

who design, finance, and deliver mental health services; (3) administers the Projects for Assistance in Transition from Homelessness (PATH) program; and (4) directs the Comprehensive Community Mental Health Services for Children with Serious Emotional Disturbances Program; (5) places priority on two target populations, adults with severe mental illness (including those who are homeless) and children and adolescents with serious mental disturbances; (6) emphasizes acquisition, exchange, and application of knowledge in all of its activities; (7) develops Guidances for Applications and requests for contracts to implement these activities; (8) monitors grants, cooperative agreements, contracts, interagency agreements, and memoranda of understanding; (9) identifies needs for and provides technical assistance to a variety of customers through both direct and indirect activities, including the development of standards and guidelines; (10) establishes and maintains collaborative relationships with other Federal, State, and local governmental agencies, national organizations, local communities, providers, consumers, and families; (11) promotes adoption of practices in communities through the Nation by synthesizing knowledge, exchanging information, and providing opportunities for consensus building, and (12) promote the prevention of HIV infection in people at risk, the delivery of effective mental health services for people with HIV infection, and the education of health care providers to address the neuropsychiatric and the psychosocial aspects of HIV infection and AIDS and maintains liaison with national organizations and other Federal departments.

Delegation of Authority

All delegations and redelegations of authority to officers and employees of SAMHSA which were in effect immediately prior to the effective date of this reorganization shall continue to be in effect pending further redelegations, providing they are consistent with the reorganization.

These organizational changes are effective.

Dated: July 23, 2008.

Terry L. Cline,
Administrator.

[FR Doc. E8-17371 Filed 7-29-08; 8:45 am]

BILLING CODE 4160-01-M

DEPARTMENT OF HOMELAND SECURITY

[Docket No. DHS-2008-0074]

The Critical Infrastructure Partnership Advisory Council

AGENCY: National Protection and Programs Directorate, DHS.

ACTION: Notice of update to DHS-2008-0074, the Critical Infrastructure Partnership Advisory Council (CIPAC) Meeting

SUMMARY: The update provides a change to the previously published FRN DHS-2008-0074, which moved the start time of the Critical Infrastructure Partnership Advisory Council meeting on July 30, 2008, from 8:20 a.m. Eastern Daylight Time (EDT) to 8 a.m. EDT. The meeting will adjourn at 4 p.m. EDT. Check-in for the meeting will begin at 7:30 a.m. EDT. Please note that the meeting may adjourn early if the committee has completed its business.

The meeting agenda is as follows:

- 7:30 a.m. Registration.
- 8 a.m. Call to Order: Sector Roll Call.
- 8:10 a.m. The Three Pillars of the CIPAC Partnership.
- 8:30 a.m. The Pathway to the Present: How We Got Where We Are Now.
- 8:50 a.m. Setting the Stage for Today's Discussions.
- 9 a.m. DHS and the National Infrastructure Protection Plan Framework.
- 9:35 a.m. Asset-Based Infrastructure Protection.
- 10:35 a.m. Systems-Based Infrastructure Protection.
- 12:15 p.m. Cross-Sector Dependencies and Interdependencies.
- 1:15 p.m. Regional Implementation of the National Infrastructure Protection Plan.
- 2:15 p.m. The National Infrastructure Protection Plan Partnership Framework: Assessment and Our Path Forward.
- 3:15 p.m. Perspective from The Hill: The National Infrastructure Protection Plan Partnership Framework.
- 3:45 p.m. Closing Remarks.
- 4 p.m. Adjournment.

DATES: The Critical Infrastructure Partnership Advisory Council will meet Wednesday, July 30, 2008. For additional information, please consult the CIPAC Web site, <http://www.dhs.gov/cipac>, or contact the CIPAC Secretariat by phone at 703-235-3999 or by e-mail at cipac@dhs.gov.

ADDRESSES: The meeting will be held in Salons III and IV of the Grand Ballroom of the J.W. Marriott, 1331 Pennsylvania

Avenue, Washington, DC 20004. While we will be unable to accommodate oral comments from the public, written comments may be sent to Nancy Wong, Department of Homeland Security, National Protection and Programs Directorate, Washington, DC 20528. Comments must be identified by DHS-2008-0074 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:* cipac@dhs.gov. Include the docket number in the subject line of the message.

