Privacy Impact Assessment
for the

Eversity Enterprise System

September 14, 2010

Contact Point
Junish A. Arora
Office for Civil Rights and Civil Liberties
(202) 254-8236

Reviewing Official
Mary Ellen Callahan
Chief Privacy Officer
Department of Homeland Security
(703) 235-0780

Abstract

The Office for Civil Rights and Civil Liberties (CRCL) Equal Employment Opportunity (EEO) Program operates the Eversity Enterprise System. Eversity is an electronic records system used in workforce analysis,[1] tracking, management, and reporting required under Equal Employment Opportunity Commission (EEOC) Management Directive (MD) 715. CRCL EEO has conducted this Privacy Impact Assessment (PIA) because Eversity collects and stores personally identifiable information (PII).

Overview

Pursuant to the regulations of EEOC at 29 CFR Part 1614, DHS operates EEO programs. CRCL directs the Department's EEO programs, including the development and implementation of Departmental EEO policy. CRCL is committed to developing an EEO program where all employees and applicants for employment enjoy equality of opportunity regardless of race, sex, national origin, color, religion, age, or disability, without fear of reprisal. The chief objectives of the EEO program include: providing leadership to component EEO offices; integrating principles of EEO into DHS leadership training; establishing model Title VII of the Civil Rights Act of 1964 and Rehabilitation Act programs; collaborating closely with the Office of the Chief Human Capital Officer (OCHCO) to develop solutions for building a high quality workforce; working with the OCHCO, General Counsel, and DHS components to create a Departmental approach to Alternative Dispute Resolution; and establishing proactive measures to reduce EEO complaints.

In an effort to ensure that federal agencies adhere to this commitment to equality of opportunity, EEOC regulations, 29 C.F.R. § 1614.601, require that each agency establish a system to collect and maintain accurate employment information on the race, national origin, sex, and disability of its employees and applicants for employment. Further, EEOC MD-715 mandates that agencies submit an annual report on the federal workforce disclosed only in the form of gross statistics, or aggregate form. In order to ensure individual privacy, agencies must use an automated data processing system in accordance with standards and requirements prescribed by the EEOC to collect or maintain any information on the race, national origin or sex of individual employees thereby providing an additional layer of separation of that information from personnel records. Eversity is the employment database and management solution DHS utilizes to fulfill this directive and issue the MD-715 annual report.

Eversity provides a Summary Analysis of Workforce that allows an agency to analyze their employees and applicants by occupational categories and groupings, minority groupings, personnel actions. The statistical records within Eversity provide an overview of workforce distribution for the current and prior fiscal year and net changes. Administration of this system is crucial to identifying barriers,[2] objectives, and action items affecting diversity and representation in DHS, which is required in the MD-715 annual report.

Employee PII used in Eversity to generate statistical analysis is pulled from the National Finance Center (NFC), the payroll/personnel system for DHS, via the DHS Office of Chief Human Capital Officer (OCHCO). The original source of the information in the system is typically employees and applicants.

---

[1] Workforce analysis is a comparison between the internal representation of designated group members in an employer's workforce and the external labor pool of designated group members from which the employer can reasonably be expected to recruit; and analysis of hiring, promotion, and termination data, along with an analysis of whether designated group members are concentrated in the lower levels of occupational groups with underrepresentation.

[2] Barrier identification is the process by which agencies uncover, examine, and remove barriers to equal participation at all levels of the workforce.

Eversity is subject to the following controls:

(1) Only those categories of race and national origin and the specific procedures for the collection and maintenance of data that are prescribed by the EEOC may be used;
(2) The agency may use the data only in studies and analyses which contribute affirmatively to achieving the objectives of the equal employment opportunity program. An agency shall not establish a quota for the employment of persons on the basis of race, color, religion, sex, or national origin; and
(3) Data on handicaps shall be collected only by voluntary self-identification.

Eversity is replacing the initial business process management tool, FALCON, which is being decommissioned. Upon decommissioning, the data in FALCON will migrate into Eversity.

