agreements without ACHP involvement. Execution of an agreement pursuant to the prototype PA presumes that DOE will conduct its government-to-government consultation responsibilities with federal recognized Indian tribes and its Section 106 consultation requirements with Native Hawaiian organizations. If DOE is notified that a particular undertaking may result in an adverse effect on historic properties of religious and cultural significance to Indian tribes or Native Hawaiian organizations, DOE must invite such Indian tribes or Native Hawaiian organizations to participate in consultation for the affected project.

Since its designation, DOE has used the prototype PA to successfully negotiate and execute 44 programmatic agreements with SHPOs and state agencies receiving DOE OWIP grants. DOE’s direct recipients may use the executed state agreement developed under the prototype PA as well. The ACHP provided guidance and technical assistance to DOE Project Officers and SHPOs during the negotiation and subsequent implementation of the agreements, for example, assisting in the determination of appropriate treatments and mitigation for individual projects that resulted in adverse effects.

In the past year, DOE and the ACHP have discussed how to extend and build upon the program established by the prototype PA. As part of this effort, the ACHP, with DOE’s participation, hosted a series of listening sessions for SHPOs. The ACHP will also provide an opportunity for SHPOs, tribes, Native Hawaiian organizations, and state agencies an opportunity to comment. The 44 agreements executed under the prototype PA have different expiration dates. Several of the agreements will expire in mid-March 2013. While the prototype PA originally proposed a three year duration clause for these agreements, it is now DOE’s and the ACHP’s intention that these agreements should extend beyond this three year term.

This Program Comment proposes to extend the duration of the existing 44 agreements executed under the prototype PA until December 31, 2020, and provide the same duration period for any future agreements that may be executed under the prototype PA. Nothing in this Program Comment would alter or modify any other provisions of the prototype PA or the 44 agreements, including the ability of the parties to amend or terminate an executed agreement prior to the expiration date.

II. Expected Benefits

As a result of the partnership with ACHP and the development and the administration of the prototype PA, DOE established internal and external training; recognized best management practices; and utilized DOE guidance and directives to ensure that the DOE weatherization programs were properly implemented in compliance with Section 106. The prototype PA established review efficiencies and protocols which allowed for the grant programs to expedite the weatherization efforts of the homes of many low income individuals across the country, as well as assisted communities in funding energy efficiency, renewable energy, and weatherization projects for public buildings such as schools and courthouses. Due to the success of the prototype PA for DOE’s weatherization programs, other departments within DOE have sought ACHP’s and OWIP staff's guidance and direction for meeting their historic preservation compliance responsibilities.

The proposed Program Comment would build upon and extend the success of the prototype PA and continue the DOE’s program of tailored, efficient compliance with Section 106. Once the public comments resulting from this notice are considered, and edits are incorporated as deemed appropriate, the ACHP will decide whether to issue the Program Comment. The ACHP expects to make that decision in mid-March 2013.

III. Text of the Proposed Program Comment

The following is the text of the proposed Program Comment:

I. Establishment and Authority

This Program Comment was issued by the ACHP on March 2013 pursuant to 36 CFR 800.14(e).

II. Date of Effect

This Program Comment went into effect on March 2013.

III. Use of this Program Comment to Extend the Duration of the Existing Agreements Executed under the DOE Prototype PA and for New Agreements Executed pursuant to the Prototype PA

The DOE may continue, through December 31, 2020, complying with its responsibilities under Section 106 of the National Historic Preservation Act for its Weatherization Assistance Program (WAP), State Energy Program (SEP), and Energy Efficiency and Conservation Block Grant (EEC BG) in the relevant States using the 44 agreements currently executed, and those to be executed, under the “Prototype Programmatic Agreement between the United States Department of Energy, the State Energy Office and the State Historic Preservation Office regarding EECBG, SEP and WAP Undertakings,” designated by the ACHP on February 8, 2010, regardless of the duration clause of those agreements. However, if any of those agreements gets terminated under its own terms, DOE may no longer use it to comply with its Section 106 responsibilities in the relevant State. This will provide continuity in the Section 106 review for those undertakings covered by the existing and any new agreements executed under the prototype PA. This Program Comment does not alter or modify any provisions of the prototype PA or the 44 executed agreements other than their duration clauses.

IV. Amendment

The ACHP may amend this Program Comment after consulting with DOE, NCSHPO, and other parties as appropriate, and publishing notice in the Federal Register to that effect.

