MEMORANDUM

Date: July 15, 2005
To: Interested Persons
From: Electronic Privacy Information Center (EPIC)
(Contact: Marc Rotenberg <rotenberg@epic.org>, Chris Hoofnagle <hoofnagle@epic.org>, Dhruv Kapadia, Guilherme Roschke)
Re: **The Pentagon Recruiting Database and the Privacy Act**

The Department of Defense has proposed the establishment of a recruiting database that will contain detailed personal information on approximately 30 million Americans, many as young as 16 years old.[1] The database will be managed by a private direct marketing firm and will include such information as grade point average, ethnicity, and social security number. The proposal raises significant questions about the Department's compliance with the Privacy Act. That law seeks to ensure that the privacy rights of Americans are protected. Already it is apparent that the Department failed to comply with the Privacy Act obligation that it provide public notice of the project before it was begun.

This memorandum describes the Department of Defense recruiting database and the various Privacy Act implications. The database description is based on the Federal Register notice, public statements by Department of Defense officials, materials on the website of the Department of Defense program that administers the database, and media accounts. Part I discusses the facts that are available from various sources concerning the database, how it operates, the sources of its data. Part II describes issues raised by this database in light of the Privacy Act and other statutes. Part III offers conclusions and recommendations for interested persons to pursue.

I. DESCRIPTION OF THE DATABASE

The Joint Advertising and Market Research Studies (JAMRS) recruiting database was established "to provide a single central facility within the Department of Defense to compile, process and distribute files of individuals who meet age and minimum school requirements or military service."[2] Over time, branches of the Armed Forces had compiled several different lists to target possible recruits.[3] The Department of Defense began consolidating this information in 2002 as well as data from motor vehicle records, the Selective Service System and commercial list brokers. The consolidation process was completed in 2003, and lists of students have been available to recruiters from at least

[1] 70 Fed. Reg. 29486 (May 23, 2005).
[2] *Id*.
[3] Some of this description is based on a Media Roundtable held by Department of Defense officers on June 27th, http://www.defenselink.mil/transcripts/2005/tr20050623-3121.html [hereinafter DOD Roundtable].

2004. In May of this year, the department filed the required public notice.[4]

This section examines the parties involved in the handling of the database; the scope of the database; the categories of individuals that are in the database; and the proposed uses of the database.

A. Parties

The Federal Register notice indicated that JAMRS' system would be located at and managed by a private direct marketing company, Benow.[5] The company was chosen as a subcontractor by Mullen, an advertising agency that has worked on several ad campaigns for the Department of Defense. It is unclear what role data provided by schools plays in this database. See the section on the No Child Left Behind Act below.

JAMRS is the Joint Advertising, Market Research and Studies program at the Department of Defense.[6] JAMRS conducts direct marketing and public relations work for the Department of Defense. The goal of this program is to increase recruitment and retention by the military services. JAMRS also conducts market research studies such as ad tracking, attitudes of mothers towards military service, and polls of young adults.

Benow is a direct marketing company located in Wakefield, Massachussets.[7] It is described as "exclusively focused on designing and managing marketing databases as an outsource service provider."[8] Benow also offers a number of marketing services, including customer segmentation and profiling.[9] Other clients include Tower Records, Saab and Metlife.[10]

According to the public notice, the system of records will be located at Benow. The JAMRS website describes Benow as the manager, "from a technical standpoint" of the direct marketing database.[11] The Department of Defense states that Benow was chosen as a subcontractor by the primary contractor, Mullen.[12] They also further describe the role of Benow as a maintainer of the data that provides expertise in removing duplicates.

Mullen Advertising is JAMRS' primary contractor, which hired Benow as a subcontractor. Mullen is a subsidiary of the Interpublic Group, an advertising conglomerate.[13] It offers a wide variety of marketing services, ranging from developing ad campaigns to handling public relations. Some of its clients include General Motors, Wachovia, Eddie Bauer and XM Satellite Radio. Mullen Advertising performs a number

[4] 70 Fed. Reg. 29486 (May 23, 2005).
[5] *Id*.
[6] http://www.jamrs.org.
[7] http://www.benow.com.
[8] CRM Buyer's Guide, available at http://www.destinationcrm.com/directory/company.asp?CompanyID=7536&CategoryID=104.
[9] http://www.benow.com/html/about_us1.asp.
[10] http://www.benow.com/html/news.asp.
[11] http://www.jamrs.org/about/affiliations.php.
[12] DOD Roundtable, *supra* note 3.
[13] http://www.interpublic.com/interact/family/ipg.php.

of services for the Department of Defense. In addition to handling direct marketing campaigns, it also provides public relations services and develops advertising websites.[14] Mullen's federal contract is for "Advertising and Integrated Marketing Solutions."[15]

B. Data: Size and Sources

According to materials on the JAMRS website, the current system comprises five basic files.[16] The data sources are commercial data brokers, state driver license records, the Selective Service System, and individual contact with and responses to recruiters.

High School Master File. JAMRS has compiled 4.5 million records of 16-18 year old students. State motor vehicle departments provide 51% of the records. The commercial data brokers American Student List (ASL) and Student Marketing Group (SMG) provide 48%. The remaining numbers are from individuals who take the Armed Services Vocational Aptitude Battery test.[17]

*Selective Service System***.** JAMRS gathers 2.5 million Selective Service registrants and distributes them to the different services for recruiting uses. About half of these records have ethnicity codes and phone numbers overlayed on them.[18]

Joint Lead Management System. JAMRS compiles about 50 thousand leads from phone, web, and business reply cards. These includes records on "influencer responders" and "prospect responders." Influencers are those who can influence prospective recruits – the prospect responders – to join.[19]

*College Students File***.** This data set contains 4.6 million records on 18-24 year old college students. It includes specific majors and ethnicities. The data comes from commercial brokers, such as ASL and SMG. About half of the records have phone numbers, and about 20% have Hispanic or African American ethnicity codes.[20]

*Permanent Suppression File***.** A suppression file is a list of contact information for those who have opted out of military recruitment. JAMRS collects a suppression file from congressional requests and names provided by the services. This file contains about 90 thousand records. This is probably the mechanism for managing the limited opt-out described below.[21]

The JAMRS website describes the consolidated database located at Benow as "arguably the largest repository of 16-25 year-old youth data in the country, containing

---

[14] http://www.jamrs.org/about/affiliations.php.
[15] Contract No. GS-23F-0257N, GSA Schedules E-library, http://www.gsaelibrary.gsa.gov/ElibMain/ElibHome.
[16] JAMRS PowerPoint Presentation the 2005 JAMRS Joint Direct Marketing Conference, Slides 85-106, http://jamrs.org/programs/dm_conference/files/Final_Presentation.ppt [hereinafter JAMRS Presentation].
[17] *Id*.
[18] *Id*.
[19] *Id*.
[20] *Id*.
[21] *Id*.

roughly 30 million records."[22] The Department of Defense representative state that currently there are 12 million names in the target audience range, though the total that has accumulated over the years is 30 million.[23] The public notice specifies that the data is retained for five years.

JAMRS purchases lists from two commercial data brokers: American Student List (ASL) and Student Marketing Group (SMG).[24] These data brokers have faced FTC and New York Attorney General actions for their deceptive practices in collecting data from students.

American Student List has settled a case with the FTC over deceptive data collection practices.[25] ASL surveyed high school students, claiming the data would be used for educational purposes, but then sold the data for general commercial purposes. In its consent agreement with the FTC, ASL promised cease distributing data collected for educational purposes to commercial brokers.

The New York Attorney General sued Student Marketing Group for collecting data under false pretenses.[26] The suit charged that SMG established a non-profit subsidiary that would represent itself to teachers and students as surveying students for scholarship and financial aid opportunities. The data collected via these surveys were then provided to direct marketers.

JAMRS also plans future lists that are not covered by the public notice. A JAMRS presentation shows plans for a "medical list," a "prior service list," and an "educator list."[27] These appear to be, respectively, lists of students with a medical career interest; individuals who have prior military experience; and teachers and other education professionals. The public notice description does not list records, purposes, categories and individuals that would be covered by all of these planned lists.

