Privacy Impact Assessment
for the

MAXHR Solution Component
e-Performance System

June 21, 2005

Contact Point
John Allen
MAXHR Human Capital Business Systems
Department of Homeland Security
(202) 357-8285

Reviewing Official
Nuala O'Connor Kelly
Chief Privacy Officer
Department of Homeland Security
(571) 227-3813

Introducton

Background

The MaxHR Program was established by the Department of Homeland Security to implement the human capital provisions of the Homeland Security Act of 2002. The MaxHR program is a collection of functions and systems centered on a core enterprise Human Resource Management System (HRMS). The MaxHR program is part of a broader "One DHS" model where a collection of disparate and redundant systems across DHS are consolidated into enterprise wide solutions.

Performance Management and Pay for Performance are key parts of the new MaxHR program, which is scheduled to publish regulations that:

Support the Government Performance and Results Act of 1993 (GPRA) and Department and organization strategic plans;

- Align individual performance expectations with the Departmental or organizational mission, strategic goals, GPRA annual performance plans, or other department objectives and measures;
- Promote individual accountability by clearly communicating performance expectations and holding employees responsible for accomplishing them; and
- Provide for meaningful distinctions in performance to support adjustments in pay, awards, promotions, and performance-based adverse actions.

These regulations and the provisions of the E-Government Act provide the basis for identifying the requirements of the new "e-Performance" management system.

Key Goals

Currently, DHS organizational elements conduct performance management using a variety of paper-based forms containing general behavior-based standards, as well as some variation of work plans or objectives. There appear to be no consistent approaches to performance management. Furthermore, after extensive analysis, an internal e-Performance Design Team concluded that the existing DHS performance management systems would not adequately support the new MaxHR program requirements that centered on pay-for-performance. A new performance management system would be needed in order to base pay on performance. A full and open competition was conducted to procure a solution for e-Performance. Softscape was selected as the overall best value package based on its ability to provide capabilities that will enable DHS to implement an enterprise system that can efficiently automate the following functions:

- Set and Communicate Performance Expectations
- Monitor Performance and Provide Feedback
- Develop Performance and Address Poor Performance
- Rate and Reward Performance

- Produce Performance-Related Reports

Points-of-Contact

John S. Allen – Chief, Human Capital Business Systems, (202) 357-8285.

Michelle Gilder – Human Capital Business Systems Analyst, (202) 357-8250.

Reviewing Officer

Nuala O'Connor Kelly – Chief Privacy Officer, (571) 227-3813.

SECTION 1 QUESTIONS ABOUT THE DATA AND ITS PURPOSES:

1. What information is to be collected (e.g., nature and source)?

The e-Performance system chosen by DHS, Softscape, will collect employee information, competencies, performance goals, progress attained toward those goals, and will compile feedback and ratings regarding how effectively employees met those goals.

2. Why is the information being collected? Is it relevant and necessary to the purpose for which the system is being designed?

The e-Performance system will support the ongoing review and evaluation process of employees by managers. This information is essential to supporting the MaxHR program and its objectives of providing an enterprise performance management system that helps to motivate and retain DHS personnel as well as ensure appropriate compensation (i.e., through performance based pay).

3. What is the intended use of the information?

The intended use of the information is to:

- plan worker's efforts in support of organizational-wide goals and objectives
- define personal goals in support of Directorate initiatives
- establish and update competency development goals
- evaluate outcomes, performance, and core competencies
- assist in the appraisal, growth and development of DHS personnel through the convenience of a secure Internet connection through a web browser.

4. What are the sources of the information in the system? Where and how are you acquiring the information?

Information is manually entered into the system by authorized users as needed and routed to appropriate parties. Options are available to attach files and associate them with a system user. In addition, information can be imported into Softscape from existing DHS systems if required.

5. How will the information be checked for accuracy?

Employees have readily available access to this system to verify progress towards goals established by supervisors. Supervisors will monitor progress, review and verify information submitted by employees throughout the rating cycle. Data inputs can require specific formats and lengths so that users are required to re-enter or change the information to the valid format before they can proceed. Role assignments will determine who has data correction rights.

