Data Safeguarding Plan

I. Project Leadership

The Principal Investigators are Dr. Kyleanne Hunter and Dr. Miriam Matthews, employees of the RAND Corp. As of November 22, 2022, all project staff have completed Human Subjects Protections training and related certifications.

II. Project Description

The objectives of the project are 1) to identify which support services and forms of assistance should be available to service member complainants of any form of harassment, including whether or not the current workforce is effectively structured to meet the needs of those service members; and 2) to determine what, if any, additional services and support may be required by military personnel reporting sexual harassment (SH) and identify the most appropriate Department of Defense (DoD) personnel, policies, and practices to meet those needs..

III. Responsibility for Data Safeguarding

Dr. Kyleanne Hunter and Dr. Miriam Matthews will assume overall responsibility for the safeguarding of project data and will be responsible for the observance of all conditions of use and for establishment and maintenance of security arrangements to prevent unauthorized use or access to data. They are also responsible for oversight of secure storage and transmission of data and have primary responsibility for familiarizing site staff with the procedures for the use and safeguarding of all data.

IV. Data Safeguarding Procedures

Access to project files will be held exclusively by analysts and investigators identified as authorized to do so in this Plan.

- All personnel with access to any study data receive training in basic principles of nondisclosure and are aware of the importance of protecting personal data from unauthorized release.
- Any exchange between project sites of data containing identifiers or indirectly identifying information shall be only in the form of files that are transmitted electronically using secure protocols (e.g., secure FTP, secure HTTP).
- RAND will securely retain all research notes.
- All project staff will report all serious violations of the Data Safeguarding Plan in writing to the Principal Investigator, with copies sent to the RAND Human Subjects Protection Committee (HSPC) and RAND Privacy Resource Office.

V. Data Files to be Created or Received

Four (4) types of data files will be created over the course of this project:

(1) A list of scheduled interviews and focus groups.
(2) Notes taken at the time of the interviews and focus groups.
(3) Transcribed interviews and focus groups.
(4) Coded data files. These files consist of coded and categorized portions of interviews and focus groups that will be used for the purpose of analysis.

VI. Data Storage and Transfer

Data collected for this project will be obtained from research notes from participant interviews and focus groups. Data from a will be transcribed, coded, and analyzed using software packages such as Dedoose, a qualitative data management software that helps mark blocks of text pertaining to a given topic. Data will be analyzed quantitatively to identify patterns and key issues, as well as qualitatively to explore the context and nuance of the needs of male sexual assault survivors.

(1) *Interview list*. The interview schedule will be uploaded directly to the project's internal Microsoft Teams site. The Teams site requires login to the RAND network for access; this is protected behind the RAND firewall.

(2) *Interview and focus group notes*. Notes will be taken either by hand or using laptops of RAND project personnel. Hand taken notes will be transcribed onto whole disc encrypted and password protected computers of RAND project personnel. They will then be uploaded to a secure RAND server accessed only by whole disc encrypted and password protected computers by project personnel. Uploaded data will be stored in a Teams folder accessible only to project staff.

(3) *Transcriptions*. All transcriptions will be stored on the internal Teams site in 'access restricted' files behind the RAND firewall.

(4) *Coded Data Files*. The transcriptions will be analyzed using a qualitative data software package. All coding and analysis will take place on whole disc-encrypted and password-protected computers by IRB-approved project personnel; Files will be stored on the RAND Teams site in 'access restricted' files behind the RAND firewall.