COOPERATION AND DATA SHARING AGREEMENT
BETWEEN
BROWN UNIVERSITY AND
THE CITY OF CENTRAL FALLS

This Agreement is made between Brown University, a nonprofit corporation formed and existing under colonial charter of 1764, on behalf of the Rhode Island Innovative Policy Lab, with an address at One Prospect Street, Providence, RI 02912 ("University"), and the City of Central Falls, a municipal corporation located at 580 Broad Street Central Falls, RI 02863 ("City"). The University and the City may herein be referred to as "Party" or collectively referred to as the "Parties."

1.0 Purpose

WHEREAS, the Central Falls Police Department ("CFPD") is an agency whose mission is to fulfill the law enforcement needs of the people with the highest degree of fairness, professionalism and integrity, and protect the inherent rights of the people to live in freedom and safety; and

WHEREAS, the CFPD possesses or shall possess data relating to traffic stops, traffic violations, crimes and law enforcement; and

WHEREAS, the Researcher, Dr. Justine Hastings ("Researcher") is Professor of Economics and International and Public Affairs at the University with expertise in econometrics and applied statistics, the use and analysis of administrative data, public economics and economic modeling of human behavior, and is the principal investigator on research projects at and the director of the Rhode Island Innovative Policy Lab (RIIPL); and

WHEREAS, the CFPD is interested in supporting rigorous research into and development of policies which would provide data and research to inform policy improvements and evaluations to further its mission to fulfill the law enforcement needs of the people with the highest degree of fairness, professionalism and integrity, and protect the inherent rights of the people to live in freedom and safety; and

WHEREAS, the City and the CFPD believe that, by providing data to the Researcher for the purposes of such research, the results of such research will further CFPD's mission to fulfill the law enforcement needs of the people with the highest degree of fairness, professionalism and integrity, and protect the inherent rights of the people to live in freedom and safety; and

NOW THEREFORE, in consideration of the mutual covenants, promises, and conditions herein contained, and for good and valuable consideration, the adequacy of which is hereby acknowledged, the City and the University agree as follows:

2.0 Definitions

The following terms shall have the following meanings:

2.1 "Criminal Justice Information" (CJI) refers to all of the FBI Criminal Justice Information Services (CJIS) provided data necessary for law enforcement and civil agencies to perform

their missions as defined in section 4.1 of the FBI's CJIS Security Policy CJISD-ITS-DOC-08140-5.5. CJI includes but is not limited to biometric, identity history, biographic, property, and case/incident history data. CJI data are considered CJI until release to the public via authorized dissemination (e.g. within a court system; presented in crime reports data; released in the interest of public safety); purged or destroyed in accordance with applicable record retention rules.

2.2 "Personally Identifiable Information" (PII) shall mean data which include any of the following: (1) the name of an individual or that of the individual's parents or guardians, (2) social security number, (3) specific home address, (4) driver's license number, (5) client or personal identification number, (6) birth date, or (7) a list of personal characteristics or other information which would make the individual's identity immediately traceable.

2.3 The term "Confidential Information" (CI) shall mean: (i) all PII; (ii) any personal information protected under federal or Rhode Island law; and, (iii) all trade secret information which is disclosed by a Party, or otherwise acquired by a receiving Party, in the course of the Parties' discussions or other activities pursuant to this Agreement and which is marked "Confidential" by the disclosing Party at the time of disclosure or is orally identified as confidential by the disclosing Party at the time of disclosure and written notice reiterating its confidentiality is sent to the receiving Party within thirty (30) days of disclosure thereof. Each Party shall have the right, upon written request, to require that the other Parties confirm in writing whether any such information disclosed but not identified as CI is to be considered CI hereunder. By way of illustration, but not limitation, CI includes data with PII which is protected by law, other information protected by law, trade secrets, processes, formulae, data, know-how, products, designs, drawings, computer aided design files and other computer files, computer software, bills of materials, ideas, improvements, inventions, training methods and materials, manufacturing processes, sales information, marketing techniques, plans, strategies, budgets, financial information, forecasts, customer lists and pricing policies. Except as otherwise provided by law, CI, however, shall not include any information which:

i. is or hereafter becomes known and legally available to the general public through a party who had the right to make the information available to the general public and through no act or omission of the receiving Party which is, directly or indirectly, in violation of the receiving Party's obligations under this Agreement;

ii. is subsequently disclosed without restriction to the receiving Party by a third-party who had the right to make such disclosure and who did not, directly or indirectly, receive such information through a Party who was obligated not to disclose the same;

