

TABLE 1.—Continued

Application No.	Drug	Applicant
NDA 10–915	Q.E.D. Hairgroom (captan)	A.R. Winarick, Inc., 783 Palisade Ave., Cliffside, NJ 07010

The Director, Center for Drug Evaluation and Research, under section 505(e) of the Federal Food, Drug, and Cosmetic Act (21 U.S.C. 355(e)), and under authority delegated by the Commissioner, finds that the holders of the applications listed in this document have repeatedly failed to submit reports required by § 314.81. In addition, under § 314.200, we find that the holders of the applications have waived any contentions concerning the legal status of the drug products. Therefore, under these findings, approval of the applications listed in this document, and all amendments and supplements thereto, is hereby withdrawn, effective September 10, 2010.

Dated: August 31, 2010.

**Janet Woodcock,**

*Director, Center for Drug Evaluation and Research.*

[FR Doc. 2010–22603 Filed 9–9–10; 8:45 am]

**BILLING CODE 4160–01–S**

## DEPARTMENT OF HOMELAND SECURITY

### Office of the Secretary

[Docket No. DHS–2010–0075]

### Privacy Act of 1974; Privacy Act of 1974: Department of Homeland Security/ALL–031 Information Sharing Environment Suspicious Activity Reporting Initiative System of Records

**AGENCY:** Privacy Office, DHS.

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

**SUMMARY:** In accordance with the Privacy Act of 1974, the Department of Homeland Security proposes to establish a new Department of Homeland Security system of records titled, “Department of Homeland Security/ALL–031 Information Sharing Environment Suspicious Activity Reporting Initiative System of Records.” This system of records will allow DHS to compile suspicious activity report data that meet the Information Sharing Environment Suspicious Activity Reporting Functional Standard and share these Suspicious Activity Reporting data with authorized participants in the Nationwide Suspicious Activity Reporting Initiative,

including other DHS components, Federal departments and agencies, State, local and Tribal law enforcement agencies, and the private sector. Additionally, the Department of Homeland Security is issuing a Notice of Proposed Rulemaking to exempt this system from certain provisions of the Privacy Act elsewhere in the **Federal Register**. This newly established system will be included in the Department of Homeland Security’s inventory of record systems.

**DATES:** Submit comments on or before October 12, 2010. This new system will be effective October 12, 2010.

**ADDRESSES:** You may submit comments, identified by docket number DHS–2010–0075 by one of the following methods:

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

- *Fax:* 703–483–2999.

- *Mail:* Mary Ellen Callahan, Chief Privacy Officer, Privacy Office, Department of Homeland Security, Washington, DC 20528.

- *Instructions:* All submissions received must include the agency name and docket number for this rulemaking. All comments received will be posted without change to <http://www.regulations.gov>, including any personal information provided.

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

**FOR FURTHER INFORMATION CONTACT:** For general questions please contact: Ronald Athmann (202–447–4332), Office of Intelligence and Analysis, Department of Homeland Security, Washington, DC 20528. For privacy issues please contact: Mary Ellen Callahan (703–235–0780), Chief Privacy Officer, Privacy Office, U.S. Department of Homeland Security, Washington, DC 20528.

#### SUPPLEMENTARY INFORMATION:

##### I. Background

In accordance with the Privacy Act of 1974, 5 U.S.C. 552a, the Department of Homeland Security (DHS) proposes to establish a new DHS system of records titled, “DHS/ALL–031 Information Sharing Environment (ISE) Suspicious Activity Reporting (SAR) Initiative System of Records.”

This system of records will allow DHS components that produce, receive, and store suspicious activity reports (SARs) pursuant to their existing authorities, responsibilities, platforms, and programs to compile and share report data that also meet the ISE–SAR Functional Standard with authorized participants in the Nationwide SAR Initiative (NSI) including, Federal departments and agencies, State, local and Tribal law enforcement agencies, and the private sector. The NSI is one of a number of government-wide efforts designed to implement guidelines first issued by the President on December 16, 2005, for establishing the ISE pursuant to section 1016 of the Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA), as amended. The NSI establishes a nationwide capability to gather, document, process, analyze and share information about suspicious activity, incidents, or behavior reasonably indicative of terrorist activities (hereafter collectively referred to as suspicious activity or activities) to enable rapid identification and mitigation of potential terrorist threats.

