Officer in consultation with counsel, when there exists a legitimate public interest in the disclosure of the information or when disclosure is necessary to preserve confidence in the integrity of DHS or is necessary to demonstrate the accountability of DHS's officers, employees, or individuals covered by the system, except to the extent it is determined that release of the specific information in the context of a particular case would constitute an unwarranted invasion of personal privacy.

DISCLOSURE TO CONSUMER REPORTING AGENCIES:

None.

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

STORAGE:

Records in this system are stored electronically or on paper in secure facilities in a locked drawer behind a locked door. The records are stored on magnetic disc, tape, digital media, and CD–ROM.

RETRIEVABILITY:

Records may be retrieved by an individual's name, social security number, or unique user ID.

SAFEGUARDS:

Records in this system are safeguarded in accordance with applicable rules and policies, including all applicable DHS automated systems security and access policies. Strict controls have been imposed to minimize the risk of compromising the information that is being stored. Access to the computer system containing the records in this system is limited to those individuals who have a need to know the information for the performance of their official duties and who have appropriate clearances or permissions.

RETENTION AND DISPOSAL:

FEMA's training and exercise records retention is generally covered under General Records Schedule (GRS) 1A–29a, 1–29a(2), and 1–29b; NARA Authority N1–311–08–2 1a, and NARA Authority N1–311–88–2 2. Under GRS 1, records are maintained for up to five years after the cutoff date and then destroyed. Under NARA Authority N1–311–08–2 1a, records are retired to the Federal Records Center (FRC) five years after the cutoff and destroyed after forty years. Under NARA Authority N1–311–88–2 2, records are maintained for six years and three months after the cutoff and then destroyed.

SYSTEM MANAGER AND ADDRESS:

Privacy Officer, Federal Emergency Management Agency, Department of Homeland Security, Washington, DC 20478.

NOTIFICATION PROCEDURE:

Individuals seeking notification of and access to any record contained in this system of records, or seeking to contest its content, may submit a request in writing to the FEMA FOIA Officer, whose contact information can be found at *http://www.dhs.gov/foia* under "contacts." If an individual believes more than one component maintains Privacy Act records concerning him or her the individual may submit the request to the Chief Privacy Officer and Chief Freedom of Information Act Officer, Department of Homeland Security, 245 Murray Drive, SW., Building 410, STOP–0655, Washington, DC 20528.

When seeking records about yourself from this system of records or any other Departmental system of records your request must conform with the Privacy Act regulations set forth in 6 CFR part 5. You must first verify your identity, meaning that you must provide your full name, current address and date and place of birth. You must sign your request, and your signature must either be notarized or submitted under 28 U.S.C. 1746, a law that permits statements to be made under penalty of perjury as a substitute for notarization. While no specific form is required, you may obtain forms for this purpose from the Chief Privacy Officer and Chief Freedom of Information Act Officer, *http://www.dhs.gov* or 1–866–431–0486. In addition you should provide the following:

- An explanation of why you believe the Department would have information on you;
- Identify which component(s) of the Department you believe may have the information about you;
- Specify when you believe the records would have been created;
- Provide any other information that will help the FOIA staff determine which DHS component agency may have responsive records; and
- If your request is seeking records pertaining to another living individual, you must include a statement from that individual certifying his/her agreement for you to access his/her records.

Without this bulleted information the component(s) may not be able to conduct an effective search, and your request may be denied due to lack of specificity or lack of compliance with applicable regulations.

RECORD ACCESS PROCEDURES:

See "Notification Procedure" above.

CONTESTING RECORD PROCEDURES:

See "Notification Procedure" above.

RECORD SOURCE CATEGORIES:

Records are obtained from all individuals who have registered for, applied for, participated in, or assisted with FEMA's training or exercise programs including FEMA employees and contractors, volunteers, other Federal employees and other participants such as instructors, course developers, observers, and interpreters.

EXEMPTIONS CLAIMED FOR THE SYSTEM:

The Secretary of Homeland Security has exempted this system from the following provisions of the Privacy Act, subject to the limitation set forth in 5 U.S.C. 552a(c)(3); (d); (e)(1), (e)(4)(G), (e)(4)(H), (e)(4)(I); and (f) pursuant to 5 U.S.C. 552a(k)(6).

Dated: March 3, 2011.

Mary Ellen Callahan,

Chief Privacy Officer, Department of Homeland Security.

[FR Doc. 2011–8089 Filed 4–5–11; 8:45 am]

BILLING CODE 9111–17–P

DEPARTMENT OF HOMELAND SECURITY

Office of the Secretary

Published Privacy Impact Assessments on the Web

AGENCY: Privacy Office, Department of Homeland Security (DHS).

ACTION: Notice of Publication of Privacy Impact Assessments (PIAs).

SUMMARY: The Privacy Office of the DHS has made available forty PIAs on various programs and systems in the Department. The assessments were approved and published on the Privacy Office's Web site between May 3, 2010 and January 7, 2011.

DATES: The Privacy Impact Assessments are available on the DHS Web site until June 6, 2011, after which they are obtained by contacting the DHS Privacy Office (contact information below).

