Privacy Certificate

August 23, 2019

Organization Name: Abt Associates Inc. **Vendor Number**: 042347643

Project Title: Survey of Inmates in Local Jails (SILJ): Design and Testing

Cooperative Agreement Number: 2015-R2-CX-K146

Grantee, **Meg Chapman, and Abt Associates**, certifies that *data identifiable to a private person* will not be used or revealed, except as authorized in 28 CFR Part 22, Sections 22.21 & 22.22. *Information identifiable to a private person* is defined in 28 CFR §22.2(e) as "information which either--(1) Is labeled by name or other personal identifiers, or (2) Can, by virtue of sample size or other factors, be reasonably interpreted as referring to a particular person."

Brief Description of Project (required by 28 CFR §22.23(b):

Abt Associates was awarded a cooperative agreement with the Bureau of Justice Statistics to re-design the survey instrument and design the study sample for the Survey of Inmates in Local Jails (SILJ) and to conduct a field test of the newly designed SILJ instrument.

One goal of this effort is to develop the next version of the Survey of Inmates in Local Jails, increasing the quality of the sample and expanding the ability to analyze both subpopulations of interest, geographic areas and trends over time. The objectives of this goal are to conduct research to develop a new survey tool that (1) covers emerging areas and current information gaps (i.e., expanded health issues), (2) is shorter and more efficient in its collection (3) is better able to deal with non-response issues, and (4) can be standardized with other general population surveys for analysis. A review of literature and feedback and advice from relevant stakeholders in the corrections field (NIC, NIJ, BJA, and the National Sheriffs Association) will be used in the development of the tools. This process will also: review the ability to use administrative data on such things as charge, sentence, and criminal history to reduce the burden on the jail respondent; develop relevant questions on women's health issues; and, increase the ability to assess mental health and infectious disease among inmates. In order to efficiently review the ability to use administrative data, Abt will develop and deploy an online Survey of Jail Administrative Records (SJAR) to document currently available administrative data and the willingness and ability of jail administrators to provide these data in support of the SILJ program.

A second goal is to develop a cross sectional sampling plan that provides adequate power to examine subpopulations, a method for stratification of jails, and of inmates within jails by key characteristics. In addition BJS is interested in a plan that will allow examination of state level estimates for a smaller number of states and/or jail types to analyze changes over time in the populations housed and trends related to local policies.

Finally, a third goal is to conduct a pretest of the newly developed survey with inmates in a sample of jails. We propose to conduct cognitive testing prior to the pretest with a sample of nine inmates, followed by pre-test data collection, which will include the collection of survey and administrative

data. The results of the pre-test will be used to inform recommendations for revisions to the instrument and sample design.

Procedures to notify subjects that such data will only be used or revealed for research or statistical purposes and that compliance with the request for information is not mandatory and participation in the project may be terminated at any time as required by 28 CFR §22.23(b)(4) or if notification of subjects is to be waived, pursuant to 28 CFR §22.27(c), please provide a justification:

Abt is using three distinct data sources as part of this effort: (1) survey data from jail administrators in the SJAR; (2) survey data from jail inmates participating in the pilot of the survey; and (3) administrative records of jail inmates maintained by jails and BJS in the pretest, such as offense information and criminal history information.

For data source 1 of the study, no human subject's data will be collected other than contact information for follow-up questions, so consent to participate in the online survey is not applicable.

For data source2 of the study, Abt researchers will obtain informed consent from jail inmates, describing the intent of the pilot and emphasizing the voluntary nature of participation. Respondents will be informed of the potential risks of participating, and procedures will be established to protect the identity of those who choose to participate.

For data source 3 of the study, consent to use administrative program data is not applicable, as these data are administrative records and are not subject to 28 CFR §22.23(b)(4). These administrative data are collected by jails as part of their administrative records and include names and individual identifiers (e.g., FBI numbers, SSN, etc.) as well as information potentially on their current offense and criminal history information. Given that we will not use, or reveal individual identities during the quantitative analysis of these data except for tracking purposes (after which identifiers will be stripped and discarded), the use of this data "presents no more than minimal risk of harm to subjects and involves no procedures for which written consent is normally required outside of the research context" (28 CFR 46.117) and notification of subjects is unnecessary.

The Abt Institutional Review Board has reviewed the study to confirm the anticipated process for notifying subjects, and will conduct a formal review after award.

Procedures developed to preserve the confidentiality of personally identifiable information, as required by 28 CFR §22.23(b)(7):

As a research and consulting company, Abt Associates collects a variety of information for research purposes. Abt policies include an information security policy that establishes a baseline for data security practices, educates users and vendors regarding their obligations to protect data assets, and provides a foundation to ensure the confidentiality, integrity and availability of client and corporate data.

For all data sources, names will be separated from the data and/or redacted. After data collection is completed, names will be removed and replaced with study identification numbers and qualitative codes. Communication between staff members will use study ID's to verify against other datasets or for internal communication.

Described below are additional procedures which are designed to maintain the confidentiality and integrity of personally identifiable information collected during the study.

Justification for the collection and/or maintenance of any data in identifiable form, if applicable:

Individual identifiers in the data will only be used for purposes of data collection (i.e., identifying, and recruiting participants), matching data with existing administrative data, authenticating data collections, or obtaining missing data (e.g., from completed surveys or correcting administrative data).