iii. is required to be disclosed by any applicable law, or judgment, order or decree of any court having jurisdiction; provided that in connection with any such disclosure, the receiving Party shall use its best efforts to give to the disclosing Party reasonable prior notice of such required disclosure if such required disclosure will include any Confidential Information; or

iv. is disclosed to a third-party on a non-confidential basis by the Party who owns such information; or

v. was known by the receiving Party prior to disclosure or independently developed by the receiving Party without knowledge of, reliance upon, or use of the disclosing Party's information. Information shall not be disqualified as Confidential Information under the foregoing exceptions merely: (1) because it is embraced by more general or generic information which is in the public domain or available from a third-party, or (2) because it can be reconstructed from information taken from multiple sources, none of which individually shows the whole combination (with matching degree of specificity), its principle of operation, and/or the relevant use or method of use, as applicable.

2.4 "CFPD Data" shall mean information or data gathered, maintained and stored by the CFPD and/or the CFPD's designee(s) in the normal course of carrying out its stated purposes and covered under the scope of this agreement. CFPD Data may include CJI, PII and/or CI, and may include, but not be limited to, data related to:

- For any stop by an officer of an individual or vehicle: personal identifiers for parties and/or vehicles involved in the stop, all data related to the location, date and time of the stop, dispatch records related to the stop, reasons for search, results of search, perceived race of the driver, an identifier for the officer sufficient to distinguish officers in the data and link officers across records and to officer demographics.
- Records from dispatch and arrest data tables including all data on location of the event, the date and time of the event, descriptive codes and classifications of the event and/or resulting charge(s), results of the event, personal identifiers and demographic information of offenders involved in the event or arrest, identification number for the involved officer(s) sufficient to distinguish officers in the data and link officers across records and to officer demographics.
- Officer demographics including birth year, race, sex, work experience, rank, and unit.

2.5 This document does not seek to define the exact data elements to be shared but is to be used as a framework for ongoing sharing of data between the parties.

2.6 Each data element shared will be listed on a separate data inventory which will be updated and cosigned by both parties prior to the first data export and each time the list is changed.

3.0 Protection of CJI

3.1 Physical protection. All CJI data will be stored in a separate encrypted file system that is dedicated to CFPD Data containing CJI and covered in this agreement. The encrypted file system, "CJI System" will live within the Researcher's dedicated, secure server system, "Stronghold," which has security and access features stipulated in Appendix B and Appendix C. The CJI System must use a two-party password with a minimum of 10 characters in each party's password. The first party consists of the Researcher and her designated research team member. The second party consists of senior CIS personnel: the University CISO, or his/her designated data science team member. Therefore, no individual person can decrypt or view the original CJI data without full knowledge of the senior team. Whenever original CJI data is decrypted for processing, both parties will be present for the entire session, and the decrypted data is shredded and wiped at the end of the session. The CJI system must be

protected by a real-time, automated monitoring software which sends real-time email alerts to both parties any time the encrypted data files are accessed.

3.2 Access to CJI. The CJI encrypted file system will only be accessed by the approved two-party team members from a single, restricted workstation located in a locked office at RIIPL. The workstation will be a university-owned machine with up-to-date patches, malicious code protection, spyware protection, and system policies that prevent external access to the Internet. The sole use of the workstation will be to initiate a session in the Stronghold environment. During this session, the encrypted files containing CJI will be decrypted within the CJI System to separate PII and Anonymous Data and statistical extracts from CJI so that non-CJI PII, non-CJI anonymous data and non-CJI statistical extracts can be analyzed by approved researchers within the Stronghold system.

3.3 Background Checks. Approved researchers with access to the encrypted CJI filesystem must complete the minimum screening requirements for each individual seeking access to CFPD's unencrypted CJI data as per section 5.12.1 Personnel Security Policy and Procedures of FBI's CJIS Security Policy (CJISD-ITS-DOC-08140-5.5), which includes state of residency and national fingerprint-based record checks and completion of the FBI CJIS Security Addendum form. See Appendix E.

3.4 Data Extraction. The parties will work together to develop an acceptable method of extracting the data from the CFPD data stores. The data extracting utility will be tested by both parties to ensure all data transferred is accounted for on the data inventory prior to the data extracting utility being used in production.

3.5 Data Transport. The parties will agree to a secure encrypted file transport utility that will be used to protect the data in transit. Brown University will receive the data on a standalone computer and immediately encrypt the data for storage within Brown's stronghold environment.