There is a long history of documenting of suspicious activity, particularly in the law enforcement community; these reports are sometimes referred to as suspicious activity reports, tips and leads, or other similar terms. Federal, State, local and Tribal agencies and the private sector currently collect and document suspicious activities in support of their responsibilities to investigate and prevent potential crimes, protect citizens, and apprehend and prosecute criminals. Since some of these documented activities may bear a nexus to terrorism, the Program Manager for the Information Sharing Environment (PM–ISE) has developed a standardized process for identifying, documenting, and sharing terrorism-related SAR data (hereinafter referred to as an “ISE–SAR”), which meet the definition and criteria set forth in the ISE Functional Standard Suspicious Activity Reporting, (Version 1.5, May 2009) to the maximum extent possible consistent with the protection of individual privacy, civil rights, and civil liberties. The Functional Standard defines an ISE–SAR as official documentation of observed behavior determined to have a potential nexus to terrorism (*i.e.*, to be reasonably

indicative of criminal activity associated with terrorism).

Several operational components within DHS regularly observe or otherwise encounter suspicious activities while executing their authorized missions and performing operational duties. Components document those observations or encounters in SARs. Across the Department the operational setting or context for activities reported in SARs are as varied as the Department's mission responsibilities. Engagement with the NSI will alter neither those underlying mission functions nor upset the current methodologies employed by DHS components collecting information on suspicious activities and issuing SARs. Rather, the NSI will facilitate the more effective sharing and discovery—both internally and between DHS and external NSI participants—by incorporating a standardized technological and functional approach for recording and storing ISE–SARs throughout DHS. Once trained in the NSI program and the application of these technical and functional standards, DHS personnel will review component SARs and submit the data only from those that meet the ISE–SAR Functional Standard into the NSI Shared Space.

In keeping with NSI standards, whenever suspicious activity is determined to have a potential nexus to terrorism, DHS personnel will extract data from the component level SARs and input that data in a standardized format to the NSI Shared Space. All ISE–SAR data introduced into the NSI Shared Space are stored locally, but made available to other authorized users when a user's search criteria are met. For example, DHS ISE–SAR data remains under the control of the Department until an authorized user queries the NSI Shared Space with terms that match the data in the DHS ISE–SAR server. The results of each user's search or query cannot be downloaded or edited.

Additionally, DHS is issuing a Notice of Proposed Rulemaking to exempt this system of records from certain provisions of the Privacy Act elsewhere in the **Federal Register**. This newly established system will be included in the Department of Homeland Security's inventory of record systems.

## II. Privacy Act

The Privacy Act embodies fair information principles in a statutory framework governing the means by which the United States Government collects, maintains, uses, and disseminates individuals' records. The

Privacy Act applies to information that is maintained in a "system of records." A system of records is a group of any records under the control of an agency for which information is retrieved by the name of an individual or by some identifying number, symbol, or other identifying particular assigned to the individual. In the Privacy Act, an individual is defined to encompass United States citizens and lawful permanent residents. As a matter of policy, DHS extends administrative Privacy Act protections to all individuals where systems of records maintain information on U.S. citizens, lawful permanent residents, and visitors. Individuals may request access to their own records that are maintained in a system of records in the possession or under the control of DHS by complying with DHS Privacy Act regulations, 6 CFR Part 5. As published elsewhere in today's **Federal Register**, the Secretary of Homeland Security has exempted this system from the notification, access, and amendment procedures of the Privacy Act because it is a law enforcement system. However, DHS will consider individual requests to determine whether or not information may be released.

