subsections are justified, on a case-by-case basis to be determined at the time a request is made, for the following reasons:

(a) From subsection (c)(3) and (4) (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 known or suspected criminal or terrorist, or other person of interest, 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. Exemptions from these particular subsections are justified, on a case-by-case basis to be determined at the time a request is made, for the following reasons: (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 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 (c)(4) (Accounting for Disclosure, notice of dispute) because certain records in this system are exempt from the access and amendment provisions of subsection (d), this requirement to inform any person or other agency about any correction or notation of dispute that the agency made with regard to those records, should not apply.

(c) From subsections (d)(1), (2), (3), and (4) (Access to Records) because these provisions concern individual access to and amendment of certain records contained in this system, including law enforcement, counterterrorism, and investigatory records. Compliance with these provisions could alert the subject of an investigation to the fact and nature of the investigation, and/or the investigative interest of intelligence or law enforcement agencies; compromise sensitive information related to law enforcement, including matters bearing on national security; interfere with the overall law enforcement process by leading to the destruction of evidence, improper influencing of witnesses, fabrication of testimony, and/or flight of the subject; could identify a confidential source; reveal a sensitive investigative or intelligence technique; or constitute a potential danger to the health or safety of law enforcement personnel, confidential informants, and witnesses. Amendment of these records would interfere with ongoing counterterrorism or law enforcement investigations and analysis activities and impose an impossible administrative burden by requiring investigations, analyses, and reports to be continuously reinvestigated and revised.

(d) From subsection (e)(1) (Relevancy and Necessity of Information) because it is not always possible for DHS or other agencies to know in advance what information is relevant and necessary for it to complete screening of cargo, conveyances, and passengers. Information relating to known or suspected criminals or terrorists or other persons of interest, is not always collected in a manner that permits immediate verification or determination of relevancy to a DHS purpose. For example, during the early stages of an investigation, it may not be possible to determine the immediate relevancy of information that is collected—only upon later evaluation or association with further information, obtained subsequently, may it be possible to establish particular relevance to a law enforcement program. Lastly, this exemption is required because DHS and other agencies may not always know what information about an encounter with a known or suspected criminal or terrorist or other person of interest will be relevant to law enforcement for the purpose of conducting an operational response.

(e) From subsection (e)(2) (Collection of Information from Individuals) because application of this provision could present a serious impediment to counterterrorism or other law enforcement efforts in that it would put the subject of an investigation, study or analysis on notice of that fact, thereby permitting the subject to engage in conduct designed to frustrate or impede that activity. The nature of counterterrorism, and law enforcement investigations is such that vital information about an individual frequently can be obtained only from other persons who are familiar with such individual and his/her activities. In such investigations it is not feasible to rely solely upon information furnished by the individual concerning his own activities.

(f) From subsection (e)(3) (Notice to Subjects), to the extent that this subsection is interpreted to require DHS to provide notice to an individual if DHS or another agency receives or collects information about that individual during an investigation or from a third party. Should the subsection be so interpreted, exemption from this provision is necessary to avoid impeding counterterrorism or other law enforcement efforts by putting the subject of an investigation, study or analysis on notice of that fact, thereby permitting the subject to engage in conduct intended to frustrate or impede that activity.

(g) From subsections (e)(4)(G), (H) and (I) (Agency Requirements) because portions of this system are exempt from the access and amendment provisions of subsection (d).

(h) From subsection (e)(5) (Collection of Information) because many of the records in this system coming from other systems of records are derived from other domestic and foreign agency record systems and therefore it is not possible for DHS to vouch for their compliance with this provision; however, the DHS has implemented internal quality assurance procedures to ensure that data used in its screening processes is as complete, accurate, and current as possible. In addition, in the collection of information for law enforcement and counterterrorism purposes, it is impossible to determine in advance what information is accurate, relevant, timely, and complete. With the passage of time, seemingly irrelevant or untimely information may acquire new significance as further investigation brings new details to light. The restrictions imposed by (e)(5) would limit the ability of those agencies' trained investigators and intelligence analysts to exercise their judgment in conducting investigations and impede the development of intelligence necessary for effective law enforcement and counterterrorism efforts.

(i) 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.

(j) From subsection (f) (Agency Rules) because portions of this system are exempt from the access and amendment provisions of subsection (d). Access to, and amendment of, system records that are not exempt or for which exemption is waived may be obtained under procedures described in the related SORN or Subpart B of this Part.

