no later than 30 days after either the date the TSP provides the participant with a notice reflecting the error or the date the TSP makes available on its Web site a participant statement reflecting the error, whichever is earlier. The employing agency must promptly notify the TSP that the participant is entitled to breakage.

(3) If a participant or beneficiary fails to file a claim for breakage for errors involving incorrect dates of birth in a timely manner, the employing agency may nevertheless, in its sound discretion, pay breakage on any such error that is brought to its attention.

* * * * *

■ 6. Amend § 1605.22, by revising paragraphs (b)(2), (c)(2), and (c)(3) to read as follows:

§ 1605.22 Claims for correction of Board or TSP record keeper errors; time limitations.

* * * * *

(b) * * *

(1) * * *

(2) For errors involving an investment in the wrong fund caused by Board or TSP record keeper error, the Board or the TSP record keeper must promptly pay breakage if it is discovered within 30 days of the issuance of the most recent TSP participant (or loan) statement, transaction confirmation, or other notice that reflected the error, whichever is earlier. If it is discovered after that time, the Board or TSP record keeper may use its sound discretion in deciding whether to pay breakage, but, in any event, must act promptly in doing so.

(c) * * *

(1) * * *

(2) For errors involving an investment in the wrong fund of which a participant or beneficiary has knowledge, he or she may file a claim for breakage with the Board or TSP record keeper no later than 30 days after the TSP provides the participant with a transaction confirmation or other notice reflecting the error, or makes available on its Web site a participant statement reflecting the error, whichever is earlier. The Board or TSP record keeper must promptly pay breakage for such errors.

(3) If a participant or beneficiary fails to file a claim for breakage concerning an error involving an investment in the wrong fund in a timely manner, the Board or TSP record keeper may nevertheless, in its sound discretion, pay breakage for any such error that is brought to its attention.

* * * * *

■ 7. Amend § 1605.31 by revising paragraph (d) to read as follows:

§ 1605.31 Contributions missed as a result of military service.

* * * * *

(d) *Breakage.* The employee is entitled to breakage on agency contributions made under paragraph (c) of this section. The employee will elect to have the calculation based on either the contribution allocation(s) on file for the participant during the period of military service or the default investment fund in effect for the participant; the participant must make this election at the same time his or her makeup schedule is established pursuant to § 1605.11(c).

[FR Doc. 2015–20273 Filed 8–14–15; 8:45 am]

BILLING CODE 6760–01–P

DEPARTMENT OF HOMELAND SECURITY

Office of the Secretary

6 CFR Part 5

[Docket No. DHS–2015–0046]

Privacy Act of 1974: Implementation of Exemptions; Department of Homeland Security DHS/CBP–001, Import Information System, System of Records, System of Records

AGENCY: Privacy Office, Department of Homeland Security.

ACTION: Notice of proposed rulemaking.

SUMMARY: The Department of Homeland Security is giving concurrent notice for the newly established ''Department of Homeland Security/CBP–001, Import Information System, System of Records'' and this proposed rulemaking. In accordance with the Privacy Act of 1974, the Department of Homeland Security concurrently proposes to consolidate, update, and rename two current Department of Homeland Security systems of records titled, ''Department of Homeland Security/U.S. Customs and Border Protection, DHS/CBP–001 Automated Commercial Environment/International Trade Data System System of Records'' and ''Department of Homeland Security/U.S. Customs and Border Protection, DHS/CBP–015 Automated Commercial System System of Records'' as one new system of records. The consolidated system of records notice will be titled, ''Department of Homeland Security/U.S. Customs and Border Protection, DHS/CBP–001 Import Information System System of Records.'' This system of records will continue to collect and maintain records on all commercial goods imported into the United States, as well as information pertaining to the carrier, broker, importer, and other persons associated with the manifest, import, or commercial entry transactions for the goods. In this proposed rulemaking, the Department proposes to exempt portions of the system of records from one or more provisions of the Privacy Act because of criminal, civil, and administrative enforcement requirements.

DATES: Comments must be received on or before September 16, 2015.