V. Sunset Clause

This Program Comment will terminate on December 31, 2020, unless it is amended to extend the period in which it is in effect.

VI. Termination

The ACHP may terminate this Program Comment by publication of a notice in the Federal Register thirty (30) days before the termination takes effect.

Authority: 36 CFR 800.14(e).


John M. Fowler,
Executive Director.

[FR Doc. 2013–04138 Filed 2–21–13; 8:45 am]
BILLING CODE 4310–K6–P

DEPARTMENT OF HOMELAND SECURITY

Office of the Secretary

Published Privacy Impact Assessments on the Web

AGENCY: Privacy Office, DHS.

ACTION: Notice of Publication of Privacy Impact Assessments.

SUMMARY: The Department of Homeland Security (DHS) Privacy Office is making available thirty-eight Privacy Impact Assessments (PIA) on various programs and systems in the Department. These assessments were approved and published on the Privacy Office’s Web
enforcement or security risk, and aids in the enforcement of customs and immigration laws, and other laws enforced by DHS at the border. AFI is used for the purposes of: (1) Identifying individuals, associations, or relationships that may pose a potential law enforcement or security risk, targeting cargo that may present a threat, and assisting intelligence product users in the field in preventing the illegal entry of people and goods, or identifying other violations of law; (2) conducting additional research on persons and/or cargo to understand whether there are patterns or trends that could assist in the identification of potential law enforcement or security risks; and (3) sharing finished intelligence products developed in connection with the above purposes with DHS employees who have a need to know in the performance of their official duties and who have appropriate clearances or permissions. Finished intelligence products are tactical, operational, and strategic law enforcement intelligence products that have been reviewed and approved for sharing with finished intelligence product users and authorities outside of DHS, pursuant to routine uses in the published Privacy Act System of Records Notice.

In order to mitigate privacy and security risks associated with the deployment of AFI, CBP has built technical safeguards into AFI and developed a governance process that includes the operational components of CBP, the oversight functions of the CBP Privacy Officer and Office of Chief Counsel, and the Office of Information and Technology. Additionally, the DHS Privacy Office provides oversight for the program.

This PIA was necessary because AFI accesses and stores PII retrieved from DHS, other federal agency, and commercially available databases. System: DHS/FEMA/PIA–027 Hazard Mitigation Grant Program (HMGP) System. Component: FEMA. Date of approval: June 29, 2012.

FEMA, Office of the Chief Financial Officer, Debt Establishment Unit, owns and operates the HMGP program. The HMGP awards grants to state and local governments to fund emergency management and mitigation projects that reduce the impact of future disasters on communities. The HMGP system is responsible for processing HMGP grant applications and ensuring that the funds are used in accordance with the terms and conditions of the grant agreement. The system also monitors the progress of the projects and ensures that the funds are used effectively and efficiently.

This PIA was necessary because the HMGP system collects, uses, maintains, retrieves, and disseminates PII, including application data, project data, and financial data. This PIA was conducted to notify the public about the purposes for which the HMGP system collects, uses, maintains, retrieves, and disseminates PII, and to provide information on how to contact the DHS Privacy Officer for further information.

System: DHS/FEMA/PIA–027 Hazard Mitigation Grant Program (HMGP) System. Component: FEMA.
investigations and prosecutions of these crimes. This expanded sharing is intended to allow law enforcement personnel to use these images during investigations to identify and rescue child victims as well as to identify and prosecute the perpetrators of these crimes. HSI is also expanding the range of images shared with law enforcement agencies that have requested a matching report of an image submitted for NCVIS comparison. The PIA for NCVIS was originally published on August 21, 2009. Because HSI is expanding the scope of NCVIS information that is shared with authorized partners, an update to the NCVIS PIA was required.

**System:** DHS/PPD/PIA–021(a) Joint Cybersecurity Services Program Defense Industrial Base (DIB)—Enhanced Cybersecurity Services (DECS).

**Component:** National Protection and Programs Directorate (NPPD).

**Date of approval:** July 18, 2012.

The Joint Cybersecurity Services Pilot (JCSSP) is the Department of Defense’s Internal Cybersecurity Services Program Defense Industrial Base (DIB) program. The purpose of this program is to enhance the cybersecurity of participating critical infrastructure entities through information sharing initiatives and partnerships with the critical infrastructure organization or their Commercial Service Provider (CSP). This update is intended to allow law enforcement personnel to use these images during investigations to identify and rescue child victims as well as to identify and prosecute the perpetrators of these crimes. HSI is also expanding the range of images shared with law enforcement agencies that have requested a matching report of an image submitted for NCVIS comparison. The PIA for NCVIS was originally published on August 21, 2009. Because HSI is expanding the scope of NCVIS information that is shared with authorized partners, an update to the NCVIS PIA was required.

