OFFICE OF THE UNDER SECRETARY OF DEFENSE
4000 DEFENSE PENTAGON
WASHINGTON, DC 20301-4000

PERSONNEL AND
READINESS

MAR 23 2009

The Honorable Carl Levin
Chairman
Committee on Armed Services
United States Senate
Washington, DC 20510-2202

Dear Mr. Chairman:

Enclosed is an interim report on Youth Information in Recruiting Databases as requested in the House Armed Services Committee Report 110-652, which accompanied the National Defense Authorization Act for Fiscal Year 2009.

The Committee report asked the Secretary of Defense to review the processes by which student information is removed from our databases upon request by parents or guardians, and to assess the overall quality of the management of those databases. The interim report focuses only on databases where responsibility and oversight rests directly with the Office of the Under Secretary of Defense for Personnel and Readiness and his staff. We have asked each Service to provide similar reports to us and we will submit them as part of a final report no later than June 30, 2009.

The interim report includes an overview of the JAMRS Recruiting Database as an essential tool in maintaining the vitality of the nation's All-Volunteer Force, and additionally, answers pertinent questions regarding "opt-out" procedures and safeguard techniques that are in place to ensure that youth information is used within the Department of Defense for recruitment purposes only.

A copy of this interim report has also been sent to the House Armed Services Committee. Thank you for your continued support of the Department's recruiting efforts.

Sincerely,

T. F. Hall

T. F. Hall
Performing the Duties of
the Under Secretary of Defense
(Personnel and Readiness)

Enclosure:
As stated

OFFICE OF THE UNDER SECRETARY OF DEFENSE
4000 DEFENSE PENTAGON
WASHINGTON, DC 20301-4000

PERSONNEL AND
READINESS

The Honorable John McCain
Ranking Member
Committee on Armed Services
United States Senate
Washington, DC 20510-0303

MAR 23 2009

Dear Senator McCain:

Enclosed is an interim report on Youth Information in Recruiting Databases as requested in the House Armed Services Committee Report 110-652, which accompanied the National Defense Authorization Act for Fiscal Year 2009.

The Committee report asked the Secretary of Defense to review the processes by which student information is removed from our databases upon request by parents or guardians, and to assess the overall quality of the management of those databases. The interim report focuses only on databases where responsibility and oversight rests directly with the Office of the Under Secretary of Defense for Personnel and Readiness and his staff. We have asked each Service to provide similar reports to us and we will submit them as part of a final report no later than June 30, 2009.

The interim report includes an overview of the JAMRS Recruiting Database as an essential tool in maintaining the vitality of the nation's All-Volunteer Force, and additionally, answers pertinent questions regarding "opt-out" procedures and safeguard techniques that are in place to ensure that youth information is used within the Department of Defense for recruitment purposes only.

A copy of this interim report has also been sent to the House Armed Services Committee. Thank you for your continued support of the Department's recruiting efforts.

Sincerely,

T. F. Hall

T. F. Hall
Performing the Duties of
the Under Secretary of Defense
(Personnel and Readiness)

Enclosure:
As stated

OFFICE OF THE UNDER SECRETARY OF DEFENSE
4000 DEFENSE PENTAGON
WASHINGTON, DC 20301-4000

PERSONNEL AND
READINESS

MAR 23 2009

The Honorable Ike Skelton
Chairman
Committee on Armed Services
U.S. House of Representatives
Washington, DC 20515-2504

Dear Mr. Chairman:

Enclosed is an interim report on Youth Information in Recruiting Databases as requested in the House Armed Services Committee Report 110-652, which accompanied the National Defense Authorization Act for Fiscal Year 2009.

The Committee report asked the Secretary of Defense to review the processes by which student information is removed from our databases upon request by parents or guardians, and to assess the overall quality of the management of those databases. The interim report focuses only on databases where responsibility and oversight rests directly with the Office of the Under Secretary of Defense for Personnel and Readiness and his staff. We have asked each Service to provide similar reports to us and we will submit them as part of a final report no later than June 30, 2009.

The interim report includes an overview of the JAMRS Recruiting Database as an essential tool in maintaining the vitality of the nation's All-Volunteer Force, and additionally, answers pertinent questions regarding "opt-out" procedures and safeguard techniques that are in place to ensure that youth information is used within the Department of Defense for recruitment purposes only.

