuss the impact of program change on privacy. The PIA can be found under the Privacy Impact Assessment Section of the Privacy Office's Web site, [www.dhs.gov/privacy](http://www.dhs.gov/privacy).  
**DATES:** The Privacy Impact Assessment will be available for a minimum of (60) days.

**FOR FURTHER INFORMATION CONTACT:** Steve Yonkers, Privacy Officer, US-VISIT, Department of Homeland Security, Washington, DC 20528, telephone (202) 298-5200, facsimile (202) 298-5201, e-mail: [usvisitprivacy@dhs.gov](mailto:usvisitprivacy@dhs.gov); Maureen Cooney, Acting Chief Privacy Officer, Department of Homeland Security, Mail Stop 0550, 601 S. 12th Street, Arlington, VA 22202-4220; by telephone (571) 227-3813, facsimile (571) 227-4171, or e-mail: [privacy@dhs.gov](mailto:privacy@dhs.gov).

**SUPPLEMENTARY INFORMATION:** The Department of Homeland Security (DHS) has updated and is making available its US-VISIT PIA to discuss

the impact of a program change on privacy. The PIA updates relate to the proposal by DHS to expand the US-VISIT population to cover additional classes of aliens under a Notice of Proposed Rulemaking titled Authority to Process Additional Aliens in US-VISIT published in today's **Federal Register**. The revised PIA is available on the Web site of the DHS Privacy Office, [www.dhs.gov/privacy](http://www.dhs.gov/privacy), under Privacy Impact Assessments, and on the US-VISIT Web site, [www.dhs.gov/usvisit](http://www.dhs.gov/usvisit). The original US-VISIT PIA was published in the **Federal Register** on January 16, 2004 (69 FR 2608); revised versions reflecting subsequent changes were published on September 23, 2004 (69 FR 57036), and on July 7, 2005 (70 FR 39300).

Dated: July 19, 2006.

**Maureen Cooney,**

*Acting Chief Privacy Officer.*

[FR Doc. E6-11994 Filed 7-26-06; 8:45 am]

**BILLING CODE 4410-10-P**

## DEPARTMENT OF HOMELAND SECURITY

### U.S. Citizenship and Immigration Services

[CIS No. 2388-06; USCIS-2006-0018]

RIN 1615-ZA35

#### Extension of the Designation of Temporary Protected Status for Somalia; Automatic Extension of Employment Authorization Documentation for Somalia TPS Beneficiaries

**AGENCY:** U.S. Citizenship and Immigration Services, Department of Homeland Security.

**ACTION:** Notice of extension of temporary protected status for Somalia.

**SUMMARY:** The designation of Somalia for Temporary Protected Status (TPS) will expire on September 17, 2006. This Notice informs the public that the TPS designation for Somalia has been extended for 18 months, until March 17, 2008, and sets forth procedures for nationals of Somalia (or aliens having no nationality who last habitually resided in Somalia) with TPS to re-register and to apply for an extension of their Employment Authorization Documents (EADs) for the additional 18-month period. Re-registration is limited to persons who have previously registered for TPS under the designation of Somalia and whose application was granted or remains pending. Certain nationals of Somalia (or aliens having