FOR FURTHER INFORMATION CONTACT: Mary Ellen Callahan, Chief Privacy Officer, DHS, Washington, DC 20528, or e-mail: *pia@hq.dhs.gov.*

SUPPLEMENTARY INFORMATION: Between May 3, 2010 and January 7, 2011, the Chief Privacy Officer of the DHS approved and published forty Privacy Impact Assessments (PIAs) on the DHS Privacy Office Web site, *http://www.dhs.gov/privacy,* under the link for

"Privacy Impact Assessments." Below is a short summary of the programs, indicating the DHS component responsible for the system, and the date on which the PIA was approved. Additional information can be found on the Web site or by contacting the Privacy Office.

System: E-Verify Program: Use of Commercial Data for Employer Verification.

Component: United States Citizenship and Immigration Services (USCIS).

Date of approval: May 4, 2010.

The Verification Division of USCIS operates the E-Verify Program, which provides verification of employment authorization for employers participating in the E-Verify program. The E-Verify Program collects additional employer business information from both registering employers and a commercial data provider, Dun and Bradstreet (D&B), to enhance the employer registration process, manage customer relationships, improve reporting capabilities and operational effectiveness. This expanded information collection pertains to registered employers participating in the E-Verify Program.

System: CRCL Matters.

Component: Civil Rights and Civil Liberties (CRCL).

Date of approval: May 6, 2010.

CRCL has established the CRCL Matters database. CRCL Matters is a database developed to respond to allegations of abuses of civil rights, civil liberties, and religious, racial, and ethnic profiling by department employees and officials. The PIA is being conducted because CRCL collects personally identifiable information (PII).

System: Exodus Accountability Referral System (EARS).

Component: Immigration and Customs Enforcement (ICE).

Date of approval: May 6, 2010.

In order to enforce U.S. federal export control laws, ICE and U.S. Customs and Border Protection (CBP) require information from federal regulatory agencies that grant export licenses on controlled items; specifically whether a license is required and whether a license has been granted. The ICE Exodus Command Center operates the EARS database that initiates, tracks, and manages requests to regulatory agencies for this information. The purpose of the PIA is to document the system's collection and use of PII.

System: Hiring Information Tracking System (HITS).

Component: ICE.

Date of approval: May 13, 2010.

HITS is an information system used by ICE to track current and prior hiring actions. HITS maintains information about individuals who are selected for vacant positions at ICE. ICE has conducted the PIA because HITS collect PII about individuals who are offered employment with ICE.

System: First Responder Technologies (R-Tech) Program.

Component: Science and Technology (S&T).

Date of approval: May 13, 2010.

The DHS S&T First Responder Technologies (R-Tech) program requires the collection of personal information and video recordings of first responder research volunteers in support of operational testing, evaluation, demonstration, and outreach activities. The PIA discusses the risks associated with the use of volunteers to test first responder technologies that are not privacy sensitive.

System: Equal Employment Opportunities (EEO) Eagle Compliant Enterprise System.

Component: CRCL.

Date of approval: June 3, 2010.

The CRCL EEO Program operates the EEO Eagle Complaint Enterprise System. EEO Eagle is an electronic records system used to track complaints and supporting documentation related to individual and class complaints of employment discrimination and retaliation prohibited by the DHS civil rights statutes. CRCL EEO has conducted this PIA because EEO Eagle collects and stores PII.

System: Security and Safety Computer Network.

Component: United States Coast Guard (USCG).

Date of approval: June 16, 2010.

The USCG operates the Coast Guard Headquarters (CGHQ) Support Command Security and Safety Computer Network (CSS LAN). The CSS LAN is a stand-alone system that encompasses multiple applications that support: physical access control to the CGHQ facility, identity verification, security camera monitoring, and key security and tracking for master keys that are used throughout CGHQ. USCG conducted this PIA because the applications that comprise the CSS LAN collect PII.

System: Digital Mail Pilot Program.

Component: DHS Wide.

Date of approval: June 18, 2010.

The DHS Office of the Chief Administrative Officer (OCAO) has implemented a Digital Mail Pilot Program for DHS Headquarters (HQ) and Components within the National Capital Region. The Digital Mail Pilot Program provides users the opportunity to receive mail via email thereby improving DHS business processes and increasing security. The purpose of this PIA is to demonstrate that the Digital Mail Pilot Program has considered and incorporated privacy protections of PII that may be collected, used, disseminated, and maintained throughout the entire lifecycle of the program.

System: Accessibility Compliance Management System (ACMS).

Component: DHS Wide.

Date of approval: June 22, 2010.

The DHS Office of Accessible Systems & Technology (OAST) operates the Accessibility Compliance Management System (ACMS). ACMS is intended to bring together a web-based DHS-wide single point-of-entry reporting system. ACMS allows documenting and reporting of all Section 508 compliance and accessibility activities it consistently tracks current status and progress towards meeting Section 508 compliance requirements for OAST and Component Accessible Systems and Technology Programs (ASTP). The PIA is being conducted to determine any privacy issues with customer information.

