determine whether or not the record within CIDR meets the requirements of the exemptions and, as appropriate, to disclose information that does not meet the requirements. This does not prevent the individual from gaining access to his records in the source systems noted below. Persons may seek access to records maintained in the source systems that feed into CIDR, currently CLAIMS 3, and in future releases, CLAIMS 4, RAPS, APSS, RNACS, and CIS.

Individuals seeking access to and notification of any record contained in this system of records, or seeking to contest its content, may submit a request in writing to the Chief Privacy Officer and to the USCIS FOIA/Privacy Act (PA) Officer whose contact information can be found at *http://www.dhs.gov/foia* under ''Contacts Information.'' 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, Washington, DC 20528–0655. Even if neither the Privacy Act nor the Judicial Redress Act provide a right of access, certain records about an individual may be available under the Freedom of Information Act.

When an individual is seeking records about himself or herself from this system of records or any other Departmental system of records, the request must conform with the Privacy Act regulations set forth in 6 CFR part 5. The individual must verify his or her identity, meaning that the individual must provide his or her full name, current address, and date and place of birth. The individual must sign the request, and the individual's 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, an individual may obtain forms for this purpose from the Chief Privacy Officer and Chief Freedom of Information Act Officer, *http://www.dhs.gov/foia* or 1–866–431–0486. In addition, the individual should:

- Explain why the individual believes the Department would have information on him or her;
- Identify which component(s) of the Department the individual believes may have the information about you;
- Specify when the individual believes the records would have been created; and
- Provide any other information that will help the FOIA staff determine which DHS component agency may have responsive records;

If an individual's request is seeking records pertaining to another living individual, he or she must include a statement from that individual certifying his/her agreement for the individual to access his/her records.

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

CONTESTING RECORD PROCEDURES:

For records covered by the Privacy Act or covered JRA records, see ''Record Access Procedures'' above. Any individual, regardless of immigration status, may file a request to access his or her information under the FOIA. Throughout the benefit determination process and prior to USCIS making a determination to deny a benefit request, USCIS provides individuals with the opportunity to address and correct the information.

NOTIFICATION PROCEDURES:

See ''Record Access Procedures.''

EXEMPTIONS PROMULGATED FOR THE SYSTEM:

The Secretary of Homeland Security has exempted this system from subsections (c)(3), (d), (e)(1), (e)(4)(G), (H), (I), and (f) of the Privacy Act, pursuant to 5 U.S.C. 552a (k)(1) and (k)(2).

Additionally, many of the functions in this system require retrieving records from law enforcement systems. When this system receives a record from another system exempted in that source system under 5 U.S.C. 552a(j)(2), DHS will claim the same exemptions for those records that are claimed for the original primary systems of records from which they originated and claims any additional exemptions set forth here.

HISTORY:

DHS/USCIS–012, United States Citizenship and Immigration Services—012 Citizenship and Immigration Data Repository, 75 FR 54642 (September 8, 2010). Final Rule for Privacy Act Exemptions, 75 FR 81371 (December 28, 2010).

Philip S. Kaplan,

Chief Privacy Officer, Department of Homeland Security.

[FR Doc. 2018–09235 Filed 4–30–18; 8:45 am]

BILLING CODE 4410–10–P

DEPARTMENT OF HOMELAND SECURITY

[Docket No. DHS–2018–0009]

Privacy Act of 1974; System of Records

AGENCY: Department of Homeland Security.

ACTION: Notice of a new system of records.

SUMMARY: In accordance with the Privacy Act of 1974, the Department of Homeland Security (DHS) proposes to establish a new DHS system of records titled, ''Department of Homeland Security/United States Coast Guard-032 Asset Logistics Management Information System (ALMIS) System of Records.'' This system of records allows the DHS/United States Coast Guard (USCG) to collect and maintain records on the maintenance, mission scheduling, and logistics for USCG aviation and surface (boats) assets. This newly established system will be included in the DHS inventory of record systems.

DATES: Submit comments on or before May 31, 2018. This new system will be effective upon publication. Routine uses will be effective May 31, 2018.

ADDRESSES: You may submit comments, identified by docket number DHS–2018–0009 by one of the following methods:

- *Federal e-Rulemaking Portal: http://www.regulations.gov*. Follow the instructions for submitting comments.
- *Fax:* 202–343–4010.
- *Mail:* Philip S. Kaplan, Chief Privacy Officer, Privacy Office, Department of Homeland Security, Washington, DC 20528–0655.

Instructions: All submissions received must include the agency name and docket number DHS–2018–0009. 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: Brian P. Burns, (202) 475–3507, *Brian.P.Burns@uscg.mil,* Acting Privacy Officer, Commandant (CG–6), United States Coast Guard, Mail Stop 7710, Washington, DC 20593.