Section 1.0 Characterization of the Information

1.1 What information is collected, used, disseminated, or maintained in the system?

Eversity captures the following subset of PII on DHS employees and applicants, which is limited to that personnel data that is necessary to perform workforce analysis:

- Unique identifier hashed[3] or encrypted from the Social Security Number (SSN);
- Gender;
- Race ID (a numeric value corresponding to a race);
- Pay plan and grade;
- Disability code;
- Training; and
- Awards.

Once current employee and applicant information is input into Eversity by payroll and personnel staff at the DHS component agencies, the system performs extensive automated statistical and comparative analyses. By automating the organization and analysis of all required MD-715 data, Eversity ensures consistency of results and provides users with the following reports, plans, summaries, and trend analyses as recommended by the EEOC:

- Number of workers, categorized by:
  - Major Occupations
  - Occupational Groupings
  - Race/Ethnicity Groupings
  - Grade and Series
  - Personnel Actions such as promotions, accessions, separations, training, & awards
- Number of agency personnel with targeted disabilities, by group
- Statement of goals for each underrepresented group

[3] Hashing is the procedure that takes the block of SSN data and returns a fixed-size bit string, the (cryptographic) hash value, such that an accidental or intentional change to the data will change the hash value. The cryptographic hash function makes it infeasible to find a message that has a given hash.

- Analysis of barriers or impediments to EEO
- Set of plans for barrier identification and removal
- Set of Diversity Management plans
- Trending analysis for each fiscal year showing current number of agency employees and indicating any changes in workforce from the previous fiscal year
- All statistical data needed for EEOC MD 715 Tables A & B
- Ad-hoc workforce reporting capabilities

1.2 What are the sources of the information in the system?

Eversity data is self-reported by the employees and applicants and applicants via OMB-approved forms and personnel systems. As part of the application to a DHS position, applicants are asked to fill out the OMB No. 3046-0046 to collect applicant flow data regarding ERI to determine whether recruitment efforts reach all segments of the population. As part of on-boarding, employees are asked to fill out an SF-181, Ethnicity and Race Identification, and SF-296, Self-Identification of Disability. Because individuals who are not DHS employees apply for positions, PII about non-DHS employees may be collected.

1.3 Why is the information being collected, used, disseminated, or maintained?

The information is collected to analyze and report on different aspects of DHS workforce data as required by MD 715, including the number of workers, categorized by Major Occupations, Occupational Groupings, Race/Ethnicity Groupings, Grade and Series, Number of agency personnel with targeted disabilities, by group, and Personnel Actions such as promotions, accessions, separations, training, and awards.

1.4 How is the information collected?

Eversity data is self-reported by the employees and applicants via OMB-approved forms and personnel systems. Employee and applicant PII is input by payroll and personnel staff at the DHS component agencies into NFC. The personnel PII is then extracted from NFC and placed into a flat file[4] at the OCHCO. If SSN is captured, it is encrypted and hashed into a unique identifier (UID). CRCL then requests quarterly data pulls from this flat file from OCHCO.

1.5 How will the information be checked for accuracy?

Upon receipt, quarterly data pulls are reviewed for accuracy based on statistical and historical trends as well as input from OCHCO Human Capital Business Services (HCBS) as to drivers for workforce trends and anomalies. Component EEO offices are also responsible for checking for accuracy in data and consulting with component human capital offices.

[4] A flat file is a means to encode a database model, usually a table, as a singular file, which contains one record per line.

1.6 What specific legal authorities, arrangements, and/or agreements defined the collection of information?

The EEOC Regulations at 29 C.F.R. § 1614.601 provide that each agency shall establish a system to collect and maintain accurate employment information on the race, national origin, sex, and disability of its employees.

Ethnicity and race indicator (ERI) information is also requested under the authority of 42 U.S.C. § 2000 e-16 and in compliance with the Office of Management and Budget's (OMB) 1997 Revisions to the Standards for the Classification of Federal Data on Race and Ethnicity.

