Privacy Impact Assessment
for the

Office for Civil Rights and Civil Liberties Matters Database

May 5, 2010

Contact Point
Jackie Mayi
Complaints Manager
Office for Civil Rights and Civil Liberties
U.S. Department of Homeland Security
(202) 357-8178

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

Abstract

The Department of Homeland Security (DHS), Office for Civil Rights and Civil Liberties (CRCL) has established the CRCL Matters database. CRCL Matters is a database developed to respond to allegations of abuses of civil rights, civil liberties, and religious, racial, and ethnic profiling by department employees and officials. This Privacy Impact Assessment (PIA) is being conducted because CRCL collects personally identifiable information (PII).

Overview

CRCL reviews and assesses information concerning abuses of civil rights, civil liberties, and profiling on the basis of race, ethnicity, or religion, by DHS employees and officials. The Office also ensures that all federally-assisted and federally-conducted programs or DHS activities comply with the provisions of Title VI of the Civil Rights Act of 1964, as amended; Title IX of the Education Amendments of 1972, as amended; the Rehabilitation Act of 1973, as amended; the Age Discrimination Act of 1975, as amended; and related Executive Orders. The Office investigates complaints in areas such as abuse of authority under color of law; discrimination; profiling; violations of the confidentiality provisions of the Violence against Women Act; conditions of detention; treatment; due process; and watch lists. CRCL Matters database collects information in order to meet its investigative and reporting responsibilities under 6 U.S.C. § 345 and 42 U.S.C. § 2000ee-1.

CRCL developed a pamphlet entitled: "How to File a CRCL Complaint." This pamphlet details the steps required for filing a complaint with DHS/CRCL. It recommends that complaints include, at minimum, the following information:

- *Contact information.* Full name; date of birth; alien registration number (A-number), if applicable; phone number; mailing address; and e-mail address, if available.
- *A written description of the specific circumstances of the alleged violation.* This should include date, time, and location; name(s) and contact information of any witness(es); and name of agency or component of the individual(s) alleged to have committed the violation, if available.
- *Relevant documents.* Copies of any paperwork related to the complaint or its circumstances.
- *A summary of other steps taken, if any, to resolve this complaint.* For example, steps could include e-mail communications with a DHS component agency regarding the complaint or letters written to the DHS Office of the Inspector General (OIG).
- *Complaints filed on behalf of a third party.* If the third party complainant is writing on behalf of someone else and wishes to receive information, which relates to them or their complaint, the third-party complainant must provide expressed written consent from that individual authorizing DHS to share information with them about the complaint. The third party complainant must also provide their name, organization (if any), and contact information.
- Complaints alleging a violation of an individual's civil rights or civil liberties by a DHS employee should be submitted in writing via letter, fax or e-mail to:

  U.S. Department of Homeland Security
  Office for Civil Rights and Civil Liberties
  Review and Compliance Unit
  245 Murray Lane, SW
  Building 410, Mail Stop #0800
  Washington, DC 20528

Email: civil.liberties@dhs.gov
Phone: (202) 401-1474 Toll Free: (866) 644-8360
Local TTY: (202) 401-0470 Toll Free TTY: (866) 644-8361.
Fax: (202) 401-4708

Complaints are initially reviewed to determine if DHS/CRCL has jurisdiction over the alleged complaint. If the complaint is within CRCL's jurisdiction and accepted, basic information about the case is input into the CRCL Matters Database: name, address, phone number, A-number, and other identifying data as may be necessary to review the complaint. If the complainant provides more PII than is necessary (e.g., Social Security number (SSN), passport number, etc.) that information is not captured in the database and will remain in the paper file and as an attached scanned document in the database but will be redacted, as necessary. CRCL sends a letter to the complainant acknowledging receipt of their formal complaint. This acknowledgement letter details the statutes or regulations under which DHS is authorized to investigate complaints, disclosure information, and Freedom of Information Act and Privacy Act information. If the incoming correspondence does not warrant being handled as a CRCL complaint, it is handled as correspondence and the concerns raised are addressed as appropriate. Correspondence items are not entered into the database.