- *Fax:* 703-235-3055

- *Mail:* Nancy Wong, Department of Homeland Security, National Protection and Programs Directorate, Washington, DC 20528.

Instructions: All submissions received must include the words "Department of Homeland Security" and 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 Critical Infrastructure Partnership Advisory Council, go to <http://www.regulations.gov>.

FOR FURTHER INFORMATION CONTACT:

Nancy Wong, CIPAC Designated Federal Officer, Department of Homeland Security, Washington, DC 20528; telephone 703-235-3999.

Dated: July 22, 2008.

Nancy Wong,

Designated Federal Officer for the CIPAC.

[FR Doc. E8-17374 Filed 7-29-08; 8:45 am]

BILLING CODE 4410-10-P

DEPARTMENT OF HOMELAND SECURITY

Transportation Security Administration RIN 1652-ZA12

Registered Traveler Interoperability Pilot Program

AGENCY: Transportation Security Administration, DHS.

ACTION: Notice.

SUMMARY: The Transportation Security Administration (TSA) published a notice in the **Federal Register** on November 24, 2006, to establish the Service Provider Key Personnel Fee and the Registered Traveler Interoperability Pilot Participant Fee for the Registered Traveler Interoperability Pilot (RTIP).

Under the RTIP, passengers who voluntarily provided biometric and biographic information to TSA, or a TSA agent, and successfully completed a TSA security threat assessment, could obtain expedited security screening at participating airports. TSA implemented the fees announced in the November 24, 2006, notice to compensate TSA for the cost of performing security threat assessments on RTIP applicants and related program operation costs. Today, TSA is announcing the completion of the RTIP and termination of the TSA RTIP fees. TSA will continue to work with private sector partners as they continue to develop the Registered Traveler business as a private sector enterprise. That business is no longer limited to the 10–20 locations outlined in the November 24, 2006 **Federal Register** notice.

DATES: This notice is effective July 30, 2008.

FOR FURTHER INFORMATION CONTACT: Thomas Cowley, Director, Aviation Credentialing, Office of Transportation Threat Assessment and Credentialing (TTAC), TSA–19, Transportation Security Administration, 601 South 12th Street, Arlington, VA 22202–4220; facsimile (571) 227–1936; e-mail: Registered.Traveler@dhs.gov.

SUPPLEMENTARY INFORMATION:

Availability of Notice Document

You can get an electronic copy using the Internet by—

- (1) Accessing the Government Printing Office's Web page at: <http://www.gpoaccess.gov/fr/index.html>; or
- (2) Visiting TSA's Security Regulations Web page at <http://www.tsa.gov> and accessing the link for "Research Center" at the top of the page.

In addition, copies are available by writing the individual in the **FOR FURTHER INFORMATION CONTACT** section.

I. Background

The Aviation and Transportation Security Act (ATSA), Public Law 107–71 (115 Stat. 597, 613, Nov. 19, 2001), sec. 109(a)(3), authorizes the Transportation Security Administration (TSA) to "establish requirements to implement trusted passenger programs and use available technologies to expedite security screening of passengers who participate in such programs, thereby allowing security screening personnel to focus on those passengers who should be subject to more extensive screening." To enable a nationwide private sector Registered Traveler (RT) business opportunity, TSA has been working, and continues to

work, with private sector providers of RT to harmonize technologies and business processes with government credentialing and screening standards and procedures to improve commercial air travel while continuing to safeguard transportation and national security.

RT has been developed through a series of three pilots. TSA announced the first pilot, the Registered Traveler Pilot Program, on July 7, 2004. The Registered Traveler Pilot Program was a federally-managed pilot conducted at five designated airports¹ that established biometrics use in identity verification and determined baselines for public acceptance. The second pilot program, named the Private Sector Known Traveler, tested the feasibility of implementing RT through a public/private partnership at a single airport. The third pilot, the RTIP, further tested and evaluated this type of trusted passenger program. The RTIP also introduced interoperability among participating airports/air carriers and operated with larger populations.