4.0 Protection of CI and PII

4.1 Protection of CI and PII. Each Party shall take all reasonable steps to protect the confidentiality of another Party's CI, specifically including, but not limited to the Researcher maintaining CFPD Data solely on a secure, dedicated computing environment with security and access safeguards and following the policies stipulated in Appendices B-E, as well as utilizing and following the Appendix A Security Pledge and the Federal Bureau of Investigation Criminal Justice Information Services Security Addendum Certification Form.

4.2 Access to CI and PII. CFPD Data will be analyzed solely on a secure, dedicated computing environment with security and access safeguards and policies stipulated in Appendix B and Appendix C. CFPD Data will be accessed and analyzed only by Researcher-approved research staff and collaborators. Researcher-approved research staff and collaborators must also complete the Security Pledge in Appendix A, FBI CJIS Security Addendum Certification Form, and complete Human Subjects Protection Training as stipulated in Appendix B. A copy of all completed Security Pledges and FBI CJIS Security Addendum Certification Forms will be made available to the CFPD upon CFPD's request.

4.3 Disclosure. The receiving Party shall not, without the prior written consent of the disclosing Party:

i. disclose the CI to any other person or entity except to the Researcher, her approved research staff and collaborators, or the CFPD, or their agents, who have a "need to know" such CI in the course of the performance of their duties, who are informed of the obligations of this Agreement, and who have executed a confidentiality agreement with the Researcher;

ii. copy or reproduce the CI except as is necessary to further the objectives of the relationship between the Parties hereto (all such copies, however, shall include a confidential identification marking and shall be governed hereby); or

iii. use the CFPD Data except to further the research goals agreed upon by the Parties.

4.4 Security and Anonymization of CFPD Data. The University and Researcher agree to transfer, store and use CFPD Data including CJI, PII and CI in accordance with security protocols set forth in Appendices A through E to this Agreement.

4.5 Cell Size Suppression Policy. The University agrees that any use of CFPD data in the creation of any document (manuscript, table, chart, study, report, etc.), regardless of whether the report or other writing expressly refers to such purpose, to the CFPD, or to the files specified in this Agreement or any data derived from such files, must adhere to the federal current cell size suppression policy. This policy stipulates that no cell less than 11 may be displayed publicly. Also, no use of percentages or other mathematical formulas may be used if they result in the public display of a cell less than 11.

5.0 Audits and Expungements.

5.1 University agrees to allow audits of the RIIPL's use of the CFPD's shared CFPD Data by the CFPD information security officer, and/or his or her designee(s), at the CFPD's request. The University agrees to assist with and facilitate such audits.

5.2 The CFPD will transmit to the University Custodian on a monthly basis a list of case identifiers which need to be expunged. The University agrees to expunge the cases from all CJI data within seven (7) working days of receipt, to expunge cases from all backup copies of CJI data within fourteen (14) working days of receipt, and to confirm the completion of the expungement process with the CFPD via email within fourteen (14) working days of receipt.

6.0 Use, Term and Termination.

6.1 Use. The University represents that the CFPD Data furnished to the University by the CFPD will be used solely for the research purposes and/or services agreed upon by the Parties. The University shall not disclose, release, reveal, show, sell, rent, lease, loan, submit or present for scholarly review, publish, answer inquiries regarding, or otherwise grant access to the data covered by this Agreement to any person without prior express, written approval by CFPD, except for approved researchers who need to analyze the data under the purposes of this agreement.

6.2 The University, as an institution of higher education, engages only in research that is compatible, consistent, and beneficial to its academic role and mission. Therefore, significant results of research activities must be reasonably available for publication. The Parties acknowledge that the Researcher shall have the right to publish the results of her research and that nothing in this Agreement shall be interpreted to restrict this right of publication; provided that no CJI, PII or CI or any other internal Agency information supplied to it by CFPD will be included in any published material without prior express, written approval by CFPD. The University will provide CFPD with the opportunity to review any and all material for legal compliance, prior to publication. The Parties agree and acknowledge that any and all CFPD Data transferred to the University will remain property of the CFPD. The Parties further agree and acknowledge that any and all research products, whether published or unpublished, prepared by the University as a result of the use of CFPD Data will be the property of the University.

6.3 Duration. This Agreement begins on the date that the last party signs this Agreement, which is the Effective Date. Subject to extension by mutual, written consent of the Parties, this Agreement shall remain in full force and effect for a period of one (1) year beginning on the Effective Date, unless sooner terminated at any time by any Party giving at least ninety (90) days prior written notice to the others. The University agrees to notify the CFPD immediately if the Researcher is no longer affiliated with the University or RIIPL, and the CFPD has the right to immediately terminate the Agreement in response to the notification.

