

Privacy Impact Assessment (PIA) SAO HITRAN Data Request

I. System Identification

1. **IT System Name:** HITRAN Data Request www.cfa.harvard.edu/hitran
2. **IT System Sponsor:** Dr. Lawrence Rothman
3. **System Sponsor Unit:** SAO
4. **IT System Manager:** Van McGlasson
5. **PIA Author:** Julie Shaw
6. **SI Unit Director or Designee:** Charles Alcock
7. **Date:** September 2009
8. **Brief (one paragraph) description of the system:**

Users may fill in a request form to download the HITRAN (HI Resolution Transmission Absorption Database) Database and associated software.

II. Privacy Assessment

1. What information is being (or will be) collected.

The registrant's contact information- name, mailing address, email address, office phone, fax, institution - is collected via a web form. Optional information – computer system description, intended use of data, comments – may also be collected. The information is displayed and the user confirms it by submitting.

2. Why the information is being collected.

The information is needed to fill the request. In additions, aggregate statistics about the uses of the data can be obtained. Email addresses are saved for notification of data updates and future HITRAN conferences.

3. The intended use of the information.

The information is emailed to the scientist in charge of HITRAN. He uses it to fill the request by emailing the user a username and password to use to download the data. He saves the email addresses for future notifications (see question 2)

4. With whom the information will be shared.

Only the SAO scientist in charge of HITRAN has access to the information. Statistics may be shared with sponsoring agencies, but not personal identifying information.

5. What notice or opportunities for consent would be provided to individuals regarding what information is collected and how that information is shared.

The personal information is not shared outside SAO. Of the information listed in question 1, only name and email address are required. Users may email www-admin@cfa.harvard.edu to update their information. Privacy Documentation may be found on the www.si.edu website under the privacy link.

6. How the information will be secured.

The information is collected using Secure Socket Layer (SSL) so that it is encrypted when going over the internet. The servers are physically protected in a secure computer room, where access is limited to authorized personnel. Intrusion detection software is deployed. OS patches are installed as required. All servers have up-to-date antivirus software. Backup tapes are kept in a locked area, with limited access. They are periodically rewritten and are destroyed when no longer usable.