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

Dated: January 21, 2010.

Mary Ellen Callahan

Chief Privacy Officer, Department of Homeland Security.

[FR Doc. 2010–2201 Filed 2–2–10; 8:45 am]

BILLING CODE 9110–06–P

DEPARTMENT OF HOMELAND SECURITY

Office of the Secretary

6 CFR Part 5

[Docket No. DHS–2009–0052]

Privacy Act of 1974: Implementation of Exemptions; Department of Homeland Security/U.S. Customs and Border Protection—007 Border Crossing Information System of Records

AGENCY: Privacy Office, DHS.

ACTION: Final rule.

SUMMARY: The Department of Homeland Security is issuing a final rule to amend its regulations to exempt portions of a Department of Homeland Security/U.S. Customs and Border Protection system of records entitled the, "Department of Homeland Security/U.S. Customs and Border Protection—007 Border Crossing Information System of Records." Specifically, the Department exempts portions of the Department of Homeland Security/U.S. Customs and Border

Protection—007 Border Crossing Information System of Records from provisions of the Privacy Act because of criminal, civil, and administrative enforcement requirements.

DATES: *Effective Date:* This final rule is effective February 3, 2010.

FOR FURTHER INFORMATION CONTACT: For general questions please contact: Laurence E. Castelli (202–325–0280), Privacy Officer, U.S. Customs and Border Protection, Office of International Trade, Mint Annex, 799 Ninth Street, NW., Washington, DC 20001–4501. 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:

Background

The Department of Homeland Security (DHS) published a notice of proposed rulemaking in the **Federal Register,** 73 FR 43374, July 25, 2008, proposing to exempt portions of a system of records from provisions of the Privacy Act because of criminal, civil, and administrative enforcement requirements. The system of records is the DHS/U.S. Customs and Border Protection (CBP)—007 Border Crossing Information system. The DHS/CBP—007 Border Crossing Information system of records notice was published concurrently in the **Federal Register,** 73 FR 43457, July 25, 2008, and comments were invited on both the notice of proposed rulemaking and system of records notice. Comments were received on the notice of proposed rulemaking and system of records notice.

Public Comments

Forty-eight comments were received on the system of records notice (SORN). Of those forty-eight comments, three comments were submitted in duplicate, one comment was submitted in triplicate, and one comment was submitted in quintuplicate. Accordingly, after accounting for the repetitive submissions, thirty-nine original comments were received on the system of records notice. Additionally, the same commenter posted comments twice on the notice of proposed rulemaking (NPRM) however, it was only one comment. Therefore only one original comment was received on the NPRM. The thirty-nine comments received on the SORN focused primarily on opposition either to the entire DHS/CBP—007 Border Crossing Information system of records or to specific aspects of the system including opposition to the proposed length of time the records would be maintained and several of the routine uses listed for the system. Several comments stated opposition to the system because they alleged that the system was unconstitutional. The one comment on the NPRM was against the proposed Privacy Act exemptions because the commenter believed that not all records within DHS/CBP—007 Border Crossing Information system of records are law enforcement data and exempting the DHS/CBP—007 Border Crossing Information system of records information from the Privacy Act would make it extremely difficult to contest and/or fix errors in the data, a right which is provided for in the Privacy Act. DHS notes that several comments submitted in conjunction with the SORN expressed disagreement with DHS' use of the Privacy Act exemptions. However, the comments were not submitted in response to the NPRM. The following is a synopsis of the comments received and DHS' response.

General Comments

Comment: No records should be maintained on law abiding U.S. citizens. Lawful border crossing of U.S. citizens should not be tracked. The focus should be on illegal entrants and non-U.S. citizens.

Response: Throughout its 219 year history, and beginning with actions by the First Congress of the United States, CBP and its principal legacy components, the Immigration and Naturalization Service (INS) and the U.S. Customs Service, have possessed the authority to stop and search all persons, conveyances, and cargo attempting to cross the U.S. border. The DHS/CBP—007 Border Crossing Information system of records is a tool that is by utilized CBP in performance of its mission at U.S. borders. The responsibility of CBP at the U.S. borders encompasses all persons crossing the borders, including U.S. citizens.

Furthermore, as explained in the DHS/CBP—007 Border Crossing Information system of records, the system does not represent a new or expanded collection of information by CBP. Rather, CBP is providing increased information regarding the agency's historical practices.

Comment: This system should be classified. The collected information should only be used for National Security purposes.

