(c) From subsection (e)(1) (Relevancy and Necessity of Information) because in the course of investigations into potential violations of Federal law, the accuracy of information obtained or introduced occasionally may be unclear or the information may not be strictly relevant or necessary to a specific investigation. In the interests of effective law enforcement, it is appropriate to retain all information that may aid in establishing patterns of unlawful activity.

(d) From subsection (e)(2) (Collection of Information from Individuals) because requiring that information be collected from the subject of an investigation would alert the subject to the nature or existence of an investigation, thereby interfering with the related investigation and law enforcement activities.

(e) From subsection (e)(3) (Notice to Subjects) because providing such detailed information would impede law enforcement in that it could compromise investigations by: Revealing the existence of an otherwise confidential investigation and thereby provide an opportunity for the subject of an investigation to conceal evidence, alter patterns of behavior, or take other actions that could thwart investigative efforts; reveal the identity of witnesses in investigations, thereby providing an opportunity for the subjects of the investigations or others to harass, intimidate, or otherwise interfere with the collection of evidence or other information from such witnesses; or reveal the identity of confidential informants, which would negatively affect the informant's usefulness in any ongoing or future investigations and discourage members of the public from cooperating as confidential informants in any future investigations.

(f) From subsections (e)(4)(G), (H), and (I) (Agency Requirements), and (f) (Agency Rules) because portions of this system are exempt from the individual access provisions of subsection (d) for the reasons noted above, and therefore DHS is not required to establish requirements, rules, or procedures with respect to such access. Providing notice to individuals with respect to existence of records pertaining to them in the system of records or otherwise setting up procedures pursuant to which individuals may access and view records pertaining to themselves in the system would undermine investigative efforts and reveal the identities of witnesses, and potential witnesses, and confidential informants.

(g) From subsection (e)(5) (Collection of Information) because in the collection of information for law enforcement purposes it is impossible to determine in advance what information is accurate, relevant, timely, and complete. Compliance with (e)(5) would preclude DHS agents from using their investigative training and exercise of good judgment to both conduct and report on investigations.

(h) From subsection (e)(8) (Notice on Individuals) because compliance would interfere with DHS' ability to obtain, serve, and issue subpoenas, warrants, and other law enforcement mechanisms that may be filed under seal, and could result in disclosure of investigative techniques, procedures, and evidence.

(i) From subsection (g) to the extent that the system is exempt from other specific subsections of the Privacy Act relating to individuals' rights to access and amend their records contained in the system. Therefore DHS is not required to establish rules or procedures pursuant to which individuals may seek a civil remedy for the agency's: Refusal to amend a record; refusal to comply with a request for access to records; failure to maintain accurate, relevant timely and complete records; or failure to otherwise comply with an individual's right to access or amend records.

Dated: December 10, 2008.

Hugo Teufel III,

Chief Privacy Officer, Department of Homeland Security.

[FR Doc. E8–29876 Filed 12–18–08; 8:45 am]

BILLING CODE 4410–10–P

DEPARTMENT OF HOMELAND SECURITY

Office of the Secretary

6 CFR Part 5

[Docket No DHS–2008–0195]

Privacy Act of 1974: Implementation of Exemptions; U.S. Customs and Border Protection—015 Automated Commercial System

AGENCY: Privacy Office, DHS.

ACTION: Notice of proposed rulemaking.

SUMMARY: The Department of Homeland Security is amending its regulations to exempt portions of a system of records from certain provisions of the Privacy Act. Specifically, the Department proposes to exempt portions of the CBP Automated Commercial System (ACS) from one or more provisions of the Privacy Act because of criminal, civil, and administrative enforcement requirements.

DATES: The public is invited to submit comments by January 20, 2009.

ADDRESSES: You may submit comments, identified by docket number DHS–2008–0195 by one of the following methods:

- *Federal e-Rulemaking Portal: http://www.regulations.gov.* Follow the instructions for submitting comments.
- *Fax:* 1–866–466–5370.
- *Mail:* Hugo Teufel III, Chief Privacy Officer, Privacy Office, Department of Homeland Security, Washington, DC 20528.