**System:** DHS/PPD/PIA–021(a) Joint Cybersecurity Services Program Defense Industrial Base (DIB)—Enhanced Cybersecurity Services (DECS).

**Component:** National Protection and Programs Directorate (NPPD).

**Date of approval:** July 18, 2012.

The Joint Cybersecurity Services Pilot (JCSSP) is the Department of Defense’s Internal Cybersecurity Services Program Defense Industrial Base (DIB) program. The purpose of this program is to enhance the cybersecurity of participating critical infrastructure entities through information sharing initiatives and partnerships with the critical infrastructure organization or their Commercial Service Provider (CSP). This update is intended to allow law enforcement personnel to use these images during investigations to identify and rescue child victims as well as to identify and prosecute the perpetrators of these crimes. HSI is also expanding the range of images shared with law enforcement agencies that have requested a matching report of an image submitted for NCVIS comparison. The PIA for NCVIS was originally published on August 21, 2009. Because HSI is expanding the scope of NCVIS information that is shared with authorized partners, an update to the NCVIS PIA was required.

**System:** DHS/PPD/PIA–021(a) Joint Cybersecurity Services Program Defense Industrial Base (DIB)—Enhanced Cybersecurity Services (DECS).

**Component:** National Protection and Programs Directorate (NPPD).

**Date of approval:** July 18, 2012.

The Joint Cybersecurity Services Pilot (JCSSP) is the Department of Defense’s Internal Cybersecurity Services Program Defense Industrial Base (DIB) program. The purpose of this program is to enhance the cybersecurity of participating critical infrastructure entities through information sharing initiatives and partnerships with the critical infrastructure organization or their Commercial Service Provider (CSP). This update is intended to allow law enforcement personnel to use these images during investigations to identify and rescue child victims as well as to identify and prosecute the perpetrators of these crimes. HSI is also expanding the range of images shared with law enforcement agencies that have requested a matching report of an image submitted for NCVIS comparison. The PIA for NCVIS was originally published on August 21, 2009. Because HSI is expanding the scope of NCVIS information that is shared with authorized partners, an update to the NCVIS PIA was required.

**System:** DHS/PPD/PIA–021(a) Joint Cybersecurity Services Program Defense Industrial Base (DIB)—Enhanced Cybersecurity Services (DECS).

**Component:** National Protection and Programs Directorate (NPPD).

**Date of approval:** July 18, 2012.

The Joint Cybersecurity Services Pilot (JCSSP) is the Department of Defense’s Internal Cybersecurity Services Program Defense Industrial Base (DIB) program. The purpose of this program is to enhance the cybersecurity of participating critical infrastructure entities through information sharing initiatives and partnerships with the critical infrastructure organization or their Commercial Service Provider (CSP). This update is intended to allow law enforcement personnel to use these images during investigations to identify and rescue child victims as well as to identify and prosecute the perpetrators of these crimes. HSI is also expanding the range of images shared with law enforcement agencies that have requested a matching report of an image submitted for NCVIS comparison. The PIA for NCVIS was originally published on August 21, 2009. Because HSI is expanding the scope of NCVIS information that is shared with authorized partners, an update to the NCVIS PIA was required.

**System:** DHS/PPD/PIA–021(a) Joint Cybersecurity Services Program Defense Industrial Base (DIB)—Enhanced Cybersecurity Services (DECS).

**Component:** National Protection and Programs Directorate (NPPD).

**Date of approval:** July 18, 2012.

The Joint Cybersecurity Services Pilot (JCSSP) is the Department of Defense’s Internal Cybersecurity Services Program Defense Industrial Base (DIB) program. The purpose of this program is to enhance the cybersecurity of participating critical infrastructure entities through information sharing initiatives and partnerships with the critical infrastructure organization or their Commercial Service Provider (CSP). This update is intended to allow law enforcement personnel to use these images during investigations to identify and rescue child victims as well as to identify and prosecute the perpetrators of these crimes. HSI is also expanding the range of images shared with law enforcement agencies that have requested a matching report of an image submitted for NCVIS comparison. The PIA for NCVIS was originally published on August 21, 2009. Because HSI is expanding the scope of NCVIS information that is shared with authorized partners, an update to the NCVIS PIA was required.