C. Scope: Record Fields and Recorded Individuals.

The public notice lists the following fields in the system of records:

- Name.
- Date of birth.
- Gender.
- Address, city, state, and zip code.
- Telephone number.
- E-mail address.
- Social Security Number.

[22]http://www.jamrs.org/about/affiliations.php
[23]DOD Roundtable, *supra* note 3.
[24]JAMRS Presentation, *supra* note 16.
[25]Press Release, Federal Trade Commission,High School Student Survey Companies Settle FTC Charges (Oct. 2, 2002), *available at* http://www.ftc.gov/opa/2002/10/student1r.htm.
[26]Press Release, Office of New York State Attorney General Elliot Spitzer, Long Island Firm Sued For Tricking Students Into Providing Private Information (Aug. 29, 2002), *available at* http://www.oag.state.ny.us/press/2002/aug/aug29a_02.html.
[27]JAMRS Presentation, *supra* note 16, slide 106.

- Ethnicity.
- High school name, graduation date, and Grade Point Average.
- Education level.
- College intent.
- Military interest.
- Field of study.
- Current college attending.
- Armed Services Vocational Aptitude Battery test date and score.

Categories of individuals in the system of records include students, military personnel, and those who have opted out of marketing. Specifically the public notice lists:

- High school students aged 16-18.
- Current college students.
- Selective Service System registrants.
- Individuals who have taken the Armed Services Vocational Aptitude Battery test .
- Individuals who have responded to advertising seeking enlistment information.
- Current military personnel on active duty or reserves.
- Individuals who have asked to be removed from any future recruitment lists.

D. Purpose and Uses of the Data

The public notice lists the purpose of the system of records as providing a single central facility within the Department of Defense to compile, process and distribute files of individuals who meet age and minimum school requirements for military service. The files are provided to the services for direct marketing purposes.

The public notice states that the routine uses of the records would be the fourteen "Blanket Routine Uses" that the Office of the Secretary of Defense has promulgated. A "routine use" is a catch-all loophole in the Privacy Act that allows an agency to disclose personal information to others without the individual's consent.[28] The fourteen proposed uses, unrelated to recruiting, are[29]:

(1) Disclosure to law enforcement of records indicating violations of the law.
(2) Disclosure to obtain information from other agencies for employment purposes.
(3) Disclosures to other agencies engaging in employment related inquiries are permitted.
(4) Congressional inquiry disclosure of an individual's record, made by a congressional office at the request of that individual.
(5) Private relief legislation.
(6) Disclosures to foreign authorities required by international agreements.

[28] 5 U.S.C. 552a(b)(3) (2004).
[29] Department of Defense Blanket Routine Uses, http://www.defenselink.mil/privacy/notices/blanket-uses.html.

(7) Disclosure to state and local tax authorities for tax purposes.
(8) Disclosure to Office of Personnel Management (OPM) for the OPM to fulfill its duties.
(9) Disclosure to the Department of Justice for litigation.
(10) Disclosure to military banking facilities overseas.
(11) Disclosure to the General Services Administration for the purposes of records management inspections.
(12) Disclosure to the National Archives and Records Administration for the purpose of records management inspections.
(13) Disclosure to the Merit Systems Protection Board for litigation and other proceedings.
(14) Disclosures for counterintelligence or for the purpose of enforcing laws which protect the national security of the United States.

These routine uses govern disclosures. Besides these disclosures, JAMRS is also developing profiles and segmenting prospective recruitees – sorting individuals into different categories based on some factor, such as educational attainment or ethnicity – to create "most likely to respond" lists.[30]

II. PRIVACY ACT AND OTHER LEGAL ISSUES

Several issues are raised by the JAMRS database in light of the Privacy Act. The Privacy Act regulates the government's collection, use and disclosure of personal data.[31] In passing the Privacy Act, Congress sought to restrict the amount of personal information that federal agencies could collect and required agencies to be transparent in their information practices.[32]

A. Federal Register Notice Requirement

The Department of Defense is in violation of the timeliness requirements to publish in the Federal Register. The Privacy Act requires that agencies "publish in the federal register upon establishment or revision a notice of the existence and character of the system of records."[33] Additionally, this must be done 30 days prior to "the publication of information under paragraph (4)(D)."[34] That paragraph refers to the routine use of records in the system.[35] The notice needs to be published 30 days before the routine use. The notice stated that the "blanket routine use" policy will apply.[36]

The maintenance of a system of records without meeting the notice requirements is a criminal violation of the Privacy Act[37]:

Any officer or employee of any agency who wilfully maintains a system of

[30]JAMRS Presentation, *supra* note 16, at slide 89.
[31]5 U.S.C. § 552a (2004).
[32]S. Rep. No. 93-1183, at 1 (1974).
[33]5 U.S.C. § 552a(e)(4).
[34]5 U.S.C. § 552a(e)(11).
[35]5 U.S.C. § 552a(e)(4)(D). ("notice shall include . . . each routine use of the records contained in the system, including the categories of users and the purpose of each use.")
[36]*See also* Department of Defense Blanket Routine Uses, *supra* note 29.
[37]5 U.S.C. § 552a(i)(2).

> records without meeting the notice requirements of subsection (e)(4) of this section shall be guilty of a misdemeanor and fined not more than $5000.

Only two other violations are criminal – knowing disclosure and requesting records under false pretenses.[38] All three have the same punishment. Congress clearly intends the violation of the notice requirement to be as serious as an improper disclosure and lying to access records.

The failure to publish this notice makes all the previous "routine uses" improper disclosures that violate the Privacy Act. The agency is not permitted to disclose information in a system of records unless allowed by one of the exemptions.[39] One of the exemptions is for a "routine use" as described in the public notice.[40] A "routine use" of a record is a form of disclosure for a purpose that is compatible with the purpose for which the record was collected.[41] When an agency fails to publish the public notice, it does not give the public adequate warning of the "routine use," and thus cannot rely upon that exception to disclose the information to others without consent. For instance, in *Doe v. Naval Air Station*, the defendant agency disclosed the plaintiff's home address and telephone number to law enforcement, claiming that such a disclosure was a "routine use" under the Privacy Act.[42] The court held that the agency could not rely upon the routine use exception, because the agency had not first published notice of the use. That is, a disclosure, even if routine, does not qualify for the "routine use" exception unless it is first published.

In *Covert v. Harrington*, the agency failed to disclose the routine uses on a form used to collect personnel security data, violating § 552a(e)(3).[43] Thus an otherwise "routine use" law enforcement disclosure was actually an improper disclosure in violation of the Privacy Act.[44] The analysis is directly transferable to a violation of § 552a(e)(4), requiring publication in the Federal Register. The publication requirement is mentioned in the description of the routine use example, whereas the form collection requirement at issue in *Covert* was not. Thus the case is even stronger for requiring that publication exist before allowing the routine use exemption to apply.

B. The Use of a (Sub)Contractor

The Privacy Act requires the agency to cause a contractor to follow the obligations of the Privacy Act.[45] It cannot currently be confirmed that the Department of Defense is in compliance with these provisions, but there is reason to believe that this has not been followed. A standard schedule on a General Services Administration website does not include the Privacy Act clauses. EPIC has filed a Freedom of Information Act request for this contract, but it has not yet yielded any documents.

---

[38] 5 U.S.C. §§ 552a(i)(1), (i)(3).
[39] 5 U.S.C. § 552a(b).
[40] 5 U.S.C. § 552a(b)(3).
[41] 5 U.S.C. § 552a(a)(7).
[42] Doe v. Naval Air Station, Pensacola, Florida, 768 F.2d 1229, 1231-32 (11th Cir. 1985).
[43] Covert v. Harrington, 876 F.2d 751 (9th Cir. 1989).
[44] *Id*. at 755.
[45] 5 U.S.C. § 552a(m).

The Privacy Act requirements apply "when an agency provides by a contract for the operation by or on behalf of the agency of a system of records to accomplish an agency function."[46] The Department of Defense representative description of the relationship fulfills this condition – the system is being operated on behalf of the agency[47]:

> We in turn task Mullen [the primary contractor] to carry out the mechanics of putting this file together. They in turn turn [sic] to a subcontractor who actually carries out that enterprise. Now they do not use it for any other purpose. They give it back to us. They are a mechanic. We get the files from the various sources including buying the files from commercial writers. We get them set, and their job is to merge those files into a single non-duplicative list.

