Department of Energy
Washington, DC 20585

March 29, 2007

MEMORANDUM FOR: INGRID A.C. KOLB
DIRECTOR
OFFICE OF MANAGEMENT

THRU: For JAMES N. SOLIT
DIRECTOR OF THE EXECUTIVE SECRETARIAT

FROM: ABEL LOPEZ, DIRECTOR
FOIA AND PRIVACY ACT OFFICE

SUBJECT: ACTION: Approval of Privacy Impact Assessments

ISSUE: ACTION: Approval of a Privacy Impact Assessment for the Office of Health, Safety and Security

The E-Government Act (eGov) requires agencies to conduct a PIA before (1) developing or procuring Information Technology (IT) systems or projects that collect, maintain, or disseminate information in identifiable form from or about members of the public; or (2) initiating, consistent with the Paperwork Reduction Act, a new electronic collection of information in identifiable form for 10 or more persons (excluding agencies, instrumentalities or employees of the federal government).

A PIA is an analysis of how information is handled: (1) to ensure handling conforms to applicable legal, regulatory, and policy requirements regarding privacy; (2) to determine the risks and effects of collecting, maintaining and disseminating information in identifiable form in an electronic information system; and (3) to examine and evaluate protections and alternative processes for handling information to mitigate potential privacy risks.

Attached is a PIA submitted by the Office of Health, Safety and Security. The PIA has been reviewed by the FOIA and Privacy Act Office and is being submitted for your review and signature.

RECOMMENDATION:

That you approve and sign the PIA.

NEXT STEPS:

The signed PIA will be submitted to OMB and posted on the FOIA/Privacy Act web page.

Department of Energy
Privacy Impact Assessment (PIA)

Name of Project: Electronic DOE Information Security System + (eDISS+)
Bureau: Department of Energy (DOE)
Project's Unique ID: 019-10-01-22-01-1013-00-401-121
Date: February 7, 2007

A. CONTACT INFORMATION:

1) Who is the person completing this document? April Stottler (HS-1.32), Office of Personnel Security, Office of Security Operations, Office of Health, Safety and Security, U.S. Department of Energy, HS-1.32, 1000 Independence Avenue, SW, Washington, D.C. 20585, 301-903-6208

2) Who is the system owner? Robert M. Lingan (HS-1.3), Office of Security Operations, Office of Health, Safety and Security, U.S. Department of Energy, HS-1.3, 1000 Independence Avenue, SW, Washington, DC 20585, 202-586-1461

3) Who is the system manager for this system or application? April Stottler (HS-1.32), Office of Personnel Security, Office of Security Operations, Office of Health, Safety and Security, U.S. Department of Energy, HS-1.32, 1000 Independence Avenue, SW\., Washington, DC 20585, 301-903-6208

4) Who is the IT Security Manager who reviewed this document? Tom Curtis (HS-1.22), Office of Information Management, Office of Health, Safety and Security, U.S. Department of Energy, HS-1.22, 1000 Independence Avenue, SW, Washington, DC 20585, 301-903-0521

5) Who is the Privacy Act Officer who reviewed this document? Abel Lopez, Director, Freedom of Information Act and Privacy Act Group, MA-74, U.S. Department of Energy, 1000 Independence Avenue, SW, Washington, DC 20585, 202-586-5955

B. SYSTEM APPLICATION/GENERAL INFORMATION:

1) Does this system contain any information about individuals? Yes

a. Is this information identifiable to the individual[i]? 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 is the central repository for all DOE security clearance information, including actions taken during clearance adjudication. Additionally, the system includes information on clearance requests (SF 86 data), classified visits to DOE facilities, and access to weapons data.

3) What legal authority authorizes the purchase or development of this system/application? 42 U.S.C. 7101 et seq.; 50 U.S.C. 2401 et seq.; 10 CFR part 710, subparts A and B; Executive Orders 10450 and 12968; 5 CFR part 732; DOE O 470.4-Safeguards and Security Program of 8-26-05; Personnel Security Program Manual DOE M 470.4-5 of 8-26-05; and Director of Central Intelligence Directive 6/4 of 7-2-98.

C. DATA in the SYSTEM:

1) **What categories of individuals are covered in the system?** Applicants for Department of Energy (DOE) and National Nuclear Security Administration (NNSA) employment; DOE employees including assignees and detailees, agents and consultants with the DOE, DOE contractors and subcontractors, and DOE access permittees processed for DOE access authorizations for access to classified matter or special nuclear materials; other Federal agency contractor and subcontractor applicants for employment, and their employees, detailees, agents, and consultants processed for DOE access authorizations; and other individuals processed for DOE access authorizations as determined by the Secretary.

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? Responses from the applicant's Questionnaire for National Security Positions (SF 86) are entered by the individual upon their electronic completion of the form using the Office of Personnel Management's eQIP (Electronic Questionnaires for Investigations Processing) system. Additional information is provided during the investigation and adjudication processes by Investigative and Personnel Security staff.

b. What Federal agencies are providing data for use in the system? Investigative information is provided by the U.S. Office of Personnel Management (OPM) and the Federal Bureau of Investigation (FBI).

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? Name, Social Security Number, Date of Birth and employer information are collected from the employee via DOE HQF 5631.2, Request for Clearance Action. Additional data associated with the employee may reside in the Personnel Security Database (PSDB), but is not collected directly from the employee.