A copy of this interim report has also been sent to the Senate Armed Services Committee. Thank you for your continued support of the Department's recruiting efforts.

Sincerely,

T. F. Hall

T. F. Hall
Performing the Duties of
the Under Secretary of Defense
(Personnel and Readiness)

Enclosure:
As stated

OFFICE OF THE UNDER SECRETARY OF DEFENSE
4000 DEFENSE PENTAGON
WASHINGTON, DC 20301-4000

PERSONNEL AND
READINESS

The Honorable John M. McHugh
Ranking Member
Committee on Armed Services
U.S. House of Representatives
Washington, DC 20515-0552

MAR 23

Dear Representative McHugh:

Enclosed is an interim report on Youth Information in Recruiting Databases as requested in the House Armed Services Committee Report 110-652, which accompanied the National Defense Authorization Act for Fiscal Year 2009.

The Committee report asked the Secretary of Defense to review the processes by which student information is removed from our databases upon request by parents or guardians, and to assess the overall quality of the management of those databases. The interim report focuses only on databases where responsibility and oversight rests directly with the Office of the Under Secretary of Defense for Personnel and Readiness and his staff. We have asked each Service to provide similar reports to us and we will submit them as part of a final report no later than June 30, 2009.

The interim report includes an overview of the JAMRS Recruiting Database as an essential tool in maintaining the vitality of the nation's All-Volunteer Force, and additionally, answers pertinent questions regarding "opt-out" procedures and safeguard techniques that are in place to ensure that youth information is used within the Department of Defense for recruitment purposes only.

A copy of this interim report has also been sent to the Senate Armed Services Committee. Thank you for your continued support of the Department's recruiting efforts.

Sincerely,

T. F. Hall

T. F. Hall
Performing the Duties of
the Under Secretary of Defense
(Personnel and Readiness)

Enclosure:
As stated

DEPARTMENT OF DEFENSE REPORT ON YOUTH INFORMATION IN RECRUITING DATABASES IN RESPONSE TO THE HOUSE ARMED SERVICES COMMITTEE REPORT TO ACCOMPANY DUNCAN HUNTER NATIONAL DEFENSE AUTHORIZATION ACT FOR FISCAL YEAR 2009 (H. REPT 110-652, P362)

Office of the Under Secretary of Defense
(Personnel and Readiness)

March 2009

Table of Contents

Introduction

This report is submitted in response to the House Armed Services Committee report to accompany the Duncan Hunter National Defense Authorization Act for Fiscal Year 2009 (H. Rept 110-652, page 362), which provides:

> *The committee is concerned about the procedures employed by the Department in managing databases that include youth information. The committee directs the Secretary of Defense to verify that well-publicized and efficient procedures are available to youth or parents or the guardian of the youth to remove information from all Department of Defense recruiting databases and to protect youth from unsolicited contact by any Department of Defense recruiting agency. In addition, the committee directs the Secretary to verify that all information maintained on youth in Department of Defense recruiting databases are carefully managed to ensure that youth information is not released to any agency outside of the Department and that it is only used to support recruiting programs within the Department. The committee directs the Secretary of Defense to submit a report on his findings and remedial actions, if any, to the Senate Committee on Armed Services and the House Committee on Armed Services by March 31, 2009.*

Included in the background section of this report is a historical overview of the Joint Advertising, Market Research Studies (JAMRS) Recruiting Database as an essential tool in maintaining the vitality of the nation's All-Volunteer military.

Background

Article I of the Constitution vests Congress with the "authority to raise and support armies" for the defense of the United States.[1] The enlistment of qualified men and women in the military forces is essential to this task. Through much of the 20th century, the majority of military personnel were drafted, but, on July 1, 1973, the authority for the draft lapsed, leaving the country reliant on an All-Volunteer Force (AVF) for its defense. As a result, the military Services must meet their extensive manpower requirements entirely by recruiting qualified individuals.