For privacy questions, please contact: Philip S. Kaplan, (202) 343–1717, *privacy@hq.dhs.gov,* Chief Privacy Officer, Privacy Office, Department of Homeland Security, Washington, DC 20528–0655.

SUPPLEMENTARY INFORMATION:

I. Background

ALMIS is a legacy system that enables efficient, flexible, and cost-effective aircraft and surface force operations, logistics, and maintenance support. It supports data entry from the start of a mission, recording the mission execution, tracking crew events, asset aging, asset configuration, asset maintenance requirements, asset part replacements, warehouse activities, and procurement actions. In order to perform these functions, USCG must collect information to confirm the identities of the individuals assigned to the assets. This includes collecting name, rank, and contact information, as well as sensitive data elements such as Social Security number (SSN). The collection and maintenance of this information will allow DHS/USCG to perform its mission and primary duties, as outlined in 14 U.S.C. 2.

Currently, ALMIS retains all records. The records retention schedule disposition is currently pending with the National Archives and Records Administration (NARA).

Consistent with DHS's information sharing mission, information stored in DHS/USCG–032 Asset Logistics Management Information System may be shared with other DHS Components that have a need to know the information to carry out their national security, law enforcement, immigration, intelligence, or other homeland security functions. In addition, DHS/USCG may share information with appropriate Federal, state, local, tribal, territorial, foreign, or international government agencies consistent with the routine uses set forth in this system of records notice.

This newly established system will be included in DHS's inventory of record systems.

II. Privacy Act

The Privacy Act embodies fair information practice principles in a statutory framework governing the means by which Federal Government agencies collect, maintain, use, and disseminate 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 from 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 U.S. citizens and lawful permanent residents. Additionally, the Judicial Redress Act (JRA) provides covered persons with a statutory right to make requests for access and amendment to covered records, as defined by the JRA, along with judicial review for denials of such requests. In addition, the JRA prohibits disclosures of covered records, except as otherwise permitted by the Privacy Act.

Below is the description of the DHS/USCG–032 Asset Logistics Management Information System (ALMIS) 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 NAME AND NUMBER

Department of Homeland Security (DHS)/United States Coast Guard (USCG)-032 Asset Logistics Management Information System (ALMIS).

SECURITY CLASSIFICATION:

Unclassified, Sensitive, For Official Use Only.

SYSTEM LOCATION:

Records are maintained at the United States Coast Guard Headquarters in Washington, DC and field offices.

SYSTEM MANAGER(S):

Commandant (CG–4), United States Coast Guard, Mail Stop 7714, Washington, DC 20593.

AUTHORITY FOR MAINTENANCE OF THE SYSTEM:

14 U.S.C. 2; 14 U.S.C. 93; 14 U.S.C. 102; 14 U.S.C. 141; 14 U.S.C. 632; 14 U.S.C. 648; 44 U.S.C. 3101; 44 U.S.C. 3534; Executive Order (E.O.) 9397, Numbering System for Federal Accounts Relating to Individual Persons, as amended by E.O. 13478, Amendments to Executive Order 9397 Relating to Federal Agency Use of Social Security Numbers; and the National Defense Authorization Act of 2014 (Pub. L. 113–66).

PURPOSE(S) OF THE SYSTEM:

The purpose of this system is to provide maintenance tracking, parts ordering/inventory, and mission information for USCG aviation and surface assets.

CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM:

USCG personnel (including military, Federal employees, and contractors) and non-DHS Federal employees whose home agencies have agreements in place with USCG to use its equipment (*e.g.,* U.S. Forest Service (USFS)).

CATEGORIES OF RECORDS IN THE SYSTEM:

USCG Military:
- SSN;
- Common Access Card number (CAC#);
- Personal Identification Number (PIN) for two-factor authentication;
- Name;
- Rate/rank;
- Employee Identification (EMPLID);
- Sector/group;
- Unit Operating Facilities Address Code (OPFAC);
- Work email address;
- Work phone number; and
- Digital signature.

Government Civilians:
- SSN;
- CAC#;
- PIN;
- Name;
- Civilian grade;
- EMPLID;
- Unit OPFAC;
- Work email address;
- Work phone number; and
- Digital signature.

Federal contractors:
- SSN;
- CAC#;
- PIN;
- Name;
- Unit OPFAC;
- Work email address;
- Work phone number;
- Digital signature;
- Contract number;
- Company name; and
- Period of contract performance.

USFS personnel:
- SSN;
- CAC#;
- PIN;
- Name;
- Civilian grade;
- EMPLID;
- Unit OPFAC;
- Work email address;
- Work phone number; and
- Digital signature.

RECORD SOURCE CATEGORIES:

Records are obtained from USCG personnel (including military, Federal employees, and contractors) and the United States Forest Service (USFS), or other agencies that have agreements in place with USCG to use its equipment.