6.4 Termination. If the CFPD determines that the University has violated a material term of this Agreement, the CFPD may terminate this agreement immediately or, at CFPD's discretion, by giving the University a period of up to thirty (30) days to cure the violation or breach. The CFPD will notify the University in either event of its decision of termination in writing. Upon request, the University will submit a Corrective Action Plan outlining the steps that the University took and will take to prevent a continuing and/or similar material breach in the future.

6.5 This Agreement may be terminated by any Party for default upon the defaulting Party's failure to cure a material breach within thirty (30) days after written notice by the non-defaulting Party specifying with sufficient detail the nature of the default.

6.6 This Agreement may be terminated by any Party by providing thirty (30) days written notice (or upon the greatest amount of notice allowed under the law or regulation) if a change of law or regulation necessitates that the Agreement be terminated to maintain any Party's compliance with such law or regulation. In such case, the Parties will work in a cooperative manner to maintain, return or destroy CFPD Data, CJI, PII and CI defined herein.

6.7 If CFPD terminates this Agreement under any provision herein, its termination shall also include, but not be limited to, termination of its right to receive any of the services or reports from the Researcher.

6.8 Survival. Except as otherwise provided by law, the obligations of confidentiality imposed by this Agreement shall survive termination of this Agreement. With respect to trade secrets, the obligations shall last for so long as the information remains a trade secret.

6.9 Data destruction. Upon termination of the Agreement, University will return or destroy all CFPD Data and will not retain, nor allow any of its agents or subcontractors to retain, any CFPD Data except for Anonymous Data or aggregated data derived from CFPD Data used for purposes of producing and/or replicating research results produced under this agreement. University's duty to destroy CFPD Data includes, but is not limited to, the obligations to destroy all copies of CFPD Data including backup tapes and other electronic backup medium, and to destroy all CFPD Data by "clearing" (which requires a minimum of three (3) passes), "purging" or "physically destroying" CFPD Data in accordance with the National Institute of Standards and Technology (NIST) Special Publication 800-88 or in another manner approved in advance by CFPD. University will certify in writing to CFPD that University (including its agents and subcontractors) has returned or destroyed all CFPD Data as this Agreement requires. If CFPD agrees that the return or destruction of CFPD Data is infeasible and determines that University's written plan to safeguard the confidentiality and security of CFPD Data is acceptable, CFPD may permit University to retain CFPD Data for the specific and limited purpose that makes return or destruction of CFPD Data infeasible. This written plan of retention must be submitted and approved by CFPD for CFPD Data to be retained.

7.0 Data from CFPD to University.

7.1 Upon reasonable request, the CFPD may provide to the Researcher, or provide access for the Researcher to receive, CFPD Data under the scope of data defined in paragraph 2.4 of this Agreement. Said updates will be provided according to mutually agreed upon timing, stipulated in Appendix D.

7.2 All CFPD Data shall be in an accessible form and format transferred to the researcher via protocol set forth in Appendix D.

7.3 CFPD represents and agrees that it has the right to contribute and to disclose CFPD Data to the Researcher pursuant to this Agreement and that the Researcher has the right to use CFPD Data, but only as set forth in this Agreement.

7.4 CFPD agrees to cooperate with the Researcher to provide CFPD Data in the most reasonably useful format. Such cooperation shall include, but not be limited to, providing information needed to understand the meaning of CFPD Data, to make it clearly usable by the Researcher. CFPD also agrees to communicate and aid in the Researcher understanding any changes CFPD makes regarding the method by which it gathers, maintains, sorts, or develops CFPD Data.

7.5 Upon reasonable request, the Researcher will provide CFPD with access to Anonymous Data which have been aggregated and/or de-identified by the Researcher to eliminate any CJI, PII or CI. The Researcher is not obligated to provide, in any format, data provided to the Researcher by any third party, including other community, governmental and non-profit agencies, and is not obliged to provide any data fields that were cleansed or derived through combination with data received from a third party.

8.0 Custodians and Points of Contact.

8.1 Custodian. The parties mutually agree that the following named individuals are designated as "Custodians" of the file(s) on behalf of the University, and will be personally responsible

for the observance of all conditions of use of the data, and for the establishment and maintenance of security arrangements as specified in this Agreement to prevent unauthorized use or disclosure. The Custodians, as designated in this Agreement, have the authority to represent within their organization; and are responsible for all use of the data specified in Paragraph(s) 2. The University agrees to notify the CFPD in writing within FIVE (5) business days of any change of Custodianship.

Brown University Custodians

Justine Hastings, PhD
Professor of Economics and International and Public Affairs, Brown University.