Pursuant to 6 U.S.C. § 345(a)(6) and internal DHS policies, CRCL refers all complaints to the OIG for handling under the Inspector General Act of 1978, as amended. A summary of the complaint is provided to the OIG for review via e-mail. The OIG then decides whether they will pursue the case or decline to investigate it and refer it back to CRCL for appropriate action. If OIG refers the case back to CRCL, CRCL determines whether it will retain the case for internal investigation or refer the complaint to the relevant DHS component(s) (e.g., Immigration and Customs Enforcement (ICE), Transportation Security Administration (TSA), Customs and Border Protection (CBP), etc.). Referred complaints are forwarded to a component's internal complaints mechanism, along with a memo informing the component that it is now their responsibility to investigate the complaint. Upon completion of their investigation, the component issues to CRCL a Report of Investigation (ROI), detailing information obtained through the investigation. Once the ROI is satisfactory, CRCL prepares a close letter to the complainant and may at that time close the complaint.

Complaints that are retained within CRCL are investigated by CRCL's Review and Compliance (R&C) unit. Complaints are more likely to be retained if the alleged violations involve several DHS components, or if the alleged DHS violation is systemic or of Department-wide concern, but complaints that do not meet these descriptions may, in some circumstances nonetheless be retained. At the conclusion of the investigation, CRCL provides a Final Report and Recommendations to the involved component. This report is protected by attorney-client and deliberative process privileges.

At each step in the process, the electronic file is updated in the database from one status to the next (e.g., New, Sent to OIG, Back from OIG, Awaiting Recommendation, Recommendation Review, Back From Officer, Kept by OIG, Referred, Retained in CRCL, Closed Referred, Closed Retained in CRCL, Closed OIG, Closed Correspondence).

The data collected in the CRCL Matters database is shared with other DHS components on a need-to-know basis in order to obtain and/or verify information required to conduct investigations. When a complaint is submitted on behalf of an individual or the individual has obtained legal representation, CRCL must obtain expressed written consent from the individual before sharing information.

Other information that may appear in the system as an attached scanned document or in the file folder on a case-by-case basis might include: photographic facial images; SSN; bank account numbers; vehicle license plates and civil or criminal history information. The PII that is unnecessary will be redacted wherever possible.

CRCL paper investigative files and documents are scanned and stored in the CRCL Matters Database. The contents of documents vary depending on the particular investigation, but may include:

- Letters, memoranda, and other documents alleging abuses of civil rights, civil liberties, and profiling from complainants;
- Internal policies and procedures, letters, memoranda, and other communications within DHS;
- ROI (resulting from a DHS component's internal investigation of the allegations);
- OIG ROI (If the OIG determines their office will investigate the complaint rather than refer the matter back to CRCL, the results of the OIG investigation will be transmitted to CRCL in the form of an ROI. CRCL may either summarize that information in the CRCL Matters database or scan and store the actual ROI in the Database, in compliance with OIG handling directives.)
- Transcripts, interview notes, investigative notes and documentation concerning requests for additional information needed to complete the investigation;
- Court documents;
- A-File and/or Detention File documents;
- Medical records;
- Passport copy;
- Evidentiary documents and material, comments, and reports relating to the alleged abuses and to the resolution of the complaint.

Similar information regarding witnesses, persons involved in the alleged incident, or any other persons with relevant information regarding the alleged abuses may also be collected.

This PIA is being conducted because CRCL collects PII and to ensure the transparency of the information being collected. This PIA will be updated to reflect any substantial changes to the CRCL Matters database.

Section 1.0 Characterization of the Information

The following questions are intended to define the scope of the information requested and/or collected as well as reasons for its collection as part of the program, system, rule, or technology being developed.