ROUTINE USES OF RECORDS MAINTAINED IN THE SYSTEM, INCLUDING CATEGORIES OF USERS AND 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 (DOJ), including the U.S. Attorneys Offices, or other Federal agency conducting litigation or proceedings before any court, adjudicative, or administrative body, when it is relevant or 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 or former employee of DHS in his/her official capacity;

3. Any employee or former employee of DHS in his/her individual capacity, only when DOJ or DHS has agreed to represent the employee; or

4. The United States or any agency thereof.

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 (NARA) or General Services Administration pursuant to records management inspections being conducted under the authority of 44 U.S.C. 2904 and 2906.

D. To an agency or organization 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 there has been a breach of the system of records; (2) DHS has determined that as a result of the suspected or confirmed breach there is a risk of harm to individuals, DHS (including its information systems, programs, and operations), the Federal Government, or national security; 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 breach or to prevent, minimize, or remedy such harm.

F. To another Federal agency or Federal entity, when DHS determines that information from this system of records is reasonably necessary and otherwise compatible with the purpose of collection to assist the recipient agency or entity in (1) responding to a suspected or confirmed breach or (2) preventing, minimizing, or remedying the risk of harm to individuals, the recipient agency or entity (including its information systems, programs, and operations), the Federal Government, or national security, resulting from a suspected or confirmed breach.

G. 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.

H. To an appropriate Federal, state, tribal, local, international, or foreign law enforcement agency or other appropriate authority charged with investigating or prosecuting a violation or enforcing or implementing a law, rule, regulation, or order, when a record, either on its face or in conjunction with other information, indicates a violation or potential violation of law, which includes criminal, civil, or regulatory violations and such disclosure is proper and consistent with the official duties of the person making the disclosure.

I. To the United States Forest Service, or other agency that has an equipment-sharing agreement in place with USCG, for the purpose of verifying personnel authorized to utilize the system and to access aircraft maintenance and logistic records.

J. To the news media and the public, with the approval of the Chief Privacy Officer in consultation with counsel, when there exists a legitimate public interest in the disclosure of the information, when disclosure is necessary to preserve confidence in the integrity of DHS, or when disclosure is necessary to demonstrate the accountability of DHS's officers, employees, or individuals covered by the system, except to the extent the Chief Privacy Officer determines that release of the specific information in the context of a particular case would constitute a clearly unwarranted invasion of personal privacy.

POLICIES AND PRACTICES FOR STORAGE OF RECORDS:

DHS/USCG stores records in this system electronically or on paper in secure facilities in a locked drawer behind a locked door. The records may be stored on magnetic disc, tape, and digital media.

POLICIES AND PRACTICES FOR RETRIEVAL OF RECORDS:

USCG retrieves records be retrieved by name of individual, Social Security number (SSN), rank, Unit Operating Facilities Address Code (OPFAC), Employee Identification number (EMPLID), and Command Access Card (CAC) number.

POLICIES AND PRACTICES FOR RETENTION AND DISPOSAL OF RECORDS:

Currently, ALMIS retains all records. The records retention schedule disposition is currently pending with NARA.

ADMINISTRATIVE, TECHNICAL, AND PHYSICAL SAFEGUARDS:

DHS/USCG safeguards records in this system according to applicable rules and policies, including all applicable DHS automated systems security and access policies. DHS/USCG has imposed strict controls 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.

RECORD ACCESS PROCEDURES:

Individuals seeking access to and notification of any record contained in this system of records, or seeking to contest its content, may submit a request in writing to the Chief Privacy Officer and the United States Coast Guard Freedom of Information Act (FOIA) Officer, whose contact information can be found at *http://www.dhs.gov/foia* under ''Contacts Information.'' 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, Washington, DC 20528–0655. Even if neither the Privacy Act nor the Judicial Redress Act provide a right of access, certain records about the individual may be available under the Freedom of Information Act.

When seeking records about one's self from this system of records or any other Departmental system of records, the request must conform with the Privacy Act regulations set forth in 6 CFR part 5. The individual must first verify his or her identity, meaning that he or she must provide his or her full name, current address, and date and place of birth. The individual must sign the request, and the 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, an individual may obtain forms for this purpose from the Chief Privacy Officer and Chief Freedom of Information Act Officer, *http://www.dhs.gov/foia* or 1–866–431–

0486. In addition, the individual should:

• Explain why he or she believes the Department would have information being requested;

• Identify which Component(s) of the Department he or she believes may have the information;

• Specify when the individual believes the records would have been created; and

• Provide any other information that will help the FOIA staff determine which DHS Component agency may have responsive records.

If the request is seeking records pertaining to another living individual, the person seeking the records must include a statement from the subject individual certifying his/her agreement for the requestor to access his or her records.

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

CONTESTING RECORD PROCEDURES:

For records covered by the Privacy Act or covered JRA records, see ''Record Access Procedures'' above.