System: Publicly Available Social Media Monitoring and Situational Awareness Initiative.

Component: Office of Operations Coordination and Planning (OPS).

Date of approval: June 22, 2010.

The OPS, National Operations Center (NOC), has launched and lead the Publicly Available Social Media Monitoring and Situational Awareness (Initiative) to assist DHS and its components involved in fulfilling OPS statutory responsibility (Section 515 of the Homeland Security Act (6 U.S.C. 321d(b)(1)) to provide situational awareness and establish a common operating picture for the federal government, and for those state, local, and tribal governments, as appropriate. While this Initiative is not designed to actively collect PII, OPS conducted this PIA because the Initiative could potentially involve PII or other information received in an identifiable form. In the event PII comes into the Department's possession under this Initiative, the NOC will redact all PII prior to further dissemination of any collected information. In the event of an *in extremis* situation involving potential life and death, OPS will share certain PII with the responding authority in order for them to take the necessary actions to save a life, such as name and location of a person calling for help buried under rubble, or hiding in a hotel room when the hotel is under attack by terrorists.

System: MyTSA.

Component: Transportation Security Administration (TSA).

Date of approval: July 1, 2010.

TSA's MyTSA consists of a mobile and an iTunes application that provides the traveling public access to relevant TSA travel information via any mobile phone with internet access. MyTSA allows individuals to access such information as the types of items that may be carried through TSA security checkpoints, basic information regarding TSA checkpoint policy, estimated wait times at TSA checkpoints, and current travel conditions. The MyTSA application does not collect or use personally identifiable information. The PIA addresses the privacy impact of TSA's use of mobile media for delivering information to the public.

System: iComplaints.

Component: CRCL.

Date of approval: July 8, 2010.

CRCL EEO Program operates the iComplaints Complaint Enterprise System. IComplaints is an electronic records system used to track complaints and supporting documentation relating to individual and class complaints of employment discrimination and retaliation prohibited by DHS civil rights statutes. IComplaints will replace EEO Eagle as EEO Eagle is being decommissioned. CRCL EEO has conducted this PIA because iComplaints collects and stores PII.

System: Operations Center Incident Management System (OCIMS) Update.

Component: TSA.

Date of approval: July 12, 2010.

Under the Aviation and Transportation Security Act (ATSA), TSA has "responsibility for security in all modes of transportation." TSA uses an operations center incident management system called WebEOC to perform incident management, coordination, and situation awareness functions for all modes of transportation. The system stores information that it receives about the following categories of individuals: (1) Individuals who violate, or are suspected of violating transportation security laws, regulations, policies or procedures; (2) individuals whose behavior or suspicious activity resulted in referrals by Ticket Document Checkers to Behavior Detection Officer or Law Enforcement Officer interview (primarily at airports); or (3) individuals whose identity must be verified, or checked against federal watch lists. Individuals whose identity must be verified includes both those individuals who fail to show acceptable identification documents to compare to boarding documents and law enforcement officials seeking to fly armed. The system collects and compiles reports from federal, state, local, tribal, or private sector security officials related to incidents that may pose a threat to transportation or national security. TSA republished this PIA to clarify that the TSA Operations Center will record telephonic communications. The PIA previously disclosed in section 1.4 that telephone calls were a source of information but did not explicitly state that telephone calls would be recorded. Daily reports will be provided to executives at TSA and DHS to assist in incident and operational response management.

System: Targeted Violence Information Sharing System (TAVISS).

Component: United States Secret Service (USSS).

Date of approval: July 13, 2010.

USSS has created the Targeted Violence Information Sharing System (TAVISS). TAVISS is used to conduct name checks and determine whether a subject is of protective interest to any agency within the TAVISS network. The Secret Service is conducting this PIA because TAVISS contains personally identifiable information (PII) regarding subjects of protective interest to the Secret Service and agencies participating in the network.

System: Watchlist Service.

Component: DHS Wide.

Date of approval: July 14, 2010.

DHS currently uses the Terrorist Screening Database (TSDB), a consolidated database maintained by the Department of Justice Federal Bureau of Investigation Terrorist Screening Center (TSC) of identifying information about those known or reasonably suspected of being involved in terrorist activity in order to facilitate DHS mission-related functions, such counterterrorism, law enforcement, border security, and inspection activities. DHS and TSC are improving the current method of transmitting TSDB data from TSC to DHS. Through a new service called the "DHS Watchlist Service" (WLS), TSC and DHS will automate and simplify the current manual process. TSC remains the authoritative source of watchlist data and will provide DHS with near real-time synchronization of the TSDB. DHS will ensure that each DHS component system receives only those TSDB records which they are authorized to use under the WLS Memorandum of Understanding and authorized under existing regulations and privacy compliance documentation between TSC and DHS (WLS MOU) and any amendments or modifications thereto. DHS conducted this privacy impact assessment (PIA) because the WLS will maintain a synchronized copy of the TSDB, which contains PII, and disseminate it to authorized DHS components.

System: Significant Event Notification (SEN) System.

Component: ICE.

Date of approval: July 26, 2010.