The Privacy Act requires each agency to publish in the **Federal Register** a description denoting the type and character of each system of records that the agency maintains, and the routine uses that are contained in each system in order to make agency record keeping practices transparent, to notify individuals regarding the uses to their records are put, and to assist individuals to more easily find such files within the agency. Below is the description of the DHS/ALL–031 system of records.

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

### SYSTEM OF RECORDS

#### DHS/ALL–031

#### SYSTEM NAME:

DHS/ALL–031 Information Sharing Environment (ISE) Suspicious Activity Reporting (SAR) Initiative System of Records.

#### SECURITY CLASSIFICATION:

Unclassified, sensitive, and law enforcement sensitive.

#### SYSTEM LOCATION:

Records are maintained at the Department of Homeland Security (DHS) Headquarters on the DHS Nationwide Suspicious Activity Report

Initiative (NSI) Shared Space Server in Washington, DC.

#### CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM:

Categories of individuals covered by this system include:

- DHS employees and contractors who have submitted ISE–SAR data to the NSI Shared.
- DHS employees and contractors who use the NSI Shared Space for conducting research and analysis with a potential terrorism nexus.
- Federal, State, local, Tribal, territorial and private sector officials whose agency or organization is part of the NSI and have submitted a ISE–SAR that meets the ISE–SAR Functional Standard and whose information DHS personnel have a need to know for the performance of their official duties.
- Federal, State, local, Tribal, territorial, and private sector officials whose agency or organization is an NSI participant and who use the NSI Shared Space for conducting research and analysis with a potential terrorism nexus.

• Individuals whose behavior is reasonably indicative of pre-operational planning related to terrorism or other criminal activity associated with terrorism.

• Witnesses who have observed individuals whose behavior reasonably is indicative of pre-operational planning related to terrorism or other criminal activity associated with terrorism.

• Individuals who have a material relationship to the activity or behavior reported in an ISE–SAR (e.g., the owner of a particular vehicle that was observed in a SAR, where it is unclear whether the person was actually driving the vehicle).

#### CATEGORIES OF RECORDS IN THE SYSTEM:

As described in the ISE–SAR Functional Standard Version 1.5 published in May 2009, the below information related to individuals may be maintained in this system. The ISE–SAR Functional Standard identifies privacy fields, which are also noted below.

- Aircraft descriptions, including:
  - Aircraft engine quality.
  - Aircraft fuselage color.
  - Aircraft wing color.
  - Aircraft ID (privacy field).
  - Aircraft make code.
  - Aircraft model code.
  - Aircraft style code .
  - Aircraft tail number (privacy field).
- Attachment:
  - Attachment type text.
  - Binary image.

