Privacy Impact Assessment
for the

Icomplaints

Complaint Enterprise System

July 8, 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

AILA InfoNet Doc. No. 10072964. (Posted 07/29/10)

Abstract

The Office for Civil Rights and Civil Liberties (CRCL) Equal Employment Opportunities (EEO) Program operates the Icomplaints Complaint Enterprise System. Icomplaints is an electronic records system used to track complaints and supporting documentation relating to individual and class complaints of employment discrimination and retaliation prohibited by Department of Homeland Security (DHS) civil rights statutes. Icomplaints will replace EEO Eagle as EEO Eagle is being decommissioned. CRCL EEO has conducted this Privacy Impact Assessment (PIA) because Icomplaints collects and stores personally identifiable information (PII).

Overview

Pursuant to the regulations of the Equal Employment Opportunity Commission (EEOC), 29 CFR Part 1614, and DHS Delegations 3095 and 19002, 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, and without fear of reprisal. Similarly, a discrimination complaint may be filed on the basis of sexual orientation, parental status, or protected genetic information, which are protected by Executive Order. 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 Chief Human Capital Officer (CHCO) to develop solutions for building a high quality workforce; working with the CHCO, General Counsel, and DHS components to create a Departmental approach to Alternative Dispute Resolution; and establishing proactive measures to reduce EEO complaints.

In order to improve reporting and base functionality, DHS is transitioning from EEO Eagle to Icomplaints. EEO Eagle will exist until all data is migrated over to Icomplaints, at which point it will be decommissioned. This will provide for enhanced reporting, greater efficiency, and lower cost.

All DHS components use Icomplaints to manage their EEO case files. 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)[1]
- Federal Law Enforcement Training Center (FLETC)
- Headquarters (HQ)[2]
- Immigration and Customs Enforcement (ICE)
- Transportation Security Administration (TSA)
- U.S. Coast Guard (USCG)

[1] FEMA has already been using Icomplaints for a number of years.
[2] 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.

AILA InfoNet Doc. No. 10072964. (Posted 07/29/10)

- U.S. Secret Service (USSS)
- Final Action--CRCL

Each component can see only data pertaining to its respective cases; only CRCL has access to all departmental data as it is responsible for final adjudication of all EEO complaints.

Aggrieved persons who believe they have been discriminated against must contact an agency EEO counselor prior to filing a formal complaint. The person must initiate counselor contact within 45 days of the matter alleged to be discriminatory. As soon as an EEO contact is established at a servicing EEO office at the component level, designated EEO personnel will create a case in Icomplaints, starting with the "New Case Options" module; the counselee and/or complainant does not have access to or cannot modify entries in Icomplaints, unless he/she is a TSA employee accessing the eFile module. The steps of a case are organized into individual modules. From the "New Case Options" module, depending on the values entered, different tasks will be assigned. This ensures that each case goes through the appropriate path in the complaints process, and that all required information is collected at each stage.

Within 30 days of the initial contact date, the aggrieved person must complete counseling with the EEO Counselor. If the matter is not resolved in that time period, the Counselor must inform the individual in writing of the right to file a discrimination complaint through a Notice of Final Interview. The complainant must file a complaint with the agency that allegedly discriminated against the individual within 15 days of receipt of the Notice of Final Interview.[3] The agency must acknowledge receipt of the complaint in writing and must investigate the complaint within 180 days of the filing date. The agency must develop a "complete and impartial" factual record of the claims raised by the complaint.[4] A copy of the investigative file must be provided to the complainant, along with a notification that, within 30 days of receipt of the file, the complainant has the right to request a hearing and a decision from an EEOC Administrative Judge (AJ) or may request an immediate final decision from the agency. The AJ must conduct the hearing and issue a decision on the complaint within 180 days of receipt of the complaint file from the agency. When an AJ has issued a decision, the agency must take final action on the complaint by issuing a final order within 40 days of receipt of the hearing file and the AJ's decision. The final order must notify the complainant whether or not the agency will fully implement the decision of the AJ and shall contain notice of the complainant's right to appeal to EEOC or to file a civil action.