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

Information relating to allegations of abuses of civil rights, civil liberties, and religious, racial,

and ethnic profiling by DHS employees and officials will be collected, as well as similar allegations relating to persons or entities under DHS control (such as contractors or programs). Basic information about complainants will be collected, including but not limited to:

- Complainant's name, mailing address, telephone and/or fax numbers, e-mail address, the party on whose behalf the complaint is filed (if it is a third-party complaint);
- Alien Registration number, if appropriate, of the party on whose behalf the complaint was filed;
- Allegation occurrence date, time, and location;
- Arab/Muslim/South Asian/Sikh Descent. CRCL does not solicit this information, it is tracked only if individuals self-identify;
- Facility name and location;
- Component referenced;
- Allegation details - primary and secondary issues, primary and secondary basis.

Other information that may appear in the system as an attached, scanned document or in the file folder on a case-by-case basis might include: photographic facial images; SSNs; bank account numbers; vehicle license plates; and civil or criminal history information. Such information will be deleted wherever possible.

CRCL paper investigative files and documents are scanned and stored in the CRCL Matters Database. The contents of documents vary depending on the particular investigation, but may include:

- Letters, memoranda, and other documents alleging abuses of civil rights, civil liberties, and profiling from complainants;
- Internal policies and procedures, letters, memoranda, and other communications within DHS;
- ROI (resulting from an OIG investigation or a DHS component's internal investigation of the allegations);
- Transcripts, interview notes, investigative notes, and documentation concerning requests for additional information needed to complete the investigation;
- Medical records;
- Court documents;
- A-File and/or Detention File documents;
- Passport copy;
- Evidentiary documents and material, comments, and reports relating to the alleged abuses and to the resolution of the complaint.

Similar information regarding witnesses, persons involved in the alleged incident, or any other persons with relevant information regarding the alleged abuses may also be collected.

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

Information is collected from individuals who file complaints, eyewitnesses, third parties, DHS employees and/or contractors, illegal aliens involved in the circumstances that gave rise to the complaint,

open sources (e.g., non-fee Internet sources, newspapers, etc.), and other entities with information pertinent to the matter under investigation. Commercial databases (e.g., Westlaw, Lexis-Nexis, etc.) may be used to obtain background information, verify addresses, confirm identities, gather contact information, identify possible witnesses, and for other investigative purposes, and information from theses sources may be scanned and loaded into the system as supportive documentation.

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

This information is collected to enable CRCL to comply with 6 U.S.C. § 345(a)(6); investigations into alleged civil rights abuses cannot be completed without the collection of PII and other sensitive information. Names of the complainant, witnesses, investigators, analysts, attorneys, employees, third party sources, non-governmental organizations (NGOs), contractors, grantees, and other persons are contained in the system in order to identify persons who have or may have information relevant to particular matters under investigation. Mailing addresses, phone numbers, e-mail addresses, zip code addresses, and facsimile numbers are collected and stored in order to facilitate communications with complainants, witnesses, NGOs, investigators, analysts, attorneys, employees, contractors, and grantees. Photographic images are stored in some files only if relevant to the matter under investigation. For example, a newspaper clipping regarding an incident may include a photograph of the alleged complainant or others involved in an investigation.

The system facilitates the efficient review and resolution of matters and provides a factual basis for the improvement of DHS policy as it relates to CRCL complaints. The collected information is also used to generate reports relating to CRCL investigations, such as but not limited to: number of referred and retained complaints; number of received and closed complaints; number of complaints received involving a particular component; number of complaints received involving a particular primary issue and reports to DHS officials. The collected information enables CRCL to meet statutory obligations requiring the submission of Quarterly and Yearly Reports to Congress.

1.4 How is the information collected?

Written complaints come to CRCL by fax, e-mail, or by regular mail. No standard complaint forms are required for submission of a complaint. CRCL investigators collect and analyze documentation in a number of ways, including interviews, review of records, and conducting site visits. The decision-making process with respect to what information is required for a specific investigation and how that information should be obtained varies considerably depending on the scope of the investigation and is therefore determined on a case-by-case basis.