Response: The DHS/CBP—007 Border Crossing Information system of records was published as part of DHS's ongoing effort to increase transparency regarding the collection of information at the Department. Accordingly, if the system were classified, the public would generally not have access to information in the system either under the Privacy Act or the Freedom of Information Act.

Moreover, in CBP's judgment the system's level of classification is commensurate with the type of information maintained in the system and the agency has put in place adequate measures to ensure the integrity of the system.

Comment: The system should not be exempted from the Freedom of Information Act.

Response: The system is not exempted from the Freedom of Information Act. The Privacy Act by its terms at 5 U.S.C. 552a(b)(2) specifically provides for access to information in a system of records, including exempt systems of records, through a request made under the Freedom of Information Act. In response to a Freedom of Information Act request, and in accordance with that statute, the government may exempt certain portions of responsive records from disclosure when providing an individual with information about him or herself.

Comment: Criminal penalties for misuse of data must be specified with no exceptions for government employees.

Response: The Privacy Act authorizes criminal penalties for misuse of data maintained in a system covered by the Privacy Act. 5 U.S.C. 552a(i). There are no exceptions for criminal conduct committed by government employees. Additionally, CBP identifies misuse of information in its information systems as a specific violation applicable to all CBP employees. Employees may be dismissed from CBP for mishandling or misusing information maintained in CBP's systems and may be subject to criminal or civil penalties.

Comment: The system should have an audit trail and information should only be accessed if there is need to know.

Response: This system has a clear audit trail of who has accessed the system and who has accessed what records, so that if there are concerns about an individual's use of the system it can be tracked. CBP's Office of Internal Affairs regularly reviews the use of the system to ensure it is being used properly. CBP recognizes the need to prevent misuse of any information it collects. Therefore, CBP has implemented several internal controls to mitigate threats to the integrity of its systems. Access to CBP's systems is governed by a strict policy that implements rights and responsibilities to information. This means that only CBP employees with a need to know have access to information that falls

within the performance of official duties. Furthermore, CBP requires that all employees participate in regular privacy awareness training to receive automated systems access and requires that employees periodically re-attend such training to continue their access. CBP also identifies misuse of information in information systems as a specific violation applicable to all CBP employees. Employees may be dismissed from CBP for mishandling or misusing information maintained in CBP's systems and may be subject to criminal or civil penalties.

Comment: DHS should have an updated System of Records Notice for TECS.

Response: A new system of records notice for TECS was published in December 2008. DHS/CBP—011 TECS (73 FR 77778, December 19, 2008).

Comment: The system security for the DHS/CBP—007 Border Crossing Information system of records data has not been adequately addressed.

Response: Multiple security measures are in place for data collected in DHS systems. CBP uses routers, firewall and intrusion detection systems to prevent unauthorized access to its systems. Any information stored via backup tape is protected through strict physical safeguards and other technical safeguards to ensure it cannot be inappropriately accessed.

Access and Redress Comments

Comment: Exempting information within the DHS/CBP—007 Border Crossing Information system of records from certain provisions of the Privacy Act will make it extremely difficult, if not impossible, for individuals to fix errors that show up in the database.

Response: CBP respectfully disagrees. CBP has not proposed exempting access to the DHS/CBP—007 Border Crossing Information system of records by individuals who have a system record that pertains to them. To the contrary, the DHS/CBP—007 Border Crossing Information system of records delineated procedures for contesting system records. The relevant section of the SORN states: "Requests to amend a record must be in writing and should be addressed to the CBP Customer Service Center (Rosslyn, VA), 1300 Pennsylvania Avenue, NW., Washington, DC 20229; Telephone (877) 227–5511; or through the "Questions" tab at *http://www.cbp.gov.xp.cgov/travel/customerservice.*" Requests should conform with the requirements of 6 CFR Part 5, Subpart B, which provides the rules for requesting access to Privacy Act records maintained by DHS and can be found at *http://www.dhs.gov/foia.* The envelope and letter should be clearly marked "Privacy Act Access Request." The request should include a general description of the records sought and must include the requester's full name, current address, and date and place of birth. The request must be signed and either notarized or submitted under penalty of perjury.