Congress has conferred broad recruitment authority upon the Under Secretary of Defense for Personnel and Readiness and the Secretaries of the Army, Navy and Air Force.[2] In recognition of the importance of attracting qualified individuals to serve in the nation's AVF, Congress has expressly directed the Services to "conduct

1 U.S. Const. Art. i, § 8, Cls. 12-13.
2 See 10 U S.C. §§ 136 (Under Secretary), 3013 (Secretary of the Army), 5013 (Secretary of the Navy), 8013 (Secretary of the Air Force).

intensive recruiting campaigns to obtain enlistments" in the military.[3] To this end, the Secretary of Defense has been provided with a broad mandate to "act on a continuing basis to enhance the effectiveness of recruitment programs of the Department of Defense (including programs conducted jointly and programs conducted by the separate Services) through an aggressive program of advertising and market research targeted at prospective recruits for the Military and those who may influence prospective recruits."[4]

Acknowledging the critical role of recruitment efforts in the maintenance of the nation's AVF, Congress annually provides for the appropriation of funds to carry out advertising and market research programs to enhance the Military's recruiting efforts. In the early 1980s, the DoD implemented a program devoted to advertising and market research for military recruiting for all of the Services, which is referred to today as the JAMRS program. In 2003, Congress expressly acknowledged the continuing efforts of the JAMRS Program "to complement the recruiting advertising programs of the military departments," providing that additional funding be appropriated to carry out this program.[5]

JAMRS Recruiting Database

JAMRS, a program under the Office of the Under Secretary of Defense for Personnel and Readiness, maintains a recruiting database to compile, process, and distribute files regarding potential recruit-aged youth to the Services' Recruiting Commands to assist them in their direct marketing recruiting efforts. The JAMRS Recruiting Database is neither a new effort nor a new system of records, but rather the continuation of decades of the Office of the Secretary of Defense's (OSD) support to the Services. At one time, each of the Services compiled direct marketing data independently. In order to achieve significant costs savings, information is now obtained by JAMRS through a variety of sources and distributed to the Services' Recruiting Commands. This database is critical to the success of the AVF as it enables the Services to contact young Americans, making them aware of the options to serve their country.

Mullen, a Massachusetts based advertising agency, is the Agency of Record (AOR) for the JAMRS program. Mullen was competitively selected in 2002 and again in 2007 for its unique ability to support JAMRS marketing communications mission, which includes management of JAMRS Recruiting Database. Mullen's responsibilities include selecting and negotiating with subcontractors as well as managing them. Mullen Advertising has subcontracted the database processing and security to Equifax Data Services, also based in Massachusetts.

3 10 U.S.C. § 503(a)(1).
4 10 U.S.C. § 503(a)(2).
5 Pub. L. 108-136, Div. A, Title V, § 548.

JAMRS is responsible for ensuring that all data collected by JAMRS, including its contractors and subcontractors, are securely compiled, handled, stored and transferred. JAMRS data are stored in a highly secure and restrictive environment that complies with all DoD and Federal Government security requirements. The JAMRS contract with Mullen prohibits the use of any data in the JAMRS database for any non-Department of Defense recruiting efforts. The contract requires Mullen to adhere to the same security requirements and practices as the government. Thus, it is unlawful for the contractor/subcontractor to use the information for any purpose other than that which has been directed by the Department. DoD oversees its contractors and subcontractors to ensure compliance using DoD security certification and accreditation standards. The contractor and subcontractors are also required under the contract to ensure private information is protected in compliance with the Privacy Act of 1974.

The Department's use of the JAMRS Recruiting Database is consistent with the protections and provisions of the Privacy Act. The JAMRS Recruiting Database only compiles information on potential recruits that is relevant and necessary for the direct marketing program. The data are gathered by the Department through a variety of sources: State Departments of Motor Vehicles (DMVs), the Selective Service System registry, and commercially purchased lists.

Database Security Requirements/Practices for the Prevention of Identity Theft

The following Federal and Departmental standards are applicable to the operating environment of the system:

- DoD Instruction (DoDI) 8510.1-M, "DoD Information Technology Security Certification and Accreditation Process (DITSCAP) Manual," July 2000
- DoD Instruction (DoDI) 8510.01 "DoD Information Assurance Certification and Accreditation Process (DIACAP)" 28 November 2007
- DoD Directive (DoDD) 8500.1, "Information Assurance (IA)," 24 October 2002
- DoDI 8500.2, "Information Assurance (IA) Implementation," 6 February 2003
- Public Law 100-235, "Computer Security Act of 1987," 8 January 1988
- Office of Management and Budget (OMB) Circular A-130, "Management of Federal Information Resources," 8 February 1996
- DoD 5200.1-R, "DoD Information Security Program," 17 January 1997

Security Overview

Direct access to information in the database is highly restricted and limited to those who require the records in the performance of their official duties. The database uses a layered approach of overlapping controls, monitoring and authentication to ensure overall security of the data, network and system resources. Sophisticated physical security, perimeter security (firewall, intrusion prevention), access control, authentication, encryption, data transfer, and monitoring solutions prevent unauthorized access from internal and external sources.