- Capture date.
- Description text.
- Format type text.
- Attachment URI.
- Attachment privacy field indicator.
- Contact information for the submitter of the ISE–SAR:
  - Person first name.
  - Person last name.
  - Person middle initial/name.
  - E-mail address.
  - Organization/Affiliation, such as DHS.
  - Full telephone number.
- Driver License:
  - Expiration date (privacy field).
  - Expiration year.
  - Issuing authority text.
  - Driver license number (privacy field).
  - Driver license endorsements, such as Hazardous Materials, Commercial Driver's License, Motorcycle.
- Follow-up Action:
  - Activity date.
  - Activity time.
  - Assigned by text.
  - Assigned to text.
  - Disposition text.
  - Status text.
- Location:
  - Location description (privacy field).
- Location Address:
  - Building description.
  - County name.
  - Country name.
  - Cross street description.
  - Floor identifier.
  - International Civil Aviation Organization (ICAO) airfield code for departure.
    - ICAO airfield code for planned destination.
    - ICAO for actual destination.
    - ICAO airfield for alternate.
    - Mile marker text.
    - Municipality name.
    - Postal code.
    - State name.
    - Street name.
    - Street number (privacy field).
    - Street post directional.
    - Street pre directional.
    - Street type.
    - Unit ID (privacy field).
- Location Coordinates:
  - Altitude.
  - Coordinate datum.
  - Latitude degree.
  - Latitude minute.
  - Latitude second.
  - Longitude degree.
  - Longitude minute.
  - Longitude second.
  - Conveyance track/intent.
- Observer:
  - Observer type text.
  - Person employer ID (privacy field).
- Owning organization:
  - Organization item.
  - Organization description.
  - Organization ID (privacy field).
  - Organization Local ID.
- Other Identifier:
  - Person identification number (PID) (privacy field).
  - PID effective date (privacy field).
  - PID effective year.
  - PID expiration date (privacy field).
  - PID expiration year.
  - PID issuing authority text.
  - PID type code.
- Passport:
  - Passport ID (privacy field).
  - Expiration date (privacy field).
  - Expiration year.
  - Issuing country code.
- Person:
  - AFIS FBI number (privacy field).
  - Age.
  - Age unit code.
  - Date of birth (privacy field).
  - Year of birth.
  - Ethnicity code.
  - Maximum age.
  - Minimum age.
  - State identifier (privacy field).
  - Tax identification number (privacy field).
- Person Name:
  - First name (privacy field).
  - Last name (privacy field).
  - Middle name (privacy field).
  - Full name (privacy field).
  - Moniker (privacy field).
  - Name suffix.
  - Name type.
- Physical descriptors:
  - Build description.
  - Eye color code.
  - Eye color text.
  - Hair color code.
  - Hair color text.
  - Person eyewear text.
  - Person facial hair text.
  - Person height.
  - Person height unit code.
  - Person maximum height.
  - Person minimum height.
  - Person maximum weight.
  - Person minimum weight.
  - Person sex code.
  - Person weight.
  - Person weight unit code.
  - Race code.
  - Skin tone code.
  - Clothing description text.
- Physical feature:
  - Feature description.
  - Feature type code.
  - Location description.
- Registration:
  - Registration authority code.
  - Registration number (privacy field).
  - Registration type.
  - Registration year.
- ISE–SAR Submission:
  - Additional details indicator.
  - Data entry date.
  - Dissemination code.
  - Fusion center contact first name.
  - Fusion center contact last name.
  - Fusion center contact e-mail address.
  - Fusion center contact telephone number.
  - Message type indicator.
  - Privacy purge data.
  - Privacy purge review date.
  - Submitting ISE–SAR Record ID.
  - ISE–SAR submission date.
  - ISE–SAR title.
  - ISE–SAR version.
  - Source agency case ID.
  - Source agency record reference name.
  - Source agency record status code.
  - Privacy information exists indicator.
- Sensitive Information Details:
  - Classification label.
  - Classification reason text.
  - Sensitivity level.
  - Tearlined indicator (information that indicates the report does not contain classified information).
- Source Organization:
  - Organization name.
  - Organization ORI.
  - System ID.
  - Fusion center submission date.
  - Source agency contact first name.
  - Source agency contact last name.
  - Source agency contact e-mail address.
  - Source agency contact phone number.
- Suspicious Activity Report:
  - Community description.
  - Community URI.
  - LEXS version.
  - Message date/time.
  - Sequence number.
  - Source reliability code.
  - Content validity code.
  - Nature of source-code.
  - Nature of source-text.
- Submitting organization:
  - Organization name.
  - Organization ID.
  - Organization ORI.
  - System ID.
- Suspicious Activity:
  - Activity end date.
  - Activity end time.
  - Activity start date.
  - Activity start time.
  - Observation description text.
  - Observation end date.
  - Observation end time.
  - Observation start date.

