Privacy Impact Assessment
for the

Recruit Analysis and Tracking System

November 30, 2009

Contact Point
Tom DeGeorge
Mission Support
United States Coast Guard Recruiting Command
(703) 235-1715

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

Abstract

The Department of Homeland Security United States Coast Guard Recruiting Command operates the Recruit Analysis and Tracking System to support the U.S. Coast Guard recruiting mission. The system gathers and distributes recruiting leads, tracks recruit progression, prepares accession forms, processes reservations for enlisted and officer candidates, manages the mission plan, provides point-in-time projections, and reports on quality, quantity, and diversity statistics for the recruiting effort. This privacy impact assessment is required as Recruit Analysis and Tracking System will collect and retain personally identifiable information (PII).

Overview

The Unites States Coast Guard (USCG) owns and operates the Recruit Analysis and Tracking System (RATS). The purpose of RATS is to support marketing and recruiting efforts for the USCG recruiting mission. The system also manages the annual mission plan for United States Coast Guard Recruiting Command (CGRC) and provides daily management of the recruiting process, to include forms preparation, reservations for boot camp and officer selection panels[1], reporting on the year-to-date results of the recruiting effort, and waiver processing. Marketing leads are also captured and distributed to recruiting offices by RATS, in conjunction with a marketing website. A marketing lead contains contact information for an individual. It may consist of as little as a name and email address, or as much as a complete set of contact information and PII, such as name, date of birth (DOB), address, social security number (SSN), race, ethnicity, gender, etc.

This system manages approximately 90,000 marketing leads and 5,000 USCG accessions annually, supporting about 365 recruiters in 90 offices in the United States and Guam. An accession is when recruits are sworn in as a Coast Guard member.

RATS stores an increasingly detailed level of PII as a marketing lead or applicant progresses through the system. An initial lead results in the capture of a limited amount of information, such as name and contact data (email, address, or phone number). As a potential recruit or officer applicant is recognized as a viable candidate, the level of PII captured becomes increasingly detailed until at the time of accession all the information required to bring a new member on board has been entered in RATS. The data required for accession includes SSN, DOB, medical history, dependent information, address, credit history, criminal background checks, results of aptitude testing, and physical exams. Less than 4% of leads progress to the point of aptitude testing and physical exams. The PII collected for the remaining 96% of leads is limited and not shared beyond CGRC. The exposure risks are mitigated by CGRC's practice of limiting in-depth collection until the information is required for the phase of accession of the potential candidate.

A recruit progression consists of multiple transactions. An interested party may visit the GoCoastGuard.com website and provide minimal contact information. An interested party may also walk-in to a USCG recruiting office or call over the phone. The data entered is transferred to a recruiting

[1] An officer selection panel convenes to review applications for Coast Guard commissioning programs.

office, based on the geographic location provided by the individual. The recruiter follows up with the individual and further background data is captured. If the recruiter and the interested individual decide to further pursue accession, the recruiter will arrange an interview or an office visit. This may result in the scheduling of aptitude testing and a physical exam. The testing and exam are done by the Department of Defense (DOD) Military Entrance and Processing Command (MEPCOM), and data stored in RATS is used to populate forms required by MEPCOM to administer testing and exams. Recruiters may then use RATS to request boot camp or officer panel reservations for successful candidates, as well as to request waivers for medical, age, time in service, civil, education, and test scores, specific training school slots, and bonuses.

Information from RATS is shared with MEPCOM, Defense Manpower Data Center (DMDC), (a component of the Department of Defense), various USCG personnel organizations, and a USCG fulfillment contractor. The contractor responds to requests for information from potential applicants, based on the information provided by the candidate.

The system consists of three sections: a marketing website: intranet website accessible within the Coast Guard Data Network (CGDN+); and a web based application and centralized database hosted at a secure USCG facility. The USCG Operations Systems Center provides web application and data base services required to support transactions, reporting, and analysis.

The legal authorities for RATS system are the following: 10 U.S.C. §§ 504, 1475-1480; 14 U.S.C. §§ 211, 350, 632; and Homeland Security Presidential Directive (HSPD) -12.

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?

RATS may include marketing data collected through the USCG recruiting website and telephone queries made by prospects who voluntary provide some or all of the following information;

- Individual's name;
- Date of birth;
- Program of interest;
- Citizenship;
- Marital state;
- Race;
- Ethnicity;
- Gender;
- E-mail and phone contact information;
- Education;

- Employment status;
- Number of dependents;
- Geographic boundaries of recruiting marketing areas, unrelated to personal information.

