CTPAT

Privacy Compliance

Last Updated: Jan. 11, 2022

In response to several questions posed regarding the publication of privacy compliance documentation for the Customs Trade Partnership Against Terrorism (CTPAT), U.S. Customs and Border Protection (CBP) offers this overview of privacy compliance at CBP under the Department of Homeland Security (DHS) through responses to several Frequently Asked Questions (FAQs) regarding CTPAT. The privacy compliance documents described below are meant to evaluate programs and systems for privacy compliance as well as provide transparency to the public. These documents focus on the protection of information about individuals, called Personally Identifiable Information (PII), in a system or program. The CTPAT Privacy FAQs that follow discuss how these privacy documents cover CTPAT, specifically, the System of Records Notice (SORN)

When is a SORN required?

Pursuant to the Privacy Act of 1974 (5 U.S.C. § 552a) a SORN is required anytime the government collects and maintains PII about U.S. citizens and lawful permanent residents. This requirement includes incidental collections of PII (such as name, address, and other point of contact information that links to the person) related to commercial transactions or PII collected through a voluntary program.

What does a SORN do?

The SORN is a standardized federal register notice that provides the legal Who (Categories of Individuals), What (Categories of Records), How (Record Source Categories), When (Retention and Disposal), Where (System Location) and Why (Purposes) of a collection of records about individuals. The SORN serves several other purposes, including:

1. Notifying the public that the government is collecting and maintaining PII about individuals.
2. Describing the reasons and legal authority permitting the government to collect the PII.
3. Describing the purposes for which the PII will be used.
4. Describing (through the routine uses) the full list of conditions permitting the sharing of PII from the system of records without an individual's consent.

a. In each of these circumstances, the receiving party must have an authorized need to know the specific information.

b. Several of these routine uses follow statutory requirements, including sharing with the Bureau of Census for statistical purposes, sharing with NARA for archival purposes, law enforcement sharing in the case of an investigation or judicial action, and others.

5. Describing any exemptions to the access and amendment provisions of the Privacy Act.

Does the SORN obligate or place new burdens on the public?

No, a SORN describes actions incumbent on the government to protect information in the system of records and provides information to assist an individual in accessing his or her records. CBP, as a matter of long-standing policy, affords the same protections to business confidential information maintained in a SORN as it does to the PII stored there.

Privacy Act Notice of Proposed Rulemaking (NPRM)

What is a Privacy Act NPRM?

A Privacy Act NPRM provides the public an opportunity to comment on the proposed exemptions to the Privacy Act for a given system of records. Under the Privacy Act of 1974, an individual may request access and amendment about his or her records in a system of records. The government may exempt itself from the access and amendment provisions of the Privacy Act through this rulemaking process. Similar to provisions in the Freedom of Information Act, exemptions are typically asserted to protect law enforcement sensitive information so that an individual may not frustrate legitimate law enforcement activities.

When is a Privacy Act NPRM required?

A Privacy Act NPRM (and subsequent Final Rule) is (are) required whenever the government intends to exempt itself from certain provisions of the Privacy Act, including provisions permitting an individual to access or amend records about himself or herself. The Privacy Act requires the government to publish a list of all exempt systems and their exemptions in an agency's Privacy Act regulations. The NPRM is the legal vehicle employed to propose an amendment to these regulations for the purpose of including the subject SORN. DHS has promulgated its Privacy Act regulations at title 6, Code of Federal Regulations (CFR), part 5.

Does the Privacy Act NPRM or Final Rule obligate or place new burdens on the public?

No. However, this process is used to allow the government to limit access or amendment to information in the system. Such limitations are constructed to protect sensitive information (such as law enforcement sensitive information), rather than inhibit an individual's access to information he or she provided to the government.

Does the Privacy Act NPRM or Final Rule allow the government to share my information with other individuals, businesses, or government agencies?

No, the NPRM and Final Rule do not provide the government with the authority to share the data in the system of records. However, they do allow the government to withhold the fact that your information was shared for law enforcement purposes from you. DHS is seeking to withhold the fact that a law enforcement agency has sought or received particular records, because it may affect an ongoing law enforcement activity. This sharing may only take place where the receiving agency has an authorized need to know as part of a law enforcement investigation.

Privacy Impact Assessment (PIA)

What is a PIA?

A PIA is a decision-making tool used to identify and mitigate privacy risks in a program or system. It helps the public understand what PII the government is collecting, why it is being collected, and how it will be used, shared, accessed, and stored. Because the PIA is a more narrative document than the SORN, it explores the program or system in greater detail. The PIA contains sections providing a description and evaluation of:

1. The authorities authorizing the program,
2. The nature of the information collected,
3. The uses of the information collected,
4. The means by which the program provides notice to individuals and their control over their information,
5. The retention of the information,
6. The sharing and limitations on sharing the information,
7. The procedures for an individual to access his or her records or seek redress, And,
8. The practices and procedures used to safeguard the information and provide accountability.

When is a PIA required?

PIAs are required by Section 208 of the E-Government Act of 2002 (44 U.S.C. § 3501 Note). A PIA is required whenever the government develops or procures information technology that collects, maintains, or disseminates PII about members of the public.

Does the PIA obligate or place new burdens on the public?

No, a PIA describes actions incumbent on the government to protect PII in the system of records and provides information to assist an individual in accessing his or her records.