**System:** DHS/PPD/PIA–021(a) Joint Cybersecurity Services Program Defense Industrial Base (DIB)—Enhanced Cybersecurity Services (DECS).

**Component:** National Protection and Programs Directorate (NPPD).

**Date of approval:** July 18, 2012.

The Joint Cybersecurity Services Pilot (JCSSP) is the Department of Defense’s Internal Cybersecurity Services Program Defense Industrial Base (DIB) program. The purpose of this program is to enhance the cybersecurity of participating critical infrastructure entities through information sharing initiatives and partnerships with the critical infrastructure organization or their Commercial Service Provider (CSP). This update is intended to allow law enforcement personnel to use these images during investigations to identify and rescue child victims as well as to identify and prosecute the perpetrators of these crimes. HSI is also expanding the range of images shared with law enforcement agencies that have requested a matching report of an image submitted for NCVIS comparison. The PIA for NCVIS was originally published on August 21, 2009. Because HSI is expanding the scope of NCVIS information that is shared with authorized partners, an update to the NCVIS PIA was required.

**System:** DHS/PPD/PIA–021(a) Joint Cybersecurity Services Program Defense Industrial Base (DIB)—Enhanced Cybersecurity Services (DECS).

**Component:** National Protection and Programs Directorate (NPPD).

**Date of approval:** July 18, 2012.

The Joint Cybersecurity Services Pilot (JCSSP) is the Department of Defense’s Internal Cybersecurity Services Program Defense Industrial Base (DIB) program. The purpose of this program is to enhance the cybersecurity of participating critical infrastructure entities through information sharing initiatives and partnerships with the critical infrastructure organization or their Commercial Service Provider (CSP). This update is intended to allow law enforcement personnel to use these images during investigations to identify and rescue child victims as well as to identify and prosecute the perpetrators of these crimes. HSI is also expanding the range of images shared with law enforcement agencies that have requested a matching report of an image submitted for NCVIS comparison. The PIA for NCVIS was originally published on August 21, 2009. Because HSI is expanding the scope of NCVIS information that is shared with authorized partners, an update to the NCVIS PIA was required.
operational environments, iris scans can be captured more quickly than fingerprints, are as or more reliable in providing a unique biometric, do not involve the touching of the subject with respect to those cultures for whom such contact poses a concern, and require less storage capacity and transmission bandwidth than fingerprints. This PIA was conducted because E3 requires the collection of PII.

**System:** DHS/ICE/PIA–015(e) Enforcement Integrated Database (EID)— EAGLE

**Component:** ICE

**Date of approval:** July 25, 2012.

ICE has established a new subsystem within EID called EID Arrest Guide for Law Enforcement (EAGLE). EAGLE is a booking application used by ICE law enforcement officers to process the biometric and biographic information of individuals arrested by ICE for criminal violations of law and administrative violations of the Immigration and Nationality Act. Once fully deployed, EAGLE will replace the existing EID booking applications, the Enforcement Preemption and Booking Module, Mobile IDENT, and WebIDENT, and will perform the identical functions of those applications as described below and in the EID PIA. EAGLE will also forge a new connection to the Department of Defense’s (DOD) Automated Biographic Information System (ABIS) and permit the comparison of the fingerprints of foreign nationals arrested by ICE with the DOD’s information in ABIS. This PIA update was conducted to provide public notice of the operation of the EAGLE booking system and its interconnection to the DOD ABIS database.

**System:** DHS/OPS/PIA–008 Homeland Security Information Network R3 User Accounts (HSIN)

**Component:** Operations Coordination and Planning (OPS)

**Date of approval:** July 25, 2012.

HSIN is maintained by the Department of Homeland Security, OPS. HSIN is designed to facilitate the secure integration and interoperability of information-sharing resources among federal, state, local, tribal, private-sector commercial, and other non-governmental stakeholders involved in identifying and preventing terrorism as well as in undertaking incident management activities. HSIN is a user-driven, web-based, information-sharing platform that connects all homeland security mission partners within a wide spectrum of homeland security mission areas. OPS conducted this PIA because the substantive material posted and shared within the HSIN collaboration contains PII about members of the public who are the subject of documents, records, or bulletins contained in those spaces.