RT is a private sector business opportunity that currently is supported and overseen by TSA, with distinct roles and responsibilities for each participating entity. Under the RTIP and its predecessor pilots, TSA was responsible for setting program standards and conducting the security threat assessment, physical screening at TSA checkpoints and certain forms of oversight. The private sector was responsible for enrollment, identity verification, concierge and related services.

Under the RTIP enrollment process, RT applicants voluntarily provided RT Sponsoring Entities (*i.e.*, participating airport authorities or air carrier operators) and Service Providers (*i.e.*, a private sector vendor chosen by a Sponsoring Entity to implement RT as its agent) with biographic and biometric data needed for TSA to conduct the security threat assessment and determine eligibility. The TSA security threat assessment included checking each applicant's biographic information against terrorist-related, law enforcement, and immigration databases that TSA maintains or uses. RT applicants who received an "approved" security threat assessment result were authorized to become program participants.

Once a traveler qualified as an approved participant, the traveler was able to take advantage of the expedited

screening process available exclusively through the RT program. At the airport screening checkpoint, RT participants entered a designated RT lane and verified their identity through biometric identity verification technologies. This process also ensured that the individual was an "approved" RT participant. After the identity and current status of the RT participant were verified, the participant entered the checkpoint lane identified for registered travelers and underwent the applicable TSA checkpoint screening. These processes will remain largely unchanged with the end of the RTIP and expansion of RT. They should provide the basis to expedite the RT participants' entrance into the screening process.

In evaluating the RTIP, TSA reached several conclusions that led to the termination of the TSA fee being announced today. First, current technology is insufficient to allow anyone, even travelers who provide biographic and biometric information and undergo a TSA security threat assessment, to bypass the minimum screening procedures at airport security checkpoints. For example, one service provider suggested that a device to scan shoes replace the requirement that the passenger remove his or her shoes. TSA tested the shoe scanner and concluded that it was less effective than existing x-ray capabilities which require a TSA officer to monitor materials to detect potential explosive or other dangerous devices in shoes, purses or other carry-on materials during TSA screening.

Second, TSA concluded that an individual's successful completion of a TSA threat assessment did not eliminate the possibility that the individual might initiate an action that threatens the lives of other passengers. Therefore, screening of these individuals should remain the same as screening of other passengers.

Third, while effective identity verification is a critically important element in a multi-layered approach to aviation security, RT is not a stand-alone security program. Finally, the interoperability of the RT is a beneficial element. RT Service Providers have demonstrated the ability to verify technically and recognize revocation of each other's cards. Based on these observations and conclusions, TSA has concluded the RTIP and has decided to focus the government role in relation to RT on its identity verification benefits.

II. Evolution of Registered Traveler

A. Roles and Responsibilities Under RT

With the conclusion of the RTIP, TSA is announcing modifications to RT.

¹ Minneapolis-St. Paul Airport, Los Angeles International Airport, George Bush International Airport/Houston, Boston Logan International Airport, and Ronald Reagan Washington National Airport.

These modifications include changes to TSA's role. TSA will set security standards for RT through modifications to the Sponsoring Entities' security programs. TSA will continue to exercise oversight of the Sponsoring Entities to ensure compliance with the security standards. These security standards will be similar in nature to the security standards currently in place for the RTIP and will enhance security features. However, TSA will no longer set other standards for, or conduct security threat assessments of, RT applicants. TSA will also continue its screening operations at the security checkpoint. RT participants will continue to be screened according to the standard TSA screening process and vetted against the No Fly and Selectee Lists of the Terrorist Screening Database.

The private sector will have the primary role in RT's future. Sponsoring Entities will continue to select their Service Providers and enter into a contractual relationship with them. The Sponsoring Entities will continue to be responsible for overseeing and monitoring their Service Providers, and for ensuring their compliance with the requirements of RT. These requirements are part of the Sponsoring Entities' security programs.

As the vendors for the Sponsoring Entities, the Service Providers will continue to provide enrollment and verification services. As discussed in further detail in Section II.B, Sponsoring Entities and Service Providers may elect to develop and implement an enhanced identity verification process. Sponsoring Entities and Service Providers may also develop other benefits and innovations for RT provided that the benefits and innovations are not inconsistent with the Sponsoring Entities' security programs.