Procedures for data storage, as required by 28 CFR §22.23(b)(5):

Procedures for data storage to be used in this study all involve the use of password-protected access to systems and records. Abt uses Microsoft Active Directory to manage user access to folders and to manage accounts. Passwords must meet minimum complexity requirements, are changed regularly, and password reuse is very limited. The project director must authorize each user's access to the project data folders.

All data transfers for research or statistical purposes will be recorded in a log consistent with 28 CFR 22.23. All data transfers to and from Abt will utilize Abt's FTPS site (Ipswitch's MOVEit DMZ) to the extent possible. Any transfer methods outside of an encrypted CD or the FTPS will be reviewed by Abt's information security team. Password protected and encrypted "zip" files will be used when electronic data is to be transferred via FTPS or encrypted CD-ROM from the originator to Abt Associates. Transfers using Abt's FTPS site meet FIPS 140-2 encryption standards and are also stored encrypted on the site. User access is linked to Active Directory and each user must also be authorized to gain access to the FTPS site.

Encrypted CDs received from local jails will be kept in a locked file cabinet at Abt and will only be accessible to key project staff. If a CD is provided unencrypted or encrypted with non-compliant (FIPS 140-2) encryption, the data will be re-encrypted and the original CD will be destroyed. Abt will request the organization modify their procedures to be compliant with applicable laws.

All Abt servers, workstations, and notebook computers are protected from viruses, spyware, and worms. The devices are continuously updated with the latest definition file and scanned regularly from a central server. Similar to antivirus services, patching is centrally managed and patches are pushed to end users per the company's patching process.

Paper records containing personally identifiable information will not be transported; electronic versions (PDFs) will be sent electronically via FTPS. Any printed data with personally identifiable information will be will be stored in locked cabinets and shredded once no longer needed,

Physically, Abt's offices require a badge and keycard for entry. The servers are located in an on-premise server room that required keycard access which is limited to select IT staff (Abt) or in a secure TIER 4 datacenter (Abt SRBI).

All Abt laptops are encrypted with a FIPS 140-2 compliant encryption product.

Description of any institutional limitations or restrictions on the transfer of data in identifiable form, if applicable:

Not applicable.

Name and title of individual with the authority to transfer data:

Abt Associates certifies that access to the data will be limited to those employees having a need for such data and that such employees shall be advised of and agree in writing to comply with the regulations in 28 CFR Part 22.

Abt Associates certifies that all project personnel, including subcontractors, have been advised of and have agreed, in writing, to comply with all procedures to protect privacy and the confidentiality of personally identifiable information.

Access to data is restricted to the following individuals, as required by 28 CFR §22.23(b)(2):

Principal Investigator: Dana Hunt and Richard Kulka
Project Staff: Meg Chapman
Sarah Jalbert
Ryan Kling
Sharmini Radakrishnan
Omri Drucker
Chris Cutler
Chris Flygare
Mandy Wong
David Judkins
Walter Campbell
Marci Schalk
Brenda Rodriguez
Stanislav Kolenikov
Maggie Elliott
Olivia Griot
Yvonne Cristy
Kevin Neary
Deirdre Rabideau
Kathryn O'Hara
Allison Ackerman
Kay Ely
Contractors, Subcontractors, and/or Consultants:
Henry Steadman
Brian Case
William Rhodes
Walter Hillabrant
Jeff Mellow
HeeCheol Chung

Abt Associates certifies that adequate precautions will be taken to ensure administrative and physical security of identifiable data and to preserve the confidentiality of the personally identifiable information.

Procedures to insure the physical and administrative security of data, as required by 28 CFR §22.25(b), including, if applicable, a description of those procedures used to secure a name index:

All data will be secured physically and electronically in Abt Associates facilities and systems. The technical safeguards to be employed in this study all involve the use of password protected access to computer systems and records. All computers to be used in the study will require passwords for operation and access to data directories. The main administrative safeguard to be used in this study is a confidentiality agreement that will be signed by all that will have access to personally identifiable information.

Procedures for the final disposition of data, as required by 28 CFR §22.25:

Public use data files, to be archived at the Inter-University Consortium for Political and Social Research at the University of Michigan, will be prepared and sent, per National Archive of Criminal Justice Data (http://www.icpsr.umich.edu/NACJD/archiving/confidential-content.html) guidelines, via email using a FIPS 140-2 compliant encryption software package. Any changes to the coding or layout will be discussed, placement of the file confirmed, and the data and full documentation submitted. Placement of the file will be determined by BJS. Data collected in this cooperative agreement is the sole property of BJS. Abt staff will not publish, present, or release information from this work without prior written permission of BJS.

As government contractors in the criminal justice field for decades, we are well versed in the protocol for the allowable use of the government's data. Abt will destroy all data that is no longer needed and a certificate of destruction will be created for all data and physical media destroyed. At project completion, all analysis data files and processing programs will be provided to BJS. All data maintained by Abt that contains personally identifying information will be destroyed upon request by BJS or 3 years after the end of the project, whichever occurs first.

Name and title of individual authorized to determine the final disposition of data:

Grantee, Abt Associates, certifies that:

- Project findings and reports prepared for dissemination will not contain information which can reasonably be expected to be identifiable to a private person, except as authorized by 28 CFR §22.22.
- The procedures described above are correct and shall be carried out.
- The project will be conducted in accordance with all the requirements of the Omnibus Crime Control and Safe Streets Act of 1968 as amended and the regulations contained in 28 CFR Part 22.
- BJS shall be notified of any material change in any of the information provided in this Privacy Certificate.

Signature(s):

Principal Investigator_  __ Date _8/23/19

Institutional Representative _  _____Date ____8/23/19_____