Department of Energy
Privacy Impact Assessment (PIA)

Name of Project: Foreign Access Central Tracking System (FACTS)
Bureau: Department of Energy
Project Unique ID: 019-10-01-22-01-7013-00
Date: 6/25/2008

A. CONTACT INFORMATION

1. Who is the person completing this document?

Name: Jennifer Emanuelson
Title: Director, Office of Foreign Visits and Assignments
Department of Energy
1000 Independence Avenue, SW
Washington, DC 20585
E-mail: Jennifer.emanuelson@hq.doe.gov

2. Who is the system owner?

Name: Jennifer Emanuelson
Title: Director, Office of Foreign Visits and Assignments
Address: DOE Headquarters
Forrestal Building
1000 Independence Avenue
Washington, DC 20585
Phone: (202) 202-586-6828
E-mail: jennifer.emanuelson@hq.doe.gov

3. Who is the system manager for this system or application?

Name: Mr. Raymond Holmer
Address: DOE Office of Health, Safety and Security
Germantown, Maryland
Phone: 301-903-7325

E-Mail: Raymond.Holmer@hq.doe.gov

4. **Who is the IT Security Manager who reviewed this document?** Vinh Le, Office of Information Management, HS-1.22, 301-903-4648.

5. **Who is the Privacy Act Officer who reviewed this document?** Kevin Hagerty, D Director, Office of Information Resources, MA-90, 202-586-8037.

B. SYSTEM APPLICATION/GENERAL INFORMATION

1. **Does this system contain any information about individuals?** Yes

   a. **Is this information identifiable to the individual?** [1] Yes

   b. **Is the information about individual members of the public?** Yes

   c. **Is the information about DOE or contractor employees?** Yes

2. **What is the purpose of the system/application?**

   The system documents and tracks access control records of international visits, a assignments, and employment at DOE facilities and contractor sites. Specifically, the system was developed, and implemented in June 2000, in response to Presidential Decision Directive (PDD) 61, *U.S. Department of Energy Counterintelligence Program*, which required the Department to develop procedures and practices, through the newly established Office of Foreign Visits and Assignments, to meet the needs to DOE's vital national security programs while providing protection from foreign threats, and specifically required DOE to provide Department-wide tracking of foreign national access.

3. **What legal authority authorizes the purchase or development of this system/application?**

   42 U.S.C. 7101 *et seq.* and 50 U.S.C. 2401 *et seq.*

   PDD-61

C. DATA IN THE SYSTEM

1. **What categories of individuals are covered in the system?**

---

[1] "Identifiable Form" - According to the OMB Memo M-02-22, this means information in an IT system or online collection: (i) that directly identifies an individual (e.g., name, address, social security number or other identifying number or code, telephone number, email address, etc.) or (ii) by which an agency intends to identify specific individuals in conjunction with other data elements, i.e., indirect identification. (These data elements may include a combination of gender, race, birth date, geographic indicator, and other descriptor).

All non-U.S. citizens seeking access to DOE facilities, contractor sites, or DOE (and NNSA) sponsored events for unclassified purposes to include employees of DOE or DOE contractors; prospective DOE or DOE contractor employees; employees of other U.S. Government agencies or their contractors or universities, of companies (professional or service staff), or of other institutions; foreign students at U.S. institutions; officials or other persons employed by foreign governments or other foreign institutions who may or may not be involved in cooperation under international agreements; lawful permanent residents; representatives or agents of foreign national governments seeking access to DOE facilities, laboratories, or contractor sites of DOE-sponsored events for purposes of high-level protocol; national security; International Atomic Energy Agency, or international relations.

2. **What are the sources of information in the system?**

   a. **Is the source of the information from the individual or is it taken from another source?**
   Information is obtained from foreign nationals requesting access.