The Federal Acquisition Regulations (FAR) implement this obligation on the agency to impose the Privacy Act upon contractors.[48] Department of Defense regulations also call for the imposing of the Privacy Act upon contractors that operate a system of records.[49] Agencies that fail to impose the Privacy Act restrictions on contractors operating systems of records on the agencies' behalf may be civilly liable to injured individuals due to subsequent failures to maintain records in conformity with the act.[50] Individuals adversely affected by an agency that does not follow the Privacy Act have grounds to sue.[51]

The government contracting officer is to insert two clauses into the contract if a system of records is being designed, developed, or operated by a contractor.[52] These are 48 C.F.R. 52.224-1 Privacy Act Notification and 48 C.F.R. 52.224-2 Privacy Act. The text of these is included in the appendix of this memo. EPIC filed Freedom of Information Act requests for this contract, but has not yet received a copy.

There is reason to believe that the Department of Defense is not in compliance with the obligation to to include the Privacy Act clauses. Some information on Mullen's contract is available at the General Services Administration E-library page.[53] Mullen's contract number[54] has the title "Advertising and Integrated Marketing Solutions." Some information on this schedule is available at its GSA page.[55] Viewing the solicitation clauses on that page leads to a list of contract clauses.[56] This list does not include the Privacy Act clauses 52.224-1 and 52.224-2.

---

[46] *Id*.
[47] DOD Roundtable, *supra* note 3.
[48] 48 C.F.R. 24.102 (2005).
[49] Department of Defense, Department of Defense Privacy Program, § C1.3 (1983), *available at* http://www.dtic.mil/whs/directives/corres/text/p540011r.txt.
[50] 48 C.F.R. 24.102(d) (2005).
[51] 5 U.S.C. § 552a(g)(1)(D).
[52] 48 C.F.R. 24.104 (2005).
[53] http://www.gsaelibrary.gsa.gov.
[54] GS-23F-0257N.
[55] http://www.gsaelibrary.gsa.gov/ElibMain/ScheduleSummary?scheduleNumber=541
[56] http://apps.fss.gsa.gov/clausesearch/searchbyschedule.cfm?scheduleNumber=541.

The primary contractor, Mullen, is responsible for ensuring that its subcontractor, Benow is bound by the Privacy Act. The mandatory clauses require that a contractor follow the Privacy Act and include the clauses in any subcontracts. Furthermore, for the purposes of agency liability, the employees of the contractor are considered to be agency employees.[57] As discussed below, the civil liability provisions only apply to agencies. Thus a breach by a contractor would lead to liability falling upon the agency, not the contractor.

For the purposes of the criminal liability provisions, employees of the contractor are considered to be agency employees.[58] The criminal liability provisions prohibit willful disclosure, the maintenance of a system or records without meeting the notice requirements, and requesting data from an agency under false pretenses.[59]

C. Improper Use of Social Security Numbers

The Privacy Act explicitly limits the collection and use of Social Security Numbers by a federal agency. In such situations, the Department of Defense must inform the individual the legal basis for the collection of the SSN, whether the disclosure is mandatory or voluntary, and what uses will be made of the individual's SSN.[60]

The Department of Defense cannot rely on a 1943 executive order to collect or use the Social Security Number. In the public notice, the Department of Defense claimed that it had authority to collect the SSN based on Executive Order 9397. This executive order was signed by President Roosevelt in 1943.[61] The Order directs agencies to use the SSN when they are establishing "accounts."[62] Individuals in the proposed database will not have an "account" with the Department of Defense. Because the Department of Defense is not administering an account system for the benefit of individuals, but rather an enumeration system for the benefit of the agency, it cannot rely upon E.O. 9397 for the collection and use of the SSN.

Social Security Numbers are not needed for the claimed purpose. An agency shall collect only such information as is relevant and necessary to to accomplish a purpose of the agency.[63] Social Security numbers are claimed to be used solely to remove duplicate

---

[57] 48 C.F.R. 52.224-2(b) (2005).

[58] 5 U.S.C. § 552a(m). ("When an agency provides by a contract for the operation by or on behalf of the agency of a system of records to accomplish an agency function, the agency shall, consistent with its authority, cause the requirements of this section to be applied to such system. For purposes of subsection (i) of this section any such contractor and any employee of such contractor, if such contract is agreed to on or after the effective date of this section, shall be considered to be an employee of an agency.")

[59] 5 U.S.C. § 552a(i).

[60] Pub.L. No. 93-579, § 7(b), 88 Stat 1896 (1974).

[61] E.O. 9397, Numbering System for Federal Accounts Relating to Individual Persons, Nov. 22, 1943.

[62] *Id*. ("…Hereafter any Federal department, establishment, or agency shall, whenever the head thereof finds it advisable to establish a new system of permanent account numbers pertaining to individual persons, utilize exclusively the Social Security Act account numbers assigned pursuant to Title 26, section 402.502 of the 1940 Supplement to the Code of Federal Regulations and pursuant to paragraph 2 of this order.")

[63] 5 U.S.C. § 552(e)(1).

records.[64] The agency may collect information "relevant and necessary to accomplish a purpose of the agency required to be accomplished by statute or by Executive order of the President."[65] Other methods are available to match the data and remove duplicates, and thus SSN's are not "necessary." This is bolstered by Department of Defense regulations that describe what is necessary to identify a record for access purposes – name, date and place of birth, which excludes social security numbers.[66] If the concern is duplicated mailings, then duplicate addresses can be removed without the need of social security numbers.

The record access procedure improperly requires an SSN. The Federal Register notice states that written requests for record access should be accompanied by a social security number. This contradicts Department of Defense regulations. Office of Secretary of Defense regulations state that individuals "shall not be denied access to their records for refusing to disclose their social security numbers."[67]

The record notification and contesting procedures also improperly require SSN's. They require more information than Department of Defense regulations define as necessary to identify the record.[68] Department of Defense regulations require name, date and place of birth, and the identification of the system of records in order to identify a records. By Department of Defense regulations, SSNs are not required in order to identify records for access purposes.

D. The Limited "Opt-Out" Should be Replaced with Opt In

The Department of Defense appears to allow a limited opt-out. This Department of Defense position needs to be clarified. When discussing the opt-out, the Department of Defense spokesman appears to incorrectly claim that it is the Privacy Act that allows this opt-out right[69]:

> Chu: You can under the Privacy Act write in and say I don't want to be on your list and we then take you out of the list.

The Privacy Act does not have a general opt-out right. EPIC finds one limited Privacy Act interpretation for Chu's words. The Privacy Act provides for the right to have one's records amended and corrected.[70] The database has a "suppression file" of people who are not to be contacted with direct marketing. Thus a possible interpretation of the opt-out right is the right to amend one's records to be added to the suppression file. This is a limited opt out right because it depends on the existence of the suppression file. It is not clear that this is what Chu was referring to.

A simpler, more privacy protecting approach should be implemented. The system

---

[64]DOD Roundtable, *supra* note 3.
[65]5 U.S.C. § 552(e)(1).
[66]32 CFR 311.6(b)(8) (2005).
[67]32 C.F.R. § 311.6(b)(6) (2005).
[68]32 CFR 311.6(b)(8) (2005).
[69]DOD Roundtable, *supra* note 3.
[70]5 U.S.C. § 552a(d)(2).

should collect data directly from individuals. This would replace this unclear, limited, opt-out right with an opt-in system.