**System:** DHS/NPPD/PIA–009 Chemical Facility Anti-Terrorism Standards (CFATS)

**Component:** NPPD

**Date of approval:** July 26, 2012.

NPPD consolidated and updated this PIA for the CFATS regulations, 6 CFR Part 27. This PIA replaced the former PIAs for the Chemical Security Assessment Tool and CFATS, in order to provide a unified analysis of the collection and use of PII as part of CFATS. CFATS is the DHS regulation that governs security at high-risk chemical facilities and represents a national-level effort to minimize terrorism risk to such facilities.

**System:** DHS/USCIS/PIA–006(a) Systematic Alien Verification for Entitlements (SAVE)

**Component:** U.S. Citizenship and Immigration Services (USCIS)

**Date of approval:** July 27, 2012.

USCIS’s Verification Division published an update to the SAVE Program PIA dated August 26, 2011. SAVE is a fee-based, inter-governmental initiative designed to help federal, state, tribal, and local government agencies confirm immigration status prior to the granting of benefits and licenses, as well as for other lawful purposes. USCIS updated this PIA to: (1) Describe the new collection of foreign passport country of issuance from agencies issuing benefits and from the United States Visitor and Immigrant Status Indicator Technology program’s Arrival and Departure Information System, and (2) describe the addition of Enterprise Citizenship and Immigration Services Centralized Operational Repository.
TSA currently conducts security threat assessments (STA) on individuals and companies that seek access to SSI necessary to prepare a proposal in the pre-contract award phase of contracting with TSA. SSI is a form of unclassified information that if publicly released would be detrimental to transportation security. The standards governing SSI are promulgated under 49 U.S.C. 114(r) in 49 CFR, part 1520. There may, however, also be circumstances under which individuals and companies will require access to SSI in order to prepare a proposal for contracts with other governmental agencies (federal, state, or local level) or with private industry. TSA updated this PIA to reflect that TSA will perform STA on individuals and companies seeking access to SSI in order to prepare a proposal with such other entities.

System: DHS/OPS/PIA–009 National Operations Center Operations Counterterrorism Desk (NCOD) Database. Component: OPS. Date of approval: July 30, 2012. The National Operations Center (NOC), within OPS, operates the NOC Counterterrorism Operations Desk (NCOD) and serves as the primary Department of Homeland Security point of contact to streamline counterterrorism Requests for Information (RFI). The NCOD Database is a tracking tool used by NCOD Officers to track all counterterrorism related incoming and outgoing inquiries. OPS conducted this PIA because the NCOD Database contains PII.

System: DHS/NPPD/PIA–026 National Cybersecurity Protection System (NCPS). Component: NPPD. Date of approval: July 30, 2012. NCPS is an integrated system for intrusion detection, analysis, intrusion prevention, and information sharing capabilities that are used to defend the federal civilian government agencies’ information technology infrastructure from cyber threats. The NCPS includes the hardware, software, supporting processes, training, and services that are developed and acquired to support its mission. NPPD conducted this PIA because PII may be collected by the NCPS, or through submissions of known or suspected cyber threats received by US–CERT for analysis. This PIA will serve as a replacement for previously published PIAs submitted by NSCD for the 24/7 Incident Handling Center (March 29, 2007), and the Malware Lab Network (May 4, 2010), and is a program–wide PIA to better characterize the efforts of NCPS and US–CERT.

System: DHS/USCIS/PIA–044 Fraud Detection and National Security Directorate (FDNS). Component: USCIS. Date of approval: July 30, 2012. USCIS created the FDNS to strengthen the integrity of the nation’s immigration system and to ensure that immigration benefits are not granted to individuals that may pose a threat to national security and/or public safety. In addition, the FDNS is responsible for detecting, deterring, and combating immigration benefit fraud. USCIS conducted this PIA to document and assess how the FDNS collects, uses, and maintains PII.

System: DHS/USCIS/PIA–045 Deferred Action for Childhood Arrivals. Component: USCIS. Date of approval: August 14, 2012. On June 15, 2012, Secretary of Homeland Security Janet Napolitano (the Secretary) issued a DHS memorandum entitled, “Exercising Prosecutorial Discretion with Respect to Individuals Who Came to the United States as Children.” The Secretary addressed the memorandum to the Acting Commissioner of U.S. Customs and Border Protection, and to the Directors of USCIS and U.S. Immigration and Customs Enforcement. The Secretary’s memorandum set forth how prosecutorial discretion may be exercised in cases involving certain people who arrived in the United States as children. The Secretary emphasized that generally, this population lacked the intent to violate the law, and that her memorandum would ensure enforcement resources would not be expended on these low priority cases.

