Privacy Impact Assessment
for the

MAXhr Corporate Leadership Council Metrics

October 7, 2005

Contact Point
Chris Cejka
Director, Strategic Planning and Evaluation Division
Human Capital Innovation
Office of the Chief Human Capital Officer
Department of Homeland Security
(202) 357-8246

Reviewing Official
Maureen Cooney
Acting Chief Privacy Officer
Department of Homeland Security
(571) 227-3813

Introduction

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

DHS has a strategic imperative to evaluate the implementation of MaxHR with a baseline measure completed by September 1, 2005. This evaluation will be accomplished with the assistance of a web-accessible Human Capital Dashboard, an analytical tool made available to DHS by the Corporate Leadership Council (CLC).

CLC's services include hosting the computer server on which will reside proprietary CLC analytic software and data sets provided by DHS. When CLC's software is applied to the DHS data sets, the result is a graphic depiction of key indicators of DHS performance in the human capital area. CLC's software also provides multiple analytical tools capable of enabling DHS managers to explore data for more precise explanations of performance. CLC maintains the server in a secure facility and control access to the server and the data.

CLC provides similar services to other federal agencies, including the Department of Justice.

Key Goals

The Human Capital Dashboard will reflect data extracted from the Human Resource Information System (HRIS) in conjunction with the National Finance Center (NFC). CLC will perform analyses on associated human capital metrics to reflect the state of DHS human resources programs and, by extension, the MaxHR program.

Points-of-Contact

Chris Cejka, Director of Human Capital Strategic Planning and Evaluation – Chris.Cejka@hq.dhs.gov, (202) 357-8246.

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

Reviewing Officer

Maureen Cooney, Acting Chief Privacy Officer – (571) 227-3813.

SECTION 1 – QUESTIONS ABOUT THE DATA AND ITS PURPOSES:

1.1 What information is to be collected?

The Corporate Leadership Council (CLC) will collect data extracts from the National Finance Center (NFC) personnel system relating to employee demographics, employment status, salaries, and organizational information. DHS will determine which specific data elements are required for analysis. The elements to be collected are derived from nature of action code data rather than from each individual's record, e.g. promotion, retirement, incentive pay, performance appraisal rating. The elements to be collected do not include names, social security number, geographic location, or any other field that would allow an individual employee to be identified. All data are aggregated prior to presentation on the dashboard. It is not possible to identify individuals with the data used. Please see the attached CLC Extract Data Fields table for the complete list of data fields.

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

The purpose of collecting these data is to assess the overall characteristics and performance of DHS human resources programs and MaxHR.

1.3 What is the intended use of the information?

The intended use of the information is to assess the effectiveness and efficiency of DHS human resources programs and MaxHR. These organizational-level performance assessments will allow DHS to develop strategies for attaining department objectives for human resource programs.

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

The only source of information that will be fed into the Human Capital Dashboard is the NFC system. There will be no permanent electronic bridge or inter-system interface between DHS and CLC. Information is transferred through CD format at least once a year if not quarterly.

In a secure environment, DHS extracts the data from NFC via FOCUS reports. The extract is imported into a Microsoft Access database where DHS creates queries to export non-sensitive data into a spreadsheet that is saved on a secure CD. The secure CD is passed onto CLC through coordination from the Human Capital Strategic Planning and Evaluation group. CLC creates the dashboard from the spreadsheet that contains non-sensitive data.

1.5 How will the information be checked for accuracy?

Once the CD that is provided to CLC is produced, it is up to date by virtue of it being the most recent information available to DHS. CLC will submit the data to a stringent verification process that includes descriptive statistical analyses (i.e., ranges, frequency distributions). This will ensure that erroneous data are identified and deleted or corrected. DHS will approve the results of the verification process, ensuring that data collected and reported upon is accurate.

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

No, the system will not create new data about an individual. DHS will make performance assessments by grouping existing data fields to reflect aggregated information and statistical insights on HR programs, e.g., how many new hires occurred during a certain period of time.

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

No new data will be placed on the individual's record.

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

No. The system will allow DHS to assess the effectiveness and efficiency of human resource management.

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

Not applicable.

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

The data elements are consistent with those described in the OPM's Central Personnel Data File (CPDF), OPM's Guide to Personnel Data Standards, and NFC records. They also are described in detail in the CLC Data Extract Template (copy attached). This template is a list of 57 field names, less than half of which are required elements for the DHS dashboard. DHS may provide optional data elements as deemed necessary.

SECTION 2 – QUESTIONS ABOUT REDRESS:

2.1 What opportunities do individuals have to decline to provide information?

Because information capable of identifying an individual is not used, this question is not applicable.