- Observation start time.
- Threat type code.
- Threat type detail text.
- Suspicious activity code.
- Weather condition details.
- Target:
  - Critical infrastructure indicator.
  - Infrastructure sector code.
  - Infrastructure tier text.
  - Structure type code.
  - Target type text.
  - Structure type text.
  - Target description text.
- Vehicle:
  - Color code.
  - Description.
  - Make name.
  - Model name.
  - Style code.
  - Vehicle year.
  - Vehicle identification number (privacy field).
    - US DOT number (privacy field).
    - Vehicle description.
- Related ISE–SAR:
  - Fusion center ID.
  - Fusion center ISE–SAR Record ID.
  - Relations description text.
- Vessel:
  - Vessel official Coast Guard number identification (privacy field).
  - Vessel ID (privacy field).
  - Vessel ID issuing authority.
  - Vessel IMO number identification (privacy field).
  - Vessel MMSI identification.
  - Vessel make.
  - Vessel model.
  - Vessel model year.
  - Vessel name.
  - Vessel hailing port.
  - Vessel national flag.
  - Vessel overall length.
  - Vessel overall length measure.
  - Vessel serial number (privacy field).
  - Vessel type code.
  - Vessel propulsion text.

**AUTHORITY FOR MAINTENANCE OF THE SYSTEM:**

The Homeland Security Act of 2002, as amended; and the Intelligence Reform and Terrorism Prevention Act of 2004, as amended; the National Security Act of 1947, as amended; Executive Order 13388.

**PURPOSE(S):**

The ISE–SAR Functional Standard is designed to support the sharing, specifically through the NSI, of information about suspicious activities that have a potential terrorism nexus throughout the ISE. The NSI participants include DHS; the Department of Justice; other Federal agencies carrying out counterterrorism mission function; State, local, and

Tribal entities, including law enforcement agencies, represented at State, regional, major urban area fusion centers; and the private sector to the extent authorized by applicable law. In addition to providing specific indicators of possible terrorism-related crimes, ISE–SARs can be used to look for patterns and trends by analyzing information at a broader level than would typically be recognized within a single jurisdiction, State, or territory. Standardized and consistent sharing of suspicious activity information regarding potential terrorist threats and possible criminal activity associated with terrorism among State and major urban area fusion centers and Federal agencies is vital to assessing, deterring, preventing, or prosecuting those involved in criminal activities associated with terrorism.

**ROUTINE USES OF RECORDS MAINTAINED IN THE SYSTEM, INCLUDING CATEGORIES OF USERS AND THE PURPOSES OF SUCH USES:**

In addition to those disclosures generally permitted under 5 U.S.C. 552a(b) of the Privacy Act, all or a portion of the records or information contained in this system may be disclosed outside DHS as a routine use pursuant to 5 U.S.C. 552a(b)(3) as follows:

A. To the Department of Justice (including United States Attorney Offices) or other Federal agency conducting litigation or in proceedings before any court, adjudicative or administrative body, when it is necessary to the litigation and one of the following is a party to the litigation or has an interest in such litigation:

1. DHS or any component thereof;
2. Any employee of DHS in his/her official capacity;
3. Any employee of DHS in his/her individual capacity where DOJ or DHS has agreed to represent the employee; or
4. The United States or any agency thereof, is a party to the litigation or has an interest in such litigation, and DHS determines that the records are both relevant and necessary to the litigation and the use of such records is compatible with the purpose for which DHS collected the records.

B. To a congressional office from the record of an individual in response to an inquiry from that congressional office made at the request of the individual to whom the record pertains.

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

D. To an agency, organization, or individual for the purpose of performing

audit or oversight operations as authorized by law, but only such information as is necessary and relevant to such audit or oversight function.

E. To appropriate agencies, entities, and persons when:

1. DHS suspects or has confirmed that the security or confidentiality of information in the system of records has been compromised;

2. The Department has determined that as a result of the suspected or confirmed compromise there is a risk of harm to economic or property interests, identity theft or fraud, or harm to the security or integrity of this system or other systems or programs (whether maintained by DHS or another agency or entity) or harm to the individuals that rely upon the compromised information; and

3. The disclosure made to such agencies, entities, and persons is reasonably necessary to assist in connection with DHS's efforts to respond to the suspected or confirmed compromise and prevent, minimize, or remedy such harm.