Collection of disability information is authorized by the Rehabilitation Act of 1973 (P.L. 93-112). The information furnished is used for the purpose of producing statistical reports to show agency progress in hiring, placement, and advancement of disabled individuals and to locate individuals for voluntary participation in surveys.

1.7 Privacy Impact Analysis: Given the amount and type of data collected, discuss the privacy risks identified and how they were mitigated.

There is an inherent risk of collecting more information than necessary when gathering data for use in any system. The scope of information collected in Eversity, however, is limited to the amount of data necessary to perform workforce analysis. Although the system stores PII provided by NFC, the privacy risks are mitigated to the extent possible because SSN is hashed before being loaded into Eversity, no name is associated with the PII, and only information that is relevant to track personnel data, and actions data (such as awards, training, promotions, disciplinary actions) is captured.

Section 2.0 Uses of the Information

2.1 Describe all the uses of information.

The information collected is used to properly collect and maintain accurate employment information on the race, national origin, sex and disability of its employees, to eliminate barriers to equal participation at all levels of the workplace, and to report to EEOC on employment by race, national origin, sex, and disability.

2.2 What types of tools are used to analyze data and what type of data may be produced?

Through this aggregation of data, one can obtain new information such as workforce trends, drivers, and factors. Evaluating current employee and demographic data will help identify future needs as well as a projected workforce strategy.

Search functionality consists of searching at the Departmental or component level, extracting data by race, national origin, sex, and disability, and analyzing employment data by quarter or fiscal year. The system has the ability to create all statistical data needed for EEOC MD 715 Tables A & B.

2.3 If the system uses commercial or publicly available data please explain why and how it is used.

Eversity does not use commercial or publicly available data.

2.4 Privacy Impact Analysis: Describe any types of controls that may be in place to ensure that information is handled in accordance with the above described uses.

The privacy risk associated with the uses of the information is that unauthorized users may view stored information or use the information for reasons that are inconsistent with the original purpose for which the information was collected. To mitigate this risk, access is limited to those who need to know the information to perform job functions based upon those pre-defined user roles and permissions. Access restrictions are based upon membership in at least two groups – a component group and permissions group. The component group is the specific DHS component. The permissions group consists of the privileges associated with specific roles relating to the user's main functions, administrative rights, system navigation, processing options, and searching and reporting options. These reduce risks because system role details can be specified and delineated.

Furthermore, approved users are trained on the proper use of EEO statistical information in the system by a combination of classroom and on-the-job training as well as complete annual privacy training. Classroom training is for both administrative users and management and functional end-users. Training includes a review of user roles and permissions. The training manual includes an overview of component and permissions groups.

Section 3.0 Retention

3.1 How long is information retained?

EEO Records are governed by General Records Schedule (GRS) 1, Item 25. Employment information may be retained for five years after the quarterly HR pull of information.

3.2 Has the retention schedule been approved by the component records officer and the National Archives and Records Administration (NARA)?

Yes, records shall be disposed of in accordance with the National Archives and Records Administration revised General Records Schedule 1, Item 25 (EEO Records).

3.3 Privacy Impact Analysis: Please discuss the risks associated with the length of time data is retained and how those risks are mitigated.

Regardless of the length of time the data is retained, the mere retention of the data creates potential risks. These risks increase over time and proportionally with the size of the database and the amount of data stored. The retention of data increases the risk of deliberate or accidental exposure of PII. However, the nature of workforce data, in particular trend analysis, requires a statistically significant pool of archival data over the course of years to properly assess the EEO climate and the efficacy of process improvement and pilot programs. Those risks are minimized by the controls and firewalls discussed herein.

Data retained in the system is primarily statistical and related to EEO workforce trends. Minimal information is retained regarding the persons being tracked. The purpose of the retention provides the agency with areas of concentration for training or potential issues for redress.