6. Will the system derive new data or create previously unavailable data about an individual through aggregation from the information collected?

Yes, the e-Performance system will derive new data or create previously unavailable data through aggregation of the collected data. Performance data will be continuously collected over time as users update their progress and supervisors assess their accomplishments. The accumulation of employee performance data combined with ratings information constitutes new data about employees.

7. Will the newly derived data be placed on the individual's record?

Yes, new information is maintained in the system as it occurs. The employee has interactive rights prior to a review cycle ending to verify the accuracy of information.

8. Can the system make new determinations about an individual that would not be possible without the new data?

Yes, the system can aggregate information that collectively derives an employee's performance rating. New determinations about individuals are made possible by the system because it provides a mechanism that allows performance information to be systematically captured and evaluated thereby improving the accuracy and quality of the performance management process.

9. How will the newly derived data be verified for relevance and accuracy?

In addition to the answer provided in question #7, during the review cycle the employee has the opportunity to verify the relevance and accuracy of the information with his or her direct manager.

10. Are the data elements described in detail and documented? If yes, what is the name of the document?

Softscape, the crux of the e-Performance system, has a technical documentation and data dictionary which will describe in detail the data elements for the system.

SECTION 2 QUESTIONS ABOUT REDRESS:

1. What opportunities do individuals have to decline to provide information?

None. The system will support OMB's performance management initiative for the department.

2. What opportunities do individuals have to consent to particular uses of the information?

Consent is given as a term of employment.

3. How do individuals grant consent concerning how their information will be used or shared?

Acceptance of position is granting consent be held accountable for performance related data. The routine process of performance management between employee and supervisor grants continual consent to this data.

4. What are the procedures for individuals to gain access to their own information?

Individual access to the e-Performance system will be username and password controlled. Individuals will only have access to their own performance information; other authorized users (e.g., supervisors) with certain access levels may also have access. System configuration will be under the control of a DHS administrator who will ensure that the appropriate hierarchical relationships are established and maintained.

5. What are the procedures for correcting erroneous information?

An editing capability will exist in the e-Performance system to allow corrections to be made interactively. Managers, supervisors and employees will be allowed to make corrections subject to access permissions.

SECTION 3 QUESTIONS ABOUT ACCESS TO THE DATA:

1. Who will have access to the data in the system (Users, Managers, System Administrators, Developers, Others) and is it documented?

The e-Performance system will allow users, supervisors, and managers to retrieve employee information. The e-Performance system was developed and architected to ensure that data security rules could be imposed and enforced based on customer specific events and activities. Some of the basic design principles that DHS intends to implement when the new system is deployed include:

- data can be segmented by entity
- aggregation and distribution rules can be enforced based on a data consumer's role
- auditing of user access events tracks data modification and review

2. How will access to the data by a user be determined?

All users must log into the system with a unique username and password. Based on this login, an employee (or supervisor/manager) is given access to performance information that he or she has been authorized to view and which is essential to job responsibilities. Access rules can be defined specifically by DHS. There are separate user profiles for function and data security rights.

3. Are criteria, procedures, controls, and responsibilities regarding access documented?

The e-Performance system has multiple levels of security, utilizing Secure Socket Layer (SSL) and usernames/passwords that guard against unauthorized access to data. Additionally, at an application level, Softscape maintains an audit log of all changes to the data on a record by record basis; all audit information is maintained within the database.

4. Will users have role-based access to data on the system limiting them to some but not all of the data?

Yes, the system is role-based and users will only have access to data determined by their roles.

5. What controls are in place to prevent the misuse (e.g. browsing, expired privileges, etc.) of data by those having access?

The e-Performance system is role-based and has username and passwords for access controls. Application level security will not allow unauthorized users to access data. Examples of controls include:

- two token authentication
- extensive audit logs of user activity within the system

- role based security only allows a user access to specific information, functions or reports within the system
- automatic log-off based on DHS defined time limit of no user activity
- strong password

6. Do other systems share data or have access to data in this system? If yes, explain. Include a discussion of who will be responsible for protecting the privacy rights of individuals affected by the interface?