1.5 How will the information be checked for accuracy?

The accuracy of the information in the system is maintained in part by collecting as much of the relevant information as possible directly from the individual to whom it pertains. Because of the nature of the system, however, it contains information reflecting opposing viewpoints with respect to incidents involving DHS employees, officers, contractors, and grantees. The accuracy of the information collected from third parties and sources regarding an individual to whom it pertains is also checked for accuracy by

investigating allegations and statements and comparing statements and facts in order to determine the truth. Findings and conclusions derived from these factual investigations are contained in final reports and recommendations to DHS component heads.

Full name; A-number, if applicable; phone number; mailing and e-mail addresses are visually verified against the incoming complaint for accuracy at the time of data-entry. Investigators are instructed to ensure accuracy and thoroughness through the investigative process, to consider confidentiality and security issues, to include disclosure caveats where appropriate, and to use electronic and other verification services to verify information as appropriate. The particular methods used to verify information compiled during the course of an investigation vary considerably depending on the type of investigation. Methods may include reference to commercial databases (e.g., Westlaw, Lexis-Nexis, etc.) to obtain background information, verify addresses, confirm identities, gather contact information, identify possible witnesses, and for other investigative purposes. In addition, each record has a unique file number to prevent duplication. CRCL verifies records by checking every incoming complaint to ensure that CRCL has not received the same complaint previously. If so, CRCL cross-references the two complaints. If the facts were not addressed in a previously complaint, the complaint is processed as a new entry.

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

The R&C Unit carries out statutory functions under 6 U.S.C. § 345 and 42 U.S.C. § 2000ee-1 to:

- review and assess information alleging abuses of civil rights, civil liberties, and racial, ethnic, or religious profiling by employees and officials of the Department;
- oversee compliance with constitutional, statutory, regulatory, policy, and other requirements relating to the civil rights and civil liberties of individuals affected by the programs and activities of the Department; and
- investigate complaints and information alleging abuses of civil rights or civil liberties, unless the OIG determines that it will investigate the complaint.

CRCL uses its investigative findings to make privileged and confidential recommendations to the involved component's senior leadership. Those recommendations are intended to strengthen and improve DHS programs and policies. Under 6 U.S.C. § 345 and 42 U.S.C. § 2000ee-1, there are no legal remedies for individuals. The unit also has authority to investigate complaints that arise under other federal laws such as Section 504 of the Rehabilitation Act of 1973, as amended, and Title VI of the Civil Rights Act of 1964, as amended.

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

Privacy Risk: A third party may file a complaint on behalf of the person who was allegedly harmed by the conduct of DHS personnel or a program or activity of the Department. Although it is

conceivable that a matter filed by a third party could be resolved without interviewing the party on whose behalf the complaint was filed, this is the exception and not the rule. In these situations, some of the information in the system may not be accurate or timely because it is not always collected directly from the individual on whose behalf the complaint was filed and may be an opinion or viewpoint of a third party.

Mitigation: To mitigate these privacy risks, CRCL conducts its investigations with due professional diligence, as follows:

- The complainant is mailed an acknowledgement letter and is directed to provide CRCL with updated contact information.
- If the complaint is filed by a third party, CRCL makes every effort to contact the party on whose behalf the complaint was filed in order to verify facts provided by the third party and as reflected in all relevant documents. If the third party complainant wishes to receive information, which relates to them or their complaint, the third party complainant must provide expressed written consent from that individual authorizing DHS to share information with them about the complaint. The third-party complainant must also provide their name, organization (if any), and contact information.
- Investigations are conducted in accordance with applicable laws and regulations, CRCL policies and procedures, and with due respect for the rights and privacy of those involved.
- Investigations are conducted in a timely manner based on resources, the variables, and complexities involved in each case.