3) Accuracy, Timeliness, and Reliability

a. How will data collected from sources other than DOE records be verified for accuracy? Investigation results are subject to a rigorous adjudication process before a clearance is granted or denied. Employees are given the chance to address questions that arise from the investigation.

b. How will data be checked for completeness? Validation routines in the e-DISS+ software applications ensure that data is complete and non-contradictory.

c. Is the data current? What steps or procedures are taken to ensure the data is current and not out-of-date? Yes. The data is current and updated daily with any changes, whether employee initiated or via request from other sources within DOE.

d. Are the data elements described in detail and documented? Yes, data elements are described in the PSDB Data Dictionary. The name of the document is "PSDB Data Dictionary 5.0.3 (04-06-06).doc" and it is maintained using version control.

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, the data is necessary to maintain adequate personnel security, including an accurate database of security clearances.

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/public that would not be possible without the new data? N/A**

5) **How will the new data be verified for relevance and accuracy? N/A**

6) **If the data is being consolidated, what controls are in place to protect the data from unauthorized access or use?** N/A

7) **If processes are being consolidated, are the proper controls remaining 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.** Data for an individual can be retrieved by name, social security number, or DOE number assigned to each applicant's personnel security file.

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 identify data associated with the individual's DOE access authorization and may include personal information. Access to these reports is restricted to appropriately cleared (i.e. Q-cleared) DOE and contractor personnel working in direct support of personnel security activities. The reports are used to aid the timely processing and management of DOE clearances.

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)?** Data are required for clearance processing. Individual's consent is given as part of SF-86 request.

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?** Consistency is maintained by policies documented in DOE Orders, Manuals, and Notices, such as: DOE Manual M 470.4-5, Personnel Security; DOE Manual M 470.4-2 Physical Protection; DOE Notice N 470.3, Reciprocal Recognition of Existing

Personnel Security Clearances; DOE Order O 470.4 Safeguards and Security Program.

2) **What are the retention periods of data in the system?** Data retention practices are conducted in accordance with the appropriate DOE Administrative Records Schedule. Specifically, eDISS+ complies with the requirements set forth in the *Security, Emergency Planning & Safety Records* schedule dated 1/23/2004 with authorization number N1-434-98-21. This record 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? Where are the procedures documented?** Data retention practices are conducted in accordance with the appropriate DOE Administrative Records Schedule. Specifically, eDISS+ complies with the requirements set forth in the *Security, Emergency Planning & Safety Records* schedule dated 1/23/2004 with authorization number N1-434-98-21. This record 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? No**

7) **What kinds of information are collected as a function of the monitoring of individuals? N/A**

8) **What controls will be used to prevent unauthorized monitoring? N/A**

9) **Under which Privacy Act system of records notice does the system operate?** DOE-43 "Personnel Security Files" and DOE-46 "Administrative Review Files."

10) **If the system is being modified, will the Privacy Act system of records notice require amendment or revision?** No. Neither the nature of the information (data fields) nor the manner in which it is stored will change.

F. <u>Access to Data:</u>

1) **Who will have access to the data in the system?** Restricted access is granted to users and their managers. System administrators have full access to all databases.

2) **How is access to the data by a user determined?** Roles with degrees of access are determined by the application administrator. Procedures, controls, and responsibilities for assigning system access are documented.

3) **Will users have access to all data on the system or will the user's access be restricted?** Access is restricted by predefined user roles. Additionally, each user is limited to data related to his or her DOE site.

4) **What controls are in place to prevent the misuse (e.g., unauthorized browsing) of data by those having access?** Application user roles limit users to the minimal subset of data that is required for their jobs. Database audit tables log all user actions and data changes to help ensure data integrity.

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?** Yes, the Privacy Act clauses are included in the contract and regulatory measures are addressed.

6) **Do other systems share data or have access to the data in the system? If yes, explain.** There are no systems that have direct, electronic access to the e-DISS+ databases. PSDB extracts are provided to OPM daily via the secure OPMIS Portal. The DOE Office of Personnel Security is responsible for protecting the rights of employees when information from e-DISS+ is released.

7) **Who will be responsible for protecting the privacy rights of the public and employees affected by the interface?** The DOE Office of Security Operations is responsible for assuring proper use of the data.

8) **Will other agencies share data or have access to the data in this system?** Clearance request data is shared with the appropriate investigating agency.

9) **How will the data be used by the other agency?** The data are used to determine the level of an employee's access to sensitive or classified data. Clearance request data are used to determine if an applicant is suitable for such access.

10) **Who is responsible for assuring proper use of the data?** The DOE Office of Security Operations is responsible for assuring proper use of the data.

The Following Officials Have Approved this Document

1) **System Manager**

_____ **(Signature)** _____ **(Date)**
Name: April Stottler

Title: eDISS+ Program Manager

2) **Privacy Act Officer**

Abel Lopez **(Signature)** 3/28/07 **(Date)**
Name: Abel Lopez

Title: Director, Freedom of Information Act and Privacy Act Officer

3) **Senior Privacy Official**

_____ **(Signature)** 30 MAR 07 **(Date)**
Name: Ingrid A. C. Kolb

Title: Senior Official for Privacy Policy