SECURITY CLASSIFICATION:

None.

SYSTEM LOCATION:

Fogarty International Center, Building 16A, Room 101, 9000 Rockville Pike, Bethesda, MD 20892

and

Division of Computer Research and Technology, Building 12A, Room 3061, National Institutes of Health, 9000 Rockville Pike, Bethesda, MD 20892

Ancillary records are located in the Office of the Associate Director for Intramural Affairs, laboratories, administrative and personnel offices where participants are assigned. Write to System Manager at the address below for the address of the Federal Records Center where records are stored.

CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM:

Health scientists at all levels of their postdoctoral or equivalent research careers who are invited to the National Institutes of Health for further training or to conduct research in their biomedical specialties under the auspices of FIC's administration of International Activities. Most of these scientists are foreign, however, some may be resident aliens or U.S. citizens.

Individuals in these categories include Visiting Associates, Visiting Scientists, Foreign Special Experts who are employees and Visiting Fellows, Guest Researchers, Exchange Scientists, International Research Fellows, Fogarty Scholars, Special Volunteers, Adjunct Scientists and Residents who are not employees.

CATEGORIES OF RECORDS IN THE SYSTEM:

History of fellowship, employment and/or stay at NIH; education, immigration data and references. For payroll purposes, social security numbers are requested of all applicants accepted into the program.

AUTHORITY FOR MAINTENANCE OF THE SYSTEM:

42 USC 2421 and section 307 of the Public Health Service Act.

PURPOSE(S)

To document the individual's presence at the NIH, to record immigration history of the individual in order to verify continued eligibility in existing programs, and to meet requirements in the Code of Federal Regulations (8 CFR, "Aliens and Nationality," and 22 CFR, "Foreign Relations"). ROUTINE USES OF RECORDS MAINTAINED IN THE SYSTEM, INCLUDING CATEGORIES OF USERS AND THE PURPOSES OF SUCH USES:

1. Information is made available to authorized employees and agents of the U.S. Government including, but not limited to, the General Accounting Office, the Internal Revenue Service, and the FBI and Immigration and Naturalization Service, Department of Justice, for purposes of investigations, inspections and audits.

2. Disclosures may be made to a congressional office from the record of an individual in response to an inquiry from the congressional office made at the request of the individual.

3. The Department of Health and Human Services (HHS) may disclose information from this system of records to the Department of Justice, or to a court or other tribunal. when (a) HHS. or any component thereof; or (b) any HHS employee in his or her official capacity; or (c) any HHS employee in his or her individual capacity where the Department of Justice (or HHS, where it is authorized to do so) has agreed to represent the employee; or (d) the United States or any agency thereof where HHS determines that the litigation is likely to affect HHS or any of its components, is a party to litigation or has any interest in such litigation, and HHS determines that the use of such records by the Department of Justice, court or other tribunal is relevant and necessary to the litigation and would help in the effective representation of the governmental party, provided, however that in each case, HHS determines that such disclosure is compatible with the purpose for which the records were collected.

POLICIES AND PRACTICES FOR STORING, RETRIEVING, ACCESSING, RETAINING, AND DISPOSING OF RECORDS IN THE SYSTEM:

STORAGE:

Records are stored in file folders, computer tapes, and computer disks.

RETRIEVABILITY:

By name, country of citizenship, country of birth, gender, fellowship case number, visa and immigration status, program category, NIH Institute and lab, sponsor, degree attained, stipend or salary level, dates of stay at NIH, termination date, work address and telephone number, and home address.

SAFEGUARDS:

A variety of safeguards is implemented for the various sets of records included under this system according to the sensitivity of the data they contain. 1. Authorized users: NIH administrative and personnel staff screened by FIC staff to access information on a need-to-know basis. Only FIC staff are authorized to add, change, or delete data. Access by other employees is granted on a need-to-know basis as specifically authorized by the system manager.

2. *Physical safeguards:* The records are maintained in file cabinets in offices that are located during off-duty hours.

3. *Procedural safeguards.* Access to files is strictly controlled by files staff. Records may be removed from files only at the request of the system manager or other authorized employees. For computerized records, access is controlled by the use of security codes known only to authorized users; access codes are changed periodically. The computer system maintains an audit record of all requests for access.

These practices are in compliance with the standards of Chapter 45–13 of the HHS General Administration Manual, "Safeguarding Records Contained in Systems of Records," supplementary Chapter PHS hf: 45–13, and Part 6, "ADP Systems Security," of the HHS Information Resources Management Manual and the National Institute of Standards and Technology Federal Information Processing Standards (FIPS Pub. 41 and FIPS Pub. 31).

RETENTION AND DISPOSAL:

Records are retained and disposed of under the authority of the NIH Records Control Schedule contained in NIH Manual Chapter 1743, Appendix 1— "Keeping and Destroying Records" (HHS Records Management Manual, Appendix B–361), item 2300–320, which allows records to be destroyed after a maximum period of 6 years after the close of a case. Refer to the NIH Manual Chapter for specific disposition instructions.

SYSTEM MANAGER AND ADDRESS:

Chief, International Services and Communications Branch, National Institutes of Health, Fogarty International Center, Building 16A, Room 101, 16A Center Drive MSC 6710, Bethesda, MD 20892–6710

NOTIFICATION PROCEDURE:

Write to the System Manager to determine if a record exists. The requester must also verify his or her identity by providing either a notarization of the request or a written certification that the requester is who he or she claims to be and understands that the knowing and willful request for acquisition of a record pertaining to an