The Significant Event Notification system (SEN) is a reporting and law enforcement intelligence transmission capability developed for DHS and ICE. The ICE Office of Homeland Security Investigations initiated the reporting capability to create reports for ICE field and headquarters managers to provide timely information about critical incidents, activities, and events that involve or impact ICE field staff. The system also handles law enforcement intelligence communication from ICE Office of Enforcement and Removal Operations field offices to field and headquarters managers and the ERO Intelligence Operations Unit. The PIA is being completed to provide notice of the existence of SEN and to publicly document the privacy protections in place.

System: Enforcement Integrated Database (EID) Update.

Component: ICE.

Date of approval: July 28, 2010.

The Enforcement Integrated Database (EID) is a DHS shared common database repository for several DHS law enforcement and homeland security applications. EID captures and maintains information related to the investigation, arrest, booking, detention, and removal of persons encountered during immigration and criminal law enforcement investigations and operations conducted by ICE and CBP, both components within DHS. The PIA for EID was published in January 2010. The information entered into EID and the scope of external information sharing is being expanded, thus necessitating an update to the EID PIA.

System: Iris and Face Technology Demonstration and Evaluation (IFTDE).

Component: Science and Technology (S&T).

Date of approval: August 12, 2010.

As part of its Multi-Modal Biometrics Projects, S&T Directorate and the National Institute of Standards and Technology (NIST) are investigating iris recognition as a promising biometric modality that may become suitable to support DHS operations in the near future. As iris recognition technologies mature, it is important to understand

the capabilities and limitations of the technologies in operational settings, as well as what additional technology development is necessary to reduce technical risk in potential future acquisitions by DHS operational components. The purpose of this evaluation of iris recognition technologies is to conduct field trials/studies of iris camera prototypes under conditions and environments of relevance (*e.g.,* humidity levels, amount of sunlight, etc.) to DHS operational users to assess the viability of the technology and its potential operational effectiveness in support of DHS operations. S&T is conducting a PIA because biometric information is being collected from individuals detained in an operational setting.

System: Freedom of Information Act (FOIA) and Privacy Act (PA) Records Program.

Component: DHS Wide.

Date of approval: August 18, 2010.

DHS and its components have established a Departmental Freedom of Information Act (FOIA) and Privacy Act (PA) Program to maintain records created by the Department's FOIA and PA staff, as well as manage a multitude of FOIA and PA systems. While DHS has established the Department's FOIA and PA program, some components have established information technology as well as paper-based systems designed to handle component-specific FOIA and PA processing. The purpose of the various systems within the FOIA and PA program is to process record requests and administrative appeals under the FOIA and PA, as well as access, notification, and amendment requests and appeals under the PA. These systems also maintain records used in litigation arising from such requests and appeals, and in assisting DHS in carrying out any other responsibilities under the FOIA and PA. The DHS Privacy Office has conducted PIA to assess the risks presented by the use of PII in the various FOIA and PA processes and systems employed by DHS' FOIA and PA program.

System: Entellitrack.

Component: CRCL.

Date of approval: August 23, 2010.

CRCL and TSA have established a new database called Entellitrak which is an enterprise tracking system that has been configured to track, search, and report on complaints data. It is a database developed to respond to allegations of abuses of civil rights, civil liberties, and religious, racial, and ethnic profiling by department employees and officials. Entellitrak will replace the legacy system CRCL Matters with all CRCL Matters data migrating onto Entellitrak in the transition. The PIA is being conducted because Entellitrak collects and stores PII.

System: Watchlist Service Update.

Component: DHS Wide.

Date of approval: September 7, 2010.

DHS currently uses the Terrorist Screening Database (TSDB), a consolidated database maintained by the Department of Justice Federal Bureau of Investigation Terrorist Screening Center (TSC) that contains identifying information about those known or reasonably suspected of being involved in terrorist activity in order to facilitate DHS mission-related functions, such counterterrorism, law enforcement, border security, and inspection activities. In July 2010, DHS launched an improved method of transmitting TSDB data from TSC to DHS through a new service called the "DHS Watchlist Service" (WLS). At that time, DHS published a PIA to describe and analyze privacy risks associated with this new service. The WLS maintains a synchronized copy of the TSDB, which contains PII, and disseminates it to authorized DHS components. DHS is issuing this privacy impact assessment update to identify two additional authorized DHS recipients of TSDB data via the WLS in the form of a computer readable extract: the DHS Office of Intelligence and Analysis and the ICE.

System: Citizenship and Immigration Data Repository (CIDR).

Component: USCIS.

Date of approval: September 8, 2010.

DHS and USCIS developed the Citizenship Immigration Data Repository (CIDR), hosted on DHS classified networks, in order to make information from multiple USCIS benefits administration systems available for querying by authorized USCIS personnel for the following three purposes: (1) Vetting USCIS application information for indications of possible immigration fraud and national security concerns; (2) detecting possible fraud and misuse of immigration information or position by USCIS employees, for personal gain or by coercion; and (3) responding to requests for information (RFIs) from the DHS Office of Intelligence and Analysis (I&A) and/or the federal intelligence and law enforcement community members that are based on classified criteria. In conjunction with this PIA, DHS is issuing a new Privacy Act system of records notice to cover the search parameters and the results of the searches.