Section 4.0 Internal Sharing and Disclosure

4.1 With which internal organization(s) is the information shared, what information is shared and for what purpose?

All DHS components will use Eversity to manage their EEO workforce data. The following is a list of component groups in the system:

- Customs and Border Protection (CBP)
- U.S. Citizenship and Immigration Services (USCIS)
- Federal Emergency Management Agency (FEMA)
- Federal Law Enforcement Training Center (FLETC)
- Headquarters (HQ)[5]
- Immigration and Customs Enforcement (ICE)
- Transportation and Security Administration (TSA)
- U.S. Coast Guard (USCG)
- U.S. Secret Service (USSS)

Each component can see only data pertaining to their respective cases; only CRCL has access to all departmental data.

4.2 How is the information transmitted or disclosed?

A flat file containing the workforce data is pulled from NFC by OCHCO HCBS. The flat file consists of both personnel data and actions data in TXT format. If SSN is captured, it is encrypted and hashed into a

[5] Directorates such as National Protection and Programs Directorate (NPPD) and Intelligence and Analysis, Office of (I&A) fall within HQ for purposes of EEO complaint tracking.

UID. Separately, USCG Community Services Command sends Non-Appropriated Fund (NAF) data in EXCEL format. The combined data file is then uploaded into Eversity.

4.3 Privacy Impact Analysis: Considering the extent of internal information sharing, discuss the privacy risks associated with the sharing and how they were mitigated.

When the flat file is transferred from OCHCO to CRCL it is password-protected. As mentioned above, SSN is encrypted and hashed into a UID to ensure privacy risks are mitigated. Eversity has a system of firewalls so that only approved users have access to confidential and sensitive data based upon pre-defined user roles and permissions, essentially access on a "need-to-know" basis. DHS components can access their records only while CRCL has access to all DHS workforce records. While certain information is mandatory, most of the information collected is captured only where it is relevant to workforce analysis.

Each user on the Eversity is a member of at least two groups – a component group and a permissions group. Together, they provide the access restrictions that determine the data available for each user. Component groups restrict a user's actions to the workforce functionalities of a specific DHS component.

Section 5.0 External Sharing and Disclosure

5.1 With which external organization(s) is the information shared, what information is shared, and for what purpose?

Routine workforce information, such as total workforce, permanent workforce, grade distribution, major occupations, applicant flow, awards, and separations, is disclosed through e-mail and telephone to Congressional offices and EEOC. In addition, information aggregated into annual reports is forwarded to EEOC.

5.2 Is the sharing of personally identifiable information outside the Department compatible with the original collection? If so, is it covered by an appropriate routine use in a SORN? If so, please describe. If not, please describe under what legal mechanism the program or system is allowed to share the personally identifiable information outside of DHS.

Yes, as part of the maintenance of an EEO program at DHS, DHS is responsible for reporting various aspects of the EEO program including but not limited to a self-assessment on at least an annual basis to monitor progress, identify areas where barriers may operate to exclude certain ERI groups and develop strategic plans to eliminate identified barriers. Information sharing is covered under the government-wide SORN OPM/GOVT-7 Applicant Race, Sex, National Origin and Disability Status Records, 71 FR 35356 published on June 19, 2006.

5.3 How is the information shared outside the Department and what security measures safeguard its transmission?

Information is shared externally via letter, e-mail, or telephone. CRCL has begun to require that all such external requests for information be made in writing to verify the identity of the requester. Written responses are always sent via certified return receipt mail.

5.4 Privacy Impact Analysis: Given the external sharing, explain the privacy risks identified and describe how they were mitigated.

The external sharing of information brings about the risk of deliberate or accidental exposure of PII. As mentioned above, CRCL requires that all such external requests for information come in writing to verify the identity of the requester and has written responses sent via certified return receipt mail. CRCL is developing SOPs to further system controls and handling guidelines.

There is also a risk that a statistical request may be on an underrepresented group composed of small numbers making the identification of specific individuals more likely. To mitigate this risk, CRCL reviews each request on a case by cases basis releasing information only when there is an articulated need-to-know and in accordance with all routine uses.

Section 6.0 Notice

6.1 Was notice provided to the individual prior to collection of information?

Yes, the Department's EEO Program operates under the government-wide SORN OPM/GOVT-7 Applicant Race, Sex, National Origin and Disability Status Records, 71 FR 35356 published on June 19, 2006.

