Department of Energy
Privacy Impact Assessment (PIA)

Name of Project:	**LLNL MSP-GSS-001**
Bureau:	**Lawrence Livermore National Laboratory, LLNS**
Project Unique ID:	**N/A**
Date:	August 1, 2008

A. CONTACT INFORMATION

1. Who is the person completing this document?

Suzanne M. Smith
Unclassified Cyber Security Site Manager
Cyber Security Program
(925) 422-4488 smith74@llnl.gov

2. Who is the system owner?

Ken Neves
Chief Information Officer
(925) 422-6712 neves3@llnl.gov

3. Who are the system managers for this system or application?

Tina M. Huston
Security Department IT Lead
(925) 424-4933 huston4@llnl.gov

Chuck Abell
Information Technology Manager
Chief Financial Officer Directorate
(925) 422-7171 abell2@llnl.gov

Marina Gonzalez
Manager Recruiting and Employment Division
(925) 423-7904 gonzalez4@llnl.gov

4. Who is the IT Security Manager who reviewed this document?

Edward J. Matsche
Cyber Security Site Manager
Cyber Security Program
Lawrence Livermore National Laboratory
(925) 422-2213 matsche1@llnl.gov

5. Who is the Privacy Act Officer who reviewed this document?

Robert Perko
LLNL Privacy Officer
Office of Laboratory Counsel
Lawrence Livermore National Laboratory
(925) 422-9501 perko1@llnl.gov

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 is an aggregation of several business applications that support the life cycle of employee and visitor management. This includes the initial pre-employment process, Security Department (Badge Office, Central Clearance and Security Awareness), and LLNL payroll systems. The applications are managed under common security architectures and share a common data aggregation (people database) and management practices. Data is protected as documented within the MSP-GSS-001 site plan.

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

N/A this is an existing system which that contains or administers information regarding LLNL employees, visitors, and vendors in identifiable form

C. DATA IN THE SYSTEM

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

Agency, contractor employees, employment candidates, and visitors are covered by this 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).

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

The system collects information for the complete life cycle of employee and visitor management. This includes job postings, interview workflow, employment offers, pre and post clearance background checks, formal clearance, training, payroll, and payment processes.

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

The system is a combination of both sources.

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

NNSA/DOE, and other outside agencies.

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, address, phone number, email address, ethnicity, gender, date of birth, education level, citizenship or visa status, work history, clearance data, physical impairments, and tax ID can be collected.

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

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

An outside vendor is used to validate accuracy of some of the data elements and the Inspector General periodically audits.

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

Internal controls within the system do initial validations at the point of data entry via software controls, through various checks by LLNL staff and by outside vendors.

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

The data is initially managed by the individual requesting consideration for employment. LLNL staff also use internal controls to ensure data currency.

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

Yes, applications which comprise this system utilize sound business practices and all data elements are described and documented within internal documents.

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, and how will this be maintained and filed?**

Yes, new data is aggregated and is protected by measures described the MSP-GSS-01 master plan and major information system appendixes.

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

The data is placed within a relational database that utilizes techniques to segregate data yet maintain normalization. The system uses a primary and composite key infrastructure to traverse the database.

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

Yes

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

An outside vendor is used for clearance material other data elements are verified for accuracy by LLNL personal with appropriate access control and roles.

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

Separation of roles and duties exist within the system for database administrators, developers, and system administrators who have elevated privileges. Operational roles exist for non-privileged users. All access is controlled by user accounts and passwords. Audit log exist and are periodically reviewed as documented in the MSP-GSS-001 security plan.

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

   Yes

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 is retrieved through control system interfaces which require a username and password. Access is also logged and retained as documented in the MSP-GSS-001 security plan.

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

   Background, education, race, gender, education, salary, home address, tax , marital status, and other employment-related reports. These reports are used to verify fair employment practices and other government mandates. Role based access controls and separation of duties provide access controls as documented in the MSP-GSS-001.

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)?**

    A limited number of individual attributes are voluntary (i.e., ethnicity).

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?**

   N/A—information is maintained at LLNL only.

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

   Retention periods are in accordance with LLNL policy. These retention periods are different for portions of the applications. Individual applications which comprise this system have documentation and procedures which clarify retention periods.

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?**

   Sensitive "paper" records are disposed of as required for Official Use Only. Electronic media is disposed in accordance with the Cyber Security Program policy.

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

   Standard commercial off the self products, well-known and agency adopted technologies are used for this system.

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

   There is no affect.

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?**

   System provides no unique monitoring capabilities. Standard physical and logical security practices are used to protect unauthorized access.

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

   This system does not fall under the Privacy Act System of Records guidance.

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

    N/A

F. ACCESS TO DATA

1. **Who will have access to the data in the system?**

   Only individuals with need to know have access to the system. This is determined by job function and application roles.

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

   Job function and need to know is used to determine access requirements.

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

   All authorized users are limited to segments of the application which fulfill their need to know criteria. This is enforced through physical and logical controls.

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

   Roles based access controls and physical access control lists are used to limit use to those with need to know.

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?**

   N/A

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

   Portions of the data are available to other LLNL systems through database links and directory services. These processes are documented, audited, and tightly controlled as documented in the MSP-GSS-001.

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

   The service managers documented in this report.

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

   No

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

   N/A

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

    N/A—data is not shared with agencies.