System: Access to Sensitive Security Information and Contract Solicitation.

Component: TSA.

Date of approval: September 9, 2010.

TSA is responsible for the acquisition of services and supplies related to protecting the nation's transportation system. If determined necessary for the proposal preparation process, TSA may permit offerors to have access to Sensitive Security Information (SSI) necessary to prepare a proposal. 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. In order to determine if a potential offer or may be granted access to SSI in the pre-contract award acquisition process, TSA will conduct a security threat assessment (STA) of the individuals and company. The STA may include a verification of site facility clearance in the National Industrial Security Program, contractor suitability determination or other federal background investigation, individual security clearance(s), and if required, a criminal history records check and/or a check against terrorism databases. Because this program entails a new collection of information about members of the public in identifiable form, the E-Government Act of 2002 and the Homeland Security Act of 2002 requires that TSA conduct a PIA.

System: Eversity Enterprise System.

Component: CRCL.

Date of approval: September 14, 2010.

The CRCL EEO Program operates the Eversity Enterprise System. Eversity is an electronic records system used in workforce analysis, tracking, management, and reporting required under Equal Employment Opportunity Commission (EEOC) Management Directive (MD) 715. CRCL EEO has conducted this PIA because Eversity collects and stores PII.

System: Social Networking Interactions and Applications (Communications/Outreach/Public Dialogue).

Component: DHS Wide.

Date of approval: September 16, 2010.

Social networking interactions and applications includes a sphere of non-government Web sites and web-based tools that focuses on connecting users, inside and outside of the DHS, to engage in dialogue, share information and media, and collaborate. Third parties control and operate these non-governmental websites; however, the Department may use them as alternative channels to provide robust information and engage with the public. The Department may also use these websites to make information and services

widely available, while promoting transparency and accountability, as a service for those seeking information about or services from the Department. This PIA analyzes the Department's use of social networking and how these interactions and applications could result in the Department receiving PII. This PIA describes the information the Department may have access to, how it will use the information, what information is retained and shared, and how individuals can gain access to and correct their information.

System: Alien Criminal Response Information Management System (ACRIMe) & Enforcement Integrated Database (EID) Update.

Component: ICE.

Date of approval: September 29, 2010.

ACRIMe is an information system used by ICE to receive and respond to immigration status inquiries made by other agencies about individuals arrested, subject to background checks, or otherwise encountered by those agencies. EID is an ICE case management system that captures and maintains information related to the investigation, arrest, booking, detention, and removal of persons encountered during immigration and criminal law enforcement investigations and operations conducted by ICE and U.S. Customs and Border Protection. ICE is combining ACRIMe and EID data via the ICE Integrated Decision Support System, a reporting sub system of EID, to enable and enhance comprehensive reporting about criminal aliens throughout the alien identification, apprehension, and removal process. To effectuate this reporting, ICE is modifying ACRIMe to expand its user base within the agency, implementing new user functionality in ACRIMe and EID, and updating IIDS to support enhanced reporting of ACRIMe and EID data. ICE is further expanding ACRIMe support for the Secure Communities initiative. ICE is conducting this PIA update to address these modifications and enhancements.

System: National File Tracking System (NFTS).

Component: USCIS.

Date of approval: October 5, 2010.

USCIS has prepared this PIA for the National File Tracking System (NFTS). NFTS is an automated file-tracking system used to maintain an accurate file inventory and track the physical location of files. The system facilitates USCIS's ability to efficiently manage and streamline access to the millions of immigration files under its control. USCIS is conducting this PIA to document, analyze and assess the current practices with respect to the PII, NFTS collects, uses and shares.

System: Standoff Technology Integration and Demonstration Program Update.

Component: S&T.

Date of approval: October 14, 2010.

S&T has updated the Standoff Explosives Detection Technology Demonstration Program (now referred to as the Standoff Technology Integration and Demonstration Program, or STIDP) PIA issued July 21, 2008 to reflect updates to the program involving live crowd testing.

The program is adding new technologies, expanding the use of the test center, enhancing object tracking technologies and beginning to distribute crowd video data to vendors. The PIA update identifies and addresses the privacy issues associated with public test and evaluation activities on technologies that will be acquired, matured, and integrated by STIDP between now and the end of the program, currently slated for 2014. Based on the privacy issues identified, three sets of privacy protective requirements were developed and implemented at all stages of the program. The Live Testing Requirements and Law Enforcement Operations Requirements apply to conducting and operating a test in a public environment and the Data Protection Requirements address the collection and protection of PII. These requirements, when systematically applied to test and evaluation plans and their implementation, ensure that privacy concerns are appropriately addressed for broad classes of technologies tested in a range of venues with and without law enforcement operations. This update assists STIDP's mission of developing an integrated countermeasure architecture to prevent person-borne improvised explosive device attacks.

System: Electronic Surveillance System (ELSUR).

Component: ICE.