RT benefits will continue to be determined locally and may vary by location. It will be the responsibility of the private sector Service Providers and Sponsoring Entities (airports or air carriers) to fashion each arrangement, consistent with the TSA approved standards for Sponsoring Entities' security programs.

RT participants voluntarily provide information to Sponsoring Entities and Service Providers as part of an enhanced identity verification business opportunity. RT participants may receive benefits such as using designated security lanes or expedited access to security screening. These benefits are determined and modified at the discretion of the Sponsoring Entities and their Service Providers.

B. Identity Verification Benefits of Registered Traveler

The name on the individual's boarding pass is the name that is used to perform watch list matching. RT can be effective in verifying that the passenger who is traveling is actually the person whose name is on the boarding pass. RT represents a private-sector alternative by which travelers can establish their identities, and biographically and biometrically link that identity to their RT cards.

RT Service Providers perform identity verification as part of the RT enrollment process. The verification process at the airport RT lanes confirms that the individual who is presenting the RT card is the individual who has established his or her identity during the enrollment process. Together, the RT enrollment and verification processes perform the main security function of the TSA Travel Document Checker (TDC) at the screening checkpoint, which is to verify the identity of travelers before they enter the sterile area. Thus RT participants may bypass the TDC if their RT cards contain the appropriate biometric and biographic information.

New Sponsoring Entities that wish to offer RT services at their respective airports will need to demonstrate that their enrollment Service Providers adopt a process that adequately establishes a RT participant's identity. This process will be similar to the process in place for the RTIP. Because identity verification is an important component of TSA's layered security approach, airport operators and aircraft operators who wish to begin to offer RT service after the effective date of this notice must adopt an amendment to their security program that satisfies the identity verification requirements and all other RT requirements prior to commencing RT operations at their respective airports.

Sponsoring Entities that currently have RT operations under the RTIP may continue with their RT operations under their existing security program amendments consistent with this notice.

C. Transition Period

TSA required interoperability as part of the RTIP with the understanding that the Service Providers would negotiate with each other to establish any fees they would charge each other to implement interoperability.

A twelve-month transition period will be provided following the effective date of this notice where Service Providers must accept all valid RT cards at all locations, ensuring that RT participants

who recently joined an RT program will have the interoperability benefits for which they enrolled. Thereafter, RT Service Providers must continue to be able to technically verify and recognize revocation of each other's cards, but they will not be required to guarantee interoperability. TSA is leaving it to the private sector (*i.e.*, Sponsoring Entities, Service Providers, customers, and other interested stakeholders) to determine how to address acceptance, including the possibility of transfer fees.

D. Rescission of Registered Traveler Interoperability Pilot Fees

TSA has determined that the current security threat assessment largely duplicates the watch list matching that is conducted on all travelers every time they fly. The other parts of the TSA are not core elements in passenger security and will no longer be required. Because TSA will no longer be conducting security threat assessments on RT participants, TSA will no longer collect a security threat assessment fee. Additionally, with the conclusion of the RTIP, TSA will no longer collect a fee to cover the cost of the RTIP. Thus, the RTIP Participant fee of \$28 is rescinded as of the effective date of this notice. After that date, TSA will no longer conduct security threat assessments on RT participants.

Additionally, TSA will no longer collect the Service Provider Key Personnel Fee. Service Providers, however, are the Sponsoring Entities' contractors. Thus, Service Providers' employees who perform certain functions, such as enrollment, must undergo a background check in accordance with TSA's existing practices covering airport-sponsored vendors, including the collection of fees.

If a Sponsoring Entity decides to create a separate, dedicated screening lane for RT participants or institute a process that requires Transportation Security Officer support beyond what TSA is currently providing for these passengers, TSA will negotiate the exact level of support and the fee necessary to match the costs of this support with the Sponsoring Entity. TSA will then charge the Sponsoring Entity the fee based upon the cost of providing the additional services and support.

TSA continues to encourage private-sector innovation that can expedite the screening process without sacrificing security results—such as the anticipated development of a “laptop bag”—and remains committed to testing such technologies in both laboratory and live settings. However, TSA will endeavor to deploy such proven technologies at all

checkpoints nationwide, not just for premium travelers or those who pay additional fees.