The records within Icomplaints are used to track and monitor EEO complaints as the complaints are processed through the administrative process outlined above. Icomplaints is also used to assign cases and manage workload, and run EEOC-mandated reports as well as custom reports. In addition to collecting PII about complainants, this system allows EEO personnel to enter data collected from the complainant's co-workers, supervisors, witnesses, and legal representatives of parties. Administration of this system is crucial to the timely adjudication of the rights of all individuals involved in the complaint process.

There are several add-on modules that components can procure such as the Quality Review Module (QRM) and efile. Efile provides an electronic option for a TSA employee to initiate the EEO complaint process and review the status of his/her complaint as it is being processed throughout the

[3] During the final interview with the aggrieved person, the EEO Counselor should discuss what occurred during the EEO counseling process in terms of attempts at resolution. The Counselor must not indicate whether s/he believes the discrimination complaint has merit. Since EEO counseling inquiries are conducted informally and do not involve sworn testimony or extensive documentation, the Counselor 1) cannot make findings on the claim of discrimination, and 2) should not imply to the aggrieved person that his/her interpretation of the claims of the case constitutes an official finding of the agency on the claim of discrimination.
[4] 29 CFR § 1614.108(b)

AILA InfoNet Doc. No. 10072964. (Posted 07/29/10)

complaint process. This module interacts with the DHS Icomplaints system for TSA-related information. This PIA covers both main functionality and TSA's use of eFile. If other components choose to procure add-on modules, this PIA will be updated.

Section 1.0 Characterization of the Information

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

The information contained in the system concerns current and former employees and applicants who file informal and formal complaints of discrimination or who are seeking resolution to employment issues, applicants for employment, individuals with factual knowledge regarding those complaints and representatives of the interests of both complainant and the agency. The information collected varies based on the type of complaint or process undertaken.

PII of complainants/representatives, witnesses, and occasionally DHS personnel involved in the investigation is captured within the records stored in Icomplaints. Information collected in this system includes the following:

- Full name;
- Last four digits of Social Security Number (SSN) (to verify the same person);
- Work address;
- Work phone number;
- Email address;
- Home address;
- Home phone number; and
- Other identifying information, as relevant to the investigation.

Results of fact-based inquires (e.g., direct, comparative, and statistical evidence and information such as forms, sworn and/or unsworn statements of fact, reports and summaries) created and collected by counselors, investigators and EEO professionals responsible for the administrative processing of the allegations of discrimination are also input into the database. Over 500 data fields are captured in Icomplaints, giving DHS the ability to not only identify the issues and bases of the complaints, the complainants, the witnesses, and other information necessary to analyze complaint activity and trends, but also the ability to track and monitor the location, status, and length of time elapsed at each stage of the complaint resolution process consistent with EEOC Management Directive (MD)-110. While certain information is mandatory, most of the information collected is captured only where it is material and relevant to an investigation.[5]

Further, as stated above, efile provides an electronic option for TSA employees to initiate the EEO complaint process and review the status of complaints as they progress through the complaint process.

[5] *See* EEOC MD-110.

AILA InfoNet Doc. No. 10072964. (Posted 07/29/10)

Privacy Impact Assessment
for the

Icomplaints

Complaint Enterprise System

July 8, 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

AILA InfoNet Doc. No. 10072964. (Posted 07/29/10)

Abstract

The Office for Civil Rights and Civil Liberties (CRCL) Equal Employment Opportunities (EEO) Program operates the Icomplaints Complaint Enterprise System. Icomplaints is an electronic records system used to track complaints and supporting documentation relating to individual and class complaints of employment discrimination and retaliation prohibited by Department of Homeland Security (DHS) civil rights statutes. Icomplaints will replace EEO Eagle as EEO Eagle is being decommissioned. CRCL EEO has conducted this Privacy Impact Assessment (PIA) because Icomplaints collects and stores personally identifiable information (PII).

