

Privacy Impact Assessment
National Museum of Natural History
Friends of the Archives Mailing List

I. System Identification

1. IT System Name: Voom (voom.si.edu)
2. IT System Sponsor: Robert Leopold, Archives Manager
3. System Sponsor Unit: Anthropology Department, NMNH
4. IT System Manager: Robert Leopold
5. PIA Author: Robert Leopold
6. SI Unit Director or Designee: J. Daniel Rogers, Chair, Department of Anthropology
7. Date: May 2009
8. Brief (one paragraph) description of the system:

Research visitors to the Collections Management Division of the Department of Anthropology request appointments by completing an online form.

II. Privacy Assessment

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

The online form requests their name and email address. Optionally, the individual may provide their occupation/title, affiliation, address, information about the reason for their visit to the web site, how often they had visited the web site, whether they had ever visited the archives in person, their level of education, and free-form comments. The form itself may be viewed here: http://www.nmnh.si.edu/naa/mailling_list.htm

2. Why the information is being collected.

To identify Friends of the Archives, learn about their reasons for visiting our web site, and the relationship between online visits and physical visits to our archives.

3. The intended use of the information.

Individuals who identify themselves as Friends of the Archives receive a periodic email message containing news about the archives.

4. With whom the information will be shared.

The information is used by the Archives Manager. It is not shared.

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

The Smithsonian's Privacy Notice is displayed on the form.

6. How the information will be secured.

The Department of Anthropology protects sensitive data from unauthorized access and/or disclosure, assures the integrity of data stored in electronic form, and protects data from unauthorized alteration or modification. The visitor database is controlled with respect to access, authority to modify, and ability to operate it.

The visitor database requires users to authenticate their identity through the entry of a user ID and password. The system allows access only to authorized users. Levels of access to the visitor database are controlled by the system administrator based on the individual needs of the user. Access is revoked promptly when a person leaves or changes jobs.

The visitor database operates on a server that is behind the SI firewall, which does not allow any access from the Internet. Client software is required in order to access the system.

The visitor database is stored on the Web Server in a directory that is not in the Web root.

The server is physically protected in a secure facility where access is limited to authorized personnel.

The system has anti-virus protection that is updated on a daily basis. System logs are reviewed frequently to check for anomalies such as hacking attempts.

All privacy-related information stored in the visitor database is retained in perpetuity because it demonstrates researcher use of particular Smithsonian collections.