When the recruiter meets with an applicant for an interview, the following information may be collected throughout the application process:

- Social security number;
- Personal history;
- Test scores, college majors, grades and transcripts;
- Professional qualifications;
- Adverse or disqualifying information, such as criminal record, medical data, and credit history;
- Mental aptitude;
- Medical documentation;
- Medical waivers;
- Physical qualifications;
- Character and interview appraisals;
- National Agency Checks and certifications, such as criminal history and fingerprints;
- Service performance;
- Advertising responses, such as marketing data, where did you hear about the Coast Guard, Website? Radio ad? etc;
- Applicant initiated inquiries;
- Electronic copies of supporting documents, such as birth certificates for the applicant and dependents, Social Security cards, marriage licenses, divorce decrees, and other civil court documents.

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

Information is provided by potential enlisted recruits and officer candidates. The DOD Defense Manpower Data Center supplies the Geographic Information System (GIS) data to the USCG. Geographic data includes: county, state, and zip code boundaries, interstate highway locations. GIS data is used to define the area of responsibility for recruiting leads. Marketing data is provided by the DOD. Marketing data includes contact information supplied by individuals interested in the Coast Guard.

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

The information is collected to identify and qualify candidates for service in the United States Coast Guard, and to manage, support, and enhance the Coast Guard's recruiting mission. GIS data is used to associate zip codes with recruiting office locations.

1.4 How is the information collected?

The information is collected via website entry by individuals interested in Coast Guard service. Information is also collected by recruiters during in-person and telephone interviews with potential

applicants. Additional information is collected using national record checks from the National Crime Information Center, and from credit reporting entities. Information is sent to RATS from MEPCOM regarding the results of physical exams and aptitude testing.

1.5 How will the information be checked for accuracy?

Information is verified at a minimum of five stages for each accessed applicant. Accession information is reviewed and approved by the applicant. The recruiter reviews the data, as does the Recruiter in Charge at each office. Department of Defense MEPCOM processing stations verify data on forms provided by USCG recruiting offices. The Reservations office at CGRC also reviews elements of enlisted member data, and Officer Program staff at CGRC review officer applicant information. The accession points for new members (USCG Cape May and the USCG Academy) also review the data.

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

The legal authorities for the collection of this data include: 10 U.S.C. §§ 504, 1475-1480; 14 U.S.C. §§ 211, 350, 632; and HSPD-12.

MOU's between MEPCOM and USCG define the PII requirements for processing USCG applicants.

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

Risk: Loss of data.

Mitigation: As a result of prior certification and accreditation reviews, the USCG is implementing a web-based application that limits access to PII via the Coast Guard Data Network, CGDN+. PII data storage on recruiting office computers and laptops is being removed to reduce risk of data loss or unauthorized access through theft or hacking. All recruiters and CGRC personnel participate in annual privacy and security training. The risk is mitigated to a degree as data is collected only on an "as needed" basis; the full set of data (SSN, medical information, etc.) is collected and stored only for the approximately four percent of leads who are progressed to accession. The PII collected for the remaining 96% of leads is limited to name and contact information, and not shared beyond CGRC. The exposure risks are mitigated by CGRC's practice of limiting in-depth collection until the information is required for the phase of accession of the potential candidate.

PII stored on local laptops and desktops is encrypted with Windows XP Encryption. Physical security of computers includes locking cables and lockable storage. Installation of additional encryption software (Safenet) on recruiter's computers was completed in Spring 2009; an in-progress technical refresh of the system's architecture will totally remove PII data from local machines by the end of Spring 2010.

The centralized database has been hardened to protect PII, both at rest and in-flight. The central database is hosted behind a firewall, on a secure network with automated intrusion monitoring. Access to the system is restricted to network connections within the CGDN+.

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.

Data is used to make recruiting contacts with potential candidates, process candidates for aptitude testing/ physical exams, and for progression to enlistment or commissioning. Information is used to qualify enlisted and officer applicants for USCG service. Data is aggregated for analysis and used as input to the USCG's HR system to initiate pay and benefits for new members.

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

Data is analyzed with a combination of Microsoft back office tools, such as Excel and Access, SQL queries, and canned, printed reports. The reports created are for aggregated statistics, detailed lists with PII, such as boot camp rosters, and officer panel applications, and performance measure reports.

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

Zip code data is imported to define marketing boundaries. Marketing data for high school students (name, class, high school name, and mailing address,) is supplied to RATS from DOD sources via secure File Transfer Protocol transmission. This data is entered in RATS and made available to recruiters. RATS does not use commercially acquired data

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

Privacy Risk: Accuracy of lead data

Privacy Mitigation: Lead data is verified and updated once contact is made with the potential applicant. Applicant reviews lead data during interviews with USCG recruiters.