If individuals are uncertain what agency handles the information, they may seek redress through the DHS Traveler Redress Program (DHS TRIP) (72 FR 2294, January 18, 2007). DHS TRIP is a single point of contact for individuals who have inquiries or seek resolution regarding difficulties they experienced during their travel screening at transportation hubs, such as airports, seaports and train stations or at U.S. land borders. Through DHS TRIP, a traveler can request correction of erroneously stored data in other DHS databases through one application. Redress requests should be sent to: DHS Traveler Redress Inquiry Program, 601 South 12th Street, TSA–901, Arlington, VA 22202–4220 or online at *http://www.dhs.gov/trip.*

Retention Period Comments

Comment: The retention period is too long for records about people that have committed no crime.

Response: The fifteen-year and seventy-five year retention periods proposed for the DHS/CBP—007 Border Crossing Information system of records were determined in order to allow CBP to effectively pursue its law enforcement mission while addressing privacy concerns. The fifteen-year retention period will allow CBP to access the data when needed for a law enforcement purpose yet permit the removal of the data in a time period significantly shorter than other systems. The seventy-five year period for non-immigrant aliens will allow for proper administration of certain immigration benefits as well as other law enforcement purposes. Furthermore, it should be noted, that while the DHS/CBP—007 Border Crossing Information system of records information is maintained for a number of years, any access to the information will always require a "need to know" by any person accessing the information. Access by persons without a proper "need to know" may result in criminal penalties and/or disciplinary actions.

Routine Uses

Comment: Under the listed Routine Uses, potential interested parties with whom the DHS/CBP—007 Border Crossing Information system of records information may be shared, such as press, foreign governments, State, prospective employers, students, contractors, etc., is too broad and not consistent with the reason for collecting the information.

Response: CBP, and its predecessor agencies, INS and the U.S. Customs Service, have signed Memoranda of Understandings (MOUs) or entered into agreements with a wide variety of Federal, State, and local agencies with an interest in maintaining border security and law enforcement; similar arrangements are in place with other nations in the form of Customs Mutual Assistance Agreements (CMAAs) and other information-sharing agreements and arrangements. The terms of these arrangements specify the necessity of sharing information and highlight the fact that the types of information sharing described in the SORN are neither unique nor a new practice for border authorities. Additionally, all MOUs and other arrangements for the sharing of information contain specific provisions relating to the responsibilities of the receiving party to keep the information confidential, protected, and secure. DHS does not share PII with domestic or foreign governments or multilateral organizations which DHS is not confident will protect the privacy interests of the data subject.

The routine uses identified are consistent with CBP's role as a law enforcement agency that enforces over 400 statutes on behalf of more than 40 agencies in the Federal Government. DHS is charged in its authorizing statute, specifically section 892 of the Homeland Security Act of 2002, to facilitate the sharing of terrorist information across the government. In addition, The Intelligence Reform and Terrorism Prevention Act of 2004 required the President to establish an Information Sharing Environment "that facilitates the sharing of terrorism information." Following this enactment, on October 25, 2005, the President issued Executive Order 13388, directing that DHS and other agencies "promptly give access to * * * terrorism information to the head of each other agency that has counterterrorism functions" and establishing a mechanism for implementing the Information Sharing Environment.

In addition, routine use O. permits CBP to share information with the press where such a release would inform the public about the performance of CBP's border security mission, such as the release of information pertaining to an arrest of a person attempting to enter the United States with bomb making materials in the trunk of his/her car.

Such uses are consistent with CBP's and DHS's overall law enforcement mission and serve to inform the public of how that mission is being accomplished. The particular routine use includes protections to balance the privacy interests of the person, whose information may be disclosed, with the public's right to know how the government is accomplishing its mission; this is the traditional balance that has always been struck between privacy and the public's right "to know what its government is up to."

Comment: The listed Routine Use for sharing for civil cases is not consistent with the mission against terrorism.

Response: The priority mission of CBP is to prevent terrorist and terrorists' weapons from entering the United States while facilitating legitimate travel and trade. In performance of its duties at the border, CBP, as a law enforcement agency, enforces over 400 statutes on behalf of more than 40 agencies in the Federal government. As such, the enforcement is not always criminal in nature and the sharing of DHS/CBP—007 Border Crossing Information system of records information in certain civil matters is understandable and consistent with CBP overall mission. Again, the DHS/CBP—007 Border Crossing Information system of records does not represent a new collection of information, and the routine use for civil purposes is consistent with CBP's historical treatment of this information.

Comment: Routine Uses are vague, overbroad and in some instances unnecessary.