Ravi Pendse, PhD
Chief Information Officer, Vice President for Computing and Information services, Brown University.

8.3 Points of Contact. The Parties mutually agree that the following-named individuals will be designated as "Point of Contact" for the Agreement on behalf of the CFPD:

CFPD Point of Contact

Colonel James Mendonca
Chief of Police, Central Falls Police Department

OR

His/her designee(s)
Christopher A. Cavallaro
IT Administrator, Central Falls Police Department

AND

Matthew Jerzyk, City Solicitor

The Parties mutually agree that the following-named individual will be designated as "Point of Contact" for the Agreement on behalf of Brown University:

Brown University DUA Point of Contact

Justine Hastings, PhD
Professor of Economics and International and Public Affairs, Brown University.

9.0 Mitigation

9.1 The Researcher, along with the University, retains the sole right, and has the obligation, to establish appropriate security mechanisms and policies to protect CFPD Data during transfer, storage, and de-encryption for use in research. Researcher will notify CFPD in the event of a

known data breach or compromise of the system where CFPD data is stored, in accordance with Section 9.2.

9.2 In the event of breach or suspected breach, the University shall, within twenty-four (24) hours, notify the CFPD security officer and/or the designated Point of Contact for this Agreement, and the FBI, of any unauthorized use or disclosure, suspected breach or breach of, or access to the aforesaid data. The notice shall contain all information available to the University at the time of the notification to aid the CFPD in examining the matter and will be supplemented by the University as additional information is obtained. The University will preserve forensic evidence relating to any breach, including log report data to be shared with CFPD. The CFPD and the University will meet to jointly develop an incident investigation and remediation plan.

9.3 The University agrees to hold CFPD harmless in the event of an unauthorized access or disclosure, including but not limited to holding the CFPD harmless in connection with any sanctions such as the termination of CJIS services. The University agrees to accept fully the legal and financial responsibility associated with mitigating any harmful effects that may or have been caused by an unauthorized disclosure or access of data obtained from the CFPD data file provided to the University.

9.4 The University will take steps to prevent a continuing and/or similar breaches should one occur. The University understands that as a result of CFPD's determination or reasonable belief that unauthorized disclosures have taken place, CFPD may refuse to release further data to the University for a period of time to be determined by CFPD.

10.0 Miscellaneous.

10.1 Third Party Beneficiaries: Each Party hereto intends that this Agreement will not benefit or create any right or cause of action in or on behalf of any person other than the Parties hereto.

10.2 Assignability: This Agreement shall be binding upon and shall inure to the benefit of each Party and its assigns and successors in interest. This Agreement shall not otherwise be assignable or assigned by any Party without prior written approval by the others first being obtained.

10.3 Governing Law; Forum. This Agreement shall be governed by and construed under the laws of the State of Rhode Island, which shall be the forum for any lawsuit arising from or incident to this Agreement.

10.4 Severability. The terms of this Agreement are severable, such that if any term or provision is declared by a court of competent jurisdiction to be illegal, void, or unenforceable, the remainder of the provisions shall continue to be valid and enforceable.

10.5 Non-Waiver. The failure of any Party to exercise any of its rights under this Agreement for a breach thereof shall not be deemed to be a waiver of such rights, nor shall the same be deemed to be a waiver of any subsequent breach, either of the same provision or otherwise.

10.6 Headings. The headings of the sections are inserted for convenience of reference only and are not intended to be a part of or to affect the meaning or interpretation of this Agreement.

10.7 Entire Agreement; Modification. This Agreement (and its attachments of Appendices A through E and the FBI CJI Security Addendum Certification Form) constitute(s) the entire understanding among the Parties with respect to the subject matter hereof and supersedes any and all prior understandings and agreements, oral and written, relating hereto. Any amendment hereof must be in writing signed by an authorized representative of the Parties.

10.8 Counterparts. This Agreement may be executed in two (2) or more counterparts, each of which shall be deemed an original but all of which together shall constitute one (1) and the same instrument.