E. Remedies for Actual Damages from Intentional or Willful Violations.

An agency will be liable for any violation of the Privacy Act to a plaintiff that shows an "adverse effect."[71] This adverse effect requirement is low. It is similar to the injury and causation requirements for standing.[72] To win a monetary award a plaintiff will have to show actual damages, conclusory allegations of harm will not suffice.[73] The courts are divided on whether pecuniary harm must be shown, as opposed to the presence of proved emotional harm without monetary loss.[74]

The Department of Defense Privacy Act violations meet the "intentional or willful" requirement of the Privacy Act.[75] This intentionality has been described as "action flagrantly disregarding others' rights under the Act."[76]

The Department of Defense knew the requirements of the Privacy Act and continued its conduct in knowing violation of the Act. The Department of Defense activities were not due to inadvertence, rather they were planned as part of the direct marketing efforts of JAMRS. The collection of records was intentional and planned. The transfer of the records to Benow was also not due to inadvertence, but rather by design.

These transfers took place at a time period when JAMRS and Department of Defense were aware of the Privacy Act requirements for a public notice. The JAMRS Direct Marketing conference materials include a presentation on the Privacy Act.[77] This presentation overviews several recruiting systems of records in existence within the recruiting commands.[78] The presentation instructs participants in the basics of the Privacy Act and shows as a "success" the "respect of personal privacy."[79] During the media roundtable, the Department of Defense spokesperson mentioned that the Privacy Act notice was contemplated when a review of the transfer of the database alerted them to the Privacy Act.[80] This transfer occurred several years ago.[81] In the intervening period, the data continued to be collected and distributed.

For the purposes of civil liability, contractors and individuals are not liable, only

---

[71] 5 U.S.C. § 552a(g)(1)(D).
[72] Doe v. Chao, 540 U.S. 614, 624 (2004).
[73] *Id.* at 620.
[74] *Id*. at 627, n.12. "The Courts of Appeals are divided on the precise definition of actual damages. Compare Fitzpatrick v. IRS, 665 F.2d 327, 331 (11th Cir. 1982) (actual damages are restricted to pecuniary loss), with Johnson v. Department of Treasury, 700 F.2d 971, 972-974 (5th Cir. 1983) (actual damages can cover adequately demonstrated mental anxiety even without any out-of-pocket loss)."
[75] 5 U.S.C. § 552a(g)(4).
[76] Andrews v. Veterans Administration, 838 F.2d 418, 425 (10th Cir. 1988).
[77] Department of Defense Privacy, presentation at 2005 JAMRS Joint DM Conference , http://jamrs.org/programs/dm_conference/files/PRIVACY_AND_RECRUITING.DLama.ppt
[78] *Id*., Slides 11-15.
[79] *Id*., Slide 18.
[80] DOD Roundtable, *supra* note 3.
[81] *Id*.

actions against the agency are permitted.[82] However, contractors' employees are considered agency employees for the purpose of agency liability.[83]

F. Specific Statutory Authority For Student Data Collection.

During the media roundtable the Department of Defense spokesperson claimed that 10 USC § 503 provides specific statutory authority for this data collection.[84] This statutory authority permits the collection of "directory information" of secondary school students. The data may be disclosed for recruiting, but no other purpose. The data may be kept for 3 years per person. The data is to remain confidential.

"Directory information" includes[85]:

> the student's name, address, telephone listing, date and place of birth, major field of study, participation in officially recognized activities and sports, weight and height of members of athletic teams, dates of attendance, degrees and awards received, and the most recent previous educational agency or institution attended by the student.

The records under the scope of the JAMRS database exceed this specific statutory authority in record breadth, disclosure, scope of individuals collected and retention period. The JAMRS records includes gender, ethnicity, social security numbers, military interest and aptitude test scores. The data includes college students and young adults. The data is kept for longer than 3 years. The Department of Defense also reserves the right to disclose the JAMRS records for reasons beyond recruiting, as the blanket routine use statement indicates. The data includes college students and young adults. The data is kept for longer than 3 years. Lastly, none of the collected data appears to come from schools. For these reasons, the data collection at issue goes beyond this statutory authority, and the Department of Defense is wrong to rely on this provision.

G. No Child Left Behind

The relationship of No Child Left Behind (NCLB) to the JAMRS database is unclear. The No Child Left Behind Act compels schools to turn over student contact information (name, address, and phone number) to a military recruiter upon such recruiter's request.[86] Students and parents may opt-out of this NCLB data collection by notifying their schools.[87] This opt-out only refers to the consent for the giving of the data by the schools. This opt-out does not generally apply to military collection of student data from other sources. It also does not operate as the "limited opt-out" of the JAMRS database.

The JAMRS website and public notice list the data sources and these do not

---

[82] 5 U.S.C. § 552a(g)(1)(D) ("the individual may bring a civil action against the agency").
[83] 48 C.F.R. 52.224-2(b) (2005).
[84] DOD Roundtable, *supra* note 3.
[85] 20 U.S.C. § 1232g(5)(a) (2004) (this definition is pointed to by 10 U.S.C. § 503 (d)).
[86] 20 U.S.C. 7908(a)(1) (2004).
[87] 20 U.S.C. 7908(a)(2) (2004).

include NCLB data. The Department of Defense representative said the database "has no connection to No Child Left Behind. We do not merge this with No Child Left Behind."[88] However, the public notice also notes that the purpose of the system of records is to "provide a *single central facility* within the Department of Defense to compile, process and distribute files of individuals"[emphasis added]. Data from the NCLB provision could populate such a central single database.

EPIC has filed Freedom of Information Act requests with the recruiting commands of the military services on the topic of how the NCLB data is collected, stored and used. Those requests have not yet yielded any information. The results will be posted on the EPIC website once they become available.

III. Conclusions and Recommendations

The Department of Defense's handling of this database has clearly violated the Privacy Act. The continuing collection, use, and maintenance of a system of records provides a basis for legal action and Congressional oversight.

The Department of Defense should not contract with commercial data brokers for compiling profile information on individuals. The particular commercial data brokers being used have been sued by federal and state authorities for the improper and deceptive data collection practices they carried out on minors.[89] The Department of Defense should maintain the database and collect the information directly from individual. The DOD should not be in the business of enriching these companies while significant attention is being focused on them by state attorneys general, the Federal Trade Commission, and the media.

The Department of Defense should remove the proposed routine use exceptions for the database. The recruitment purpose of the database would still be maintained. As the Department of Defense spokesperson claimed, it is not the intent to distribute this data outside of recruitment purposes. It would increase privacy to curtail these "routine uses" and require that disclosure of the data for non-recruitment purposes be done with written permission of the subjects, and according to the restrictions of the Privacy Act.

The Department of Defense should not collect Social Security Numbers (SSN's).The Department of Defense does not have proper authority under E.O. 9397 to use SSN's. The collection of SSN's is unnecessary for the enumeration of the records. Finally, the collection of SSN's increases the risk of identity theft, should they fall into the wrong hands.

The Department of Defense should collect personal information directly from prospective recruits wherever possible. The creation of detailed profiles on young Americans without their knowledge or consent should be curtailed.

Pending the resolution of these issues, it is EPIC's view that further development

---

[88] DOD Media Roundtable, *supra* note 3.

[89] EPIC Student Privacy Page, http://www.epic.org/privacy/student/ (Citing and FTC action against ASL and a New York Attorney General suit against SMG).

of the JAMRS database should be suspended.

STATUTORY APPENDIX

[FAR] 52.224-1 Privacy Act Notification.

As prescribed in [FAR] 24.104, insert the following clause in solicitations and contracts, when the design, development, or operation of a system of records on individuals is required to accomplish an agency function:

PRIVACY ACT NOTIFICATION (APR 1984)

The Contractor will be required to design, develop, or operate a system of records on individuals, to accomplish an agency function subject to the Privacy Act of 1974, Public Law 93-579, December 31, 1974 (5 U.S.C. 552a) and applicable agency regulations. Violation of the Act may involve the imposition of criminal penalties.

[FAR] 52.224-2 Privacy Act.

