Department of Energy
Privacy Impact Assessment (PIA)

Name of Project: HSS Electronic Visitor Management System (HSEVMS)
Bureau: Department of Energy, Office of Health, Safety and Security
Project Unique ID: 019-10-01-22-02-3036-00
Date: May 22, 2008

A. CONTACT INFORMATION

1) **Who is the person completing this document?**
Marc Smith, Office of Headquarters Security Operations, Office of Health, Safety and Security, US Department of Energy, HS-1.31, 1000 Independence Ave., S.W., Washington, D.C. 20585, 202-586-4441

2) **Who is the system owner?**
Marc Smith, Office of Headquarters Security Operations, Office of Health, Safety and Security, US Department of Energy, HS-1.31, 1000 Independence Ave., S.W., Washington, D.C. 20585, 202-586-4441

3) **Who is the system manager for this system or application?**
William Dwyer, Office of Headquarters Security Operations, Office of Health, Safety and Security, U.S. Department of Energy, HS-1.31, 1000 Independence Ave., S.W., Washington, D.C. 20585, 202-586-7885

4) **Who is the IT Security Manager who reviewed this document?**
Vinh Le, Office of Information Management, Office of Health, Safety and Security, U.S. Department of Energy, HS-1.22, 1000 Independence Ave., S.W., Washington, D.C. 20585, 303-903-4648.

5) **Who is the Accrediting Official's Representative who reviewed this document?**
Raymond Holmer (HS-1.22), Director, Office of Information Management, Office of Resource Management, Office of Health, Safety and Security, U.S. Department of Energy, HS-1.22, 1000 Independence Avenue, SW, Washington D.C. 20585, (301) 903-7325.

6) **Who is the Privacy Act Officer who reviewed this document?**
Kevin T. Hagerty (MA-90), Director, Office of Information Resources, FOIA and Privacy Act Office, Office of Management, U.S. Department of Energy, MA-90, 1000 Independence Avenue, SW, Washington D.C. 20585, (202) 586-8037

B. SYSTEM APPLICATION/ GENERAL INFORMATION

1) **Does this system contain any information about individuals?**
Yes, this system contains name, addresses, government ID number, date of birth, facial image, times of visits to a facility, purpose of visit to a facility, and images of individuals' identification documents.

a. **Is this information identifiable to the individual?**
Yes, this information may be identifiable to an individual.[1]

b. **Is this information about individual members of the public?**
Yes, some of the visitors may be employees of other government agencies or members of the public.

c. **Is the information about employees?**
Yes, the system data contains information about employees who have lost/forgotten their issued access control credential, or are in the process of obtaining a permanent credential.

2) **What is the purpose of the system/ application?**
The HSS Electronic Visitor Management System records are maintained and used by the Department to track and control individuals accessing DOE Headquarters Departmental facilities and classified information areas, and to provide a means for retrieving individual and general statistical data about visitors to the headquarters complex.

3) **What legal authority authorizes the purchase or development of this system/application?**
The Department of Energy Organization Act, 42 U.S.C. 7101–7385o, the Energy Reorganization Act of 1974 (ERA), 42 U.S.C. 5801 5911, and the Atomic Energy Act of 1954, as amended, (AEA) 42 U.S.C. 2011, require DOE to protect the public safety and health, as well as the safety and health of workers at DOE facilities, in conducting its activities, and grant DOE broad authority to achieve this goal. Authority for maintenance of the system is given by 42 U.S.C. 7101 et seq. and 50 U.S.C 2401 et seq.

C. DATA IN THE SYSTEM

1) **What categories of individuals are covered in the system? (e.g., agency employees, contractor employees, visitors, volunteers, etc.)**
DOE and DOE contractor and subcontractor employees who have lost./forgotten their issued access control credential, or are in the process of obtaining a permanent credential, and employees of other government agencies who do not have a recurring need to access DOE facilities and infrequent visitors which may be employees of commercial businesses, family members or guests of individuals who have access credentials, or customers of the Energy Federal Credit Union who chose to conduct business at branch located in a DOE Headquarters facility.

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

---

[1] Identifiable Form – According to the OMB Memo M 03-22, this means information in an IT system or online collection: (i) that directly identified 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 information (These data elements may include a combination of gender, race, birth date, geographic indicator, and other descriptors).

a **Is the source of the information from the individual or is it taken from another source?**
The source of the information is from the individual.

b. **What Federal Agencies are providing data for use in the system?**
None

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

d. **What other third party sources will data be collected from?**
None

e. **What information will be collected from the employee?**
The information collected from the employee will be name, address, government ID number, date of birth, facial image, times of visits to the facility, purpose of visit to the facility, and images of individuals' identification documents .