F. To contractors and their agents, grantees, experts, consultants, and others performing or working on a contract, service, grant, cooperative agreement, or other assignment for DHS, when necessary to accomplish an agency function related to this system of records. Individuals provided information under this routine use are subject to the same Privacy Act requirements and limitations on disclosure as are applicable to DHS officers and employees.

G. To an appropriate Federal, State, Tribal, local, international, or foreign law enforcement agency or other appropriate public or private sector organization who is a participant in the Nationwide SAR Initiative and authorized access through the NSI Shared Space for the purpose of supporting an authorized law enforcement, counterterrorism, national security, or homeland security function.

H. To Federal government counterterrorism agencies where DHS becomes aware of an indication of a threat or potential threat to national or international security, and where such use is to assist in anti-terrorism efforts.

I. To an organization or individual in either the public or private sector, either foreign or domestic, where there is a reason to believe that the recipient is or could become the target of a particular terrorist activity or conspiracy, to the extent the information is relevant to the protection of life, property or other vital interests of a data subject and disclosure is proper and consistent with the official

duties of the person making the disclosure.

**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. The records are stored on magnetic disc, tape, digital media, and CD-ROM.

**RETRIEVABILITY:**

Much of the data within this system does not pertain to an individual; rather, the information pertains to locations, geographic areas, facilities, and other things or objects not related to individuals. However, personal information may be captured. Personal data may be retrieved by name, Social Security number, any privacy fields noted under Categories of Records, and other identifiers listed under the Categories of Records section.

**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:**

DHS is in the process of developing a retention schedule for DHS ISE-SAR data. This retention schedule will be based upon the underlying retention schedules of the information identified in existing components' retention schedules. DHS components maintain the authority to withdraw and/or edit any and all ISE-SAR data that they have entered into the NSI Shared Space in accordance with their respective policies. The NSI Shared Space does not have any internal retention mandates independent of the retention policies of the DHS components that enter their information into the NSI Shared Space.

**SYSTEM MANAGER AND ADDRESS:**

Ronald Athmann (202) 447-4332, Office of Intelligence and Analysis, Department of Homeland Security, Washington, DC 20528.

**NOTIFICATION PROCEDURE:**

The Secretary of Homeland Security has exempted this system from the notification, access, and amendment procedures of the Privacy Act because it is a law enforcement system. However, DHS will consider individual requests to determine whether or not information may be released. Thus, 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 Headquarters or component's 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 ISE-SARs submitted by Federal, State, local, Tribal, and territorial agencies and private sector organizations who are NSI participants. The respective mission sets of DHS components are varied and entail coverage across multiple sectors. DHS components use a standardized technical approach across DHS to incorporate SAR data into the NSI Shared Space. DHS personnel, trained in the ISE-SAR program, will review component SARs and submit only those SAR data that meet the ISE-SAR Functional Standard to the NSI Shared Space.

**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 limitations set forth in 5 U.S.C. 552a(c)(3) and (4); (d); (e)(1), (e)(2), (e)(3), (e)(4)(G), (e)(4)(H), (e)(4)(I), (e)(5), (e)(8), and (e)(12); (f); (g)(1); and (h) of the Privacy Act pursuant to 5 U.S.C. 552a(j)(2). Additionally, 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) of the Privacy Act pursuant to 5 U.S.C. 552a(k)(2), and (k)(3).

Dated: September 7, 2010.

**Mary Ellen Callahan,**

*Chief Privacy Officer, Department of Homeland Security.*

[FR Doc. 2010-22636 Filed 9-9-10; 8:45 am]

**BILLING CODE 9110-9B-P**

**DEPARTMENT OF HOMELAND SECURITY**

[Docket ID FEMA-2010-0033]

**Federal Emergency Management Agency**

**Agency Information Collection Activities: Submission for OMB Review; Comment Request, OMB No. 1660-0030; Request for the Site Inspection and Landowners Authorization/Ingress-Egress Agreement**

**AGENCY:** Federal Emergency Management Agency, DHS.