As prescribed in [FAR] 24.104, insert the following clause in solicitations and contracts, when the design, development, or operation of a system of records on individuals is required to accomplish an agency function:

PRIVACY ACT (APR 1984)

(a) The Contractor agrees to--
(1) Comply with the Privacy Act of 1974 (the Act) and the agency rules and regulations issued under the Act in the design, development, or operation of any system of records on individuals to accomplish an agency function when the contract specifically identifies--
(i) The systems of records; and
(ii) The design, development, or operation work that the contractor is to perform;
(2) Include the Privacy Act notification contained in this contract in every solicitation and resulting subcontract and in every subcontract awarded without a solicitation, when the work statement in the proposed subcontract requires the design, development, or operation of a system of records on individuals that is subject to the Act; and
(3) Include this clause, including this subparagraph (3), in all subcontracts awarded under this contract which requires the design, development, or operation of such a system of records.
(b) In the event of violations of the Act, a civil action may be brought against the agency involved when the violation concerns the design, development, or operation of a system of records on individuals to accomplish an agency function, and criminal penalties may be imposed upon the officers or employees of the agency when the violation concerns the operation of a system of records on individuals to accomplish an agency function. For purposes of the Act, when the contract is for the operation of a system of records on individuals to accomplish an agency function, the Contractor and any employee of the Contractor is considered to be an employee of the agency.
(c)(1) "Operation of a system of records," as used in this clause, means performance of any of the activities associated with maintaining the system of records, including the collection, use, and dissemination of records.
(2) "Record," as used in this clause, means any item, collection, or grouping of information about an individual that is maintained by an agency, including, but not limited to, education, financial transactions, medical history, and criminal or employment history and that contains the person's name, or the identifying number, symbol, or other identifying particular assigned to the individual, such as a fingerprint or voiceprint or a photograph.
(3) "System of records on individuals," as used in this clause means a group of any records under the control of any agency from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual.

additional information contact the system manager.

[FR Doc. 05–10214 Filed 5–20–05; 8:45 am]

BILLING CODE 5001–06–P

DEPARTMENT OF DEFENSE

Office of the Secretary

Privacy Act of 1974; System of Records

AGENCY: Office of the Secretary, DoD.

ACTION: Notice to add a system of records; DHRA 04—Joint Advertising and Market Research Recruiting Database.

SUMMARY: The Office of the Secretary of Defense proposes to add a system of records to its inventory of record systems subject to the Privacy Act of 1974 (5 U.S.C. 552a), as amended.

DATES: The changes will be effective on June 22, 2005, unless comments are received that would result in a contrary determination.

ADDRESSES: Send comments to OSD Privacy Act Coordinator, Records Management Section, Washington Headquarters Services, 1155 Defense Pentagon, Washington, DC 20301–1155.

FOR FURTHER INFORMATION CONTACT: Ms. Juanita Irvin at (703) 601–4722, extension 110.

SUPPLEMENTARY INFORMATION: The Office of the Secretary of Defense notices for systems of records subject to the Privacy Act of 1974 (5 U.S.C. 552a), as amended, have been published in the **Federal Register** and are available from the address above.

The proposed systems reports, as required by 5 U.S.C. 552a(r) of the Privacy Act of 1974, as amended, were submitted on May 4, 2005, to the House Committee on Government Reform, the Senate Committee on Homeland Security and Governmental Affairs, and the Office of Management and Budget (OMB) pursuant to paragraph 4c of Appendix I to OMB Circular No. A–130, 'Federal Agency Responsibilities for Maintaining Records About Individuals,' dated February 8, 1996 (February 20, 1996, 61 FR 6427).

Dated: May 18, 2005.

Jeannette Owings-Ballard,

OSD Federal Register Liaison Officer, Department of Defense.

DHRA 04

SYSTEM NAME:

Joint Advertising and Market Research Recruiting Database.

SYSTEM LOCATION:

BeNOW, 500 Edgewater Drive, Suite 525, Wakefield, MA 01880.

CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM:

Names of high school students, aged 16–18; current college students; and Selective Service System registrants. Individuals who have taken the Armed Services Vocational Aptitude Battery (ASVAB) test; Individuals who have responded to various paid/non-paid advertising campaigns seeking enlistment information since July 1992; Current military personnel who are on Active Duty or in the Reserves. Individuals who are in the process of enlisting. Individuals who have asked to be removed from any future recruitment lists.

CATEGORIES OF RECORDS IN THE SYSTEM:

Full name, date of birth, gender, address, city, state, zip code, and where available Social Security Number (SSN), e-mail address, ethnicity, telephone number, high school name, graduation date, Grade Point Average (GPA) code, education level, college intent (if documented), military interest (if documented), field of study, current college attending, ASVAB Test date, ASVAB Armed Forces Qualifying Test Category Score.

AUTHORITY FOR MAINTENANCE OF THE SYSTEM:

5 U.S.C. 301, Departmental Regulation; 10 U.S.C. 136, Under Secretary of Defense for Personnel and Readiness, and E.O. 9397 (SSN).

PURPOSE(S):

The purpose of the system of records maintained by the Joint Advertising, Market Research and Studies (JAMRS) is to provide a single central facility within the Department of Defense to compile, process and distribute files of individuals who meet age and minimum school requirements for military service. The information will be provided to the Services to assist them in their direct marketing recruiting efforts. The system also provides JAMRS with the ability to measure effectiveness of list purchases through ongoing analysis and to remove the names of individuals who are currently in, or are enlisting, in the Armed Forces or who have asked that their names be removed from future recruitment lists.

ROUTINE USES OF RECORDS MAINTAINED IN THE SYSTEM, INCLUDING CATEGORIES OF USERS AND THE PURPOSES OF SUCH USES:

In addition to those disclosures generally permitted under 5 U.S.C. 552a(b) of the Privacy Act, These records or information contained therein may specifically be disclosed outside the DoD as a routine use pursuant to 5 U.S.C. 552a(b)(3) as follows:

The DoD 'Blanket Routine Uses' set forth at the beginning of OSD's compilation of systems of records notices apply to this system.

POLICIES AND PRACTICES FOR STORING, RETRIEVING, ACCESSING, RETAINING, AND DISPOSING OF RECORDS IN THE SYSTEM:

STORAGE:

Records are maintained on electronic storage media.

RETRIEVABILITY:

Records may be retrieved by individual's name, Social Security Number, or by address.

SAFEGUARDS:

Access to personal information is restricted to those who require the records in the performance of their official duties. Access to personal information is further restricted by the use of passwords that are changed periodically. Physical entry is restricted by the use of locks, guards, and administrative procedures.

RETENTION AND DISPOSAL:

Destroy when 5 years old or 5 years after completion of a specific training program (General Records Schedule 1, Item 29(a)(1)).

SYSTEM MANAGER(S) AND ADDRESS:

Program Manager, Executive Information/Decision Support Program Office, Six Skyline Place, Suite 809, 5111 Leesburg Pike, Falls Church, VA 22041–3201.

NOTIFICATION PROCEDURE:

Individuals seeking to determine whether information about themselves is contained in this system should address written inquiries to the Department of Defense, Defense Human Resources Activity, c/o JAMRS, Direct Marketing Program Officer, Defense Human Resources Activity, 4040 N. Fairfax Drive, Suite # 200, Arlington, Virginia 22203–1613.

Requests should contain the full name, Social Security Number, date of birth, current address, and telephone number of the individual.

RECORD ACCESS PROCEDURES:

Individuals seeking to determine whether this system of records contains information about themselves should address written inquiries to the Department of Defense, Defense Human Resources Activity, c/o JAMRS, Direct Marketing Program Officer, Defense Human Resources Activity, 4040 N.

Fairfax Drive, Suite # 200, Arlington, Virginia 22203–1613.

The written requests should contain the full name, Social Security Number, date of birth, current address, and telephone number of the individual.

CONTESTING RECORD PROCEDURES:

The OSD rules for accessing records, for contesting contents and appealing initial agency determinations are contained in OSD Administrative Instruction 81; 32 CFR part 311; or may be obtained from the system manager.

RECORD SOURCE CATEGORIES:

Individuals; state Department of Motor Vehicle offices; commercial information brokers/vendors; Selective Service System; Defense Manpower Data Center (DMDC); United States Military Entrance Processing Command for individuals who have taken the ASVAB test; and the Military services and Congressional offices for individuals who have asked to be removed from any future recruitment lists.

EXEMPTIONS CLAIMED FOR THE SYSTEM:

None.