The basis for the Secretary’s memorandum is the Secretary’s authority to exercise prosecutorial discretion by deferring action in appropriate cases. Prosecutorial discretion is the authority to determine how and when to exercise enforcement authority in line with agency priorities. Deferred action is an exercise of this prosecutorial discretion to defer removal action against certain individuals who are unlawfully present in the United States in order to devote scarce enforcement resources to the highest priority removal cases, including individuals who pose a danger to national security or public safety or have been convicted of specific crimes. USCIS published this PIA because the deferred action for childhood arrivals process associated with this memorandum involves the collection and use of PII.


System: DHS/S&T/PIA–001(a) Border Network (BorderNet) and Northeast Test Bed (NET–B). Component: S&T. Date of approval: August 23, 2012. BorderNet (formerly named the Border and Transportation Security Network, or BTSNet) is a technology test bed developed and maintained by the Department of Homeland Security (DHS), Science and Technology Directorate (S&T) located at the United States-Mexico border. The purpose of the test bed is to test and evaluate technologies in an operational environment that assist DHS Customs and Border Protection field agents in securing our nation’s borders. S&T updated this PIA to reflect the addition of mobile enrollment technology and surveillance cameras, and the deployment of an additional test bed site at the United States-Canada border, called NET–B.

System: DHS/S&T/PIA–024 Rapid Deoxyribonucleic Acid (DNA) System. Component: S&T. Date of approval: September 14, 2012. S&T developed the Rapid DNA System primarily to meet the need of U.S. Citizenship and Immigration Services (USCIS) to verify family relationships in refugee immigration processes. The Rapid DNA System performs rapid, low-cost DNA analysis to meet this USCIS need and may also address operational needs of other DHS components. S&T conducted this PIA because the collection and analysis of DNA information raises potential privacy concerns.

System: DHS/TSA/PIA–038 Performance and Results Information System (PARIS). Component: TSA. Date of approval: September 18, 2012. TSA PARIS system is a database used for maintaining information associated with TSA’s regulatory investigations, security incidents, and enforcement actions, as well as for recording the
details of security incidents involving passenger and property screening.

PARIS maintains PII about individuals, including witnesses, involved in security incidents or regulatory enforcement activities. PARIS also creates and maintains a list of individuals who, based upon their involvement in security incidents of sufficient severity or frequency, are disqualified from receiving expedited screening for some period of time or permanently. The purpose of this PIA is to inform the public of changes in the use of PARIS and any resulting impact to personal privacy.

System: DHS/CBP/PIA–004(f)
Western Hemisphere Travel Initiative (WHTI).
Component: CBP.
Date of approval: September 24, 2012.
CBP published this PIA to give notice of an update to the WHTI PIA. This update describes Phase I of the Beyond the Border entry/exit program, which is an initiative of the U.S.-Canada Beyond the Border Action Plan. The Beyond the Border entry/exit program will expand the sharing of border crossing information with the Canada Border Services Agency by exchanging biographic, travel document, and other border crossing information collected from individuals entering the United States from Canada and vice versa at land ports of entry. This exchange of border crossing entry information will assist both countries so that the record of an entry into one country establishes an exit record from the other, ultimately supporting both nation in their immigration and law enforcement missions, as well as facilitating cross-border travel. This PIA update covered Phase I of the entry/exit program only, which is limited to exchanging entry records from certain individuals (other than U.S. and Canadian citizens) at certain land ports of entry to measure the ability to reconcile biographic entry records between Canada and the United States. DHS will publish additional updates to this PIA in advance of deployment of any subsequent phases to the Beyond the Border entry/exit program.

Component: National Protection and Programs Directorate (NPPD).
Date of review: October 4, 2012.
This PIA was reviewed using the three-year PIA checklist. U.S. Immigration and Customs Enforcement (ICE), Federal Protective Service (FPS), Information Support Tracking System (FISTS), Contract Suitability Module is a web-based application used to automate the process for assessing the suitability of FPS and General Services Administration contract personnel to work in secure Federal buildings, and to track periodic background re-investigations of those contract employees. The system collects and maintains information on applicants and contractor personnel who work in secure Federal buildings such as security officers, childcare workers, cleaners, and other contracted service positions. FPS conducted this PIA because FISTS collects and uses PII on members of the public who seek or are currently employed in these positions within Federal facilities.