CTPAT Privacy FAQs

Several concerns have been raised about the publication of the CTPAT System of Records Notice (SORN),1 the Privacy Act Notice of Proposed Rulemaking (NPRM),2 and the Privacy Impact Assessment (PIA).3 CBP would like to address these concerns to allay any fears about the publication of the SORN, the Privacy Act NPRM, and the PIA.

What prompted the SORN, Privacy Act NPRM, and PIA now?

As part of its ongoing review of programs that collect information from the public, CBP published the SORN, NPRM, and PIA to ensure that the personally identifiable information (PII) in CTPAT is properly safeguarded and complies with all applicable privacy laws and policy.

Do the SORN, Privacy Act NPRM, and PIA make changes to the CTPAT program?

No. Businesses that participate in CTPAT will not experience any changes as a result of the publication of these documents or the subsequent Final Rule. These documents and the rulemaking process are used to reaffirm and provide notice to the public that PII associated with CTPAT businesses is protected under the Privacy Act of 1974 and will not be improperly collected, used, or disseminated. The Privacy Act, NPRM and Final Rule process is used to protect law enforcement sensitive information generated through the vetting of a business from being accessed by the subjects of an investigation.

Under the SORN, Privacy Act NPRM, and PIA, what level of protection is granted to CTPAT information?

CTPAT information for businesses and individuals is still protected to the same degree as before the publication of these documents. CTPAT information concerning businesses is still protected under the Trade Secrets Act. The publication of the SORN, Privacy Act NPRM, and PIA are to ensure that information about individuals is protected under the Privacy Act as well.

The SORN lists a series of Routine Uses, which permit the official sharing of individual PII and business information without consent. These Routine Uses provide the outermost boundaries of information sharing, and define for the public the existing restrictions on sharing CTPAT information. Information may not be shared from CTPAT outside of DHS unless (1) you provide consent to the sharing, (2) a statutory requirement compels the sharing, or (3) the sharing conforms to one of the listed Routine Uses and the receiving party has an official need to know the specific information being sought. Many of these Routine Uses follow statutory requirements (specifically, routine uses pertaining to the Bureau of the Census, for statistical research, to the National Archives, pursuant to a law enforcement request, to protect the health or safety of an individual, pursuant to a request from Congress to the General Accounting Office for audit purposes, pursuant to a court order, and pursuant to the Debt Collection Act).

With regard to the routine use permitting the sharing of information with the media, the language is specifically limited to those situations where it "is necessary to preserve confidence in the integrity of DHS or is necessary to demonstrate the accountability of DHS's officers, employees, or individuals covered by the system, except to the extent it is determined that release of the specific information in the context of a particular case would constitute an unwarranted invasion of personal privacy."

Sharing under this Routine Use requires approval by the DHS Chief Privacy Officer and the office of General Counsel before the information may be disseminated.

Is my data protected and not shared with a competitor or other business without my consent?

Information in CTPAT is protected under the Trade Secrets Act, as well as the Privacy Act, and is not shared with other businesses, except under the following conditions:

1. CTPAT partners that opt into the Status Verification Interface (SVI) may provide their business partners with their SVI number allowing those business partners to retrieve the CTPAT partner's company name and its "certified/non-certified" status. Participation in this function is voluntary and requires consent. Business partners have no obligation to keep confidential the certification status of any participant once access has been granted to them by the CTPAT partner.
2. A CTPAT Partner may authorize the release of its Supply Chain Security Profile (SCSP) to a third party CTPAT partner. This function allows CTPAT partners to evaluate the security practice of another partner for inclusion in their own supply chain profile. Participation in this function is also voluntary and requires consent.

The Privacy Act prevents DHS from sharing the PII in CTPAT unless you provide your consent or Routine Use permits sharing without your consent. If another individual or business requests access to your information, DHS is prevented under the Privacy Act from providing the records without your consent. DHS, however, is required to share information with other governments and governmental agencies by statute or by formal interagency agreement. All of these circumstances are limited by law and policy to share the minimal amount of information necessary to accomplish the task and only with an individual or entity with an official need to know the information.

Do these documents restrict my access to my own information?

No. The exemptions sought by DHS will not affect an individual or business's ability to access their information, which they submitted to CBP, or affect access through the CTPAT Portal. This means that individuals and businesses may still access their company profile, supply chain information, and other information provided during the application and validation process. Similarly, individuals and businesses may still access their final membership determination. DHS is seeking the exemptions listed in the NPRM to withhold the fact that a law enforcement agency has sought or received particular records, because it may affect ongoing law enforcement activities, and to protect the results of information shared with or developed by DHS in the process of performing vetting on the CTPAT application.

1 DHS/CBP-018 - Customs--Trade Partnership Against Terrorism (CTPAT) March 13, 2013 78 FR 15889. http://www.gpo.gov/fdsys/pkg/FR-2013-03-13/html/2013-05674.htm
2 Notice of Proposed Rulemaking for Privacy Act Exemptions March 13, 2013 78 FR 15889. http://www.gpo.gov/fdsys/pkg/FR-2013-03-13/html/2013-05673.htm
3 Customs-Trade Partnership Against Terrorism (CTPAT), February 14, 2013. http://www.dhs.gov/sites/default/files/publications/privacy/PIAs/privacy-pia-cbp-ctpat-feb2013.pdf