[FR Doc. 05–10216 Filed 5–20–05; 8:45 am]

BILLING CODE 5001–06–P

DEPARTMENT OF DEFENSE

Defense Information Systems Agency

Privacy Act of 1974; System of Records

AGENCY: Defense Information Systems Agency, DoD.

ACTION: Notice to add a system of records; K890.08—Recall Roster/Locator Records.

SUMMARY: The Defense Information Systems Agency proposes to add a system of records notice to its inventory of record systems subject to the Privacy Act of 1974 (5 U.S.C. 552a), as amended.

DATES: This proposed action will be effective without further notice on June 22, 2005, unless comments are received which result in a contrary determination.

ADDRESSES: Send comments to the Defense Information Systems Agency, Attn: Records Manager (SPI21), P.O. Box 4520, Arlington, VA 22204–4502.

FOR FURTHER INFORMATION CONTACT: Ms. Jeanette Jenkins at (703) 681–2103.

SUPPLEMENTARY INFORMATION: The Defense Information Systems Agency systems of records notices subject to the Privacy Act of 1974, (5 U.S.C. 552a), as amended, have been published in the **Federal Register** and are available from the address above.

The proposed system report, as required by 5 U.S.C. 552a(r) of the Privacy Act, was submitted on May 4, 2005, to the House Committee on Government Reform, the Senate Committee on Homeland Security and Governmental Affairs, and the Office of Management and Budget (OMB) pursuant to paragraph 4c of Appendix I to OMB Circular No. A–130, 'Federal Agency Responsibilities for Maintaining Records About Individuals,' dated February 8, 1996, (61 FR 6427, February 20, 1996).

Dated: May 18, 2005.

Jeannette Owings-Ballard,

OSD Federal Register Liaison Officer, Department of Defense.

K890.08

SYSTEM NAME:

Recall Roster/Locator Records.

SYSTEM LOCATION:

Defense Information Systems Agency (DISA), ATTN: SPI21, P.O. Box 4502, Arlington, VA 22204–4502 and DISA organizations elements.

CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM:

DISA Civilian employees, Military personnel assigned or detailed to DISA, and Contractors assigned to all DISA elements, including DISA field activities. Family members of DISA civilian, military personnel, and contractors.

CATEGORIES OF RECORDS IN THE SYSTEM:

Individual's name, duty title, grade, social security number, home address, name of spouse and family members, work/home/cellular telephone numbers, work and home electronic mail addresses, facsimile number, pager number (if applicable).

AUTHORITY FOR MAINTENANCE OF THE SYSTEM:

5 U.S.C. 301, Departmental Regulation; 10 U.S.C. chp 8; DoD Directive 5105.19, Defense Information Systems Agency (DISA); E.O. 9397 (SSN).

PURPOSE(S):

Information is collected and maintained to ensure that DISA has the capability to recall personnel to their place of duty when required for operational reasons. Sure emergency notification may be required when necessary to perform relevant functions/requirements/actions consistent with the DISA mission.

ROUTINE USES OF RECORDS MAINTAINED IN THE SYSTEM, INCLUDING CATEGORIES OF USERS AND THE PURPOSES OF SUCH USES:

In addition to those disclosures generally permitted under 5 U.S.C. 552a(b) of the Privacy Act, these records or information contained therein may specifically be disclosed outside the DoD as a routine use pursuant to 5 U.S.C. 552a(b)(3) as follows:

The 'Blanket Routine Uses' set forth at the beginning of the DISA's compilation of systems of records notices apply to this system.

POLICIES AND PRACTICES FOR STORING, RETRIEVING, ACCESSING, RETAINING, AND DISPOSING OF RECORDS IN THE SYSTEM:

STORAGE:

Paper records are maintained in file folders, index cards, Rolodex-type files, loose-leaf and bound notebooks. Computer files are maintained on magnetic tape, diskette, or other machine-readable media.

RETRIEVABILITY:

Records are retrieved by Social Security Number and/or name of individual.

SAFEGUARDS:

Buildings are secured by guards during non-duty hours. Access to records is controlled by management personnel, who are responsible for maintaining the confidentiality of the records and using the information contained therein only for official purposes related to emergency notification. Access to computerized data is restricted by passwords.

RETENTION AND DISPOSAL:

Records are continuously updated. Records that are no longer current are destroyed by tearing into pieces, shredding, pulping, or burning. Obsolete computer records are erased or overwritten.

SYSTEM MANAGER(S) AND ADDRESS:

Records Manager, SPI21, Defense Information Systems Agency, P.O. Box 4520, Arlington, VA 22204–4502.

NOTIFICATION PROCEDURE:

Individuals seeking to determine whether information about themselves is contained in this system should address written inquiries to Records Manager, SPI21, Defense Information Systems Agency, P.O. Box 4520, Arlington, VA 22204–4502.

The individual should make reference to the office where he/she is/was assigned or affiliated and include address and telephone number applicable to the period during which the record was maintained. Social

U.S. Department of Defense
Office of the Assistant Secretary of Defense (Public Affairs)

News Transcript

On the Web:
http://www.defenselink.mil/transcripts/2005/tr20050623-3121.html
Media contact: +1 (703) 697-5131

Public contact:
http://www.dod.mil/faq/comment.html
or +1 (703) 428-0711

Presenter: Deputy Under Secretary of Defense for Personnel and Readiness David Chu **Thursday, June 23, 2005**

Media Roundtable with Deputy Under Secretary of Defense for Personnel and Readiness David Chu

Chu: Good afternoon, everyone. Thank you for joining us. I've asked a couple of my people to join us -- Sharon Cooper who is effectively the Chief Operating Officer of Consumer Resources Activity and Bill Carr, who watches out for Military Personnel Policy, to join me. They'll answer all the difficult questions. [Laughter].

Let me provide some context here which I think is important in understanding this issue. I know most of you are aware of this context but I think it is important to just very briefly summarize it.

Thirty-two years ago now, I guess, President Nixon made a very important decision that returned the United States to its tradition which is that we staff our military on a voluntary basis. It's easy to forget for those of us who were born during the Cold War, grew up in that period of time, that the United States typically, unlike continental European powers but like the United Kingdom, has typically staffed its military with volunteers. That was true during the Civil War, by the way. A very interesting point. Much of the Civil War staffing was volunteers. Only during the 1st World War and the 2nd World War and then in the period after the 2nd World War in the Cold War, did the United States use conscription, and Nixon decided in '73 to end that.

We went to what people call the All Volunteer Force, and that issue of course has been debated in our political system.

Recently, as you recall last year I think in the legislative cycle, Mr. Rangels's bill was brought up and lost, to return to conscription, lost 400 to 2. So the country has I think very decisively, even Rangel voted against it. [Laughter]. Why did you propose this? [Laughter]. So the country has spoken decisively, we want a volunteer force.

I think what some of you, and I know Vince appreciates this, know in a way the phrase volunteer force is a bit of a misnomer. This is a recruited force. Professional recruiters speak of it this way, as an all recruited force because while I suspect some in the public think people simply walk in the door and sign up, that's not how it works. People have to be made aware that we're interested in them, that they are good candidates for military service, and we have to convey to them what the attributes of military service entail and what the elements that might be attractive to them include. And of course for those who are seeking to go on to college, one of the very important benefits this country established starting in the 2nd World War in different forms over the decades I would acknowledge, is the GI Bill. That we will help finance your college education if you serve in the military.

For those who are headed to college already, one of the very important attributes in the last 10-15 years has been the ROTC scholarship. The majority of ROTC commissionees these days are scholarship students, so the ROTC scholarship is a very important way for young Americans who want to go, particularly to a private university which can be, as any of you paying the bills these days know, very expensive. It can be a very important way particularly for a middle class youngster who's not going to qualify for financial aid under most standards, to be able to help finance that $40,000 a year bill which is typically what it costs at a private university today.

And it's even aimed at people in graduate school or acceding graduate school. The Health Professional Scholarship Program for medical students. It's aimed -- and I have personal knowledge of this -- at people who have finished a graduate program. We recruit doctors. Our recruiters send out nice little notes to doctors saying wouldn't you like to think about coming and serving in our facilities?

To sustain this we need a source of names and addresses, or more accurately, the military recruiters need a source of names and addresses and that's what was reported in the Washington Post this morning.