Equifax Database Services (Equifax) hosts and operates the JAMRS Recruiting Database within the Equifax Data Center. Access to the database is restricted to key dedicated personnel within Equifax Data Center only for database maintenance and processing. No one from JAMRS, Mullen or the Services has direct access to the database. Mullen and JAMRS staffs only have access to standard reports containing summaries of aggregated data. Equifax provides dedicated server space for the JAMRS system that is separate from other client environments to ensure that the information is secure.

Equifax meets or exceeds DoD standards on all aspects of security control for the prevention of identity theft, including:

- Alarm systems, access controls, fire detection and suppression systems, video surveillance, security guard, and visitor and employee identification.
- Proper safeguarding of client data, logical access controls, e.g., password protection of applications, data files, libraries, etc., server security software, tape management systems and procedures, and timely rotation of tapes.
- Secure computer rooms and tape libraries with access restricted to systems personnel.
- Offsite back-up of all critical computer applications and data files.
- System mirroring and redundancy.

Equifax maintains written standards and procedures instructing Equifax employees on the protection of client information. Four important procedures regarding security to prevent identity theft include: physical, perimeter, data exchange and access control.

Physical Security

Equifax Data Center security is ensured through use of zoned HID access cards coupled to an access control system, and through use of a 24x7 monitored alarm

system. The computer room area is also monitored by remote controlled video cameras that may be accessed via the Internet in trouble situations. The office park provides a 24x7 guard who patrols seven buildings at that location, and Equifax provides a separate off-hours on-site guard for their office. Equifax only permits access to the Data Center by Equifax IT staff members. All visitors (vendors, Client personnel, Equifax employees) to the Data Center are escorted by an Equifax IT staff member at all times during their visit.

Perimeter Security

Equifax utilizes a firewall from Checkpoint Software as a perimeter firewall. Separate firewall modules are used to protect Equifax corporate and production networks from unauthorized access. Due to the extreme granularity of the firewall software, Equifax custom tunes access rights and rules for JAMRS.

Equifax uses a SmartDefense network system to detect and report on potential intrusions. The software monitors network traffic for unusual patterns or known hacker exploits. In addition, operating system and application software logging processes are enabled on all host and server systems. Where possible, alarm and alert functions, as well as logging and monitoring systems are enabled. Significant events are reported via email and text messages sent to appropriate IT personnel for review and resolution.

Additional network-based software from Sophos and Clearswift provides anti-virus and email content filtering respectively. All inbound/outbound email and connected PCs are automatically scanned for viruses and SPAM.

Data Exchange Security

Equifax employs encryption technologies to secure data communications between the Equifax data center and Input Data Source providers so that Client data requested by or submitted to Equifax are transferred encrypted. Equifax uses Secure File Transfer Protocol (SFTP) over Secure SHell (SSH) as the standard for data interchange. They also use encryption software for data files at rest.

Access Control Security

Equifax has a standard policy that applies to user access rights. All applications developed for JAMRS have a login process to authenticate all application users and control the type of access granted. Capabilities for adding and removing user logins are tightly controlled and restricted to system administrators. All applications have a pre-determined number of authorized login attempts limiting the possibility of

unauthorized access to the system. Only system administrators can reset these passwords and allow further use of the application.

Access to the network, servers, and systems are achieved by individual and unique logins, including the use of passwords or other recognized forms of authentication.

All users of systems that contain high risk or confidential data have a "strong password," using a mix of alpha, numeric and special characters that meets the standards established and documented by the Equifax IT Group.

Equifax uses Secure Sockets Layer (SSL) and other similar encryption methods for access to the entire database application.

Review of Security Procedures

Equifax has a program of self-monitoring for security compliance. Equifax's automated systems management and security software provide the IT team with network performance, access, denials, and intrusion detection. Security reviews of servers, firewalls, routers and monitoring platforms are conducted on a regular basis. These reviews include monitoring access logs and results of intrusion detection software checks.

