

e-SAFE Privacy Notice

This Privacy Notice serves to inform you of why U.S. Customs and Border Protection (CBP) is requesting the information on this web form.

AUTHORITY:

The information requested on these forms are collected under the Immigration and Nationality Act (INA) §§ 212(d)(3)(A)(ii), 212(a)(9)(A) or (C) and Title 8 of the Code of Federal Regulations (CFR), sections 212.2 and 212.4. The 212(d)(3)(A) waiver, as further described in 8 CFR 212.4, allows inadmissible visa exempt nonimmigrants to apply for advance permission to temporarily enter the United States. INA section 212(a)(9)(A) or (C) and 8 CFR 212.2 prescribe relief for eligible aliens who have been deported from the United States and need to apply for permission to reapply “consent to reapply” to reenter the United States. Section 103 of the INA and 8 CFR 2.1 authorize the Secretary of Homeland Security to administer and enforce the INA and other laws relating to the immigration and naturalization of aliens, and to establish such authority as she deems necessary for carrying out her authority. Various provisions of the INA and corresponding regulations place limits on the conditions of aliens’ entry. *See, e.g.*, INA §§ 215(a), 235; 8 CFR 235.1.

PURPOSE:

The primary purpose for providing the requested information is to determine whether an alien can be granted discretionary relief to seek entry to the United States, and whether there exists a law enforcement or security risk in permitting, the alien to enter to the United States. The Secretary of Homeland Security will use the information provided to grant or deny the temporary discretionary relief sought by the alien.

SHARING:

CBP may share the information provided on this application with other Federal, state, local, and foreign government agencies and authorized organizations. This information may be available to all component agencies within the Department of Homeland Security (DHS) on a need to know basis consistent with the component’s mission and other Federal Partners. CBP may also share the information, as appropriate in the interest of national security.

DISCLOSURE FOR FAILURE TO PROVIDE INFORMATION:

The information provided by the alien is voluntary. However, failure to provide the requested information or any additional information may delay a final decision or result in the denial of the application.

How long is my application data stored?

CBP will retain information submitted as part of the e-SAFE website for 5 years after the CBP Admissibility Review Office (ARO) has rendered the final decision. After this period, the inactive account information will be purged from online access and archived for 12 years. Data linked at any time during the 17-year retention period (generally 5 years active, 12 years archived) to active law enforcement lookout records will be matched by CBP to enforcement activities, investigations, or cases, including e-SAFE applications. This retention schedule also applies to incomplete and not submitted applications.

Once the information is archived, the number of officials with access to it will be further limited. Data linked to active law enforcement lookout records, CBP matches to enforcement activities, and/or investigations or cases, including e-SAFE applications that are denied, will remain accessible for the life of the law enforcement activities to which they are related.

Information Collected and Stored Automatically

When you browse, read pages or download information on DHS websites, the department gathers and stores certain technical information about the visit. This information never identifies who the individual is. The information DHS collects and stores about a visit is listed below:

- The Internet domain (for example, "xcompany.com" if you use a private Internet access account, or "yourschool.edu" if you connect from a university's domain) and IP address (an IP address is a number that is automatically assigned to your computer whenever you are surfing the Web) from which you access our website
- The type of browser (e.g., Google, Internet Explorer) and operating system (Windows, Unix, Linux, OS) used to access the site
- The date and time you access the site
- The pages you visit
- If you linked to the DHS website from another website, the address of that website

This information is used to help DHS makes the site more useful and user friendly. With this data we learn about the number of visitors to the site and the types of technology the visitors use. We never track or record information about individuals and their visits.

Cookies

When you visit some websites, their web servers generate pieces of information known as cookies. Some cookies collect personal information to recognize the computer in the future. This is not the case at DHS, where we only use non-persistent cookies or "per-session cookies." These cookies do not collect personal information on users and are erased as soon as the individual leaves the website. Per-session cookies allow seamless navigation on the website. These cookies do not permanently record data and they are not stored on your computer's hard drive. DHS

cookies are stored in memory and are only available during an active browser session. Again, once the browser is closed, the cookie disappears.

Site Security

- For site security purposes and to ensure that this service remains available to all users, this government computer system employs commercial software programs to monitor network traffic to identify unauthorized attempts to upload or change information, or otherwise cause damage
- Except for authorized law enforcement investigations, no other attempts are made to identify individual users or their usage habits. Raw data logs are used for no other purposes and are scheduled for regular destruction in accordance with National Archives and Records Administration guidelines
- Unauthorized attempts to upload information or change information on this service are strictly prohibited and may be punishable under the Computer Fraud and Abuse Act of 1984.

Is my information secure?

Yes. This Web site is operated by the United States Government and employs technology to prevent unauthorized access to the information an individual enters and views.