Overview

Pursuant to the regulations of the Equal Employment Opportunity Commission (EEOC), 29 CFR Part 1614, and DHS Delegations 3095 and 19002, 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, and without fear of reprisal. Similarly, a discrimination complaint may be filed on the basis of sexual orientation, parental status, or protected genetic information, which are protected by Executive Order. 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 Chief Human Capital Officer (CHCO) to develop solutions for building a high quality workforce; working with the CHCO, General Counsel, and DHS components to create a Departmental approach to Alternative Dispute Resolution; and establishing proactive measures to reduce EEO complaints.

In order to improve reporting and base functionality, DHS is transitioning from EEO Eagle to Icomplaints. EEO Eagle will exist until all data is migrated over to Icomplaints, at which point it will be decommissioned. This will provide for enhanced reporting, greater efficiency, and lower cost.

All DHS components use Icomplaints to manage their EEO case files. 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)[1]
- Federal Law Enforcement Training Center (FLETC)
- Headquarters (HQ)[2]
- Immigration and Customs Enforcement (ICE)
- Transportation Security Administration (TSA)
- U.S. Coast Guard (USCG)

[1] FEMA has already been using Icomplaints for a number of years.
[2] 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.

AILA InfoNet Doc. No. 10072964. (Posted 07/29/10)

- U.S. Secret Service (USSS)
- Final Action--CRCL

Each component can see only data pertaining to its respective cases; only CRCL has access to all departmental data as it is responsible for final adjudication of all EEO complaints.

Aggrieved persons who believe they have been discriminated against must contact an agency EEO counselor prior to filing a formal complaint. The person must initiate counselor contact within 45 days of the matter alleged to be discriminatory. As soon as an EEO contact is established at a servicing EEO office at the component level, designated EEO personnel will create a case in Icomplaints, starting with the "New Case Options" module; the counselee and/or complainant does not have access to or cannot modify entries in Icomplaints, unless he/she is a TSA employee accessing the eFile module. The steps of a case are organized into individual modules. From the "New Case Options" module, depending on the values entered, different tasks will be assigned. This ensures that each case goes through the appropriate path in the complaints process, and that all required information is collected at each stage.

Within 30 days of the initial contact date, the aggrieved person must complete counseling with the EEO Counselor. If the matter is not resolved in that time period, the Counselor must inform the individual in writing of the right to file a discrimination complaint through a Notice of Final Interview. The complainant must file a complaint with the agency that allegedly discriminated against the individual within 15 days of receipt of the Notice of Final Interview.[3] The agency must acknowledge receipt of the complaint in writing and must investigate the complaint within 180 days of the filing date. The agency must develop a "complete and impartial" factual record of the claims raised by the complaint.[4] A copy of the investigative file must be provided to the complainant, along with a notification that, within 30 days of receipt of the file, the complainant has the right to request a hearing and a decision from an EEOC Administrative Judge (AJ) or may request an immediate final decision from the agency. The AJ must conduct the hearing and issue a decision on the complaint within 180 days of receipt of the complaint file from the agency. When an AJ has issued a decision, the agency must take final action on the complaint by issuing a final order within 40 days of receipt of the hearing file and the AJ's decision. The final order must notify the complainant whether or not the agency will fully implement the decision of the AJ and shall contain notice of the complainant's right to appeal to EEOC or to file a civil action.

The records within Icomplaints are used to track and monitor EEO complaints as the complaints are processed through the administrative process outlined above. Icomplaints is also used to assign cases and manage workload, and run EEOC-mandated reports as well as custom reports. In addition to collecting PII about complainants, this system allows EEO personnel to enter data collected from the complainant's co-workers, supervisors, witnesses, and legal representatives of parties. Administration of this system is crucial to the timely adjudication of the rights of all individuals involved in the complaint process.

There are several add-on modules that components can procure such as the Quality Review Module (QRM) and efile. Efile provides an electronic option for a TSA employee to initiate the EEO complaint process and review the status of his/her complaint as it is being processed throughout the

[3] During the final interview with the aggrieved person, the EEO Counselor should discuss what occurred during the EEO counseling process in terms of attempts at resolution. The Counselor must not indicate whether s/he believes the discrimination complaint has merit. Since EEO counseling inquiries are conducted informally and do not involve sworn testimony or extensive documentation, the Counselor 1) cannot make findings on the claim of discrimination, and 2) should not imply to the aggrieved person that his/her interpretation of the claims of the case constitutes an official finding of the agency on the claim of discrimination.
[4] 29 CFR § 1614.108(b)

AILA InfoNet Doc. No. 10072964. (Posted 07/29/10)

complaint process. This module interacts with the DHS Icomplaints system for TSA-related information. This PIA covers both main functionality and TSA's use of eFile. If other components choose to procure add-on modules, this PIA will be updated.