   b. **What Federal agencies are providing data for use in the system?**
   DOE

   c. **What tribal, state, and local agencies are providing data for use in the system?**
   None

   d. **From what other third party sources will data be collected?**
   None

   e. **What information will be collected from the individual and the public?**
   Personal data: Full name (including Also Known As (A.K.A.'s), visitor request number, gender, place of birth, city and country, date of birth, country(ies) of citizenship, date of last visit to country of citizenship, passport number and passport expiration date, immigration status, type of visa and expiration date, country of current residence and how long at current residence, language interpretation needs, work phone, e-mail and fax, name of current employer, place of work, street, city, zip code, country; position title or description of requester's duties. Visit/Assignment Request Information: Date of request, purpose of request (including subjects to be discussed or researched and specific activities involved); requestor's current whereabouts (i.e., is proposed visitor currently in the United States), specific visa status and purpose (i.e., exchange visitor (J-1) Visa), time duration of proposed visit, assignment or activity (desired start and end dates), identification of specific international agreement(s) or delegations related to

the proposed requests, name, organization, telephone number of DOE contact, name of financial sponsor, cost if sponsor is other than DOE. Visit/Assignment Facility Information: Name, location and room number of facility or organization to be accessed during visit/assignment, name of the host responsible for the visit/assignment, host's telephone number, building and room numbers, number of days on site, visit/assignment relationship to program, subject codes, subjects to be discussed or statement of research, determination of computer access, and sensitive subject designation. Visit/Assignment Program Information and Remarks: Designation of high-level protocol visit, cost to DOE, visit or assignment purpose code, purpose or justification of visit/assignment including benefits to DOE program(s) and certification of DOE mission advancement, technology transfer determination, name of requesting official or contractor, title and organization of requesting official or contractor, date, signed, name of site manager and local headquarters approving official, signature(s) of field site, headquarters approving official, date signed and remarks, the kind of business or organization of visitor/assignee's employer (e.g., government, company, laboratory, university), education background of requestor including college or university training with degrees and dates conferred; field of research, and family members who will accompany or join the applicant later. Management Reviews and Approvals: Level, type or topic of review, name of reviewer and/or approval authority(ies), the date of the review approval, and remarks.

3. **Accuracy, Timeliness, and Reliability**

a. **How will data collected from sources other than DOE records be verified for accuracy?**

Information is verified with the foreign national upon start of visit/assignment. System records, when used to create new visit/assignment requests, must be reviewed by the hosting entity to ensure currency/correctness of information.

b. **How will data be checked for completeness?**

System will not allow submission of access requests without population of all required fields. Site/Headquarters program elements hosting visits and assignments are responsible for ensuring provision of adequate data to conduct informed access approval determinations. Site self-assessments and field office assessments, and inspections and audits by independent DOE entities also review data for completeness.

c. **Are the data current? What steps or procedures are taken to ensure the data are current and not out-of-date?**

Yes, the data is current. System records, when used to create new visit/assignment requests, must be reviewed by the hosting entity to ensure currency/correctness of information. Site self-assessments and field office

assessments, and inspections and audits by independent DOE entities also review data for completeness.

d. Are the data elements described in detail and documented?

Yes.

D. ATTRIBUTES OF THE DATA

1. Is the use of the data both relevant and necessary to the purpose for which the system is being designed?

Yes. Data is used for access requests by foreign nationals to DOE/NNSA sites.

2. Will the system derive new data or create previously unavailable data about an individual through aggregation from the information collected, and how will this be maintained and filed?

No.

3. Will the new data be placed in the individual's record?

N/A.

4. Can the system make determinations about employees/the public that would not be possible without the new data?

N/A.

5. How will the new data be verified for relevance and accuracy?

The system will not allow submission of access requests without population of all required fields. Site/headquarters program elements hosting visits and assignments are responsible for ensuring provision of adequate data to conduct approval determinations. System records, when used to create new visit/assignment requests, must be reviewed by the hosting entity to ensure currency/correctness of information. Information is verified with the foreign national upon start of the visit/assignment. Site self-assessments and field office assessments, and inspections, assessments and audits by independent DOE entities are also conducted to ensure data completeness.

6. If the data are being consolidated, what controls are in place to protect the data from unauthorized access or use?

N/A.

7. **If processes are being consolidated, do the proper controls remain in place to protect the data and prevent unauthorized access?**

N/A.

8. **How will data be retrieved? Does a personal identifier retrieve the data? If yes, explain, and list the identifiers that will be used to retrieve information on the individual.**

Records may be retrieved by name and other personal identifiers including visitor number and request number.