Vulnerability and risk-assessment tests of external network connections are conducted on a regular basis. The vulnerability and risk assessments are performed both in-house and by a third-party security vendor under contract with JAMRS.

Equifax works with JAMRS to perform security reviews, test the JAMRS Recruiting Database system network, and service security in order to evaluate the security risks and provide recommendations. JAMRS performs security reviews to ensure that Equifax is using sound practices and that they maintain compliance with DoD security requirements under the DoD Information Technology Security Certification and Accreditation Process (DITSCAP). These include physical inspection of Equifax Data Center; reviews of security policies and procedures; and information on application, operating system and server and equipment configurations. Additionally, JAMRS and Equifax are progressing toward completion of the Defense Information Assurance Certification and Accreditation Process (DIACAP) as mandated by instruction.

Opt-Out Procedures

Currently, the Department of Defense processes opt-out requests from individuals who are 15 1/2 years old or older, or parents or legal guardians acting on behalf of individuals who are between the ages of 15 1/2 and 18 years old, seeking to have

their name or the name of their child or ward, as well as other identifying data, removed from this system of records (or removed in the future when such information is obtained). Information on how such individuals can accomplish submission of an opt-out request can be found at the following locations:

The Federal Register. The Federal Register is the official daily publication for rules, proposed rules, and notices of Federal agencies and organizations, as well as executive orders and other presidential documents. The JAMRS Recruitment Database System of Records Notice is published in the Federal Register, Vol. 72, No. 5, page 952 and contains language regarding record access procedures as well as opt-out procedures.

DefenseLINK. The mission of DefenseLINK is to support the overall mission of the Department of Defense by providing official, timely and accurate information about defense policies, organizations, functions and operations. Information regarding JAMRS opt-out procedures is posted to DefenseLINK, specifically at http://www.defenselink.mil/sites/jamrs_optout.html

Additionally, there are non-governmental organizations that provide information specifically regarding how to opt-out of the JAMRS Recruitment Database.

Opt-out requests are submitted by mail to:

Direct Marketing Program Officer
Joint Advertising, Marketing Research & Studies (JAMRS)
ATTN: Opt-Out
4040 N. Fairfax Drive, Suite 200
Arlington, VA 22203–1613

Such requests must contain the full name, date of birth, and current address of the individual.

Opt-out requests are received at JAMRS and are scanned/converted to an electronic form. This opt-out information is then added to the JAMRS Permanent Suppression file.

The JAMRS Permanent Suppression file is used to remove names from direct marketing recruitment mailing lists prior to releasing the mailing lists to the Services. This ensures that any opt-out request has been honored by removing the individual's name from the mailing list before releasing it to the Services. Due to potential timing issues of when an opt-out is received and a mail file is created, JAMRS also provides an updated and comprehensive JAMRS Permanent Suppression File to the Services on a monthly basis. Services are required to use the

most recent and updated JAMRS Permanent Suppression File to suppress (eliminate from mailing) any new additional opt-outs received between the time a file was prepared and ultimately mailed.

Opt-out requests are honored for ten years. However, because opt-out screening is based, in part, on the current address of the individual, any change in address requires submission of a new opt-out request with the new address.

Database Management Overview

Information maintained on the JAMRS Recruitment Database is carefully managed to ensure that youth information is not released to any agency outside of the Department and that it is used for recruitment purposes only. This is accomplished through a series of safeguards:

Memorandum of Agreement

The existing Memorandum of Agreement (MOA) between the Department and the Services details the terms and conditions that apply to, and govern the use of, all data provided by JAMRS to each Service, its personnel, advertising agency, contractors, sub-contractors, consultants and other workers inclusive of any and all 3rd parties ("Authorized Personnel") involved in military recruitment activities on behalf of the Service.

The terms of said MOA are as followed:

Data sets provided by JAMRS to each Service and/or its authorized personnel at the program/product level include:

High School Master Files (HSMF)
Selective Service System (SSS) Registrant Files
College Files
Joint Leads Fulfillment (JLF; responder) Files
Permanent Suppression Files
Defense Manpower Data Center (DMDC) Suppression Files

Each Service and its authorized personnel, as identified above, must comply fully with the Privacy Act of 1974 (5 U.S.C. §552a) and all the following terms and conditions of usage:

Each Service shall accept full responsibility and take whatever steps are necessary to ensure that all JAMRS-provided data are secure and sufficiently protected from unauthorized disclosure or use.

