Operational Reserve Employer Impact Study

Susan Gates
Principal Investigator

Project Description

The objective of this research is to examine the effects of using the Reserve Components (RC) as an "operational force" on the employers of RC members. Specifically, this project will provide analytically-based insights for determining whether changes are needed to the current Uniformed Services Employment and Reemployment Rights Act (USERRA) and to current programs managed by the National Commission on Employer Support of the Guard and Reserve (ESGR), given changes in policy governing reserve utilization and the continuing need to balance the rights, duties, and obligations of employers, RC members, and their families. To accomplish this objective, the project will be analyzing existing secondary data and also gathering primary interview/focus group data from two sources: managers of transition assistance for RC members and representatives from organizations that employ RC members.

Data Sources

The proposed project will obtain primary qualitative interview/focus group data from two sources: Department of Defense (DoD) employees (either military or civilian) who play a role in managing or supporting RC members as they transition back to civilian employment after military duty (RC leaders) and representatives from companies or organizations that are employers; some of these will have employed RC members (RC employers) and others will be non-RC employers**.**

In addition, we will receive and/or use the following data sets from DoD, the Department of Labor (DoL) or Defense Manpower Data Center (DMDC):

A. Data from the DoD National Survey of Employers. This survey will be fielded by DMDC in February 2011 and the data will be available to RAND for analysis around July 2011. The responding entity for these data is the firm or organization, not an individual.
B. Status of Forces Survey (RC) Data: FY 2000 to present. These are public use data files.
C. Data on USERRA complaints violations from the DoD Ombudsman and the Department of Labor. We are still working to determine what data will be available to us for analysis. The unit of analysis is a complaint of a USERRA violation filed by a reservist. Most likely we will not obtain any data that contain any direct individual identifiers or even information that would allow us to identify the individual by inference. At this point, it appears we will receive only aggregate tabulations regarding the counts of complaints and perhaps their

resolution by broad characteristics. If it appears we will receive any direct or indirect identifiers, we will notify HSPC as soon as possible.

D. Defense Enrollment Eligibility Reporting System (DEERS): We have obtained summary statistics by zip code on the number of reservists by component and the number of activations from the most recent DEERS file available in-house at RAND. This project will not be accessing individual-level data. Only the programmer who works with the DEERS file on a regular basis has done so and sent aggregate tabulations for use by project team members.

HUMAN SUBJECTS ISSUES

Primary Data: RC employers will be asked to provide information on the experiences of their organization. We do not seek the personal opinion of these individuals and the interview questions will pose minimal risk to participants. Interviews with RC leaders will cover their perspectives, observations and expert opinion about how effectively DoD systems currently support RC members as they transition back to work with their civilian employer. As such, the interviews will likely elicit expert opinion, but the topic is not particularly sensitive and these opinions are unlikely to place participants at risk. The study team will not present results in a manner that conveys private information in a potentially identifiable way.

Secondary Data: At this point, we expect that the secondary data analysis will involve only aggregate (not individual-level) data, data on individual organizations (but not individual people) or de-identified public use data from individual surveys. Secondary data analysis will involve only de-identified data that is unlikely to be identifiable by inference (either directly or indirectly). The data from the DoD National Survey of Employers will be covered by a non-disclosure agreement with DMDC. Although the data to be obtained from DMDC will not contain the names of employers, the employers (although not the individual respondent) are potentially identifiable by inference based on some combination of data elements (e.g. location, industry and firm size). Our study team will not make any attempt to identify individual employer identities. Moreover, the study team will not present results in a potentially identifiable way. Furthermore, the de-identified data will be stored on a password-protected network location and access will be limited. The risk to the organizations of disclosure of confidential information once the data has been de-identified is remote and the magnitude of harm of such a disclosure, were it to occur, is small.

RAND's Human Subjects Protection Committee (HSPC) has reviewed and approved the research design. The Committee serves as RAND's Institutional Review Board for review of federally funded research involving human subjects, as required by the Department of Health and Human Services. See Appendix A for a complete Data Safeguarding Plan (DSP).

Appendix A:
Data Safeguarding Plan

Responsibility for Data Safeguarding

Susan Gates, the principal investigator on the project, will have overall responsibility for data safeguarding, and will be designated as "Custodian" in Data Use Agreements. A member of the RAND research programming team will encrypt any sensitive secondary data and store it in a locked container when not in use. The PI will ensure that all project staff are familiar with the data safeguarding plan. Project staff members who collect or access sensitive data will take secondary responsibility for safeguarding the data while it is under their control.