COOPERATION AND DATA SHARING AGREEMENT SIGNATURE PAGE

BROWN UNIVERSITY AUTHORIZED AGENT

(Signature) _____ (Date) 4/11/17

Name: Ravi Pendse, PhD

Title: Chief Information Officer, Vice President for Computing and Information Services

Acknowledged:

_____
Justine Hastings, Researcher

CITY OF CENTRAL FALLS AUTHORIZED AGENT

By: _____
James Diossa
Mayor and Director of Public Safety

By: _____
As to Form and Correctness
Matthew Jerzyk
City Solicitor

By: _____ 5/5/17
Reviewed
Leonard Morganis
Administrative and Finance Officer

Date: 5/8/17

Approved as to Form
James M. Green
Deputy Counsel
Office of the General Counsel
Brown University
Date: 04/11/2017

Appendix A

Security Pledge for the Use of Confidential Data from City of Central Falls Police Department ("CFPD")

I, _____, through my involvement with and work on research projects with Professors Justine Hastings will have access to the secure data provided by the CFPD to be used in producing research results. By virtue of my employment as a research assistant to Dr. Hastings on her research projects, and as a member of her research team, I have access to confidential information and use of data that are deemed confidential, personal, and private to the CFPD for the sole limited purpose of performing research for and under the direction of Dr. Hastings. I understand that access to this confidential data carries with it the responsibility to guard against unauthorized use and the possibility of unauthorized access or use. To treat information as confidential means not to divulge it to anyone who is not a project member, or to cause it to be accessible to anyone who is not a project member. Designation of research team membership and approval for access to these data reside solely with Professor Justine Hastings. Transfer of any information off of the designated secure computers, or between the designated secure computers, or access to information on secure computers by anyone other than myself, must be cleared through and approved by Professor Justine Hastings.

I understand that disclosing confidential information directly, or allowing non-authorized access to such information, may subject me to criminal prosecution and/or civil recovery and may violate the code of research ethics at Brown University and the National Bureau of Economic Research.

I acknowledge that I have read and understand this "Security Pledge" and agree to fulfill my responsibilities on this project in accordance with the following guidelines:

1. I will not permit non-project personnel to access these sensitive data, either electronically or in hard copy.
2. I will not disclose confidential information, directly or indirectly, to anyone who is not a project member.
3. I will not attempt to identify individuals, families, or households.
4. I agree that in the event an identity of an individual, family, or household is discovered inadvertently, I will (a) make no use of this knowledge, (b) advise Professor Justine Hastings of the incident, (c) safeguard or destroy the information as directed by Professor Justine Hastings, (d) not inform any other person of the discovered identity.
5. I will not transfer information off of the designated secure computers without the prior approval of Professor Justine Hastings.

Researcher: **Witness:**

Name: _____ Name: _____

Signature: _____ Signature: _____

Date: _____ Date: _____

Appendix B

Storage of Secure Data from the CFPD

Stronghold System Requirements:

The Stronghold server system has been established by Brown University to be compatible with Federal and Rhode Island Law standards for data privacy and protection and resources dedicated for use by the Rhode Island Innovative Policy Lab (RIIPL) and Dr. Hastings, who is the principal investigator and director of RIIPL. The hardware resides in the central datacenter located in dedicated, private facility which is protected by a card access system maintained by the Brown Department of Public Safety, under security camera monitoring and equipped with fire suppression systems. Within the data center, an additional layer of protection is provided via a locked enclosure for the Stronghold hardware with additional combination and key access. Physical access to the data center is granted to approved Brown Computing and Information Services (CIS) staff and escorted hardware vendors only. Redundant power feeds, a 600kW generator and redundant uninterruptible power supplies (UPS) guarantee constant power and cooling. Brown has established and will maintain a security infrastructure covering its Stronghold system and other devices, including any networks connecting its computers. The security system includes, at a minimum, secure user authentication protocols including two-factor authentication and access measures as well as multiple layers of firewall protection, intrusion detection (IDS) protections, operating system security patches at least monthly and remote access via virtual private network (VPN) protocol. In addition, Brown will provide an environment that segregates user data and access by security priority via secure virtual protocols and isolates the environment and user sessions from having any ability to download or copy data outside of the computing environment. In the event of a failed disk, the Information Security Group (ISG) provides a service to crush and dispose of the storage device which meets NSA evaluation standards. Access to the systems and data will be limited to authorized users and system administrators, who need root level access to maintain the system. User access is restricted to Dr. Hastings, approved research analyst staff, and co-investigators. All administrative access is logged to individual accounts that are not shared. Policies and procedures are in place to remove access to users when they leave Brown or are no longer affiliated with RIIPL. Administrative passwords are changed on a regular basis and whenever an administrative user leaves the University. Access to all files will be logged and audited for unusual behavior via daily review by an impartial security group in ISG.