Section 2.0 Uses of the Information

The following questions are intended to delineate clearly the use of information and the accuracy of the data being used.

2.1 Describe all the uses of information.

CRCL uses information maintained in this system in order to conduct investigations relating to allegations of abuses of civil rights, civil liberties, and profiling on the basis or race, ethnicity, or religion by employees and officials of DHS. CRCL most commonly uses PII, such as A-Number and home address, to confirm the identity of individuals. CRCL collects information only where it has specific legal authority to do so, and the information is required to meet CRCL's responsibilities to investigate all allegations under its jurisdiction.

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

The CRCL Matters system is not used for data mining. CRCL does conduct trend analysis with respect to the information in the system, but the system itself does not conduct this analysis. Instead, analysis is performed by individuals who merely use information from the system. No electronic tools apart from standard spreadsheet software are used to perform the analysis.

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

The particular methods used to verify information compiled during the course of an investigation vary considerably depending on the type of investigation. Methods may include reference to commercial databases (e.g., Westlaw, Lexis-Nexis, etc.) to obtain background information, verify addresses, confirm identities, gather contact information, identify possible witnesses, and for other investigative purposes, and information from theses sources may be scanned and loaded into the system as supportive documentation.

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.

Privacy Risk: With the collection of information in CRCL Matters, there is the risk that PII may be misused or taken out of context.

Mitigation: To mitigate this risk, appropriate safeguards are employed to ensure data gathered is protected from unauthorized disclosure and maintained in the investigative case file. Sources of investigative information are documented in sufficient detail to provide a basis for assessing credibility. Further, access to the electronic database is limited to CRCL leadership and employees of the R&C unit in order to preserve the integrity of the information in the system.

Section 3.0 Retention

The following questions are intended to outline how long information will be retained after the initial collection.

3.1 What information is retained?

CRCL Matters case files are retained on the basis of classification:

1) Referred Matters: Matters that are referred to DHS components for resolution;

2) Retained Matters: Matters that are either retained by CRCL because of the significance of the issue, which may result in policy change, or matters returned from the component for resolution; and

3) Significant Case Files: Files that a) involve allegations made against senior DHS officials; b) attract national media or congressional attention; c) present significant or novel questions of law or/and policy; d) result in substantive changes in DHS policies and procedures. From these criteria, CRCL selects significant cases on a case-by-case basis.

3.2 How long is information retained?

For Referred Matters, the components will maintain the record copy and follow their agency's record disposition schedule. DHS CRCL will maintain a reference copy containing the original complaint, all related and relevant documents, and the competent memorandum of resolution. Records will be destroyed or deleted 7 years after resolution of closure of the case.

For Retained Matters, records will be destroyed or deleted 75 years after resolution or closure of the case.

For Significant Case Files, files are transferred to the Federal Records Center for temporary storage at the end of the fiscal year in which the case is closed. Files are transferred to the National Archives for permanent retention 20 years after the case is closed.

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

Retention scheduled has been approved by DHS Senior Records Officer and by NARA under the revised General Records Schedule number N1-563-07-06, Civil Rights and Civil Liberties Case Files. The retention periods described in Section 3.2 above are derived from the schedule approved by NARA.

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

Privacy Risk: There is a risk that CRCL Matters data could be maintained for a period longer than necessary to achieve the agency's mission.

Mitigation: Although there is always risk inherent in retaining personal data for any length of time, the data retention periods based on case type identified in the NARA schedules are consistent with the concept of retaining personal data only for as long as necessary to support the agency's mission. In addition, these risks are minimized by the DHS Interactive Portal that is protected from unauthorized access through appropriate technical safeguards, including multi-layer firewall architectures, access codes, and passwords and is monitored by DHS's Chief Information Officer (CIO).

Section 4.0 Internal Sharing and Disclosure

The following questions are intended to define the scope of sharing within the Department of Homeland Security.