The ePerformance system will share final performance rating data with DHS' core HR system and/or National Finance Center payroll records. The Office of the Chief Human Capital Officer will be responsible for protecting privacy rights.

7. Will other agencies share data of have access to data in this system (International, Federal, State, Local, Other)?

No, this is DHS internal data. Protection of employee evaluation data will adhere to existing policies.

8. How will the data be used by these other agencies?

N/A.

9. Who is responsible for assuring proper use of the data by other agencies?

N/A.

10. How will the system ensure that other agencies only get the information they are entitled to?

N/A.

SECTION 4 QUESTIONS ABOUT MAINTENANCE OF ADMINISTRATIVE CONTROLS:

1. Are the data secured consistent with agency requirements under the Federal Information Security Management Act? Specifically:

a. Affirm that the agency is following IT security requirements and procedures required by federal law and policy to ensure that information is appropriately secured.

Softscape and its hosting provider, ServerVault, will comply with appropriate security requirements and procedures under FISMA, applicable federal law, and policy for the e-Performance system. This includes establishment of effective security and privacy controls, testing of such controls, establishment of periodic monitoring of controls, and training in security awareness for personnel.

b. Acknowledge that the agency has conducted a risk assessment, identified appropriate security controls to protect against that risk, and implemented those controls.

As part of system planning, CHCO is using the Risk Management System (RMS) to generate C&A documentation for the e-Performance system. Softscape and ServerVault acknowledged that they have conducted a risk assessment, identified appropriate security controls to protect against risk, and implemented those controls.

c. Describe the monitoring/testing/evaluating on a regular basis to ensure that controls continue to work properly, safeguarding the information.

CHCO will monitor, test, and evaluate the e-Performance system on an on-going basis to ensure that controls are sufficient. Response to 1.a above relates.

d. Provide a point of contact for any additional questions from users.

John Allen, John.S.Allen@hq.dhs.gov (202) 357-8285

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

Current planning (and budget limitations) calls for the e-Performance system to be operated at one hosting facility.

3. What are the retention periods of data in the system?

Active employee records require on-line access for the duration of employment. All records, including records for separated employees, are retained in the database until they are archived. Performance records that may no longer be used should be destroyed. The General Records Schedule specifies that performance records for non-senior Executive Service employees should be destroyed when 4 years old or no longer needed; for senior Executive Service employees, when 5 years old or no longer needed. OCHCO will follow this and the NARA guidance on Employee Performance File System Records.

4. What are the procedures for expunging the data at the end of the retention period and are these procedures documented?

At DHS direction, Softscape will utilize system administrative functions to expunge data at the end of a retention period in accordance with federal security standards. Procedures will include expunging data from hard drives, tape backups, and memory to ensure complete destruction. The system will adhere to federal data archiving procedures and regulations.

5. Will the system provide the capability to monitor individuals or groups of individuals? If yes, explain.

Yes, the system is configurable for executive, administrative, and managerial users to have specialized access rights to monitor privileges for specified users and groups. The system maintains audit logs of all transactions as well as the status of individual events and all system processes from the reporting tools.

6. What controls are in place to prevent unauthorized monitoring of individuals or groups of individuals?

Softscape has a multi-tiered security model including:

- two token authentication to gain network access
- SSL (128 bit encryption)
- strong passwords
- role based security limiting privileges and access within the system

7. Under which Systems of Record Notice (SORN) does the system operate? Provide Number and Name.

This system is covered by the Office of Personnel Management's (OPM) Government 2 – Employee Performance File System Records.

SECTION 5 DECISION ANALYSIS:

1. Did you evaluate competing technologies on their privacy handling capabilities? If yes, explain.

Yes, a market survey was conducted and, through the solicitation process, all products were evaluated for their privacy handling capabilities.

2. Were any changes made to system architectures, hardware, software, or implementation plans as a result of doing a PIA? If yes, explain.

No. The system was configured with privacy concerns up front.