3) **Accuracy, Timeliness, and Reliability?**

a. **How will data collected from sources other than DOE records and the subject be verified for accuracy?**
N/A, data is not collected from sources other than DOE records and identification documents presented by the subject.

b. **How will data be checked for completeness?**
Data will be compared with the documents presented by the individual at time of entry to the complex.

c. **Is the data current? How do you know?**
The data is current. Credentials presented by the individual for entry verification must be current.

4) **Are the data elements described in detail and documented? If yes, what is the name of the document?**
The data elements are not described in detail and documented.

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.

2) **Will the system derive new data or create previously unavailable data about an individual through aggregation from the information collected?**
Yes, the system will be able to derive patterns of individuals' visits. The system will be able to identify who individuals are visiting, how often and at what times through aggregation of information collected.

3) **Will the new data be placed in the individual's record?**
Yes, any individual's visit is considered new data and stored within the system under the individual's identifier. Derived data, created about an individual through aggregation from the information collected, will only be available as a report but not stored in the individuals record.

4) **Can the system make determinations about the record subject that would not be possible without the new data?**
Yes, the system will be able to derive data about an individual, through aggregation from the information collected, to show patterns of visits across time.

5) **How will the new data be verified for relevance and accuracy?**
Individual records are verified at time of input. Input time, location and purpose of visit are verified at time of input.

6) **If data is being consolidated, what controls are in place to protect the data from unauthorized access or use?**
No.

7) **If processes are being consolidated, are the proper controls remaining in place to protect the data and prevent unauthorized access?**
No.

8) **How will the data be retrieved? Is it retrieved by personal identifier? If yes, explain.**
Information may be retrieved by subject individual's name, social security number or document ID number recorded from subject individuals presented credentials (e.g., Drivers license, Passport).

9) **What kinds of reports can be produced on individuals? What will be the use of these reports? Who will have access to them?**
Listings of subject individuals' visits to DOE Headquarters facilities, including time in, time out, purpose and who they visited are available as reports. These reports are available to Protective Force personnel supervisors, administrators and privilege users. 1. 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. 2. 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. 3. 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. 4. Records from this system may be disclosed to Department of Defense contractors and National Aeronautics and Space Administration to authorize access to classified information and areas.

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)?**
Information is provided voluntary, but is required to enter the facility.

E. MAINTENANCE OF ADMINISTRATIVE CONTROLS

1) **If the system is operated at more than one location, how will consistent use of the system and data be maintained?**
The system is operated at the DOE Headquarters guard stations in Germantown, Forrestal, L'Enfant Plaza and Cloverleaf buildings. Consistent use of the system and data is maintained by training in the use of the system and an annual security refresher.

2) **What are the retention periods of data in the system?**
The retention periods of data are in accordance with DOE Records Schedule 18, Items 17, 18, and 19. The limit of retention is five years. See http://cio.energy.gov/documents/ADM_18.pdf for specific records.

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? Where are the procedures documented?**
Data is maintained on digital media until the end of the retention period. Records are then deleted from the system. Digital storage media containing old records are sanitized as prescribed in the security plan. Complete backups of the system are accomplished on a monthly basis. Data at the end of its retention period will end up residing on digital storage media for an extra month due to this process. Reports are generated in real time and only exist during the duration of the log in session. The system owner reviews records as needed to determine whether there is still a valid need to keep the information according to the records schedule described in DOE Records Schedule 18, Items 17, 18, and 19.

4) **Is the system using technologies in ways that the DOE has not previously employed?**
No

5) **How does the use of this technology affect public/employee privacy?**
N/A. The system is not using technologies in ways that the DOE has not previously employed.

6) **Will this system provide the capability to identify, locate, and monitor individuals? If yes, explain.**
Yes, the purpose of the system is to monitor visitor's visits to DOE Headquarters facilities.

7) **What kinds of information are collected as a function of the monitoring of individuals?**
The system contains name, addresses, government ID number, date of birth, facial image, times of visits to the facility, purpose of visit to the facility, and images of individuals' identification papers.