Data Sensitivity

- Audio recordings and transcripts of (focus group) interviews may be considered sensitive information.

- Data from the DoD Survey of Employers is not individual-level data, but is considered sensitive by DoD.
- Data from the DoD Ombudsman and the DoL may contain sensitive information. At this point, we do not expect the data to contain such information and we do not address this issue in the DSP. If the data do contain sensitive individual information, we will return to the HSPC with an amendment to the DSP.

Data Transmittal

Sensitive data will be provided to RAND by the DMDC via CD or secure FTP. Data from the DoD Ombudsman and the Department of Labor will be provided via CD or encrypted e-mail.

Project team members will transmit data within the project according to the RAND sensitive data transmittal matrix guidance (http://smdbsrv1/DataProtection/Default.aspx?r=172,180). In general, for the level of sensitivity of the data to be obtained by this project, that means that team members will use the RAND e-mail network or drops to exchange information.

All reports will provide data in aggregate or anonymous form.

Disclosure Risks

The effect of inappropriate disclosure could include the following:

- Release of contact information of individuals participating in interviews or focus groups. There is no stigma attached to participation in the interviews

of focus groups. As such, this risk is no greater than risks associated with daily life.

- Release of de-identified survey responses where the organization/employer could be identified by inference. This would not harm an individual but could pose risks for RAND.

Audit and Monitoring Plans

No special audits or monitoring procedures will be utilized for this project.

Data Safeguarding Procedures

All audio recordings will be downloaded to an encrypted RAND laptop as soon as possible after the interviews have been completed and the interview files deleted from the recording device.

Audio recordings will be deleted once transcripts have been completed. Transcripts will not include any names of individual interviewees or focus group participants.

Data from the DoD Survey of Employers will be available only to project team members for use on their encrypted and password-protected RAND computers or via a password-protected LINUX system.

Any inadvertent or intentional disclosure of private information to unauthorized parties should be reported to the HSPC using the Adverse Event Reporting form at http://intranet.rand.org/groups/hspc/adverse.html. This includes situations in which private information is not disclosed but potentially might be. If the incident occurs in a field location where the researcher will not have access to RAND's intranet or to email for some time, a preliminary report should be made to the HSPC by phone and followed by a full written report.

In addition, the basic set of procedures which are generally utilized to protect identifiable private and proprietary data will be utilized by the project. These procedures include:

1. Preparing and maintaining a log of all sensitive data collected or acquired, including hardcopy and computer files. The date that materials are received and returned or destroyed will be included.

2. Training staff on data sensitivity and data safeguards being employed.
3. Storing and processing sensitive hardcopy in a centralized location with established access control procedures.
4. Securing sensitive hardcopy in locked files when not in use.

5. Removing all names, addresses and other direct identifiers from hardcopy and computer readable data. Using scrambled identifiers for identification.
6. Restricting access to shared disk files through appropriate use of UNIX file permissions. Employing systematic monitoring procedures to insure that file permissions are correctly set for all files.
7. Using privacy labeled tapes for sensitive computer readable data.
8. Restricting access to locally stored disk files by utilizing encryption, password protection, or by storing the files on removable media which are kept in locked files when not in use.
9. Using Certified Mail, return receipt requested, for sensitive data and Registered Mail for very sensitive data when transferring materials by mail.
10. Encrypting files containing sensitive information using a program, such as PGP, that provides RSA level security before sending them by email. The passwords for encrypted files must not be sent through e-mail, but may be transmitted through U.S. mail, commercial mail service, or directly to the intended recipient over the telephone (do not leave passwords on voice mail systems or phone answering machines).
11. Protecting laptop computers as indicated at /computing/security.away.html. Any files containing sensitive information should be password protected in addition to password protecting access to the laptop.
12. Re-training staff and reviewing sensitive data inventory and data safeguards annually.
13. Deleting or modifying identifiers or data which would allow individuals to be readily identified prior to the release of data outside the project or RAND.
14. Destroying all individual linkages to data after the final report has been issued and reviewed unless specific plans for longitudinal research have been proposed and approved by the person or group supplying the data.
15. Reporting all serious violations of the Data Safeguarding Plan in writing to the Principal Investigator, with a copy to the Privacy Resource Office.