Section 1.0 Characterization of the Information

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

The information contained in the system concerns current and former employees and applicants who file informal and formal complaints of discrimination or who are seeking resolution to employment issues, applicants for employment, individuals with factual knowledge regarding those complaints and representatives of the interests of both complainant and the agency. The information collected varies based on the type of complaint or process undertaken.

PII of complainants/representatives, witnesses, and occasionally DHS personnel involved in the investigation is captured within the records stored in Icomplaints. Information collected in this system includes the following:

- Full name;
- Last four digits of Social Security Number (SSN) (to verify the same person);
- Work address;
- Work phone number;
- Email address;
- Home address;
- Home phone number; and
- Other identifying information, as relevant to the investigation.

Results of fact-based inquires (e.g., direct, comparative, and statistical evidence and information such as forms, sworn and/or unsworn statements of fact, reports and summaries) created and collected by counselors, investigators and EEO professionals responsible for the administrative processing of the allegations of discrimination are also input into the database. Over 500 data fields are captured in Icomplaints, giving DHS the ability to not only identify the issues and bases of the complaints, the complainants, the witnesses, and other information necessary to analyze complaint activity and trends, but also the ability to track and monitor the location, status, and length of time elapsed at each stage of the complaint resolution process consistent with EEOC Management Directive (MD)-110. While certain information is mandatory, most of the information collected is captured only where it is material and relevant to an investigation.[5]

Further, as stated above, efile provides an electronic option for TSA employees to initiate the EEO complaint process and review the status of complaints as they progress through the complaint process.

[5] *See* EEOC MD-110.

AILA InfoNet Doc. No. 10072964. (Posted 07/29/10)

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

Information pertaining to the claims and issues raised within the complaint is collected primarily from complainants, co-workers, supervisors, witnesses, legal representatives, and any other individual with knowledge of the allegations of discrimination. Because individuals who are not DHS employees may file a complaint, information about non-DHS employees may also be collected.

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

The information is collected to process and facilitate the adjudication of EEO complaints.

1.4 How is the information collected?

Information is acquired from individuals who initiate contact with a servicing EEO office and supply background information to support allegations of discrimination. Once accepted, investigators, usually contractors external to the EEO office, interview complainants and witnesses and gather relevant documents to create a factual record of the allegations. EEO offices ensure that contract investigators follow privacy guidelines outlined by privacy and security requirements in the Statement of Work that solicits the bids for proposal. Information may be collected electronically, in paper form, or orally through phone call or interview in person. Information is primarily input by keystroke data entry, scanning of paper files, and attachment of electronic files.

The information contained in the eFile system, an add-on module, concerns current and former employees who elect this process to file an informal complaints of discrimination or who are seeking resolution to employment issues. The employee must access the system via TSA Intranet; therefore, someone who started the process (current employee) and then left TSA sometime during or following the process (former employee) would no longer have access to this information. The information collected varies based on the type of complaint or process undertaken. PII of complainants is captured within the records stored in eFile.

1.5 How will the information be checked for accuracy?

Individual complainants who contact a servicing EEO office fill out and sign forms soliciting PII and are instructed to inform the EEO servicing office when the information changes. During the pendency of their complaint, complainants frequently request changes in their file (new address and phone numbers, change of legal representation, etc). Complainants are afforded the opportunity to examine their investigative file for errors and make a request to correct any errors. If the servicing EEO office agrees with the request to modify information, the change is noted. If the servicing EEO office does not agree with the changes, a rationale for not making the change is included in the investigative file. A reviewing official, such as an EEOC AJ can later review the file to determine whether agency's refusal to make a requested change resulted in an adverse inference or decision.