NOTIFICATION PROCEDURES:

See ''Record Access Procedures.''

EXEMPTIONS PROMULGATED FOR THE SYSTEM:

None.

HISTORY:

None.

Philip S. Kaplan,

Chief Privacy Officer, Department of Homeland Security.

[FR Doc. 2018–09231 Filed 4–30–18; 8:45 am]

BILLING CODE 9110–04–P

DEPARTMENT OF HOUSING AND URBAN DEVELOPMENT

[Docket No. FR–7001–N–21]

30-Day Notice of Proposed Information Collection: Choice Neighborhoods

AGENCY: Office of the Chief Information Officer, HUD.

ACTION: Notice.

SUMMARY: HUD submitted the proposed information collection requirement described below to the Office of Management and Budget (OMB) for review, in accordance with the Paperwork Reduction Act. The purpose of this notice is to allow for 30 days of public comment.

DATES: *Comments Due Date:* May 31, 2018.

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: HUD Desk Officer, Office of Management and Budget, New Executive Office Building, Washington, DC 20503; fax: 202–395–5806, Email: *OIRA Submission@omb.eop.gov*.

FOR FURTHER INFORMATION CONTACT: Colette Pollard, Reports Management Officer, QMAC, Department of Housing and Urban Development, 451 7th Street SW, Washington, DC 20410; email *Colette.Pollard@hud.gov,* or telephone 202–402–3400. This is not a toll-free number. Person with hearing or speech impairments may access this number through TTY by calling the toll-free Federal Relay Service at (800) 877–8339. Copies of available documents submitted to OMB may be obtained from Ms. Pollard.

SUPPLEMENTARY INFORMATION: This notice informs the public that HUD is seeking approval from OMB for the information collection described in Section A. The **Federal Register** notice that solicited public comment on the information collection for a period of 60 days was published on February 28, 2018 at 83 FR 8690.

A. Overview of Information Collection

Title of Information Collection: Choice Neighborhoods.

OMB Approved Number: 2577–0269.

Type of Request: Revision of currently approved collection.

Form Number: SF–424, SF–LLL, HUD 2880, HUD 53150, HUD 53152, HUD 53232, HUD 53151, HUD 53154, HUD–53233, HUD–53234, HUD–53238, HUD–53231, HUD–53235, HUD–53237, HUD–53236, HUD–53239, HUD–2530, HUD–2991, HUD–2995, HUD–53421, HUD–53230, HUD–52515, HUD–50163.

Description of the need for the information and proposed use: The information collection is required to administer the Choice Neighborhoods program, including applying for funds and grantee reporting.

Respondents (*i.e. affected public*): Potential applicants and grantees (which would include local governments, tribal entities, public housing authorities, nonprofits, and for-profit developers that apply jointly with a public entity).

Estimated Number of Respondents: 264 annually.

Estimated Number of Responses: 440 annually.

Frequency of Response: Frequency of response varies depending on what information is being provided (*e.g.,* once per year for applications and four times per year for grantee reporting).

Average Hours per Response: Burden hours per response varies depending on what information is being provided (*e.g.,* Choice Neighborhoods Implementation grant application: 71.09; Choice Neighborhoods Planning grant application: 36.59; Choice Neighborhoods information collections unrelated to the NOFA, including grantee reporting and program management: 14.58).

Total Estimated Annual Burden and Cost: Total burden hours is estimated to be 4,562.45. Total burden cost is estimated to be $192,672.26.

B. Solicitation of Public Comment

This notice is soliciting comments from members of the public and affected parties concerning the collection of information described in Section A on the following:

(1) Whether the proposed collection of information is necessary for the proper performance of the functions of the agency, including whether the information will have practical utility;

(2) The accuracy of the agency's estimate of the burden of the proposed collection of information;

(3) Ways to enhance the quality, utility, and clarity of the information to be collected; and

(4) Ways to minimize the burden of the collection of information on those who are to respond: Including through the use of appropriate automated collection techniques or other forms of information technology, *e.g.,* permitting electronic submission of responses.

HUD encourages interested parties to submit comment in response to these questions.

Authority: Section 3507 of the Paperwork Reduction Act of 1995, 44 U.S.C. Chapter 35.

Dated: April 24, 2018.

Colette Pollard,

Department Reports Management Officer, Office of the Chief Information Officer.

[FR Doc. 2018–09179 Filed 4–26–18; 4:15 pm]

BILLING CODE 4210–67–P

DEPARTMENT OF HOUSING AND URBAN DEVELOPMENT

[Docket No. FR–7001–N–22]

30-Day Notice of Proposed Information Collection: Application for Displacement/Relocation/Temporary Relocation Assistance for Persons

AGENCY: Office of the Chief Information Officer, HUD.

ACTION: Notice.