Date of approval: November 2, 2010.

The Electronic Surveillance System (ELSUR) is owned by ICE. ELSUR allows ICE to track and search for ICE applications for court orders that authorize ICE to intercept oral, wire, or electronic communications during the course of a criminal investigation. ICE conducted this PIA because ELSUR contains PII and to publicly document the privacy protections that are in place.

System: Immigration Benefits Background Check Systems (IBBCS).

Component: USCIS.

Date of approval: November 5, 2010.

As part of its benefits adjudication process and as required by law, USCIS conducts background checks on petitioners and applicants who seek certain immigration benefits. These background checks consist of four separate checks against systems within Department of Justice (DOJ), Federal Bureau of Investigation (FBI), and DHS. In order to facilitate the collection and transmission of information necessary to complete background check processes, USCIS maintains five information technology electronic systems: The Fingerprint Masthead Notification System (FMNS), the Customer Identity Capture System (CICS), the FD–258 Tracking System—Mainframe (FD–258 MF), the Benefits Biometrics Support System (BBSS), and the Interagency Border Inspection System (IBIS) Manifest. USCIS is conducting this PIA because FMNS, CICS, FD–258 MF, BBSS, and IBIS Manifest collect, use, and share PII. The PIA replaces the previously published USCIS PIA for the "Background Check Service (BCS)" which describes planned background check-related systems that were never implemented. Upon publication of this PIA, the BCS PIA will be retired.

System: Quality Assurance Recording System (QARS).

Component: Federal Emergency Management Agency (FEMA).

Date of approval: November 10, 2010.

FEMA, Response and Recovery Bureau operates the QARS. The proposed system of telephone call and computer screen capture recording is for internal employee and contractor performance evaluation, training and quality assurance purposes to improve customer service to disaster assistance applicants requesting assistance under the Robert T. Stafford Disaster Relief and Emergency Assistance Act. FEMA is conducting the PIA because QARS call recordings and screen captures information about the FEMA employees and/or contractors as they provide customer service to disaster assistance applicants. The system will maintain information about disaster assistance applicants, but the focus of this system is on employee and contractor quality assurance.

System: Protective Research Information System Management (PRISM–ID).

Component: USSS.

Date of approval: November 12, 2010.

USSS has created and used the PRISM–ID system to record information that in accordance with Secret Service criteria is required to assist the agency in meeting its protective mission that includes the protection of the President, Vice President, their immediate families, former Presidents and First

Ladies, major candidates for the presidency and vice presidency, foreign heads of state visiting the United States, and other individuals authorized to receive Secret Service protection. The PIA is being conducted because PRISM–ID collects PII.

System: Department of Homeland Security Information Sharing Environment Suspicious Activity Reporting Initiative (ISE–SAR).

Component: DHS Wide.

Date of approval: November 17, 2010.

The Office and Intelligence and Analysis, primarily through the State and Local Program Office in coordination with the Office of Operations Coordination Planning, is leading the DHS effort to implement the Nationwide Suspicious Activity Reporting Initiative (NSI). The NSI is a key aspect of the federal Information Sharing Environment (ISE) that Congress created in the Intelligence Reform and Terrorism Prevention Act of 2004 (IRPTA). The NSI is overseen by DOJ and is designed to support the sharing of information through the ISE about suspicious activities which are defined as "official documentation of observed behavior reasonably indicative of pre-operational planning related to terrorism or other criminal activity [related to terrorism]." The Office of Intelligence and Analysis and the Office of Operations and Coordination Planning have been jointly coordinating activities throughout DHS to develop a department-level interface with the NSI that will enable DHS to share Suspicious Activity Reporting (SAR) that meet the ISE–SAR Functional Standard Version 1.5 (hereinafter referred to as ISE–SAR). Throughout this PIA, the term "SAR" refers to suspicious activity reporting, which may include activities that do not have a nexus to terrorism, and the term "ISE–SAR" refers to a subset of SAR that meet the ISE–SAR Functional Standard. The ISE–SAR Functional Standard Version 1.5 defines an ISE–SAR as official documentation of observed behavior reasonably indicative of: Pre-operational planning related to terrorism or other criminal activity associated with terrorism. DHS conducted the PIA because ISE–SAR may contain PII. The PIA describes the coordinated activities of the DHS ISE–SAR Initiative, including the process for DHS component level review, identification, and submission of ISE–SAR to the NSI Shared Space as well as the technology that DHS developed to support DHS' participation in the NSI.

System: Research Project Involving Volunteers.

Component: S&T.

Date of approval: November 23, 2010.

An integral part of the S&T mission is to conduct research, development, testing, and evaluation (RDT&E) on technologies or topics related to improving homeland security and combating terrorism. Some S&T RDT&E activities use volunteers to test, evaluate, provide feedback, or otherwise collect data on certain research topics, technologies, equipment, and capabilities related to S&T's mission. Volunteer RDT&E activities require the collection of a range of information from volunteers including work experience, biographic data and images. RDT&E activities will vary in the types and breadth of data elements and information collected from volunteers. S&T is conducting this PIA to establish protections for all volunteer S&T RTD&E activities. Volunteer RDT&E activities that are covered by the PIA are listed in the appendix, updated periodically.

