Military Child Development Program Staffing Assessment
Data Safeguarding Plan

Laura Werber and Lynn Karoly
Principal Investigators

Project Description

This study's objectives are to 1) improve strategies currently in use to recruit, train, develop, compensate, and retain qualified military child development program (CDP) staff and 2) inform decisions regarding additional strategies, policy revisions, and future resource allocations intended to address staffing challenges.

The second phase of this assessment will be informed by a survey of the CDP workforce and military installation-based case studies. This data safeguarding plan pertains to the installation-based case studies. To carry out the case studies, we will conduct interviews with an array of CDP stakeholders and staff.

The study already has an approved data safeguarding plan for the first phase of this assessment, which included semi-structured interviews and analysis of deidentified military child development center workforce data.

Data Safeguarding Plan

1. Responsibility for Data Safeguarding

The principal investigators, Laura Werber and Lynn Karoly, have overall responsibility for data safeguarding. The Data Safeguarding Plan will be distributed to all project staff handling data. All project staff will be responsible for safeguarding any data to which they have access and are expected to comply with RAND's policies on protecting sensitive information as well as the requirements of this DSP.

2. Data Sensitivity

a. Interviews with installation leadership, CDP leadership, CDP staff, and other CDP stakeholders

RAND will conduct interviews with members of installation leadership, CDP leadership, and CDP staff, and other CDP stakeholders at up to six case study installations. This target population includes installation leaders (e.g., installation commander or equivalent), center managers (e.g., directors and assistant directors), direct-care classroom staff (i.e., lead teachers and assistant teachers), technical support staff (e.g., special education teachers, training and curriculum [T&C] specialists, behavioral specialists, nurses), and support staff (e.g., administrative assistants, kitchen staff, and custodial and maintenance staff), family child care providers, and local human resources subject matter experts (as applicable), including those with responsibility for supporting CDP program staffing, and community-based organizations, such as Child Care Aware.

Contact Information and Employment Information
Personal data that the study team will receive includes some or all of the following: names, work telephone numbers, work email addresses of prospective participants, and employment information (e.g., job title). Identifiers of CDP leadership (e.g., installation commanders, local subject matter experts, center managers) will be provided by our research sponsor.

To recruit direct care staff, technical support staff, support staff, and family child care providers for interviews, the study team will obtain from interview volunteers their names, telephone numbers, and email addresses as well as employment information (e.g., position, child care setting, length of time served in their current position and in the military CDP in general). This information will be collected on a web-based form hosted by Qualtrics, a FedRamp authorized vendor.

The direct identifiers are necessary to allow the RAND project team to explain the study, schedule the interview, and provide consent materials in advance of the telephone interviews. The employment information is necessary to help us ensure important attributes are represented in our interview sample.

These identifiers will be protected as sensitive data per RAND's data sensitivity guidance (https://randus.sharepoint.com/data/protection/Pages/30.aspx).

Interview Data
Interview data could be sensitive because participants may indicate opinions about shortcomings in current military CDP leadership practices and current operations. As a result, such disclosure could result in employment harm or social injury should confidentiality be breached and such disclosures be attributed to the individual. However, the probability of such an injury is minimal given the study data safeguarding plan.

3. Disclosure Risks

Contact Information and Employment Information
Risk of disclosure of the PII and employment information obtained to facilitate participant recruitment and interview scheduling is minimal given the study data safeguarding plan, and disclosures would result in limited harm given the nature of the information. We plan to minimize the possibility of a breach of confidentiality by instituting data safeguarding procedures as described below, and retaining direct identifiers for only a limited period.

Interview Data
If an interviewee's answers were disclosed due to a breach in confidentiality and such disclosures were able to be attributed to a specific individual, some harm may result if negative opinions were shared. However, the probability of such an injury is minimal given the study data safeguarding plan. It is possible that interview participants might be exposed to embarrassment or damage to their social standing/reputation if they made negative comments that were later disclosed and attributed to them. It is also possible they could suffer damage to their employability or financial standing if in the interview they make negative comments about their employer that were later disclosed and attributed to them.

4. Data Transmittal

Contact Information and Employment Information
The PII of CDP leadership (e.g., installation commanders, local subject matter experts, or center managers) will be transmitted to official RAND email addresses.

For direct care staff, technical support staff, support staff, and family child care providers who have volunteered for interviews, direct identifiers and employment information will be transmitted from the interview volunteer's web browser to a form hosted on the Qualtrics server via secure https protocol, and the RAND study team will download information off the Qualtrics service using secure https protocol. Qualtrics uses Transport Layer Security (TLS) encryption (also known as HTTPS) for all transmitted data.

Interview Data

The interview data will be captured in deidentified notes, which will be shared between RAND project team members using a secure RAND-based MS Teams/ SharePoint site.

5. Data Storage

Contact Information and Employment Information
For direct care staff, technical support staff, support staff, and family child care providers who have volunteered for interviews, the volunteer information form and the information shared by prospective interviewees via that form will be stored in a Qualtrics data center that is independently audited using the industry standard SSAE-18 method. Qualtrics holds an ISO 27001 certification. The direct link to the information and certificate is https://www.schellman.com/certificate-directory?certificateNumber=1723268-3. The status of the certification can be independently verified at https://www.schellman.com/certificate-directory. After the volunteer recruiting is complete and all information downloaded to password-protected RAND computers, all information stored on the Qualtrics site will be deleted.

For all prospective interviewees, contact information and employment information will be stored on password-protected RAND computers and on a secure RAND SharePoint site. The lists of prospective and/or interview participants, their contact information, and employment information that the team retains on RAND assets will be destroyed at the conclusion of the study.

Interview Data
Interview participant names will not be retained in notes, nor will their names be used in file names. Interview data will be kept on the aforementioned MS Teams/ SharePoint site and/or in encrypted files using approved software with FIPS 140-2 validation on password-protected RAND computers. Permission to access the RAND MS Teams/ SharePoint will be limited to RAND project team members.

Interview notes will only be printed when absolutely necessary and will be immediately retrieved upon printing. Printed copies will be disposed of in sensitive waste disposal bins. All interview data will be destroyed five years after the completion of the project.

6. Participant Agreements

The study team plans to obtain interview participants' consent by first emailing information about the study to them prior to the interview. The mailing will be followed up with an email to confirm participants' consent, answer questions as needed, and, if the subject agrees to participate, schedule a time for his or her interview. At the start of the interview, the interviewer will ask if he or she has any questions and will offer to review the key details regarding their consent to participate in the interview and the study generally. The subject will be asked if he or she agrees to participate and consents to recording the interview (i.e., oral consent will be obtained).

7. Additional Data Safeguarding Measures

Any inadvertent or intentional disclosure of private information to unauthorized parties will be reported to RAND National Security Research Division with a copy to the Privacy Resource Office and RAND's Human Subjects Protection Committee. This includes situations in which private information is not disclosed but potentially might have been. 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.

All serious violations of the Data Safeguarding Plan will be reported in writing to the Principal Investigators, with a copy to the Privacy Resource Office.