The Congress actually sanctioned this with statutory language. It goes back at least to 1982. It may go back earlier. That said you will, this is Section 503 of Title 10, United States Code, and reads, "The Congress finds in order for Congress to carry out," I think you could put Secretary of Defense, "to carry out effectively its [inaudible] to raise and support armies, and essentially the Secretary of Defense obtain and compile directory information pertaining to students enrolled in secondary schools throughout the United States."

So this is something that Congress has properly directed the Secretary to undertake, in other words, to contact people.

Now how do we put this list together, and I think that's what's triggered the current interest? For many years we simply acquired various lists. Some of them were purchased, commercial lists, some of them were government lists. The services did it for a period of time on a decentralized basis. In the last decade or so we've tried to give this a more organized supervision and have as we've come in the last few years, to one list for everybody that is a merger of these various lists.

Now I should emphasize, we don't give this list out to other people. It is given only to the military recruiters and again what they get basically is what's in these lists. Typically it's name, address. There are occasions where the commercial list contains some other fields. Apparently some of the commercial list compilers ask students what's your GPA [grade point average] and so on, and the list could preserve that information, but people have volunteered that information.

One point that did come up in the story is that were we retaining social security numbers. The short answer is no. We do get the social security numbers and they're used in a scrambled manner from the Selective Service system file. They're used to purge the list of duplicates and to ensure its cohesion, but they are not maintained.

What I'd emphasize is this is, to come to the key points here, contacting young Americans, making them aware of their option in the service is critical to the success of the volunteer force; it is an activity that Congress sanctioned in statutory language 23 years ago. This is not new. It was done by the Department in various ways over the years, in a more organized fashion in the last few years. That is what triggered, as I understand it, the Post attention. The responsibility for this changed locations within Ms. Cooper's enterprise and under the statutes governing the maintenance of records. The Privacy Act statute, we have to file a new notice. So it's the new notice that gained people's attention and I think created this impression that somehow we were doing something new and different. The short answer is generically this is something we've done for a couple of decades or more.

Media: That was a new notice in the Federal Register?

Chu: The Federal Register, May 23rd.

Media: So you have in the past, I'm the author of the Washington Post story, by the way. You have in the past contracted with a private database marketing firm in order to conduct collection analysis of data to --

Chu: That's a bit of a misnomer. Again, the Department does a lot of things through contractors. We do a number of recruiting/marketing activities through Mullen, which helps provide some of our advertising copy. We in turn task Mullen to carry out the mechanics of putting this file together. They in turn turn to a subcontractor who actually carries out that enterprise.

Now they do not use it for any other purpose. They give it back to us. They are a mechanic. We get the files from the various sources including buying the files from commercial writers. We get them set, and their job is to merge those files into a single non-duplicative list.

One of the last things you want to do when you're sending people material is to send the same person five copies of the same thing. That's, I know as a recipient, that's a quick turnoff, that I couldn't even take the trouble to make sure I only sent it to you once. So their job is to put together a single file, give it back to us, we give it to the military departments to use. That's the contractor's involvement. That's the extent of it.

Media: Why did you say it was in the Federal Register?

Chu: There Under the Privacy act if you maintain a system of records -- If a government agency maintains a system of records, both through a private organization, you have to give public notice if you're doing so. What the purpose is, what the constraints are, et cetera. And we move responsibility for this within our organization which, I'm not the lawyer here so forgive me, I don't want to be accused of practicing law without a license if I'm not quite precise, but as I understand it, the notice applies to the organization and the situation for which it was originally filed. The movement triggered a conclusion by the legal staff that we had to refile.

Media: Why would you use a vendor that specializes in targeted marketing if all you're doing is aggregating a list?

Chu: We didn't choose this vendor.

Media: Who chose them?

Chu: Mullen chose the vendor. We give the task to Mullen, Mullen chooses a subcontractor. That's standard contracting procedure. There's nothing --

Media: Why would they have chosen them but for their expertise in targeted marketing?

Chu: I can't speak to how they chose a particular vendor.

Media: Do you know the value of the contract?

Chu: I'm not sure, but we can get it for you if it's releasable.

There's nothing sinister in giving it to the subcontractor. They're the mechanic. They have no policy role.

Media: Sinister is I don't think the issue. I think the issue is that under the Privacy Act there are restrictions to how much data the government can collect. And as you know, many of the privacy groups have said that by transferring this function to a private database marketing firm --

Chu: They don't collect the data. We collect the data. We give it to them to create a single file.

Media: That's not what the notice says. The notice says that the vendor can collect the data from multiple sources.

Chu: I'm not the lawyer here. I'll defer to the legal staff as to why this is worded the way it is.

Media: How many names are in the database?

Chu: I don't know. Sharon, do you know how many names there are?

Cooper: No. Do you know how many --

Carr: 4.5 million.

Media: That's called the high school master file?

Chu: That's essentially it.

Media: 4.5 million.

Media: So that does not include the college students then that will be in this database. Because the database says all college students.

Carr: The high school master file is one component of the database as well as the college file. There are a number of components within the consolidated database that houses this data.

Media: Is 4.5 the total number of names? No, that's not what I asked. I said how many people's names are in this database. It's high school, college, people registered with the Selective Service. What's the total number in this database?

Carr: Now it's approximately 12 million names.

Media: Thank you.

Media: One of your web sites says there are 30 million names, ages 16-25 I think.

Carr: If you look over the reports of the last few years, the database is robust at that number, but as far as keeping a maintenance of names on an annual basis, based on the target audience range, on the prospects that we're trying to recruit it usually is about 12 million names.

Media: So the 30 is more accumulated over the years.

Carr: Correct.

Media: When was it centralized?

Chu: I think 2003.

Cooper: We started in 2002 and it was finalized in 2003.

Media: Is it because of the centralization that you're required to put out a public notice?

Cooper: It was because it changed organizations. It had been under one sub-organization and that data then was not covered under that sub-organization, it was covered under that sub-organization, it was covered under another one that did not --

Media: When did that occur?

Cooper: That occurred in 2002 also.

Media: Why did it take so long --

Cooper: He thought we were still covered under 2002, under that particular, under the Privacy Act. We were going with the rules that were under that, and then we were informed that we needed, in 2004 we were informed that we needed to do this and we've been working on it since we were informed to do that. Then we put it in the Federal Register.

Media: So since this database was consolidated in 2003 you should have put a notice in the Federal Register under the Privacy Act, correct? And that notice has just gone in last month?

Chu: The consultation doesn't quite trigger the notice. That's Sharon's main point.

Media: What I'm saying is --

Chu: If we had conducted a consolidation under the aegis of the organization where it was originally housed, no new notice would be required. We changed the sub-organization within our [Division] Resource Activity that oversees this. By doing so, upon reflection, the legal staff concluded we needed to file a new notice covering that organization.

Media: That change was made in 2002 you just said though.

Chu: Right.

Media: So since that time, you should have put something in the Federal Register and --

Chu: That was the --

Media: -- and that didn't happen until last month.

Chu: That's a fair point. That's a retrospective conclusion on the part of the legal staff. These things are reviewed. The review suggested we should file notice. We did so.

Media: Why did Mullen choose to subcontract?

Chu: That's standard practice. Your prime contractors, whether it's a weapon system or a software system or a service, prime contractors typically subcontract tasks that are the province of a high quality provider to the best quality, best cost source.

Media: So they would be looking for the expertise that the subcontractor --

Chu: There's nothing inappropriate about that.

Media: My point is they would be looking for the primary expertise that the subcontractor provided.

Chu: The expertise that the subcontractor brings is the manipulation of large files of this sort to ensure that you wind up with a unique entry for each person rather than five times having John Smith at 2300 Oak Tree Lane. That's all that's involved here. Again, I would emphasize, this is a straightforward matter of recruiting young Americans to serve and contacting them with information to say would you be interested. If they then respond positively, then there's a followup from the recruiter. This is nothing more than starting the conversation from a central perspective, because each service does this for its offering. People don't join the Department of Defense, I think that's something most of you appreciate. They join particular services, so each service wants to contact young Americans, it wants to push from a central point its literature. The stuff is really very good. I have teenage kids so I've seen it. In fact my son is insulted only his sister got something because he's not quite old enough to make it to these lists. So they want to push their literature out so people can see what they have. And it's different literature for different communities.