Notice is provided at the component level to the individual prior to the collection of the information. As part of the application to a DHS position, applicants are asked to fill out an OMB-approved form, such as OMB No. 3046-0046, to collect applicant flow data regarding ERI to determine whether recruitment efforts reach all segments of the population. As part of on-boarding, employees are asked to fill out an SF-181, Ethnicity and Race Identification, and SF-296, Self-Identification of Disability. Individuals are provided a privacy statement that explains use of this information by DHS.

6.2 Do individuals have the opportunity and/or right to decline to provide information?

Individuals may decline to provide the requested ERI information, but doing so may result in the agency identifying the employee's ERI based upon the records supporting the employment or by visual observation.

6.3 Do individuals have the right to consent to particular uses of the information? If so, how does the individual exercise the right?

Complainants consent to uses of the information to the extent such information is used for EEO purposes. To the extent that such information is used not in the ordinary course of business, individuals' consent would be solicited.

6.4 Privacy Impact Analysis: Describe how notice is provided to individuals, and how the risks associated with individuals being unaware of the collection are mitigated.

Notice is provided in the SF-181 and SF-256. DHS OCHCO and component HC Offices are responsible for capturing ERI data in the forms according to their internal operating procedures. Such notices ensure that the individual is aware that the collection of information will be included in an agency system of records.

Section 7.0 Access, Redress and Correction

7.1 What are the procedures that allow individuals to gain access to their information?

Individuals may file a request under the Privacy Act or Freedom of Information Act (FOIA) or contact their servicing HC Office. FOIA requests for HC purposes should be mailed to Department of Homeland Security, Office of Chief Human Capital Officer, 245 Murray Lane, SW, Bldg. 410, MS 0175, Washington DC, 20528. Once an individual reviews their information they may make a written request to the component HC Officer to correct information. Contact information for the component HC Officer is available on the component intranet web sites. An individual can typically e-mail, telephone, or write to their HC office.

7.2 What are the procedures for correcting inaccurate or erroneous information?

Individuals may contact their servicing HC Office or file a request under the Privacy Act or the FOIA. Contact information for the component HC Officer and servicing HC office is available on the component intranet web sites. An individual can typically e-mail, telephone, or write to HC office. HC Officers correct information upon written request.

7.3 How are individuals notified of the procedures for correcting their information?

Mechanisms for correcting information are set forth above as well as in OPM/GOVT-7, 71 FR 35356.

7.4 If no formal redress is provided, what alternatives are available to the individual?

Appropriate redress is provided.

7.5 Privacy Impact Analysis: Please discuss the privacy risks associated with the redress available to individuals and how those risks are mitigated.

Any risk that an individual may not be afforded adequate opportunity to correct information is mitigated by allowing individuals to request access or amendment of their records at any time. Privacy risks are further minimized as an individual seeking redress may bypass the component HC office and seek redress directly from OCHCO.

Section 8.0 Technical Access and Security

8.1 What procedures are in place to determine which users may access the system and are they documented?

Eversity has a system of firewalls so that only approved users have access to confidential and sensitive data based upon pre-defined user roles and permissions. DHS components can only access their own records while CRCL has access to all records as it is responsible for the final aggregation of all DHS workforce data.

Each user on the Eversity system is a member of at least two groups – a component group and a permissions group. Together, they provide the access restrictions that determine the actions available for each user. Component groups restrict a user's actions to the reports, documents, and functionalities of a specific DHS component.

Permission groups restrict a user's actions to certain types of functionality. The following is a list of some permission groups in the Eversity system:

- System Administrator
- IT Administrator
- Eversity Administrator
- Advanced User
- Basic User
- ERI User
- Targeted Disability (TD) User

In addition, logon names and passwords control access.

The individual designated as the "System Administrator" by each Component EEO Director grants

access to Eversity based on the user's role. System Administrators will have universal access to his/her Component's workforce data within Eversity. An individual may have access to tracking as few as 4000 employees or as many as over 190,000 employees, which comprises the entirety of the Eversity database, depending upon the user's permissions and role.