Witnesses who give sworn statements are afforded the opportunity to review their statements in writing prior to signing. Component EEO offices are responsible for checking investigation results for sufficiency and accuracy.

AILA InfoNet Doc. No. 10072964. (Posted 07/29/10)

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

Pursuant to 42 U.S.C. §§ 2000e-5(b), 42 U.S.C. §§ 2000e-16(a), (b) and (c) and 29 CFR 1614.102, this information is being collected to develop a factual record upon which determinations on individual and class discrimination allegations can be made within the prescribed regulatory standards and timeframes, to provide relief when appropriate, and to prepare reports required by federal statute, regulation, executive order or special request on behalf of DHS and its components.

DHS is required to operate an EEO program per the regulations of the EEOC outlined at 29 CFR Part 1614. 29 CFR Section 1614.102(a)(2) specifically provides for the prompt, fair, and impartial processing of EEO complaints in accordance with the regulations and EEOC MD-110. 29 CFR Section 1614.602 specifically provides for agencies to report to EEOC information concerning EEO counseling and the status, processing, and disposition of EEO complaints.

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

A privacy risk exists that more information may be collected than is necessary to adjudicate an EEO complaint. To mitigate this risk, CRCL limits the scope of information collected in Icomplaints to the amount of data necessary to act upon the complaints filed. Although the system stores PII provided in the complaint, this information is captured only where it is relevant to an investigation.

There is also a privacy risk that information may be erroneously transposed, scanned, or attached into Icomplaints. To mitigate this risk, EEO personnel are trained on the proper handling of EEO data and further the accuracy of the data is checked at various stages of complaint processing by agency personnel, the complaint investigator, and the EEOC administrative law judge.

Section 2.0 Uses of the Information

2.1 Describe all the uses of information.

The information collected is used to properly administer and adjudicate EEO complaints for each respective component. Appropriate action cannot be taken to resolve EEO matters without complainant and/or witness contact information and factual accounts of alleged incidents. Icomplaints may aggregate data in order to show trends, whether the information is an aggregate of Component data, Fiscal Year data, or benchmark data. CRCL uses all of this information to determine the status of compliance with EEOC MD-715 and its standards of a "model EEO program status." Other Internal Uses:

- To comply with statutory, regulatory or executive reporting requirements relative to departmental attempts to maintain a continuing program to promote equal employment opportunity and eliminate discriminatory practices;

- To complainants, co-workers, supervisors, potential witnesses and others within DHS to the extent necessary to extract relevant testimony and evidence regarding discrimination allegations;

- To legal and lay representatives with defensive responsibilities;
- Consideration and/or imposition of personnel or disciplinary action when necessary to comply with remedial orders; and
- To the Office of the Secretary for vetting for appropriateness of Presidential Rank awards.

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

Icomplaints may aggregate data in order to show trends. Through the aggregation of data, new information may become self-evident such as individuals who frequently file complaints and managers who are repeatedly named as Responsible Management Officials (RMOs) found to have discriminated. An individual who frequently files complaints may have his or her complaint dismissed for abuse of process, though this is unlikely as the complainant would have to systematically abuse the EEO complaint process, i.e., flooding the EEO Office with EEO complaints and related correspondence. A manager who frequently is named as RMO may have the EEO complaint filing history considered when the agency is making a determination of agency awards and other distinctions.

Search functionality consists of two types of search – basic and ad hoc. In either one, any or all fields may be filled in; if none are filled in, the search will return every case in the system that the user has permissions to view within the controls that are in place. (Permission groups are set forth in Section 8.1.) Basic search allows any user to find a case based on Case Number and Complainant Name. Ad hoc search expands the number of fields by which a user can search for a case to include any field in the categories of complaint, contacts, corrective actions, frequently used events, all events, claims, fees, and statutes.

Advanced users, such as Administrators, Managers, and Super Users, will have the ability to create the Annual EEO Statistical Report of Discrimination Complaints (EEOC Form 462) for a given fiscal year. This functionality can be accessed by clicking on the "Reports" tab in the left-hand navigation bar and selecting the "462 Report" link. Users who can create a 462 report can also generate a list of cases that are missing necessary data to be included on the report. Advanced users can create the No FEAR Act[6] quarterly data posting, generate a list of cases that are missing the necessary data to be included in the posting, and create ad hoc or customized reports. There is also a Documents section that stores form letters and other document templates to use in official correspondence. Its contents can only be edited by Administrators at each component. Furthermore, EEOC MD-715 requires extensive reporting on hiring and termination statistics at the Department.