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

Not applicable. Individual data will not be reflected on the human capital dashboard.

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

Not applicable. Individual data will not be reflected on the human capital dashboard.

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

Not applicable. Individual data will not be reflected on the human capital dashboard.

2.5 What are the procedures for correcting erroneous information?

Not applicable. Individual data will not be reflected on the human capital dashboard.

SECTION 3 – QUESTIONS ABOUT ACCESS TO THE DATA:

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

DHS will develop a system access plan that will limit access to managers and analysts who have the responsibility of assessing the management of human resources. CLC and DHS will maintain documentation to track access.

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

Access to the system will be determined by the DHS/CLC team through user and role maintenance.

3.3 Are criteria, procedures, controls, and responsibilities regarding access documented?

Yes, CLC and DHS will maintain documentation to track access. The ability to grant access is controlled through role-based security.

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

Yes, role-based security will be applied to all users.

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

Access is controlled through role-based security. Accounts can be made active or inactive and accounts expire automatically if not used within a specific time period.

3.6 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?

No. No other systems share this data.

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

No. No other agencies will have access to the data in this system. Aggregated information on the dashboard may be viewed by CLC only in order to create benchmarks for comparison to other agencies, but DHS can only view its own information and other agencies cannot view DHS' information.

3.8 How will the data be used by these other agencies?

Not applicable. Data will not be used by other agencies.

3. 9 Who is responsible for assuring proper use of the data by other agencies?

Not applicable. Data will not be used by other agencies.

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

Not applicable. Data will not be used by other agencies.

SECTION 4 – QUESTIONS ABOUT MAINTENANCE OF ADMINISTRATIVE CONTROLS:

4.1 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.

DHS/CLC will follow all applicable security requirements and apply the necessary procedures required by federal law and policy to ensure that information remains secure.

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 all system planning, the Office of the Chief Human Capital Officer (OCHCO) is using the Risk Management System (RMS) to generate C&A documentation. The Department of Justice (DOJ) has already awarded an Authorization to Operate for this system; therefore, DHS will generate an Interconnect System Agreement (ISA) with DOJ to satisfy the C&A requirement.

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

Although there will be no electronic bridge between DHS and CLC, OCHCO will monitor, test, and evaluate the CLC system on an on-going basis to ensure that controls are sufficient. MaxHR will conduct site visits to ensure compliance with NIST SP 800-53 and 800-26 requirements, additional site visits will include vulnerability and patch management verifications for compliance with CSIRC Alerts. Site Visits will cover areas such as (but not limited to) auditing, account management, records management, Configuration Management, firewall, and intrusion detection logs.

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

The DHS POC is Chris Cejka, Chris.Cejka@hq.dhs.gov, (202) 357-8246.
Systems questions can be directed to John Allen, John.S.Allen@hq-dhs.gov, (202) 357-8285.

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

Not applicable. The system will be housed in one site.

4.3 What are the retention periods of data in the system?

Data will be available for up to four years.

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

CLC will expunge data after four years. CLC is familiar with data retention policies in the federal sector. Their clients include Department of Justice and General Accountability Office.

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

No. While this tool has the capability of collecting and analyzing workforce metrics, the purpose of the Human Capital Dashboard is monitor the overall health of HR programs. OCHCO has no intention to monitor specific individuals. Data configuration will preclude monitoring at the individual level.

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

Role-based access controls will be used to prevent unauthorized use of the CLC tool.

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

Design and construction of the DHS dashboard has only recently begun. Data elements need to be verified and the system has to be tested. The deployment schedule calls for the dashboard to be operational in September 2005. Currently a SORN is not planned because the CLC Metrics system will not collect or retrieve data based on personal identifiers.

SECTION 5 – DECISION ANALYSIS:

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

The CLC metrics tool was selected based on its unique capabilities to portray workforce metrics, its proven track record in the human capital management area, and the Council's experience providing similar services to other federal agencies such as the Department of Justice and the General Accountability Office.

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

Yes. After completing this PIA and consulting with the Privacy Office, it was determined that rather than using full date of birth for evaluation purposes that the birth year was sufficient.

Responsible Officials

Chris Cejka, Director of Human Capital Strategic Planning and Evaluation – Chris.Cejka@hq.dhs.gov, (202) 357-8246.

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

Department of Homeland Security, Office of the Chief Human Capital Officer

Approval Signature Page

_____ October 7, 2005

Maureen Cooney
Acting Chief Privacy Officer
Department of Homeland Security