8) **What controls will be used to prevent unauthorized monitoring?**
As part of a four tier access level implemented in the system, the Protective Force personnel collect the visitors' information and check in/out visitors. They do not have monitoring ability. All personnel, especially those with augmented abilities that may allow access to all information

and those that receive generated reports that may allow for monitoring, receive training and are cognizant of security, privacy and confidentiality requirements involved with handling and properly disposing of such information.

9) **Under which Systems of Record notice does the system operate? Provide number and name.**
The system operates under the Systems of Record notice; "*Privacy Act of 1974; Publication of Compilation of Systems of Records; DOE-51 Employee and Visitor Access Control Records*". Federal Register, Vol. 68, No. 125

10) **If the system is being modified, will the system of record require amendment or revision? Explain.**
The system of record will not require amendment or revision.

F. ACCESS TO DATA

1) **Who will have access to the data in the system (Users, Managers, System Administrators, Developers, Other)?**
Protective Force personnel, Protective Force personnel Supervisors, Administrators, Super Users, System Administrators, and Database Administrators will have access to the data in the system. 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 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. Records from this system may be disclosed to Department of Defense contractors and National Aeronautics and Space Administration to authorize access to classified information and areas.

2) **How is access to the data by a user determined? Are criteria, procedures, controls, and responsibilities regarding access documented?**
User profiles are established and roles are defined for those profiles. Roles determine which users see which data. Criteria, procedures, controls, and responsibilities are documented in the system security plan.

3) **Will users have access to all data on the system or will the user's access be restricted?**
User's access will be restricted. Each user of the system is assigned a role: Guards, Guard Supervisors, Administrators and System Administrators. Each role is assigned an access level which restricts what that user type may access. Administrators and System Administrators by virtue of managing the entire system have access to all data on the system. The other user roles do not.

4) **What controls are in place to prevent the misuse (e.g., browsing) of data by those having access?**
Profiles/role control will ensure that only the data that should be accessible to that individual will appear on the screen. Each user of the system is assigned a role: Guards, Guard Supervisors, Administrators and System Administrators. Each role is assigned an access level which restricts what that user type may access. Administrators and System Administrators by virtue of managing the entire system have access to all data on the system. The other user roles do not. All users have periodic security refresher training. Windows Server logs and application logs are reviewed weekly for inappropriate activities, in accordance with DOE HQ policy and procedures, by the HSVMS operations team.

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 Privacy Act contract clauses included in their contracts and other regulatory measures addressed?**
DOE contractors are involved with the design, development and maintenance of the system. Privacy Act contract clauses and other regulatory measures are addressed in their contracts. In particular it is stated in section 13. *Protection of Federal Personally Identifiable Information (PII)*, "The Contractor is reminded of its obligation under FAR 52.224-2, Privacy Act, which is incorporated by reference into this Master Task Order under Paragraph 14 below, to protect PII on laptops and removable storage media, whether in a government facility or accessed remotely. Current DOE policy is summarized in Attachment 4 to this Modification, dated August 28, 2006 and issued by Ms. Ingrid Kolb, Director of the Office of Management. Required Action: Immediately upon execution of this award, the Contractor is required to forward a copy of this policy to all employees and subcontractor employees; a sample format cover letter is provided as Attachment 6 to this Modification. In addition to the FAR 52.224-2 clause requirements, additional guidance from the U.S. Office of Management and Budget (OMB) and the DOE Chief Information Officer (CIO) is posted on the Internet".

6) **Do other systems share data or have access to data in this system? If yes, explain?**
No data is shared with other systems. However: 1. 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. 2. 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. 3. 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. 4. Records from this system may be disclosed to Department of Defense contractors and National Aeronautics and Space.

7) **Who will be responsible for protecting the privacy rights of the employees affected by the interface?**
There is no interface to be responsible for.

8) **Will other agencies share data or have access to data in this system?**
Records from this system will not be shared with other agencies. However: 1. 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. 2. 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. 3. 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. 4. Records from this system may be disclosed to Department of Defense contractors and National Aeronautics and Space

9) **How will the data be used by the other agency?**
Records from this system will not be shared with other agencies. However: 1. 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. 2. 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. 3. 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. 4. Records from this system may be disclosed to Department of Defense contractors and National Aeronautics and Space.

10) **Who is responsible for assuring proper use of the data?**
The system owner is responsible for assuring proper use of the data. Data is generally not shared with other agencies.

PIA Approval Signatures

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