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

Icomplaints does not use commercial or publicly available data.

[6] Pursuant to Title III of the No FEAR Act, federal agencies are required to post quarterly on their public websites certain summary statistical data relating to equal employment opportunity complaints filed against the respective agencies.

AILA InfoNet Doc. No. 10072964. (Posted 07/29/10)

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. To mitigate this risk approved users are trained on the proper use of EEO information in the system by a combination of classroom and on-the-job 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.

There is also a privacy risk that information may be used for reasons not consistent with the original purpose. 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.

Section 3.0 Retention

3.1 How long is information retained?

Records shall be retained for four years after case closure in accordance with the National Archives and Records Administration revised General Records Schedule 1, Item 25 (Equal Employment Opportunity Records). There is also a provision in the EEO GRS that covers statistical information. This provision states that statistical information may be retained for 5 years. DHS plans to convert case file information into statistical information within the 4 year complaint case file retention period under GRS 25, providing the agency with an additional 5 years from the point of conversion to maintain that statistical information for trend analysis.

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 (Equal Employment Opportunity 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 EEO complaints, in particular the incidents of reprisal, the potential for litigation in EEOC and federal district court, and the lengthy appellate process all require that data be retained for a significant amount of time. Data retained in the system is primarily action-related (dates activities were undertaken and trend information (types of issues and basis identified, where complaints are occurring), regarding EEO complaints filed. Minimal information is retained regarding the person filing the complaint. The

AILA InfoNet Doc. No. 10072964. (Posted 07/29/10)

purpose of the retention provides the agency with areas of concentration for training or potential issues for redress. The risks are mitigated by the limited access to information contained in the system by controlled password access and defined user roles.

In addition, trend analysis requires a statistically significant pool of archival data over the course of years to properly assess the EEO clime and the efficacy of process improvement and pilot programs. Those risks are minimized by the controls and firewalls in the Icomplaints database discussed above.

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 listed below use Icomplaints to manage their own EEO case files.

- CBP
- USCIS
- FEMA
- FLETC
- HQ
- ICE
- TSA
- USCG
- USSS
- Final Action--CRCL

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

Other Internal Uses:

- To comply with statutory, regulatory or executive reporting requirements relative to departmental attempts to maintain a continuing program to promote equal employment opportunity and eliminate discriminatory practices;
- To complainants, co-workers, supervisors, potential witnesses and others within DHS to the extent necessary to extract relevant testimony and evidence regarding discrimination allegations;
- To legal and lay representatives with defensive responsibilities;
- Consideration and/or imposition of personnel or disciplinary action when necessary to comply with remedial orders; and

AILA InfoNet Doc. No. 10072964. (Posted 07/29/10)

- To the Office of the Secretary for vetting for appropriateness of Presidential Rank performance awards.

4.2 How is the information transmitted or disclosed?

Users upload into Icomplaints documents that are part of the investigative file, such as the Counselor's Reports, Acceptance of Issues letters, and Final Agency Decisions. A document can then be downloaded through Icomplaints by another component user who has the necessary permissions; if Icomplaints is unavailable, a case file may be e-mailed as an encrypted PDF. In addition, routine case information such as complainant name and case number is disclosed through e-mail during the processing of the case, primarily between CRCL and DHS components.

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.

CRCL encrypts PDFs of case files to ensure privacy risks are mitigated. Icomplaints 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 only access complaints records for their employees while CRCL has access to all complaint records as it is responsible for the final adjudication of all DHS complaints. While certain information is mandatory, most of the information collected is captured only where it is relevant to an investigation.

Each user on the Icomplaints system is a member of at least two groups – a component group, such as CBP, TSA, or HQ, 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 cases, documents, and functionalities of a specific DHS component. In some cases, component groups are broken down to more specific levels, restricting actions by location or sub-unit.