System: NOC Patriot Report Database.

Component: OPS.

Date of approval: December 7, 2010.

The NOC in OPS operates the NOC Patriot Report Database. The NOC Patriot Report Database is a repository for reports generated to record and track suspicious activity that may implicate terrorism-related or criminal activity. OPS has conducted this PIA because the NOC Patriot Report Database may contain PII.

System: Electronic Discovery Software System (EDSS).

Component: ICE.

Date of approval: December 10, 2010.

The Electronic Discovery Software System (EDSS) is owned by the Office of the Principal Legal Advisor (OPLA) within ICE. EDSS supports the collection and organization of paper and electronic documents for analysis, review, redaction, and production to meet litigation discovery requirements. ICE may also use the system to process agency records in response to FOIA or PA requests. ICE conducted this PIA because EDSS collects, analyzes, and stores PII.

System: TECS System: CBP Primary and Secondary Processing.

Component: CBP.

Date of approval: December 23, 2010.

The TECS (not an acronym) System is the updated and modified version of the former Treasury Enforcement Communications System. TECS is owned and managed by CBP. TECS is both an information-sharing platform, which allows users to access different databases that may be maintained on the platform or accessed through the platform, and the name of a system of records that include temporary and permanent enforcement, inspection, and operational records relevant to the antiterrorism and law enforcement mission of CBP and numerous other federal agencies that it supports. TECS not only provides a platform for interaction between these systems and defined TECS users, but also serves as a data repository to support law enforcement "lookouts," border screening, and reporting for CBP's primary and secondary inspection processes, which are generally referenced as TECS Records or Subject Records. In order to provide more transparency as it relates to the functions and data in TECS, CBP published separate PIAs and Privacy Act System of Records Notices (SORNs) for the CBP sub-systems based on the purpose and use of the information. CBP also maintains other federal agency data on TECS to stage the information for use by CBP at the time an individual presents himself/herself to CBP. This allows TECS to work more efficiently and reduces the performance impact on the originating systems. The PIA focuses on CBP's use and modernization of TECS as it relates to the primary and secondary inspection processes (including information collected in advance of arrival, during inspections at the United States (U.S.) port of entry (POE), and retention of information and reports following interactions during U.S. border crossing activities) to ensure compliance with the numerous laws enforced by CBP, including determining the admissibility of persons attempting to enter the U.S. CBP will issue a separate PIA to address the information access and system linkages facilitated for CBP, DHS, and other federal agency systems that link to TECS and share data within the TECS user community.

System: ELBC System: Exit Line Breach Control System.

Component: TSA.

Date of approval: December 28, 2010.

TSA has conducted an assessment of ELBC systems for use in airports. The assessment will evaluate the ELBC systems' capability to monitor traffic flow at the exit lanes from the sterile areas of the airport and initiate an automated response if it appears that an individual is entering the sterile area through the exit lane. TSA will make results of the assessment available to airports seeking to implement such systems. This PIA is being conducted to provide transparency into TSA testing affecting the public and the collection of images as part of the assessment. If TSA decides to implement such systems for

its own use, a new PIA will be conducted.

System: NICC SARS: National Infrastructure Coordinating Center Suspicious Activity Reporting Initiative (NICC).

Component: National Protection and Programs Directorate (NPPD).

Date of approval: December 29, 2010.

NPPD Office of Infrastructure Protection (IP) National Infrastructure Coordinating Center (NICC) has published this PIA to reflect activities under its Suspicious Activity Reporting (SAR) Initiative. The NICC SAR Initiative serves as a mechanism by which a report involving suspicious behavior related to an observed encounter or reported activity is received and evaluated to determine its potential nexus to terrorism. NICC is conducting this PIA because SAR occasionally contain PII and NICC will be collecting and contributing SAR data for reporting and evaluation proceedings.

System: Publicly Available Social Media Monitoring and Situational Awareness Initiative Update.

Component: OPS.

Date of approval: January 7, 2011.

OPS, NOC, leads the Publicly Available Social Media Monitoring and Situational Awareness (Initiative) to assist the DHS and its components involved in fulfilling OPS statutory responsibility (Section 515 of the Homeland Security Act (6 U.S.C. 321d(b)(1)) to provide situational awareness and establish a common operating picture for the federal government, and for those state, local, and tribal governments, as appropriate. The NOC and participating components may also share this de-identified information with international partners and the private sector where necessary and appropriate for coordination. While this Initiative is not designed to actively collect PII, OPS is conducting this update to the PIA because the initiative may now collect and disseminate PII for certain narrowly tailored categories. For example, in the event of an in extremis situation involving potential life and death, OPS will share certain PII with the responding authority in order for them to take the necessary actions to save a life, such as name and location of a person calling for help buried under rubble, or hiding in a hotel room when the hotel is under attack by terrorists. In the event PII comes into the Department's possession under circumstances other than those itemized herein, the NOC will redact all PII prior to further dissemination of any collected information. After conducting the Second Privacy Compliance Review, it was determined that the PIA should be updated to allow for collection and dissemination of PII in a limited number of situations in order to respond to the evolving operational needs of the NOC. The PIA will be reviewed every six months to ensure compliance. The review will be done in conjunction with a Privacy Office-led Privacy Compliance Review (PCR) of the Initiative and of OPS social media monitoring Internet-based platforms and information technology infrastructure.