ADDRESSES: You may submit comments, identified by docket number DHS–2015–0046, 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:* Karen L. Neuman, 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 notice. 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: John Connors (202) 344–1610, CBP Privacy Officer, Office of the Commissioner, U.S. Customs and Border Protection, Washington, DC 20229. For privacy questions, please contact: Karen L. Neuman, (202) 343–1717, Chief Privacy Officer, Privacy Office, Department of Homeland Security, Washington, DC 20528–0655.

SUPPLEMENTARY INFORMATION:

I. Background

In accordance with the Privacy Act of 1974, 5 U.S.C. 552a, the Department of Homeland Security (DHS), U.S. Customs and Border Protection (CBP) proposes to consolidate, update, and rename as one system of records notice (SORN) the information currently contained in two DHS SORNs titled, ''DHS/CBP–001 Automated Commercial Environment/International Trade Data System (ACE/ITDS) System of Records'' (71 FR 3109, January 19, 2006) and ''DHS/CBP–015 Automated Commercial System (ACS) System of Records'' (73 FR 77759, December 19, 2008) . This new SORN, entitled ''DHS/CBP–001 Import Information System (IIS),'' will inform the public about changes to the

categories of individuals, categories of records, and routine uses contained in the consolidation of the former ACS and ACE/ITDS SORNs.

ACS, a decades old trade information database and information technology (IT) system, was deployed to track, control, and process all commercial goods imported into the United States. ACE, part of a multi-year modernization effort since 2001 to replace ACS, continues to be designed to manage CBP's import trade data and related transaction information. ACE/ITDS serves three sets of core stakeholders: The internal DHS/CBP users, Participating Government Agencies (PGA), and the trade community. ACE is the IT backbone for the ITDS, an interagency initiative formalized under the SAFE Port Act of 2006 to create a single window for the trade community and PGAs involved in importing and exporting. DHS/CBP has provided notice to the public and trade community that in the future, ACS, the IT system, will be fully phased out and replaced by ACE. As such, and to simplify the trade community's and the public's understanding of how trade information will be handled after ACE implementation, DHS/CBP is publishing this Import Information System (IIS) SORN to identify a single repository for import trade information. DHS/CBP is also publishing a combined ACE–ITDS/ACS Privacy Impact Assessment on its Web site (*http://www.dhs.gov/privacy*) to inform the public of the operation and inter-connectedness of the IT systems, ACS and ACE, and to assess the privacy impact of these systems using the fair information practice principles. This IIS system of records allows DHS/CBP to collect and maintain records on all commercial goods imported into the United States, along with related information about persons associated with those transactions, and manifest information.

As part of this consolidation and issuance of IIS, the category of individuals and category of records sections in the former ACS and ACE–ITDS have been merged to account for the data in both IT systems, as well as paper records related to the information in these systems. The category of individuals section is amended to remove reference to DHS/CBP employees and employees of other federal agencies for purposes of maintaining their user access accounts to the ACE–ITDS Portal, because these individuals are now covered under a DHS-wide SORN, ''DHS/ALL–004 General Information Technology Access Account Records System (GITAARS) (77 FR 70792, November 27, 2012). The category of records for IIS will also include notations and results of examinations and document review for cleared merchandise to clarify and better identify DHS and PGA-generated information related to the processing of the import entry transaction. Additionally, the category of records is being expanded to address the expansion of information DHS/CBP proposes to collect on its revised Importer ID Input Record (CBP Form 5106). DHS/CBP is adding required elements for the name (First, Middle, Last) and business contact information (job title and phone) of Senior Company Officers of the Importer; DHS/CBP is also adding optional data fields on the form for the Senior Officers to provide Social Security number (SSN) or Passport Number and Country of Issuance. These latter, optional data elements are to facilitate Importer screening and verification.

The authorities sections from the previous SORNs have been combined, reconciled to address duplication, and updated to account for expanded information collected about business associations as part of the ACE–ITDS Portal user account. The purpose section for IIS reflects an update to the combined purposes for ACS and ACE–ITDS and addresses DHS/CBP's broad use of its import trade transaction IT systems (ACS and ACE) to collect and manage records to track, control, and process all commercial goods imported into the United States.