Media: But presumably the recruiters want to be efficient in their jobs so that's why there are target marketers, to sort of help make the decision of who you want to go after.

Chu: They don't do it for us. We give these lists back to the, gives these files. What's being considered here is a file, period. They give the file back to the military department for its recruiting apparatus to use in deciding to whom it wants to send its literature. Literature ranges from literature appropriate to someone who's going to enlist right out of high school, to literature appropriate for someone who is aiming at college, to literature -- My wife has received this stuff. It's very well done. It's actually very interesting.

Media: But that file is going to include all of these extra fields now that --

Chu: On the extra field point, that comes off of commercial lists. It's not from government lists. That's from commercial lists.

Media: Understood.

Chu: Those are commercial fields. They're generally populated from questionnaires that people fill out.

Media: but the military recruiters, whether it's services or whether it's a private contractor --

Chu: No, no. We use military recruiters. We don't --

Media: You're saying the military services use the database for their recruiting.

Chu: They do.

Media: But presumably they use the database in order to tailor, to identify, to look up dead profiles, to identify people who are more likely to be susceptible to a pitch, and to tailor their message to --

Chu: Presumably. Although I think most of it is stratifying it by is this someone who is a candidate for enlistment versus someone who is further along in the educational process and is more a candidate for a different kind of program.

Media: How much integration might there be with other government databases such as Department of Education databases on college students, and so on and so forth?

Chu: I don't think we use those. This is a very, again, I would urge we keep this in perspective. This is a very straightforward, simple activity. We're not trying to create very fancy files here. Our main purpose is to create a reasonably complete file and to purge duplicates. So this is not high end, this is not like the magazines targeting different advertising inserts for every city in the country. We're not -- Maybe we'd like to be at that level of sophistication, but that's not what we are.

Media: What do you say to privacy advocates who view this as government intrusion into the privacy of citizens and that this is a big brother situation?

Chu: I don't think so. We're only using it to mail stuff to people.

Media: You're not calling recruits?

Chu: I don't think this contains telephone numbers.

Media: Yeah, it does.

Media: It certainly does.

Carr: One portion is --

Chu: Oh, okay.

Media: And the data that's collected from No Child Left Behind is included in this database, is that right?

Chu: No, no. It's not. This has no connection to No Child Left Behind.

Media: Why wouldn't that be included if you're going to be --

Chu: I think it was included, if I may say so, only in your article. Let me put on the record. It has no connection to No Child Left Behind. We do not merge this with No Child Left Behind --

Media: I was told that you do merge it with the opt outs from No Child Left Behind.

Chu: You can under the Privacy Act write in and say I don't want to be on your list and we then take you out of the list.

Media: How can anyone have opted out if they didn't know the program existed?

Chu: That's why we have a notice in the Federal Register.

Media: [Laughter].

Chu: I grant, most citizens don't read the Federal Register, but it is there. We also, actually probably the largest source is people who get the literature and say I don't want to hear from you. We put their names -- We do maintain a master list of people who don't want to be heard from and I think we do merge it with -- We try to take advantage of all the information about who doesn't want to be contacted. We don't want to intrude on people who don't want to hear from us, so we try to be very respectful of that fact.

Media: Earlier though you said you've been moving toward a system where you're consolidating your efforts and it makes perfect sense from an efficiency standpoint. So why would you keep the data that is collected via No Child Left Behind separate?

Chu: No Child Left Behind is basically a local and decentralized operation which gives recruiters at your local recruiting station the same right that private companies have if the high school is giving out information, to have a list of the kids in that high school. High schools give it out to the yearbook companies, they give it out to ring companies. I think the status in the Congress, and this is statutory, again, I want to emphasize both the activity we're describing this afternoon and No Child Left Behind, are the product of statutes voted by the Congress.

Media: But you request it.

Chu: Well this actually, this goes back 20-some years. This is back to Congress trying to ensure, and that's I think the main point I want to make this afternoon. Congress wants to ensure the success of the volunteer force. Congress does not want conscription. The country does not want conscription. If we don't want conscription you have to give the Department of Defense, the military services, an avenue to contact young people to tell them what is being offered. And you would be naive to believe in any enterprise that you're going to do well just by waiting for people to call you.

Media: Then why not simply restrict the data fields to name, address, telephone number?

Chu: Well I'm not trying to argue with you, sir. The information that goes beyond that comes off of commercial lists. Anybody could buy that information. We're not, this is not a government file. This is off a commercial file, commercial providers. So we're not intruding -- And typically that information has come off of forms people have voluntarily filled out to a commercial source. So I don't see the --

Media: They may not have intended it to be the property of the U.S. military.

Chu: Well, I'm not sure I see the big issue there, quite candidly. If it were a government file, different matter. But it's not, that stuff is not coming off a government file. It's coming off commercial files.

Media: On this issue of social security numbers, you said something, if you could clarify. You said they're used in a scrambled manner, --

Chu: They are scrambled. We don't retain them. We use them to deconflict the file so that we don't have the same person twice.

Media: so the Selective Service stuff comes over and it's got their social security number on it. So what, it runs through some kind of algorithm that mixes it up?

Carr: It's actually scrambled before we even receive it. Once we receive it via SecureNet, an FTP site, it's therefore housed in our consolidated database.

Media: And it's only used to deconflict.

Chu: Correct, sir.

Carr: The thing is, we can do address, basic zip code, but social security number, when we have that it's [inaudible]. So it's really a great tool to suppress those duplicate files that --

Media: What other sources would you get it from other than the Selective Service? How can you use it to deconflict if it only comes from one place?

Chu: We don't get any other social security numbers from any other place.

Carr: The deconflict would be deconflicting within government records those who are already in the military or those who have already enlisted. That's where it's used.

Media: There was some question about, you said earlier the information is not given out to anybody else. There was some question whether the information was actually given to other government sources or --

Chu: My understanding -- As a matter of policy we don't give it to anyone else.

When the notice was filed, as I understand it, and again I'm not the lawyer here. The standard disclaimer is put in that you can give it as lawfully required to other government agencies. I think that's boilerplate for the most part. It is, it's my understanding, intended to deal with situations where there is a legitimate government purpose for the other agencies inquiry, but as a practical matter we have not given it to other government agencies, we do not intend to give it to other government agencies, and I would be hard-pressed to think of what would be the use of it outside of wanting someone's name and address which could conceivably be of somebody's interest but also obtainable from most other sources.

Media: Do you know if any names have been provided to law enforcement or tax collectors or anything along those lines?

Chu: I don't think so.

Media: You don't know or they haven't?

Carr: They have not based on our capabilities. We have not released any additional information. It goes straight to the recruiting commands and that is it.

Media: So it's never gone to any other government agency?

Chu: No. Nor is it our intent. It wasn't put together for that purpose. I think this is a safeguard. I should emphasize throughout this, those who understand how the recruiting system works I think have long appreciated that this is the kind of data we maintain. It is a directive of the Congress we ought to do this. I think it's an appropriate directive. And the change here is a change of bureaucratic status that has triggered this notice which has given a person set on doing something new and different. This is not something different.

Media: From which office to which office did it --

Chu: It went from Defense Manpower Data Center to our Joint Advertising --

Carr: -- Recruitment and Advertising --

Chu: Thank you.

Media: But it went there a number of years ago and nothing was put into the Federal Register until last month. Even if you decided last year that it should have gone into the Federal Register, you're still dealing with a significant delay in putting it in the Federal Register.

Chu: That's a fair complaint.

Media: What was the reason for the delay? Even once you realized it should have been in there?

Chu: First, it was only triggered by a review of where we stood on all these matters that we realized we should be filing a new notice. And these notices do take a while to prepare. I don't have, I'm not trying to defend the delay, don't get me wrong.

Media: -- numbers of [inaudible] and those who opt out of the No Child Left Behind --

Chu: I'll be glad to get those for you.

Thank you all very much.