Procedures for roles-permissions/access are documented in the Eversity Users' Guide.

Paper records, primarily relating to the MD 715 Reports and other Diversity Reports, are also archived periodically per NARA General Records Schedule for EEO Records.

Permission to view audit trails in Eversity is currently restricted to advanced users onlyand is controlled by CRCL.

8.2 Will Department contractors have access to the system?

DHS contractors have access to Eversity depending upon their role and permissions. Within Component EEO Offices and CRCL, there are contractors in the positions of EEO Assistants, EEO Specialists, and Program Managers who are required to use the database to complete their contracted duties. However, administrator functionalities for the database are limited to federal employees, typically senior EEO Specialists or EEO Managers.

8.3 Describe what privacy training is provided to users either generally or specifically relevant to the program or system?

DHS employees are required to take annual privacy and security training.

8.4 Has Certification & Accreditation been completed for the system or systems supporting the program?

Certification and accreditation with FISMA will occur before that system goes live.

8.5 What auditing measures and technical safeguards are in place to prevent misuse of data?

Inactive sessions will be expired according to MD 4300 to prevent unauthorized access. Passwords expire every 90 days. Search, view, edit, and/or deletion of data is limited by roles.

8.6 Privacy Impact Analysis: Given the sensitivity and scope of the information collected, as well as any information sharing conducted on the system, what privacy risks were identified and how do the security controls mitigate them?

Each DHS component maintains paper records of EEO diversity reports and workforce tables. These reports and documents are stored in file cabinets in areas restricted to EEO professionals. Reports can only be accessed if there is a need-to-know. Paper records are transferred intra-agency when necessary. Paper records are also archived periodically per NARA General Records Schedule for EEO Records.

Section 9.0 Technology

9.1 What type of project is the program or system?

The Eversity system is a fully operation IT system developed under DHS standards and in conformance with the requirements of OMB, EEOC, and Congress for EEO programs.

9.2 What stage of development is the system in and what project development lifecycle was used?

Eversity is fully operational.

9.3 Does the project employ technology which may raise privacy concerns? If so please discuss their implementation.

No. The technology employed is standard IT case management software supported by the DHS network.

Approval Signature

Original signed copy on file with the DHS Privacy Office

Mary Ellen Callahan
Chief Privacy Officer
Department of Homeland Security

APPENDIX

Privacy Act Notice: Collection of this information is authorized by the Equal Employment Opportunity Act of 1972, 42 U.S.C. § 2000e-16; the Age Discrimination in Employment Act of 1967, as amended, 29 U.S.C. §633a; the Rehabilitation Act of 1973, as amended, 29 U.S.C. § 794a; and Executive Order 11478, as amended. This information will be used to adjudicate complaints of alleged discrimination and to evaluate the effectiveness of the Equal Employment (EEO) program. As a routine use, this information may be disclosed to an appropriate government agency, domestic or foreign, for law enforcement purposes; where pertinent, in a legal proceeding to which Office of Civil Rights and Liberties (OCRL) is a party or has an interest; to a government agency in order to obtain information relevant to a OCRL decision concerning employment, security clearances, contract, licenses, grants, permits or other benefits; to a government agency upon its request when relevant to its decision concerning employment, security clearances, security or suitability investigations,contracts, licenses. Grants or other benefits; to a congressional office request, to an expert, consultant or other person under contract with the OCRL to fulfill an agency function; to the Federal Records Center for storage; to the Office of Management and Budget for review of private relief legislation; to an independent certified public accountant during an official audit of finances; to an investigator, administrative judge or complaints examiner appointed by the Equal Opportunity Commission for investigation of a formal EEO complaint under 29 CFR 1614; to the Merit Systems Protection Board or Office of Special Counsel for proceedings or investigations involving personnel practices and other matters within their jurisdiction; and to a labor organization as required by the National Labor Relations Act. Under the Privacy Act provision, the information requested is voluntary for the complainant, and for OCRL employees and other witnesses.