9. **What kinds of reports can be produced on individuals? What will be the use of these reports? Who will have access to them?**

Reports of foreign national visits and assignments to DOE sites can be produced and printed from the system. These reports can only be produced by users with system rights for the specific site, are marked Official Use Only, and cannot be further distributed without permission from site management and the FACTS system manager. Paper output is maintained in locked cabinets and desks. Electronic records must be controlled as Official Use Only information. Access is limited to those whose official duties require access to the records.

10. **What opportunities do individuals have to decline to provide information (e.g., where providing information is voluntary) or to consent only to particular uses of the information (other than required or authorized uses)?**

None – individuals can decline to request a visit or assignment.

E. Maintenance and Administrative Controls

1. **If the system is operated in more than one site, how will consistent use of the system and data be maintained in all sites?**

FACTS is the Departmental system for unclassified foreign national visits and assignments. The system is web-based and available to all DOE/NNSA sites. Requirements for use of the system in support of the DOE Unclassified Foreign Visits and Assignments Program are detailed in DOE Order 142.3. Compliance with policy, and with requirements for use of the system and data, is determined through site and field office assessments, and line management is ultimately responsible for compliance by their sites and headquarters program elements, and for ensuring that issues identified in assessments are corrected. FACTS access requires electronic acceptance of the system Rules of Behavior, which details use of the system and data, and continued access requires annual re-acceptance.

2. **What are the retention periods of data in the system?**

Data retention procedures are in accordance with DOE Administrative Records Schedule N1-434-98-21 "Security, Emergency Planning and Safety Records."

This information can be obtained at http://cio.energy.gov/records-management/adminrs.htm.

3. **What are the procedures for disposition of the data at the end of the retention period? How long will the reports produced be kept?**

Data retention procedures are in accordance with DOE Administrative Records Schedule N1-434-98-21 "Security, Emergency Planning and Safety Records." This information can be obtained at http://cio.energy.gov/records-management/adminrs.htm.

4. **Is the system using technologies in ways that DOE has not previously employed (e.g., monitoring software, Smart Cards, Caller-ID)?**

No.

5. **How does the use of this technology affect public/employee privacy?**

N/A.

6. **Will this system provide the capability to identify, locate, and monitor individuals?**

The system provides the capability to identify foreign nationals who visit or are assigned to DOE/NNSA sites on given dates or during specific date ranges.

7. **What kinds of information are collected as a function of the monitoring of individuals?**

Personal Data, Visit/Assignment Request Information, Visit/Assignment Facility Information, Visit/Assignment Program Information and Remarks, and Management Reviews and Approvals Information are collected to create visit/assignment records for foreign nationals at DOE/NNSA sites. A complete list of information collected is shown in section C.2.e.of this document.

8. **What controls will be used to prevent unauthorized monitoring?**

Use of system data is allowed only for purposes supporting the DOE Unclassified Foreign Visits and Assignments Program. In addition, data for visits/assignments to specific sites can only be accessed by those individuals who have Unclassified Foreign Visits and Assignments Program responsibilities for those sites.

9. **Under which PA system of records notice does the system operate?**

DOE-52

10. **If the system is being modified, will the PA system of records notice require amendment or revision?**

The system is not being modified, and requires no related revision to the PA system of records.

F. ACCESS TO DATA

1. **Who will have access to the data in the system?** DOE/NNSA site and Headquarters program element federal and contractor staff with responsibilities related to the DOE Unclassified Foreign Visits and Assignments Program, FACTS system administrators and FACTS Help Desk staff, and Office of the DOE Inspector General and Office of Health, Safety and Security personnel who have responsibilities for independent oversight of the program have access to the system. Access to the system must be approved by site/program office management and the FACTS program manager. Access control to FACTS data is included in the FACTS System Security Plan, dated December, 2005. Access to FACTS data is based on a need-to-know basis related to the responsibilities of the individual as related to the DOE Unclassified Foreign Visits and Assignments Program or to international visits and assignments.

2. **How is access to the data by a user determined?**

   User access to data must be approved by the user's site or Headquarters program element management, to include the identification of system-based rights in line with the user's responsibilities. Access is limited to the DOE/NNSA site(s) for which the user has responsibilities related to foreign visits and assignments.

3. **Will users have access to all data on the system or will the user's access be restricted?**

   User access is restricted to data for the site(s) for which the user has responsibilities related to foreign visits and assignments. User ability to modify data is further restricted through application of user rights for the site(s).