Response: CBP is a law enforcement agency that enforces over 400 statutes on behalf of more than 40 agencies in the Federal government. In addition, CBP and its predecessor agencies, the INS and U.S. Customs Service, have signed MOUs or similar agreements with a wide variety of Federal, State and local agencies with border security and law enforcement interests and have similar accords with other nations in the form of CMAAs and other information sharing agreements or arrangements. The DHS/CBP—007 Border Crossing Information system of records Routine Uses are established to facilitate the sharing of specific information in furtherance of these shared law enforcement missions. The Routine Uses set forth at great length in the DHS/CBP—007 Border Crossing Information system of records also provides notice and transparency to the public as to nature and extent of the sharing of system data while containing appropriate parameters to limit the sharing to discrete purposes.

Privacy Act Statutory Comments

Comment: The system is not consistent with DHS principles of minimization and the Fair Information Practice Principles, specifically the length of retention, and as such should be amended to comply with these standards.

Response: CBP collects the minimum amount of information to properly record the border crossing event of an individual and facilitate CBP's border security, law enforcement and counterterrorism functions. Additionally, as discussed, the length of retention for information stored in the system was established to allow CBP to effectively pursue its border security, law enforcement and counterterrorism missions, while addressing privacy concerns.

Legal or Constitutional Comments

Comment: The system is unconstitutional. No records should be maintained in the system without probable cause that something is illegal nor should any records be shared without probable cause.

Response: As the U.S. Supreme Court has stated, "[i]t is axiomatic that the United States, as sovereign, has the inherent authority to protect, and a paramount interest in protecting, its territorial integrity." *United States* v. *Flores-Montano,* 541 U.S. 149, 153 (2004). Indeed, "the Government's interest in preventing the entry of unwanted persons and effects is at its zenith at the international border." *Id.* at 152. For this reason, the U.S. Supreme Court has held that stops and examinations are reasonable in the absence of a warrant or probable cause when they are conducted at the U.S. border, *see Carroll* v. *United States,* 267 U.S. 132, 153–54 (1925), and the "functional equivalent of the border," such as international airports, *see United States* v. *Irving,* 432 F.3d 401, 414 (2nd Cir. 2005).

Under the border search exception, routine stops and examinations conducted at the border are reasonable for Fourth Amendment purposes "simply by virtue of the fact that they occur at the border," and may be conducted without any individualized suspicion. *United States* v. *Ramsey,* 431 U.S. 606, 616 (1977). In addition, the Congress has specifically authorized CBP to collect the information maintained in the system. (*see,* e.g., 49 U.S.C. 44909 for information collected through the DHS/CBP—005 Advance Passenger Information system of records (73 FR 68435, November 18, 2008)).

Comment: The system is prohibited by the Privacy Act because it involves the collection and retention of records pertaining to activities protected by the First Amendment (i.e., "right of assembly").

Response: The broad authority of CBP to conduct activities relating to the entry or exit of persons or things into or out of the United States is codified at title 19 of the United States Code (U.S.C.), in sections 482, 1461, 1496, 1499, and 1581–83, and title 8, U.S.C. 1357. The system is a decision-support tool used by CBP officers to execute this lawful border enforcement authority and does not violate the right of citizens to assemble.

Privacy Act Exemptions Comments

Comment: There is no good reason for exempting a system of this type from the Privacy Act. All people for whom the government holds records ought to have the ability to review, amend, or correct information maintained by the government.

Response: The suggested exemptions from the Privacy Act listed in the DHS/CBP—007 Border Crossing Information NPRM (73 FR 43374, June 25, 2008) were selected to allow maximum transparency of data collected in the system while simultaneously allowing CBP to perform its border enforcement mission. For example, if the system did not have the proposed exemption from subsection (c)(3) of the Privacy Act, (5 U.S.C. 552a (c)(3)), the fact that certain DHS/CBP—007 Border Crossing Information system of records information was shared with a law enforcement agency could disclose to the subject of an investigation the existence of such an investigation, and reveal investigative interest on the part of DHS as well as the recipient agency. Disclosure of the accounting could possibly allow the suspect individual to impede the investigation and present a serious concern to successful law enforcement efforts and possibly compromise national security.