Privacy Risk: Mistake made by recruiter when entering

Privacy Mitigation: Data is progressively audited and verified as an applicant is progressed, by entities independent of one another (Recruiters, Recruiter in Charge, MEPCOM, USCG Cape May,

USCG Academy, Reservations office, officer programs staff). Users are required to read and sign a Rules of Behavior agreement that details the proper use and handling of the data collected. Update access to the data is limited by assigned office and to CGRC central staff.

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?

All data collected from the applicants is retained.

3.2 How long is information retained?

Electronic data for all applicants is retained through the end of the second fiscal year after the year of collection. Data is archived off-line for an additional two years. Information on selected applicants (those who accessed) is forwarded for inclusion in Official Military Personnel Files (OMPF).

For officer applicants, hard-copy information on non-selected officer applicants is destroyed 6 months after deadline dates for the class for which application is made. Hard copy Information collected for Commissioning Programs on selected applicants is forwarded for inclusion in OMPF and destroyed 1 year from date of board by which considered.

For enlisted applicants, Individual Personnel Applicant Records for successful and unsuccessful applicants for enlistment in the Coast Guard are destroyed 1 year after enlistment or rejection.

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

Yes, SSIC 1000, COMDTINST M5212.12A.

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: The information is out of date and could be inappropriately used for a decision.

Mitigation: This is mitigated by keeping the information on the applicants current, and deleting the information for those not chosen to proceed for a short period. The safeguards in place to protect the data in general also apply to retained data. The retention period has been minimized to limit the volume of data subject to risk. Historical data beyond the retention period used for analysis is limited to summary

and aggregated data, the PII is not available after the retention period. For summary and aggregate data during the retention period, the PII will be redacted.

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?

Data is shared at accession points with the USCG Cape May and the USCG Academy. Data is also shared with USCG Headquarters personnel (CG-1), and with the data warehousing function within the USCG information technology structure. The complete set of individual PII is shared with the accession points, in order to populate the USCG's HR system with new member data.

4.2 How is the information transmitted or disclosed?

Accession points and USCG personnel organizations receive reports and data via encrypted (256 bit AES) email attachments, and as hard-copy, hand carried reports and forms. The data warehouse technical group extracts data via direct database access, within the data center secured network.

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.

PII is handled by personnel organizations within the USCG. Multiple end users have access to various PII components.

USCG users are vetted before being given access to personnel data. Data in transit are encrypted, and electronic movement takes place over a secure network.

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?

Information is shared with MEPCOM, DMDC, and a third party contractor performing marketing support.

- MEPCOM requires access to RATS data and forms in order to process applicants for aptitude testing, physical exams, and for statistical analysis and reporting.
- DMDC uses RATS data (and data from all the Defense Department services) for the study of accession issues, manpower projections, analysis of recruit quality, and comparative study of the service's recruiting efforts.
- The third party fulfillment vendor provides email confirmation and program details to visitors to the GoCoastGuard.com website, solely in support of marketing for CGRC.

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, RATS data sharing is compatible with the original collection. Sharing data is integral to marketing and comparitive analysis, as covered by the USCG Recruiting Files Systems of Records Notice (SORN), DHS/USCG-027.

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

MEPCOM receives printed data and forms from recruiters which are generally hand-carried to MEPCOM centers that process recruits. DMDC receives periodic data extracts from RATS. These originate from CGRC and are sent via encrypted email (256 bit AES).

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

Privacy Risk: Misuse by third party

Mitigation: The third party fulfillment vendor deletes PII and contact data once an email response to the interested party has been generated. There is no retention of personal data by the vendor, beyond 24 hours (72 hours on weekends).

Privacy Risk: Transmission of data is not secure.

Mitigation: PII is transmitted manually and via email, both of which have exposure risk. To mitigate this risk, data are encrypted before transmission. Hard copy documents are shredded by the accession points after updates to the HR system are complete.

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. Notice is provided by the USCG Recruiting Files SORN, 73 FR 77804, the Privacy Act statement on the bottom of the form, and this PIA.

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

Yes. The applicant can chose not to provide the information; however, they may not qualify for enlistment or commissioning if they chose not to disclose the information necessary to select them for accession.

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

No, data collected are used to populate electronic and physical forms. Uses are defined and limited by the Office of Management and Budget, the Department of Defense, HSPD-12, and USCG directives.

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.