CJI System Requirements:

Additionally, all CJI data will be stored in a separate encrypted file system that is dedicated to the CJI covered by this agreement. This encrypted file system will use a two-party password with a minimum of 10 characters in each party's password. The first party consists of Dr. Hastings and her designated senior research team member. The second party consists of senior CIS personnel: the Director of Data Science, the CISO, or their designated data scientist. Therefore, no individual person can decrypt or view the original CJI data without full knowledge of the senior team. Whenever original CJI data is decrypted for processing, both parties are present for the entire session, and the decrypted data is shredded and wiped at the end of the session. In addition, any time the encrypted data files are accessed, Stronghold's automated monitoring software sends a real-time email alert to all parties.

The CJI encrypted file system will only be accessed from a single, restricted workstation located in a locked office at RIIPL. The workstation will be a university-owned machine with up-to-date patches, malicious code protection, spyware protection, and system policies that prevent external access to the Internet. The sole use

of the workstation will be to initiate a session in the Stronghold environment. During this session, the CJI encrypted file system will be decrypted inside Stronghold to separate PII and de-identified data from CJI. Once this processing is complete and has been validated, all original CJI data will be destroyed.

Human Subjects Protections Training:

The Researcher and approved staff working for the Researcher on data covered under this agreement will complete Human Subjects Protections Training as required by Brown University, and will keep certification up-to-date as required by the Brown University Program in the Protection of Human Research Participants.

Appendix C

Replacing Personal Identifiers

Data received from CFPD may include an identification number to link households over time and across CFPD Data. CFPD Data may also include sensitive personal identifiers such as social security numbers or names or addresses, if determined to be needed for linking individuals across administrative data sets. Sensitive personal identifiers in the CFPD data will be replaced with a scrambled identifier once the data are received by Dr. Hastings. Any personally identifiable information will be stripped from the data immediately once they are no longer needed for joining data sets. The crosswalk from the personal identifiers in the CFPD Data to the scrambled identifier will reside in an encrypted file system that uses a two-party password with a minimum of 10 characters in each party's password. The first party consists of Dr. Hastings and her designated senior research team member. The second party consists of senior CIS personnel: the Director of Data Science, the CISO, or their designated data scientist. Therefore, no individual person can decrypt or view the crosswalk files without full knowledge of the senior team. Whenever the crosswalk is decrypted or accessed for processing, both parties are present for the entire session, and the decrypted data is shredded and wiped at the end of the session. In addition, any time the encrypted crosswalk files are accessed, Stronghold's automated monitoring software sends a real-time email alert to all parties.

Appendix D

Procedure for Transferring Files from the CFPD to RIIPL

CFPD will provide updated data to Researcher at a frequency needed for particular research projects, but no less than quarterly. CFPD will encrypt the data using AES-256 encryption, then use the secure copy (scp) or secure FTP (sFTP) protocol to transfer the encrypted data from host system to a staging area in the University's secure computing environment, called Stronghold. A password or key for decrypting the file will be established prior to the first transfer, and any changes to the password or key will be communicated by the CFPD to Researcher by phone. All transfers will take place over a dedicated VPN or network path between CFPD and the University's data center, which will be established and tested prior to the first transfer. All transfers will be logged and authentication to Stronghold will use two factors. Once data has been transferred to the staging area, it will be copied by the University into an encrypted file system inside Stronghold, and the original data in the staging area will be destroyed. The Researcher will provide a chain-of-custody report to CFPD showing the complete audit history of the data while it is in the staging area, and confirming that the original data were destroyed.

Appendix E

FEDERAL BUREAU OF INVESTIGATION
CRIMINAL JUSTICE INFORMATION SERVICES
SECURITY ADDENDUM

The goal of this document is to augment the CJIS Security Policy to ensure adequate security is provided for criminal justice systems while (1) under the control or management of a private entity or (2) connectivity to FBI CJIS Systems has been provided to a private entity (contractor). Adequate security is defined in Office of Management and Budget Circular A- 130 as "security commensurate with the risk and magnitude of harm resulting from the loss, misuse, or unauthorized access to or modification of information."

The intent of this Security Addendum is to require that the Contractor maintain a security program consistent with federal and state laws, regulations, and standards (including the CJIS Security Policy in effect when the contract is executed), as well as with policies and standards established by the Criminal Justice Information Services (CJIS) Advisory Policy Board (APB).

This Security Addendum identifies the duties and responsibilities with respect to the installation and maintenance of adequate internal controls within the contractual relationship so that the security and integrity of the FBI's information resources are not compromised. The security program shall include consideration of personnel security, site security, system security, and data security, and technical security.

The provisions of this Security Addendum apply to all personnel, systems, networks and support facilities supporting and/or acting on behalf of the government agency.