Component: FEMA.
Date of approval: October 12, 2012.
DHS FEMA FIMA National Flood Insurance Program (NFIP) owns and operates the NFIP Information Technology System (ITS). The NFIP ITS processes flood insurance policies and claims, specifically, policies and claims from the FEMA Direct Servicing Agent (DSA) contractor on behalf of the NFIP and by Write Your Own Companies (WYO) that sell and service flood insurance policies. An NFIP flood insurance policy can be obtained directly from a DSA through a licensed insurance broker or from WYOs. Since 1983, participating insurance companies have delivered and serviced NFIP policies in their own names, through the "Write Your Own" arrangement. The policy coverage and premiums do not differ if purchased from the DSA or WYOs. FEMA conducted this PIA because NFIP ITS collects, uses, maintains, retrieves, and disseminates PII about individuals who purchase, as well as those who process, flood insurance policies from NFIP and individuals requesting access to the system.

Component: TSA.
Date of approval: November 13, 2012.
TSA will conduct terrorism watch list checks of workers at PANYNJ facilities and job sites, including critical infrastructure such as airports, marine ports, bus terminals, rail transit facilities, bridges, tunnels, and real estate such as the World Trade Center memorial site. TSA will also conduct terrorism watch list checks of individuals identified by PANYNJ as requiring checks for access to sensitive information, and for workers at facilities and job sites of PANYNJ regional partners. Results of the checks will not be reported to PANYNJ, but instead will be forwarded to the Federal Bureau of Investigation Terrorist Screening Center. This PIA was conducted pursuant to the E-Government Act of 2002 because PII will be collected to conduct terrorism watch list checks of workers at PANYNJ facilities and job sites.

System: DHS/TSA/PIA–039 Trends and Patterns Branch (TPB).
Component: TSA.
Date of approval: November 13, 2012.
TSA, Trends and Patterns Branch (TPB) seeks to improve the ability to identify potential risks to transportation security by discovering and analyzing previously unknown links or patterns among individuals who undergo a TSA security threat assessment, aviation passengers identified as a match to a watch list, and passengers who do not present acceptable identification documents to access the sterile area of an airport whose identity is unverified. TSA conducted this PIA because the TPB will collect and use PII to perform these functions.

System: DHS/FEMA/PIA–012(a) Disaster Assistance Improvement Program (DAIP).
Component: FEMA.
Date of approval: November 16, 2012.
FEMA, Office of Response & Recovery, Recovery Directorate, National Processing Service Center Operations Branch, sponsors and funds the DAIP. In accordance with Executive Order 13411 “Improving Assistance for Disaster Victims,” DAIP developed the Disaster Assistance Center (DAC) system. As a part of DAIP, DAC maintains disaster survivor application and registration information collected through various media including: (1) DAIP paper forms, (2) the www.disasterassistance.gov Web site, (3) the http://m.fema.gov mobile Web site, and (4) via telephone. DAIP/DAC shares the information with the National Emergency Management Information System– Individual Assistance (IA) module to facilitate eligibility determinations and with other federal, tribal, state, local, and non-profit agencies/organizations that also service disaster survivors. FEMA conducted this PIA because DAIP/DAC collects, uses, maintains, retrieves, and disseminates PII of disaster survivors who either request IA benefits from FEMA or whom FEMA may refer to its partners.

Component: S&T.
Date of approval: November 16, 2012.
SkT and the State of Oklahoma are partnering on the RAPS project to test and evaluate Small Unmanned Aircraft Systems (SUAS) for potential use by the first responder community and DHS operational components. SUAS include small aircraft (typically under 55 pounds and having wingspans of 3–6 feet or less) that are operated using a wireless ground control station. The aircraft are equipped with sensors and cameras that can capture images and transmit them to a ground control system to provide aerial views of emergency situations and situational awareness. SkT conducted a PIA to address the privacy impact of the system’s surveillance and image capturing capabilities.

System: DHS/USCG/PIA–001(b) Homeport Internet Portal.

Component: USCG.

Date of approval: November 16, 2012.