4. **What controls are in place to prevent the misuse (e.g., unauthorized browsing) of data by those having access?**

   Technical controls including identification and authentication, logical access controls, public access controls, and audit trails are in-place and operational on the system. These controls are detailed in section 4.0, Technical Controls, of the FACTS 2005 Security Plan. System support contractor personnel with specific job responsibilities that mandate access to customer systems, customer data, customer applications, and customer user interaction are provided specifically approved access, via the network and physical controls, only to the information and areas necessary to perform their jobs. These accesses are monitored for unauthorized access attempts. Core critical functions are divided between system support staff to prevent a single person from taking an action that could put the system or its information in jeopardy. Physical access into the FACTS system is audited via biometric authentication for positive identity and timestamp of

individual access. System support contractor controls are detailed in section 3.0, Operational Controls, of the FACTS 2005 Security Plan.

Cyber security controls including authentication, authorization, auditing, malicious code removal, continuity of service, encryption, web application security, secure messaging and Official Use Only marking are in-place and operational on the system, and are detailed in section 1.8, Cyber Security Controls, of the FACTS 2005 Security Plan.

5. **Are contractors involved with the design and development of the system and will they be involved with the maintenance of the system? If yes, were PA contract clauses included in their contracts and other regulatory measures addressed?**

Yes, contractors were involved in the Calendar Year 2000 development of the system, and are involved in the maintenance of the system. PA contract clauses are included in their contracts, and information on related contractor requirements is detailed in section 3.1, Personnel Security, of the FACTS 2005 Security Plan.

6. **Do other systems share data or have access to the data in the system? If yes, explain.**

No.

7. **Who will be responsible for protecting the privacy rights of the public and employees affected by the interface?**

N/A.

8. **Will other agencies share data or have access to the data in this system?**

Yes – routine uses of records maintained in the system include instances of data sharing with other agencies.

9. **How will the data be used by the other agency?**

- A record from this system may be disclosed as a routine use to Department of Defense contractors responsible for security, controlling access to sensitive information and sensitive equipment, and sensitive property areas.

-A record from this system may be disclosed as a routine use to contractors, grantees, participants in cooperative agreements, collaborating researchers, or their employees, in performance of national security, international visit and assignment, or foreign access related responsibilities.

-A record from this system may be disclosed as a routine use to a Federal, State or local agency to obtain information relevant to a Departmental decision concerning the hiring or retention of an employee, the issuance of a security clearance, the letting of a contract, or the issuance of a license, grant or other benefit. The

Department must deem such disclosure to be compatible with the purpose for which the Department collected the information.

- A record from this system may be disclosed to a Federal agency to facilitate the requesting agency's decision concerning the hiring or retention of an employee, the issuance of a security clearance, the reporting of an investigation of an employee, the letting of a contract, or the issuance of a license, grant, or other benefit, to the extent that the information is relevant and necessary to the requesting agency's decision on the matter. The Department must deem such disclosure to be compatible with the purpose for which the Department collected the information.

- A record from the system may be disclosed as a routine use to the appropriate local, state, or Federal agency when records alone or in conjunction with other information, indicates a violation or potential violation of law whether civil, criminal, or regulatory in nature, and whether arising by general statute or particular program pursuant thereto.

- A record from this system of records may be disclosed to a member of Congress submitting a request involving the constituent when the constituent has requested assistance from the member with respect to the subject matter of the record. The member of Congress must provide a copy of the constituent's request for assistance.

- A record from this system of records may be disclosed to foreign governments or international organizations in accordance with treaties, international conventions, or executive agreements.

- A record from the system may be disclosed as a routine use to DOE contractors in performance of their contracts, and their officers and employees who have a need for the record in the performance of their duties. Those provided information under this routine use are subject to the same limitations applicable to Department officers and employees under the Privacy Act.

-A record from this system of records may be disclosed as a routine use to members of the DOE Advisory committees and interagency boards charged with responsibilities pertaining to international visits and assignments and/or national security.

10. Who is responsible for assuring proper use of the data?

The Department must deem the disclosure to be compatible with the purpose for which the information was collected. FACTS records must only be provided to those persons who require the information to perform their jobs or other DOE-authorized activities.

PIA Approval Signatures

Original copy signed and on file with the DOE Privacy Office.