Consistent with DHS's information-sharing mission, information stored in the DHS/CBP–001 Import Information System (IIS) may be shared with other DHS Components that have a need to know the information to carry out their national security, law enforcement, immigration, or other homeland security functions. In addition, information may be shared with appropriate federal, state, local, tribal, territorial, foreign, or international government agencies consistent with the routine uses set forth in this SORN and as otherwise authorized under the Privacy Act.

Information in IIS may be shared for the same routine uses as were previously published in ACS and ACE–ITDS, and are now updated in this document:

- ACS's former Routine Use K is now reclassified as Routine Use G.
  - Routine Use G permits sharing of data under the following circumstances: ''To appropriate federal, state, local, tribal, or foreign governmental agencies or multilateral governmental organizations responsible for investigating or prosecuting the violations of, or for enforcing or implementing, a statute, rule, regulation, order, license, or treaty where DHS determines that the information would assist in the enforcement of civil or criminal laws.''
- ACE–ITDS's former Routine Use 3 is now reclassified as Routine Use K.
  - Routine Use K permits sharing of data under the following circumstances: ''To a federal, state, local, tribal, territorial, foreign, or international agency, maintaining civil, criminal or other relevant enforcement information, or other pertinent information, which has requested information relevant to or necessary to the requesting agency's or the bureau's hiring or retention of an individual, or issuance of a security clearance, license, contract, grant, or other benefit.''

Additionally, DHS/CBP is adding another routine use to IIS, Routine Use R, to provide explicit coverage for the mandated release of Manifest Information as set forth in section 1431 of title 19, United States Code and implemented through title 19, Code of Federal Regulations, part 103:

- Routine Use R permits sharing of data under the following circumstances: ''To paid subscribers, in accordance with applicable regulations, for the purpose of providing access to manifest information as set forth in 19 U.S.C. 1431.''

DHS/CBP will not assert any exemptions with regard to information provided by or on behalf of an individual. However, this data may be shared with law enforcement and/or intelligence agencies pursuant to the routine uses identified in the IIS SORN and as otherwise authorized under the Privacy Act. The Privacy Act requires that DHS maintain an accounting of such disclosures. Disclosing the fact that a law enforcement and/or intelligence agency has sought particular records may interfere with or disclose techniques and procedures related to ongoing law enforcement investigations. As such, 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 updated 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 personally identifiable information. 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 the 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. 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 non-immigrant aliens.

The Privacy Act allows government agencies to exempt certain records from the access and amendment provisions. If an agency claims an exemption, however, it must issue a Notice of Proposed Rulemaking to make clear to the public the reasons why a particular exemption is claimed.

DHS is claiming exemptions from certain requirements of the Privacy Act for DHS/CBP–001 Import Information System System of Records.

No exemption shall be asserted with respect to information maintained in the system as it relates to data submitted by or on behalf of a person who travels to visit the United States, nor shall an exemption be asserted with respect to the resulting determination (authorized to travel, not authorized to travel, pending).

Some information in DHS/CBP–001 Import Information System System of Records relates to official DHS national security, law enforcement or intelligence activities. This system may contain records or information pertaining to the accounting of disclosures made from IIS to other law enforcement or intelligence agencies (Federal, State, local, foreign, international, or tribal) in accordance with the published routine uses. For the accounting of these disclosures only, in accordance with 5 U.S.C. 552a(j)(2) and (k)(2), DHS will claim the original exemptions for these records or information from subsection (c)(3), (e)(8), and (g) of the Privacy Act of 1974, as amended, as necessary and appropriate to protect such information. Moreover, DHS will add this exemption to Appendix C to 6 CFR part 5, DHS Systems of Records Exempt from the Privacy Act. Such exempt records or information may be law enforcement or national security investigation records, law enforcement activity and encounter records, or terrorist screening records.

DHS needs these exemptions in order to protect information relating to law enforcement investigations from disclosure to subjects of investigations and others who could interfere with investigatory and law enforcement activities. Specifically, the exemptions are required to: Preclude subjects of investigations from frustrating the investigative process; avoid disclosure of investigative techniques; protect the identities and physical safety of confidential informants and of law enforcement personnel; ensure DHS's and other federal agencies' ability to obtain information from third parties and other sources; protect the privacy of third parties; and safeguard sensitive information.