USCG currently uses the Homeport Internet Portal to provide secure information dissemination, advanced collaboration for Area Maritime Security Committees, electronic submission and approval for facility security plans, and complex electronic notification capabilities. Homeport includes a subsystem called the Alert Warning System (AWS), which provides USCG Headquarters, Districts, Sectors, and other units an enterprise solution for sending alerts and warnings to maritime security (MARSEC) partners, stakeholders, and appropriate port constituents for MARSEC level changes and other MARSEC-related activities requiring port-wide notifications. Through a Memorandum of Agreement between the USCG and the Transportation Security Administration (TSA), use of AWS capabilities will be shared between these two DHS components, thereby leveraging DHS investment in the system and avoiding duplicative operations and maintenance costs within DHS. The USCG issued this PIA update to include TSA operations center personnel as authorized users of Homeport’s AWS, which contains non-sensitive PII and disseminates airport security information to authorized recipients.


Component: ICE.

Date of approval: November 27, 2012.

ICE maintains medical records on aliens that ICE detains for violations of U.S. immigration law. Aliens held in ICE custody in a facility staffed by the ICE Health Services Corps, a division of ICE’s Office of Enforcement and Removal Operations, receive physical exams and treatment, dental services, and pharmacy services, depending on the alien’s medical conditions and length of stay. To properly record the medical assessments and services, ICE operates the following information technology systems that maintain electronic medical record information: CaseTrakker, MedeZ, Dental X-Ray System, the Criminal Institution Pharmacy System, the Medical Payment Authorization Request Web System (MedPAR), and the Medical Classification Database. This PIA was originally published on July 25, 2011, and described the information in these medical record systems, the purposes for which this information was collected and used, and the safeguards ICE had implemented to mitigate the privacy and security risks to PII stored in these systems. The PIA was republished in full primarily to modify the description of the MedPAR system, which originally was to be hosted by the U.S. Department of Veterans Affairs, but now remains at ICE.


Jonathan R. Cantor,
Acting Chief Privacy Officer, Department of Homeland Security.

[FR Doc. 2013–04109 Filed 2–21–13; 8:45 am]
BILLING CODE 9110–9L–P

DEPARTMENT OF HOUSING AND URBAN DEVELOPMENT

[Docket No. FR–5687–N–04]

Notice of Proposed Information Collection: Comment Request; Funds Authorization

AGENCY: Office of the Assistant Secretary for Housing, HUD.

ACTION: Notice.

SUMMARY: The proposed information collection requirement described below will be submitted to the Office of Management and Budget (OMB) for review, as required by the Paperwork Reduction Act. The Department is soliciting public comments on the subject proposal.

DATES: Comments Due Date: April 23, 2013.

ADDRESSES: Interested persons are invited to submit comments regarding this proposal. Comments should refer to the proposal by name and/or OMB Control Number and should be sent to: Reports Liaison Officer, Department of Housing and Urban Development, 451 7th Street SW., Washington, DC 20410, Room 9120 or the number for the Federal Information Relay Service (1–800–877–8339).

FOR FURTHER INFORMATION CONTACT: Program Contact, Harry Messner, The Office of Asset Management, Department of Housing and Urban Development, 451 7th Street SW., Washington, DC 20410, telephone (202) 402–2626 (this is not a toll free number) for copies of the proposed forms and other available information.

SUPPLEMENTARY INFORMATION: The Department is submitting the proposed information collection to OMB for review, as required by the Paperwork Reduction Act of 1995 (44 U.S.C. chapter 35, as amended).

This Notice is soliciting comments from members of the public and affected agencies concerning the proposed collection of information to: (1) Evaluate whether the proposed collection is necessary for the proper performance of the functions of the agency, including whether the information will have practical utility; (2) Evaluate the accuracy of the agency’s estimate of the burden of the proposed collection of information; (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 the use of appropriate automated collection techniques or other forms of information technology, e.g., permitting electronic submission of responses.

This Notice also lists the following information:

Title of Proposal: Funds Authorization.

OMB Control Number, if applicable: 2502–0555.

Description of the need for the information and proposed use: the purpose of this information collection is to ensure that advances from the Reserve for Replacement and/or Residual Receipts Funds are reviewed and authorized by HUD in accordance with regulatory and administrative guidelines.

Agency form numbers, if applicable: form HUD–9250.

Estimation of the total numbers of hours needed to prepare the information collection including number of respondents, frequency of response, and hours of response: The number of burden hours is 20,595. The number of respondents is 9,153, the number of responses is 9,153, the frequency of response is on occasion, and the burden hour per response is 30 minutes.

Status of the proposed information collection: This is an extension of a previously approved collection.