Public Recommendations

The submitted public comments offered numerous suggestions concerning DHS/CBP—007 Border Crossing Information system of records. Those suggestions ranged from cancellation of the system in its entirety, to proposed modifications to the system to enable it to meet concerns raised in the comments. Some of the suggested modifications included the following:

- Records not be shared without probable cause support by a court order (already in Privacy Act);
- Penalties for misuse of data (already exist);
- This system should be classified;

• Retention of records should only be in cases were there is a reasonable suspicion of criminal or terrorist activity;

• The retention period should be shortened;

• Records should only be maintained on non-U.S. Citizens; and

• Records should only be shared pursuant to a court order.

Responses to all these recommendations have been provided elsewhere within this document.

Upon careful review of the submitted public comments, having taken into consideration public comments resulting from this NPRM and SORN, as well as the Department's position on these public comments, DHS has determined that for the reasons stated, it is important that the exemptions remain in place. DHS will implement the rulemaking as proposed.

List of Subjects in 6 CFR Part 5

Freedom of information; Privacy.

■ For the reasons stated in the preamble, DHS amends 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. Subpart B also issued under 5 U.S.C. 552a.

■ 2. Add at the end of Appendix C to Part 5, Exemption of Record Systems under the Privacy Act, the following new paragraph "46":

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

* * * * *

46. The DHS/CBP—007 Border Crossing Information system of records will maintain border crossing information on travelers who are admitted or paroled into the United States. This information includes: certain biographical information; a photograph (if available); certain itinerary information provided by air and sea carriers and any other forms of passenger transportation, including rail, which is or may subsequently be mandated, or is or may be provided on a voluntary basis; and the time and location of the border crossing. This system may contain records or information pertaining to the accounting of disclosures made from DHS/CBP—007 Border Crossing Information system of records to agencies (Federal, State, Local, Tribal, Foreign, or International), in accordance with the published routine uses. For the accounting of these disclosures only, 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. 552(c)(3); (e)(8); and (g) pursuant to 5 U.S.C. 552a(j)(2). Additionally, for the accounting of these disclosures only, 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. 552(c)(3); (e)(8); and (g) pursuant to 5 U.S.C. 552a(k)(2). Further, no exemption shall be asserted with respect to biographical or travel information submitted by, and collected from, a person's travel documents or submitted from a government computer system to support or to validate those travel documents. 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 or records is recompiled or is created from information contained in other systems of records subject to exemptions for the following reasons:

(a) From subsection (c)(3) (Accounting for Disclosures) because making available to a record subject to 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 expect to compromise ongoing efforts to investigate a violation of U.S. law, including investigations of a known or suspected terrorist or criminal, or other person of interest, by notifying the record subject that he or she is under investigation. This information could also permit the record's 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 to 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: January 21, 2010.

Mary Ellen Callahan,

Chief Privacy Officer, Department of Homeland Security.

[FR Doc. 2010–2200 Filed 2–2–10; 8:45 am]

BILLING CODE 9110–06–P

NUCLEAR REGULATORY COMMISSION

10 CFR Part 50

RIN 3150–AI01

[NRC–2007–0008]

Alternate Fracture Toughness Requirements for Protection Against Pressurized Thermal Shock Events; Correction

AGENCY: Nuclear Regulatory Commission.

ACTION: Final rule; correction.

SUMMARY: This document corrects a rule that appeared in the **Federal Register** on January 4, 2010 (75 FR 13), that amends the NRC's regulations to provide alternate fracture toughness requirements for protection against pressurized thermal shock (PTS) events for pressurized water reactor (PWR) pressure vessels. This document is necessary to correct formatting and typographical errors in paragraph (g).

DATES: The correction is effective February 3, 2010, the date the original rule becomes effective.

FOR FURTHER INFORMATION CONTACT: Michael T. Lesar, Chief, Rulemaking and Directives Branch, Office of Administration, Nuclear Regulatory Commission, Washington, DC 20555–0001, telephone 301–492–3663, e-mail *Michael.Lesar@nrc.gov.*

SUPPLEMENTARY INFORMATION: In FR doc. E9–31146, published on January 4, 2010, make the following correction:

§ 50.61a [Corrected]

■ 1. On page 27, paragraph (g) of § 50.61a is corrected to read as follows:

(g) *Equations and variables used in this section.*

$$\text{Equation 1: } RT_{MAX-AW} = MAX\left\{\left[RT_{NDT(U)-plate} + \Delta T_{30-plate}\right], \left[RT_{NDT(U)-axial\ weld} + \Delta T_{30-axial\ weld}\right]\right\}$$

$$\text{Equation 2: } RT_{MAX-PL} = RT_{NDT(U)-plate} + \Delta T_{30-plate}$$