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

CRCL shares information in the Matters database and related paper files, as appropriate, with any DHS Headquarter Offices and with components or offices involved in the complaint. The latter category includes, but is not limited to ICE, TSA, CBP, United States Citizenship and Immigration Services (USCIS), United States Coast Guard (USCG), Federal Emergency Management (FEMA), National Protection and Programs Directorate (NPPD), and United States Secret Service (USSS).

Access to the system is granted to the attorneys at the Office of General Counsel (OGC) assigned to assist with the complaint process. At the beginning of the complaint process, OGC reviews and signs all retention and referral memos sent to component heads. During the closure process with respect to retained complaints, OGC reviews and signs all Final Report and Recommendations memos before they are sent to component heads. OGC is available throughout the investigation process to provide legal advice as necessary. Reports are shared with any DHS official with a need to know just as the incoming complaint information is also shared on a need to know basis.

4.2 How is the information transmitted or disclosed?

CRCL transmits information to the OIG, OGC, and DHS components involved in the complaint in a variety of ways, including electronically, during oral briefings and interviews, in writing, and by telephone. The method of transmission depends on the nature of the information, including its classification level, privacy interests, status of the investigation, and confidentiality concerns. All transmitted documents are labeled as For Official Use Only (FOUO) and handled in accordance with DHS Management Directive 11042.1.

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.

Privacy Risk: When sharing data internally there is a risk of unauthorized access to and inappropriate use and dissemination of CRCL Matters data.

Mitigation: All documents pertaining to any investigation are closely safeguarded in accordance with applicable laws, rules and policies as previously stated and all DHS facilities are protected from the outside by security access ID. In addition, all DHS employees including DHS components are notified and must attend mandatory training on the sensitivity of data collection and the sharing of records and information, and are made aware of restrictions on disclosure required by the Privacy Act and other statutory and regulatory safeguards. All information transmitted internally within or between DHS components is marked according to its sensitivity level as "FOUO;" and handled in accordance with DHS Management Directive 11042.1 and contain other warnings as appropriate, such as: "*This message may contain attorney-client communications, attorney work product, and agency deliberative communications, all of which may be privileged and not subject to disclosure outside the agency or to the public. Please consult with the Department of Homeland Security, Office of General Counsel before disclosing any information contained in this email/letter."*

Section 5.0 External Sharing and Disclosure

The following questions are intended to define the content, scope, and authority for information sharing external to DHS which includes Federal, state and local government, and the private sector.

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

The information collected and retained in the CRCL Matters database may be shared with the Terrorist Screening Center (TSC) administered by the Federal Bureau of Investigation (FBI). An example is when DHS works with the TSC to resolve complaints from individuals experiencing repeated screening delays or difficulties that may be related to the consolidated terrorist watch list. When necessary, CRCL will send copies of complainant's passport to TSC along with the incoming complaint and ROI to confirm whether an individual is on the watch list.

In order to meet its statutory obligations, CRCL submits Quarterly and Yearly Reports to Congress which summarize the office's activities and accomplishments. The R&C Unit Summarizes some or all of the complaints for a given timeframe and reports statistical data on all the complaints that were opened and closed during that timeframe. No PII is revealed in these reports; the reports themselves as well as the information contained in them are also posted on CRCL's website. The following questions are directed at notice to the individual of the scope of information collected, the right to consent to uses of said information, and the right to decline to provide information.

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.

The system is covered under the Civil Rights and Civil Liberties (CRCL) Matters System of Records Notice (SORN), DHS/CRCL-001, December 6, 2004, 69 FR 70464, which is currently being updated.

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

CRCL transmits information in a variety of secure ways, including electronically and U.S. Postal Service. No specific training is required of users from outside agencies; however, any federal agency receiving this information is required to handle it in accordance with the Privacy Act and their applicable SORNs. In addition, federal agencies and their contactors are subject to information security requirements of the Federal Information Security Management Act (FISMA), Title III if the E-Government Act, Pub. L. 107-347.