1.1 Definitions

1.2 Contracting Government Agency (CGA) - the government agency, whether a Criminal Justice Agency or a Noncriminal Justice Agency, which enters into an agreement with a private contractor subject to this Security Addendum. For the purposes of this Agreement the CGA is the City of Central Falls.

1.3 Contractor - a private business, organization or individual which has entered into an agreement for the administration of criminal justice with a Criminal Justice Agency or a Noncriminal Justice Agency. For the purposes of this Agreement the Contractor is Brown University ("the University").

2.1 Responsibilities of the Contracting Government Agency.

2.2 The CGA will ensure that each Contractor employee receives a copy of the Security Addendum and the CJIS Security Policy and executes an acknowledgment of such receipt and the contents of the Security Addendum. The signed acknowledgments shall remain in the possession of the CGA and available for audit purposes. The acknowledgement may be signed by hand or via digital signature (see glossary for definition of digital signature).

3.1 Responsibilities of the Contractor.

3.2 The Contractor will maintain a security program consistent with federal and state laws, regulations, and standards (including the CJIS Security Policy in effect when the contract is

executed and all subsequent versions), as well as with policies and standards established by the Criminal Justice Information Services (CJIS) Advisory Policy Board (APB).

4.1 Security Violations.

4.2 The CGA must report security violations to the CJIS Systems Officer (CSO) and the Director, FBI, along with indications of actions taken by the CGA and Contractor.

4.3 Security violations can justify termination of the appended agreement.

4.4 Upon notification, the FBI reserves the right to:

a. Investigate or decline to investigate any report of unauthorized use;

b. Suspend or terminate access and services, including telecommunications links. The FBI will provide the CSO with timely written notice of the suspension. Access and services will be reinstated only after satisfactory assurances have been provided to the FBI by the CJA and Contractor. Upon termination, the Contractor's records containing CHRI must be deleted or returned to the CGA.

5.1 Audit

5.2 The FBI is authorized to perform a final audit of the Contractor's systems after termination of the Security Addendum.

6.1 Scope and Authority

6.2 This Security Addendum does not confer, grant, or authorize any rights, privileges, or obligations on any persons other than the Contractor, CGA, CJA (where applicable), CSA, and FBI.

6.3 The following documents are incorporated by reference and made part of this agreement: (1) the Security Addendum; (2) the NCIC 2000 Operating Manual; (3) the CJIS Security Policy; and (4) Title 28, Code of Federal Regulations, Part 20. The parties are also subject to applicable federal and state laws and regulations.

6.4 The terms set forth in this document do not constitute the sole understanding by and between the parties hereto; rather they augment the provisions of the CJIS Security Policy to provide a minimum basis for the security of the system and contained information and it is understood that there may be terms and conditions of the appended Agreement which impose more stringent requirements upon the Contractor.

6.5 This Security Addendum may only be modified by the FBI, and may not be modified by the parties to the appended Agreement without the consent of the FBI.

6.6 All notices and correspondence shall be forwarded by First Class mail to:

Assistant Director

Criminal Justice Information Services Division, FBI
1000 Custer Hollow Road
Clarksburg, West Virginia 26306

FEDERAL BUREAU OF INVESTIGATION
CRIMINAL JUSTICE INFORMATION SERVICES
SECURITY ADDENDUM CERTIFICATION FORM

CERTIFICATION

I hereby certify that I am familiar with the contents of (1) the Security Addendum, including its legal authority and purpose; (2) the NCIC Operating Manual; (3) the CJIS Security Policy; and (4) Title 28, Code of Federal Regulations, Part 20, and agree to be bound by their provisions.

I recognize that criminal history record information and related data, by its very nature, is sensitive and has potential for great harm if misused. I acknowledge that access to criminal history record information and related data is therefore limited to the purpose(s) for which a government agency has entered into the contract incorporating this Security Addendum. I understand that misuse of the system by, among other things: accessing it without authorization; accessing it by exceeding authorization; accessing it for an improper purpose; using, disseminating or re-disseminating information received as a result of this contract for a purpose other than that envisioned by the contract, may subject me to administrative and criminal penalties. I understand that accessing the system for an appropriate purpose and then using, disseminating or re-disseminating the information received for another purpose other than execution of the contract also constitutes misuse. I further understand that the occurrence of misuse does not depend upon whether or not I receive additional compensation for such authorized activity. Such exposure for misuse includes, but is not limited to, suspension or loss of employment and prosecution for state and federal crimes.

Employee Name PRINTED	Employee Signature	Date of Birth	Today's Date

Manager Name PRINTED	Manager Signature	Today's Date

Company Name PRINTED	Company Phone