Dated: March 17, 2011.

Mary Ellen Callahan,

Chief Privacy Officer, Department of Homeland Security.

[FR Doc. 2011–8086 Filed 4–5–11; 8:45 am]

BILLING CODE 9110–9L–P

DEPARTMENT OF HOMELAND SECURITY

Federal Emergency Management Agency

[Internal Agency Docket No. FEMA–1960–DR; Docket ID FEMA–2011–0001]

Illinois; Major Disaster and Related Determinations

AGENCY: Federal Emergency Management Agency, DHS.

ACTION: Notice.

SUMMARY: This is a notice of the Presidential declaration of a major disaster for the State of Illinois (FEMA–1960–DR), dated March 17, 2011, and related determinations.

DATES: *Effective Date:* March 17, 2011.

FOR FURTHER INFORMATION CONTACT: Peggy Miller, Office of Response and Recovery, Federal Emergency Management Agency, 500 C Street, SW., Washington, DC 20472, (202) 646–3886.

SUPPLEMENTARY INFORMATION: Notice is hereby given that, in a letter dated March 17, 2011, the President issued a major disaster declaration under the authority of the Robert T. Stafford Disaster Relief and Emergency Assistance Act, 42 U.S.C. 5121 *et seq.* (the "Stafford Act"), as follows:

I have determined that the damage in certain areas of the State of Illinois resulting from a severe winter storm and snowstorm during the period of January 31 to February 3, 2011, is of sufficient severity and magnitude to warrant a major disaster declaration under the Robert T. Stafford Disaster Relief and Emergency Assistance Act, 42 U.S.C. 5121 *et seq.* (the "Stafford Act"). Therefore, I declare that such a major disaster exists in the State of Illinois.

In order to provide Federal assistance, you are hereby authorized to allocate from funds available for these purposes such amounts as you find necessary for Federal disaster assistance and administrative expenses.

You are authorized to provide Public Assistance in the designated areas and Hazard Mitigation throughout the State. You are further authorized to provide emergency protective measures, including snow assistance, under the Public Assistance program for any continuous 48-hour period during or proximate to the incident period. You may extend the period of assistance, as warranted. This assistance excludes regular time costs for the sub-grantees' regular employees. Consistent with the requirement that Federal assistance is supplemental, any Federal funds provided under the Stafford Act for Public Assistance and Hazard Mitigation will be limited to 75 percent of the total eligible costs.

Further, you are authorized to make changes to this declaration for the approved assistance to the extent allowable under the Stafford Act.

The Federal Emergency Management Agency (FEMA) hereby gives notice that pursuant to the authority vested in the Administrator, under Executive Order 12148, as amended, Gregory W. Eaton, of FEMA is appointed to act as the Federal Coordinating Officer for this major disaster.

The following areas of the State of Illinois have been designated as adversely affected by this major disaster:

Adams, Bond, Boone, Brown, Bureau, Calhoun, Carroll, Cass, Christian, Clark, Clay, Coles, Cook, Crawford, Cumberland, DeKalb, Douglas, DuPage, Edgar, Effingham, Fayette, Ford, Fulton, Hancock, Henderson, Henry, Jasper, Jo Daviess, Kane, Knox, Lake, LaSalle, Lee, Logan, Marion, Marshall, Mason, McDonough, McHenry, Menard, Mercer, Morgan, Moultrie, Ogle, Peoria, Pike, Putnam, Richland, Rock Island, Schuyler, Scott, Shelby, Stark, Tazewell, Warren, Washington, Whiteside, Will, Winnebago, and Woodford Counties for Public Assistance.

Bureau, Calhoun, Carroll, Cass, Cook, DeKalb, DuPage, Fulton, Hancock, Henry, Jo Daviess, Kane, Lake, LaSalle, Lee, Logan, Marshall, Mason, McDonough, Mercer, Morgan, Ogle, Peoria, Pike, Putnam, Rock Island, Schuyler, Stark, Tazewell, Warren, Whiteside, Will, Winnebago, and Woodford Counties for emergency protective measures (Category B), including snow assistance, under the Public Assistance program for any continuous 48-hour period during or proximate to the incident period. This emergency assistance will be provided for a period of 72 hours for the counties of Adams, Boone, Brown, Ford, Henderson, Knox, McHenry, Menard, and Scott.

All counties within the State of Illinois are eligible to apply for assistance under the Hazard Mitigation Grant Program.

The following Catalog of Federal Domestic Assistance Numbers (CFDA) are to be used for reporting and drawing funds: 97.030, Community Disaster Loans; 97.031, Cora Brown Fund; 97.032, Crisis Counseling; 97.033, Disaster Legal Services; 97.034,