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

Privacy Risk: The primary privacy risk associated with external sharing is the risk of disclosure to unauthorized recipients during transmission of information to external entities.

Mitigation: This risk is mitigated because CRCL has implemented access controls within the system and ensures that electronic transmissions are secured by encryption or password protection. All Federal agencies are required to take appropriate actions to protect PII and handle it in accordance with the Privacy Act and FISMA requirements.

Section 6.0 Notice

The following questions are directed at notice to the individual of the scope of information collected, the right to consent to uses of said information, and the right to decline to provide information.

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

Yes, information in the complaint is provided by the individual, or someone acting on behalf of the individual. Upon receipt of the complaint, notice of potential uses of the information is provided via CRCL's online privacy policy, which is posted on the DHS website, and through the CRCL Matters SORN and this PIA. Further notices of potential uses are included in the CRCL pamphlet entitled: How to File a CRCL Complaint pamphlet and in all CRCL's form letters, e.g., acknowledgement, retention, and referral letters, In third party complaint situations, the individual about whom the information is collected is only notified about collection after we contact them to get more information regarding the third party complaint (unless the third party filed with the knowledge of the person about whom the complaint was filed.

Individuals, who are interviewed by CRCL employees but are not the filers of a CRCL complaint, receive all of the same notification as above with the exception of CRCL form letters. Every individual may request that their information be kept confidential, and CRCL will honor those requests to the extent to which confidentiality can be provided under applicable laws and regulations..

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

Individuals are not compelled to provide any PII but are informed in the Privacy Act statement contained in the "How to File a Complaint" pamphlet (as well as in the online privacy policy) that failure to provide sufficient information may impair CRCL's ability to review their allegations.

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

Depending on the nature of the investigation, CRCL investigators may ask persons if they wish to consent to a particular use of the information they provide. For example, complainants who request confidentiality will be advised of the extent to which confidentiality can be provided under applicable laws and regulations. Section 552a of the Privacy Act specifies a number of permitted uses and releases of information retained in a system of records. Each disclosure will be evaluated to ensure the disclosure is legally permissible, including, but not limited to, ensuring the purpose of the disclosure is compatible with the purpose for which the information was collected and the disclosure is limited to the minimum amount of information necessary to accomplish the purpose of the disclosure. When disclosures are made, PII will be redacted to the extent permissible.

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.

Privacy Risk: There is a risk that the individual may not know the uses to which their information will be put once it is collected.

Mitigation: Reviewing allegations and responding to complainants would be difficult if not impossible without this information. The system of records is thus necessary to facilitate the efficient review and resolution of matters, to provide a factual basis for the improvement of DHS policy and to enable CRCL to meet its statutory obligations. Notice of potential uses is posted in the Federal Register SORN in accordance with the Privacy Act of 1974. Furthermore, such notices are also available via CRCL's online privacy policy, which is posted on the DHS website, and in the notice relating to potential routine uses of the data under 2(c) above, "*intended use and disclosure of the information.*" Notices of potential uses are included in the CRCL pamphlet entitled: "How to File a CRCL Complaint" and in all CRCL's form letters, e.g., acknowledgement, retention, and referral letters.

Section 7.0 Access, Redress and Correction

The following questions are directed at an individual's ability to ensure the accuracy of the information collected about them.

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

Individuals may gain access to their information through a Privacy Act or Freedom of Information Act (FOIA) request, directed to FOIA / PA D-3, The Privacy Office U.S. Department of Homeland Security, 245 Murray Drive SW, Building 410, STOP-0550, Washington, DC 20528-0550. The Privacy Office will evaluate these written requests on a case-by-case basis and will determine which records are releasable to the requesting individual. DHS will assert applicable exemptions where appropriate.