JAMRS data are only to be used for the singular, express purpose of military recruiting. Anyone who, with or without proper authorization, knowingly accesses, obtains, uses or discloses the personal information contained in a JAMRS-provided record for a use other than to carry out authorized recruitment oriented functions, may be subject to criminal prosecution and/or may be liable for civil penalties.

Access to JAMRS-provided data is to be granted only to authorized personnel involved in the process of military recruitment. User IDs, Passwords, etc., should be safeguarded using appropriate measures. Downloading JAMRS-provided data to discs, cartridges, any portable mediums, etc… is strictly prohibited. Data provided by JAMRS are not to be resold, exchanged, shared, given, transferred, etc. to any "outside" or unauthorized 3rd party, etc., under any circumstances. Data obtained from JAMRS may not be treated as public records.

The Federal Driver's Privacy Protection Act of 1994, 18 U.S.C. §2721 et seq. (DPPA) also regulates the terms and conditions of use of any driver data provided in JAMRS deliverables. Driver data constitute one source of HSMF data.

Each Service must maintain and keep current a list of names, titles and contact information for all authorized personnel who receive or handle JAMRS data. Upon request, the Service must be able to provide a copy of the list to JAMRS. The Service must immediately report to JAMRS any security breach or unauthorized access to any of their systems housing JAMRS data.

In addition, the DPPA requires that an authorized recipient of personal information obtained from motor vehicle records (DMVs), who discloses such information, must maintain for a period of 5 years, records identifying each person or entity that received the information. The permitted purpose for which the information will be used must also be maintained. Each Service must make such records available upon request to the DMV from which the information was obtained.

HSMFs and College Files provided by JAMRS have been coded with expiration dates indicative of how long the records may be used for marketing/mailing and analytic purposes. These dates must be strictly adhered to.

Permanent Suppression data provided by JAMRS are to be used strictly and only for suppression purposes, i.e. individuals in this data set should never be sent recruitment mailings nor should they be considered candidates for military service.

Upon signing, each Service accepts full responsibility for enforcing compliance with all terms and conditions of the MOA, as well as those of the DPPA, where applicable, amongst all its authorized personnel who have access to JAMRS data.

Annual Field Command Briefings

The project officer assigned to the JAMRS Direct Marketing program is required to coordinate annual visits with each of the Services' Recruiting Commands in order to conduct a review of the existing MOA, the applicable laws that govern the JAMRS program, discuss the Services' usage of JAMRS data, and answer questions or concerns the Services may have.

Seed Names

JAMRS embeds "seed names" to mailing lists provided to the Services as a way to monitor Service mailings. Seed names are inconspicuous names and addresses that, when mailed to, are received by JAMRS and Mullen Advertising. Each mailing is coded in a way that when JAMRS or Mullen receives a mailing, it is easy to identify who the mail came from and what mailing list was used. This is helpful in identifying unauthorized use or misuse of JAMRS data.

Conclusion

Thirty-five years ago a very important decision was made to staff the U.S. Military on a voluntary basis. The draft was revoked and an All-Volunteer Force was established, creating a need to recruit young adults into the Military. The JAMRS Recruiting Database allows the Services to contact young Americans to make them aware of the varied opportunities to serve their country, and it is critical to successful recruiting efforts. The database saves taxpayers millions of dollars annually by avoiding duplicate acquisition and processing costs for each Service.

Publicized procedures are in place to allow individuals to opt-out from receiving recruitment materials from the Services.

The JAMRS Recruiting Database is maintained in a manner that is consistent with the Privacy Act and other statutes and regulations related to the Department's recruitment authority. The information in the database is used only for recruiting purposes and is maintained in accordance with Federal and DoD security standards. These standards are designed to prevent unauthorized access or inadvertent disclosure of the data which could lead to identity theft.

TAB 4 COORDINATION SHEET

AGENCY	NAME	DATE
P&IP	[illegible]	12 [illegible]
MPP	[illegible]	17 [illegible]
LA	Attached	9 Mar 09
DHRA 066	[illegible]	17 [illegible]