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 case information, such as complainant name, case number, and status, is disclosed through e-mail and telephone to Congressional Offices, Office of Special Counsel (OSC), and EEOC for specific purposes as well as upon request. Typically, the complainant or his representative will contact the external office in an effort to expedite the processing of the complaint. In addition, information aggregated into annual reports is forwarded to EEOC.

Other External Uses:

- To the OSC for investigation of allegations of prohibited employment practices;
- To the Department of Justice for the purpose of representing the interests of the department, or any officer, supervisor or employee therein, in pending or potential litigation.

AILA InfoNet Doc. No. 10072964. (Posted 07/29/10)

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 volume of complaints, types of complaints, resolution rates of complaints, and varying other reporting factors. Information sharing is covered under the EEOC/GOVT-1 Equal Employment Opportunity in the Federal Government Complaint and Appeal Records SORN, 67 FR 49338 published on July 30, 2002.

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

CRCL will either respond to external requests for information via letter, e-mail, or telephone. Congressional inquiries are almost always handled via letter. CRCL has begun to require that all such external requests for information come 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 personal information. 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 working to develop SOPs to further system controls and handling guidelines.

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 EEOC/GOVT-1 Equal Employment Opportunity in the Federal Government Complaint and Appeal Records SORN, 67 FR 49338 published on July 30, 2002.

Notice is provided at the component level to the individual prior to the collection of the information. Each component is responsible for both pre-complaint EEO counseling and investigating all formal complaints accepted with their own internal procedures. Some components provide a Privacy Act Notice to the Request for Counseling forms mailed to individuals. Other components provide a Privacy Act

AILA InfoNet Doc. No. 10072964. (Posted 07/29/10)

Notice once a formal complaint has been filed that explains use of this information by the investigator. See Appendix.

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

Individuals who contact EEO servicing offices may decline to provide requested information, but doing so may result in the dismissal of their allegation(s) because of failure to respond or proceed in a timely fashion. Individuals who contact EEO servicing offices are generally provided a privacy statement before providing requested information. Individuals may decline to provide requested information or otherwise cooperate during an investigation but their declination may eventually subject the agency to sanctions by the complaint adjudicator, including, but not limited to, the entering of a decision against the agency. Individuals who are federal employees may also be subjected to an adverse personnel action(s) as a result of their declination. Individuals are generally notified of this possible course of action by investigators only after they decline to provide the requested information.

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, as outlined for the purposes above, 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.

Components are responsible for the EEO counseling and investigation phases and process those cases. Feedback from component EEO Complaint Managers indicates that notice is provided either in Request for Counseling forms mailed to counselees or in Privacy Act Notices to Complainant during the investigation interview. Such notices ensure that the individual is aware that the collection of information will be included in an agency system of records. These notices are incorporated into the record and are part of the Investigative File that is retained past the closure of the case per archiving procedures. The complainant receives a copy of the Investigative File and the specific EEO documents that provide notice as to the collection of personal information.

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 EEO office. Privacy Act or FOIA requests for EEO purposes should be mailed to Department of Homeland Security, Office of Civil Rights and Civil Liberties, Room 5608-9, Washington DC, 20528. Contact information for the component EEO Officer and servicing EEO office is available on

AILA InfoNet Doc. No. 10072964. (Posted 07/29/10)

the component intranet websites. An individual can typically e-mail, telephone, or write to their EEO office. The System Manager is Stephen Shih, Deputy Director and Officer, DHS EEO Programs, located in the Office for Civil Rights and Civil Liberties, U.S. Department of Homeland Security, Washington, DC 20528.

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

Individuals may contact their servicing EEO office or file a request under the Privacy Act or the FOIA to correct their information as outlined in Section 7.1. Contact information for the component EEO Officer and servicing EEO office is also available on the component intranet websites. An individual can typically e-mail, telephone, or write to EEO office. EEO 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 EEOC/GOVT-1, 67 FR 49338.

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

Appropriate redress is provided as outlined above.

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 has bypassed the component EEO office and gone directly to the CRCL Master Administrator, a manager out of the individual's chain of command.

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?