FOR FURTHER INFORMATION CONTACT: For general questions please contact: Laurence E. Castelli (202–325–0280), Chief, Privacy Act Policy and Procedures Branch, U.S. Customs and Border Protection, Regulations and Rulings, Office of International Trade, 1300 Pennsylvania Ave., NW., Washington, DC 20229. For privacy issues please contact: Hugo Teufel III (703–235–0780), Chief Privacy Officer, Privacy Office, U.S. Department of Homeland Security, Washington, DC 20528.

SUPPLEMENTARY INFORMATION:

Background

The Department of Homeland Security (DHS), elsewhere in this edition of the **Federal Register**, published a Privacy Act system of records notice describing records in the Automated Commercial System (ACS).

To help prevent terrorist weapons from being transported to the United States, vessel carriers bringing cargo to the United States are required to transmit certain information to Customs and Border Protection (CBP) about the cargo they are transporting prior to lading that cargo at foreign ports of entry. CBP is issuing an interim final rule that requires both importers and carriers to submit additional information pertaining to cargo to CBP before the cargo is brought into the United States by vessel. This information must be submitted to CBP by way of a CBP-approved electronic data interchange system. The required information is necessary to improve CBP's ability to identify high-risk shipments so as to prevent smuggling and ensure cargo safety and security, as required by section 203 of the Security and Accountability for Every (SAFE) Port Act of 2006 and section 343(a) of the Trade Act of 2002, as amended by the Maritime Transportation Security Act of 2002.

The proposed rule was known to the trade as both the ''Importer Security Filing proposal'' and the ''10 + 2 proposal.'' The name ''10 + 2'' is shorthand for the number of advance data elements CBP was proposing to collect. Carriers would be generally required to submit two additional data elements—a vessel stow plan and container status messages regarding certain events relating to containers loaded on vessels destined to the United States—to the elements they are already required to electronically transmit in advance (the ''2'' of ''10 + 2''); and importers, as defined in the proposed regulations, would be required to submit ten data elements—an Importer Security Filing containing ten data elements (the ''10'' of ''10 + 2'').

The Automated Commercial System (ACS) is the comprehensive system used

by U.S. Customs and Border Protection to track, control, and process all commercial goods imported into the United States. ACS is a sophisticated and integrated large-scale business-oriented system which employs multiple modules to perform discrete aspects of its functionality: including receiving data transmissions from a variety of parties involved in international commercial transactions, and providing CBP with the capability to track both the transport transactions and the financial transactions associated with the movement of merchandise through international commerce. Through the use of Electronic Data Interchange (EDI), ACS facilitates merchandise processing, significantly cuts costs, and reduces paperwork requirements for both Customs and the importing community.

ACS has two principal methods for electronic data interchange, the Automated Broker Interface (ABI) and the Automated Manifest System (AMS). Under the ''10 + 2'' program, importers who submit the Importer Security Filing (ISF), will use either ABI or Vessel AMS to provide their information to CBP. ACS, upon receipt of the ISF, will transfer the data to the Automated Targeting System (ATS) for screening and targeting purposes. Once screened the ISF data will be returned with embedded targeting links to ACS to be maintained in accordance with the ACS stated retention policy.

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).

This system may contain records or information pertaining to the accounting of disclosures made from ACS to other law enforcement 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: Public Law 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 the following new paragraph ''14'':

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

* * * * *

14. DHS/CBP–015, Automated Commercial System (ACS). A portion of the following system of records is exempt from 5 U.S.C. 552a(c)(3), (e)(8), and (g) pursuant to 5 U.S.C. 552a(j)(2) and (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 may impede a law enforcement or 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) (Civil Remedies) to the extent that the system is exempt from other specific subsections of the Privacy Act.

Dated: December 10, 2008.

Hugo Teufel III,

Chief Privacy Officer, Department of Homeland Security.

[FR Doc. E8–29839 Filed 12–18–08; 8:45 am]

BILLING CODE 4410–10–P

DEPARTMENT OF HOMELAND SECURITY

Office of the Secretary

6 CFR Part 5

[Docket No. DHS–2008–0171]

Privacy Act of 1974: Implementation of Exemptions; DHS/CBP–009 Nonimmigrant Inspection System

AGENCY: Privacy Office, Department of Homeland Security.

ACTION: Notice of proposed rulemaking.

SUMMARY: The Department of Homeland Security is amending its regulations to exempt portions of a system of records from certain provisions of the Privacy Act. Specifically, the Department