As stated in the notice, Registered Traveler Interoperability Fees, 71 FR 67899 (Nov. 24, 2006), TSA will not refund any TSA RT fees collected prior to the effective date of this notice.

Issued in Arlington, Virginia, on July 25, 2008.

Gale D. Rossides,

Deputy Administrator.

[FR Doc. E8-17493 Filed 7-29-08; 8:45 am]

BILLING CODE 9110-05-P

DEPARTMENT OF HOMELAND SECURITY

U.S. Citizenship and Immigration Services

Agency Information Collection Activities: Form I-602, Extension of an Existing Information Collection; Comment Request

ACTION: 30-Day Notice of Information Collection Under Review: Form I-602, Application by Refugee for Waiver of Grounds of Excludability; OMB No. 1615-0069.

The Department of Homeland Security, U.S. Citizenship and Immigration Services (USCIS) has submitted the following information collection request to the Office of Management and Budget (OMB) for review and clearance in accordance with the Paperwork Reduction Act of 1995. The information collection was previously published in the **Federal Register** on May 13, 2008, at 73 FR 27548 allowing for a 60-day public comment period. USCIS did not receive any comments for this information collection.

The purpose of this notice is to allow an additional 30 days for public comments. Comments are encouraged and will be accepted until August 29, 2008. This process is conducted in accordance with 5 CFR 1320.10.

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), and to the Office of Information and Regulatory Affairs, Office of Management and Budget (OMB), USCIS Desk Officer. Comments may be submitted to: USCIS, Chief, Regulatory Management Division, Clearance Office, 111 Massachusetts Avenue, 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, and to the OMB USCIS Desk Officer via facsimile to 202-395-6974 or via e-mail at oir_submission@omb.eop.gov.

When submitting comments by e-mail please make sure to add OMB Control Number 1615-0069 in the subject box. Written comments and suggestions from the public and affected agencies should address one or more of the following four points:

- (1) Evaluate whether the 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 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 respond, including 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 a currently approved information collection.

(2) *Title of the Form/Collection:* Application by Refugee for Waiver of Grounds of Excludability.

(3) *Agency form number, if any, and the applicable component of the Department of Homeland Security sponsoring the collection:* Form I-602. U.S. Citizenship and Immigration Services.

(4) *Affected public who will be asked or required to respond, as well as a brief abstract:* *Primary:* Individuals and households. This form is necessary to establish eligibility for waiver of excludability based on humanitarian, family unity, or public interest.

(5) *An estimate of the total number of respondents and the amount of time estimated for an average respondent to respond:* 2,500 responses at 15 minutes (.25) per response.

(6) *An estimate of the total public burden (in hours) associated with the collection:* 625 annual burden hours.

If you have additional comments, suggestions, or need a copy of the proposed information collection instrument with instructions, or additional information, please visit the

USCIS Web site at: <http://www.regulations.gov/search/index.jsp>.

If additional information is required contact: USCIS, Regulatory Management Division, 111 Massachusetts Avenue, Suite 3008, Washington, DC 20529, (202) 272-8377.

Dated: July 22, 2008.

Stephen Tarragon,

Management Analyst, Regulatory Management Division, U.S. Citizenship and Immigration Services, Department of Homeland Security.

[FR Doc. E8-17433 Filed 7-29-08; 8:45 am]

BILLING CODE 9111-97-P

DEPARTMENT OF HOMELAND SECURITY

U.S. Citizenship and Immigration Services

Agency Information Collection Activities: Form I-914, Extension of a Currently Approved 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) 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 September 29, 2008.

Written comments and suggestions regarding items contained in this notice, and especially with regard to the estimated public burden and associated response time, should be directed to the Department of Homeland Security (DHS), USCIS, Chief, Regulatory Management Division, Clearance Office, 111 Massachusetts Avenue, NW., 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. When submitting comments by e-mail, please add the OMB Control Number 1615-0099 in the subject box.

During this 60-day period, USCIS will be evaluating whether to revise the Form I-914. Should USCIS decide to