Disclosure is voluntary, and requires positive action on the part of the individual. All collection is initiated and approved by the individual concerned. No information on an individual is collected without their consent and participation.

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?

Applicants and recruits see paper copies of their data packages. Accessed individuals are given a complete copy of the accession package, in hard copy form. Applicants that don't access, or have not yet accessed, can obtain a hard copy of any form or data concerning them from their recruiter or from CGRC.

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

Applicants and recruits can report errors to their recruiter before accession and their servicing personnel office after their accession as a member or officer in the USCG.

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

USCG Business Intelligence and Direct-Access systems provide guidance and/or self-service tools that show how an employee may correct their personal data. A recruiter is able to update information about applicants/recruits upon notification of an error by the individual.

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

Individuals in the process of qualification or accession may have the recruiter correct self-disclosed data at any time in the recruiting progression, up to the point of accession. Information that requires correction and is relevant for the qualification for service must be supported by documentation.

The USCG Recruiting Files SORN (DHS/USCG-027) outlines contact information for individuals who may desire it, and describes the nature and details of the information retained within the system.

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

Privacy Risk: Changes requested to information for individuals may be fraudulent, or initiated by unauthorized persons.

Mitigation: CGRC personnel and recruiters will not modify information collected regarding an individual unless positive identification of the requestor has been made, and the changes are supported by documentation.

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?

New users request access via a data center help desk call. The data center will not grant access to a new user until CGRC has confirmed the request is legitimate. User access procedures are documented via formal agreements between the data center and CGRC, and include role limitations, periodic expiration of user id's, and periodic review of users granted access.

8.2 Will Department contractors have access to the system?

Yes; technical support is provided by contracting staff at the data center. Some data entry is accomplished at CGRC by contracted staff.

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

Recruiters receive RATS training at their recruiter office. All users with access to RATS sign a Rules of Behavior document that addresses protection of PII, destruction of hard copy reports, and deletion of hard copy within defined time limits.

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

Yes, the C&A review was completed in January 2008. RATS plan of action and milestone document includes actions and progress in addressing risk for identified concern areas.

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

Changes to applicant information are time and data stamped, and are restricted to the recruiter or reservation staff member who is responsible for the information. The system's centralized data base is within the USCG's secure network, behind a firewall, and the network is monitored for intrusion and other unauthorized access.

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?

Military recruiting, by necessity, requires the gathering of an extraordinary volume of sensitive data concerning an individual. The information may be compromised by intentional or accidental act.

The business processes used in USCG recruiting uses a gradual escalation of collection: the quantity of PII collected increases only as the potential applicant moves closer to accession. The PII collected for the vast majority of leads is limited to name and email or mailing address, and perhaps age and gender. Less than 4% of leads progress to the point of aptitude testing and physical exams. The PII collected for the remaining 96% of leads is limited and not shared beyond CGRC. The exposure risks are mitigated by CGRC's practice of limiting in-depth collection until the information is required for the phase of accession of the potential candidate.

An individual's information is only accessible to those recruiters assigned to the recruiting office where the individual is being progressed. Once an individual has been progressed to the point of shipping out, update access to his PII is further restricted to the Reservation Staff or Officer Programs staff at CGRC.

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, RFID, biometrics and other technology.

9.1 What type of project is the program or system?

RATS uses Windows Server, web based, and Windows client system; the Windows client is Visual Basic and .Net based. The local client interface will be eliminated in the technical refresh, and replaced by Internet Explorer. Data is stored using Windows SQL Server database, and network connectivity is via Ethernet and TCP/IP.

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

The technical refresh is in the Planning and Development phase, using Coast Guard's Software Development Life Cycle process.

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

No; the technologies used are mainstream, and in widespread usage. The risks and vulnerabilities of these technologies are commonly known, documented, and well mitigated. The system does not employ any leading edge or high risk technologies related to portable devices or data communications.

Approval Signature

Original signed and on file with the DHS Privacy Office

Mary Ellen Callahan
Chief Privacy Officer
Department of Homeland Security

Appendix A:

Recruit Analysis and Tracking System Privacy Act Statement

AUTHORITY: 14 U.S.C. 211 and 350, Coast Guard / Recruiting campaigns, and United States Coast Guard Commandant Instruction M1100.2F, Coast Guard Recruiting Manual.

PURPOSE: To obtain necessary information to respond to your request for information regarding a career in the United States Coast Guard.

ROUTINE USE: No disclosure of this information will be made outside of the Department of Homeland Security.

DISCLOSURE: Voluntary; however, if you do not provide the information, we will be unable to contact you and inform you of the Coast Guard opportunities that might be available to you.