Nonetheless, DHS will examine each request on a case-by-case basis, and, after conferring with the appropriate component or agency, may waive applicable exemptions in appropriate circumstances and where it would not appear to interfere with or adversely affect the law enforcement or national security investigation.

Again, DHS will not assert any exemption with respect to information maintained in the system that is collected from a person and submitted by that person's air or vessel carrier, if that person, or his or her agent, seeks access or amendment of such information.

List of Subjects in 6 CFR Part 5

Freedom of information, Privacy.

For the reasons stated in the preamble, DHS proposes to amend Chapter I of Title 6, Code of Federal Regulations, as follows:

PART 5—DISCLOSURE OF RECORDS AND INFORMATION

■ 1. The authority citation for Part 5 continues to read as follows:

Authority: Pub. L. 107–296, 116 Stat. 2135, 6 U.S.C. 101 *et seq.;* 5 U.S.C. 301. Subpart A also issued under 5 U.S.C. 552.

■ 2. At the end of Appendix C to Part 5, add paragraph ''74'' to read as follows:

Appendix C to Part 5—DHS Systems of Records Exempt From the Privacy Act.

* * * * *

74. DHS/CBP–001, Import Information System (IIS). A portion of the following system of records is exempt from 5 U.S.C. 552a(c)(3), (e)(8), and (g)(1) pursuant to 5 U.S.C. 552a(j)(2), and from 5 U.S.C. 552a(c)(3) pursuant to 5 U.S.C. 552a(k)(2). Further, no exemption shall be asserted with respect to information maintained in the system as it relates to data submitted by or on behalf of a person who travels to visit the United States and crosses the border, nor shall an exemption be asserted with respect to the resulting determination (approval or denial). After conferring with the appropriate component or agency, DHS may waive applicable exemptions in appropriate circumstances and where it would not appear to interfere with or adversely affect the law enforcement purposes of the systems from which the information is recompiled or in which it is contained. Exemptions from the above particular subsections are justified, on a case-by-case basis to be determined at the time a request is made, when information in this system of records is may impede a law enforcement, intelligence activities and national security investigation:

(a) From subsection (c)(3) (Accounting for Disclosure) because making available to a record subject the accounting of disclosures from records concerning him or her would specifically reveal any investigative interest in the individual. Revealing this information could reasonably be expected to compromise ongoing efforts to investigate a violation of U.S. law, including investigations of a known or suspected terrorist, by notifying the record subject that he or she is under investigation. This information could also permit the record subject to take measures to impede the investigation, *e.g.,* destroy evidence, intimidate potential witnesses, or flee the area to avoid or impede the investigation.

(b) From subsection (e)(8) (Notice on Individuals) because to require individual notice of disclosure of information due to compulsory legal process would pose an impossible administrative burden on DHS and other agencies and could alert the subjects of counterterrorism or law enforcement investigations to the fact of those investigations when not previously known.

(c) From subsection (g)(1) (Civil Remedies) to the extent that the system is exempt from other specific subsections of the Privacy Act.

Dated: July 31, 2015.

Karen L. Neuman,

Chief Privacy Officer, Department of Homeland Security.

[FR Doc. 2015–19726 Filed 8–14–15; 8:45 am]

BILLING CODE 9111–14–P

NUCLEAR REGULATORY COMMISION

10 CFR Chapter I

[NRC–2015–0176]

Abnormal Occurrence Reports

AGENCY: Nuclear Regulatory Commission.

ACTION: Proposed revision to policy statement; request for comments.

SUMMARY: The U.S. Nuclear Regulatory Commission (NRC) is proposing revisions to its policy statement on reporting abnormal occurrences (AO) to Congress. The proposed revisions would clarify and restructure the criteria used by the NRC and Agreement States for determining whether to consider an incident or event as an AO. The proposed revisions to the policy statement would ensure consistency with current NRC guidance and