Icomplaints 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 records while CRCL has access to all records as it is responsible for the final adjudication of all DHS complaints. While certain information is mandatory, most of the information collected is only captured where it is relevant to an investigation.

Each user on the Icomplaints 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 cases, documents, and functionalities of a specific DHS component. In some cases, component groups are broken down to more specific levels, restricting actions by location or sub-unit. The nine DHS components using Icomplaints are: CBP, USCIS, USCG, FEMA, FLETC, HQ, ICE, USSS, and TSA. Permission groups restrict a user's actions to certain types of functionality. For a full list, see the permissions section later in this Icomplaints User Manual. The following is a list of some permission groups in the Icomplaints system:

- Master Administrator
- Administrator
- Informal/Formal Reviewer
- Informal/Formal Processer
- Informal/Formal Super User
- Informal/Formal Manager
- Informal Processer
- Informal Super User
- Informal Manager
- Formal Processer
- Formal Super User
- Formal Manager
- Final Action Processer
- Final Action Manager

In addition, logon names and passwords control access. DHS employees must register with DHS Online (DHSO) before being added to the Icomplaints System. Registration can be done through the DHSO Help Desk. Once a user is registered with DHSO, only then can he or she be added to the Icomplaints system by an Administrator. Users also may change their password in the Icomplaints system by changing it through the Administrator.

EEO personnel at the components and members of the CRCL staff who have responsibility for the discrimination complaint process are granted access to Icomplaints using a roles-based permissions strategy. Icomplaints can be accessed from any computer.

The individual designated as the Administrator by each component EEO Director grants access to Icomplaints based on the user's role within the complaint process. System Administrators will have universal access to his/her component's complaint data within Icomplaints. An individual may have access to as few as 25 EEO records or as many as over 3,500 EEO records, which comprises the entirety of the Icomplaints database, depending upon the user's permissions and role.

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

Each DHS component maintains significant paper records, in some cases records for over a thousand complaint files, specific to matters raised therein. These cases are stored in file cabinets (that are

usually locked) in areas restricted to EEO professionals. Final Action records are maintained by the CRCL Complaint Adjudication Manager in a locked file room. Paper records are transferred intra-agency when necessary. Paper records are also archived periodically per NARA General Records Schedule for EEO Records.

Permission to view audit trails in Icomplaints is currently restricted to advanced users only. These permissions can be granted or removed at the discretion of CRCL

8.2 Will Department contractors have access to the system?

DHS contractors have access to Icomplaints 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. Additionally, EEO professionals, specifically EEO Counselors and Investigators, are required to meet annual training requirements as outlined in EEOC MD-110, specifically 32 hours for new staff and 8 hours for experienced staff. Training for new EEO Counselors includes an overview of the entire EEO process, the roles and responsibilities of the EEO Counselor, and the rights of the aggrieved, including privacy rights. Training for new EEO Investigators includes case management issues and investigative techniques, including securing sworn affidavits from the complainant and witnesses.

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

Certification and accreditation with Federal Information Security Management Act (FISMA) will be done for the system before it 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 DHS MD 4300 to prevent unauthorized access. Passwords expire every 90 days. Search, view, edit, and deletion of data is limited by permission-based 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 significant paper records, in some cases records for over a thousand complaint files, specific to matters raised therein. These cases are stored in file cabinets in areas restricted to EEO professionals. Final Action records are maintained by the CRCL Complaint Adjudication

AILA InfoNet Doc. No. 10072964. (Posted 07/29/10)

Manager in a locked file room. Cases can only be accessed if there is a need-to-know and cases must be signed out according to file room procedures. 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 Icomplaints system will be a fully operation IT system developed under DHS standards and in conformance with the requirements of Office of Management and Budget, EEOC, and Congress for EEO programs.

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

Icomplaints is currently in the system development lifecycle stage. This includes configurations of the application (a COTS product), data migration from the legacy application, and the setup of the hosting environment. The application will also go through the certification and accreditation process as a minor application.

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

AILA InfoNet Doc. No. 10072964. (Posted 07/29/10)

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.

AILA InfoNet Doc. No. 10072964. (Posted 07/29/10)