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

When a complaint is accepted by CRCL, the complainant is mailed an acknowledgement letter where they are provided contact information for the CRCL office. A complainant or any other individual can correct their PII by simply notifying the CRCL office, or may follow the procedures outlined in Section 7.1.

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

As stated above in 7.2. Also, the mechanism for requesting correction of information is specified in the CRCL Matters SORN, DHS/CRCL-001.

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

As stated above in 7.2.

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

Risk of erroneous information being collected is mitigated by allowing individuals to request access or amendment of their records at any time. Individuals may access their information by using the PA/FOIA process outlined above or by contacting the DHS CRCL office directly.

Section 8.0 Technical Access and Security

The following questions are intended to describe technical safeguards and security measures.

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

All DHS employees are assigned network accounts after their clearance has been validated. The system's administrator grants each new CRCL employee assigned to the R&C unit access to the CRCL Matters Database.

CRCL restricts access to CRCL Matters Database to those personnel with a need to use the retained data. Access to the automated portion of the system will be controlled by username and password, granted to those persons whom the Officer for CRCL, or the Officer's delegate, has determined to have a need-to-know the information in order to complete the investigation. Information systems administrators will have access to the system for the limited purpose of system maintenance. The personnel with authority to access CRCL Matters Database are DHS and CRCL personnel and contractors. The privileges extended to such personnel will be "user" level, which will allow the individual accessing the data to view all information in the database but to edit only that portion of the system of records for which the accessing individual has authority. The CRCL Privacy Policy mandates the revocation of password and username access when any person with access to the system leaves DHS employment.

The system administrator has a higher level of access to the system that allows the administrator to view and edit all information in the database. Other personnel within DHS and the federal government will not have access to data in the system.

8.2 Will Department contractors have access to the system?

Yes, DHS has contractors providing Information Technology (IT) programming support for CRCL Matters Database and CRCL has contractors providing administrative support to the office. CRCL administrative contractors with access to CRCL Matters Database have received privacy training.

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

All new DHS employees must attend mandatory security training during orientation that addresses privacy issues, nondisclosure, methods of protecting data and outputs, and general confidentially and security concerns. Annual refresher security awareness training is also required for all employees. Further, CRCL facilitates yearly privacy/security training at All Hands Staff meetings. All the R&C unit team members have certified that they completed DHS privacy training entitled "A Culture of Privacy Awareness."

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

Yes, the Certification & Accreditation has been completed on the Matters database.

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

Yes, representatives of the CIO conduct routine auditing on the Matters database.

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?

Privacy Risk: Unauthorized persons could potentially gain access to the PII on the system and misuse the data.

Mitigation: CRCL information is closely safeguarded in accordance with applicable laws, rules and policies as stated elsewhere within this document. In addition, the DHS server is located in a controlled, secure zone to provide a layer of physical security to the server and backup tapes. All records are also protected from unauthorized access through appropriate technical safeguards, including multi-layer firewall architectures, access codes, and passwords. CRCL file areas are locked at all times or kept in otherwise secure areas, and the facilities are protected from the outside by security access identification. Access to files is strictly limited to authorized personnel who require access to perform their official duties. Upon separation from employment, the Office of Security personnel or their designees will follow the guidance in accordance with Management Directive 11005 and suspend an ex-employees access to DHS facilities, sensitive information, and IT systems.

Section 9.0 Technology

The following questions are directed at critically analyzing the selection process for any technologies utilized by the system, including system hardware, Radio Frequency Identification (RFID), biometrics and other technology.

9.1 What type of project is the program or system?

This system is an external complaints tracking system customized on a Java based application with an Oracle database.

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

The CRCL Matters Database is operational.

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

No major technology privacy concerns exist at this time.

Responsible Officials

Jackie Mayi
Complaints Manager
Office for Civil Rights and Civil Liberties
Department of Homeland Security

Approval Signature

Original signed copy on file with the DHS Privacy Office

Mary Ellen Callahan
Chief Privacy Officer
Department of Homeland Security