NSF/NCSES Restricted-Use Data Procedures Guide

Contents

Introduction

Chapter 1: Laws
- 1.1 Privacy Act of 1974
- 1.2 National Science Foundation Act of 1950
- 1.3 Confidential Information Protection and Statistical Efficiency Act of 2002

Chapter 2: Licensing Procedures
- 2.1 Only Restricted-use Data are Licensed
- 2.2 Restricted-Use Data Procedures for NCSES Staff/Fellows and Contractors
- 2.3 What is a License?
- 2.4 Applying for a License
- 2.5 NCSES Review/Approval of the License Application
- 2.6 After Approval of the License Request
- 2.7 Licensee and Principal Researcher Responsibilities
- 2.8 Amending or Extending a License
- 2.9 Closing-Out the License

Chapter 3: Security Procedures
- 3.1 Risk Management
- 3.2 General Security Requirements
- 3.3 Physical Security (Handling, Storage, and Transportation)
- 3.4 Computer Security Requirements

Chapter 4: On-Site Inspections
- 4.1 On-Site Inspection Procedures
- 4.2 Violations, Penalties, and Prosecution

Appendices
- A. Definition of Terms
- B. NSF/NCSES Scientists and Engineers Survey Data
- C. NSF/NCSES License for the Use of Restricted-Use Data
- D. Security Plan Form
- E. NSF/NCSES Affidavit of Nondisclosure Form
- F. Amendment Forms to NSF/NCSES License for Restricted-Use Data
  - Amendment to Add Additional Restricted-Use Data
  - Amendment to Add Collaborating Researcher
  - Amendment to Extend License Time Period

Introduction

This *Restricted-Use Data Procedures Guide* (hereafter referred to as the *Guide)* is provided to assist organizations interested in obtaining access to NSF/NCSES restricted-use data, and licensed organizations that currently have access to NSF/NCSES restricted-use data. The mechanism that NSF/NCSES uses to provide access to restricted-use data is a License. The goal of having a restricted-use data License is to maximize the use of statistical information while protecting individually identifiable information from disclosure. The *Guide* outlines the procedures to apply for the NSF/NCSES restricted-use data License and provides an introduction to the laws and regulations governing these data.

We hope that this *Guide* answers any questions or concerns you may have regarding the process of applying for a License.

SOME IMPORTANT POINTS TO NOTE

- This *Guide* does not replace the provisions of the laws governing the protection of the confidentiality of the data or NCSES implementation of these laws.
- The License Agreement is a legal document and may not be altered without prior consultation with and written approval by NSF.
- The licensee must follow all terms and provisions presented within the License.
- Under no circumstances may a licensed data file be physically removed or electronically transmitted from a Licensee's approved site.
- Licensees are subject to unannounced, unscheduled on-site inspections to assess compliance with requirements.
- The License data are Federal data belonging to NSF/NCSES. They are on loan and must be returned to NCSES upon expiration of the license.

Restricted-Use Data

Federal Agencies collect survey data containing individually identifiable information (including corporate or organizational information), which is confidential and protected by law. Agencies use the term “restricted-use data” for such information. (See appendix A, Definition of Terms.)

Public-Use Data

Agencies use the term “public-use data“ for survey data created for release without a license because potentially individually identifiable information has been coded or deleted to produce a file that protects the confidentiality of survey respondents. Access to public-use data does not require a license. It is available to the general public. For more information on the available NCSES public-use data, see appendix B.

Overview

Chapter 1: Laws

The **Privacy Act of 1974, as amended**; **the National Science Foundation Act of 1950, as amended, and the Confidential Information Protection and Statistical Efficiency Act of 2002**, Title V; provide for the security and privacy of personally identifiable statistical data maintained by the NSF and the Federal Government. Sections of these laws make unlawful the disclosure or improper use of restricted use data. Violators are subject to a ***fine and/or imprisonment.***

Chapter 2: Licensing Procedures

The NCSES will loan restricted-use data only to qualified organizations in the United States, using a strict licensing process described in chapter 2. Individual researchers must apply through an organization (e.g., a university, a research institution). To apply for a license, an organization must submit:

- Formal Letter of Request,
- Signed License Agreement,
- Data Requirements,
- Research Plan,
- Security Plan, and
- Executed Affidavits of Nondisclosure.

Chapter 3: Security Procedures

Restricted-use data must be SAFE at all times. SAFE means that the data are secure from unauthorized disclosure in accordance with the applicable laws, the license, and specified Security Procedures. The Security Procedures, described in chapter 3, specify the computer security requirements for a stand-alone computer. A stand-alone computer is the only type of computer permitted -- a laptop computer does not qualify as a stand-alone computer.

Chapter 4: On-Site Inspections

Under the terms of the license, NCSES has the right to conduct unannounced, unscheduled inspections of the licensee’s site to assess compliance with the provisions of the license, the Security Procedures, and the licensee's security plan. The inspection procedures are described in chapter 4.

Chapter 1: Laws

As an overriding principle, Federal agencies are required to collect, maintain, use, or disseminate any record of identifiable personal information in a manner that assures that adequate safeguards are provided to prevent misuse of such information. The laws requiring the protection of confidential, statistical data collected by NSF/NCSES, include:

- Privacy Act of 1974, as amended, 5 U.S.C. 552a;
- The National Science Foundation Act of 1950, as amended, section 14(i), 42 U.S.C. 1873(i); and
- Confidential Information Protection and Statistical Efficiency Act of 2002, Title V, 44 U.S.C. 3501 note.

Further, under the direction of the Office of Management and Budget, key Federal agencies issue policies, standards, and guidelines for protecting personal data.

1.1 Privacy Act of 1974, amended, 5 U.S.C. 552a

The Privacy Act protects the privacy of individuals' personal data maintained by the Federal Government in systems of records. It imposes numerous requirements upon Federal agencies to safeguard the confidentiality and integrity of this personal data, and limits the uses to which one may put the data, and the disclosures that may be made of the data.

WARNING
Anyone who violates the confidentiality provisions of the Privacy Act may be found guilty of a misdemeanor and fined up to $5,000.

See http://www.usdoj.gov/foia/privstat.htm for text of the statute, Privacy Act of 1974.
A related source of information is the Federal Information Processing Standard Publication (FIPSPUB) 41, *Computer Security Guidelines for Implementing the Privacy Act of 1974*. FIPSPUB 41 provides guidance to ensure that government-provided individually identifiable information is adequately protected in accordance with Federal statutes and regulations.

1.2 The National Science Foundation Act of 1950, as amended, 42 U.S.C. 1873(i)

The NSF Act also places restrictions on the use of survey data collected by NCSES. Survey information supplied to the Foundation or a contractor of the Foundation by an individual, by an industrial or commercial organization, or by certain educational institutional respondents under a pledge of confidentiality may not be disclosed to the public unless such information has been transformed into statistical or aggregate formats that do not allow the identification of the supplier. The names of organizations supplying such information may not be disclosed to the public. Explicit authorization (from NCSES) is required to use the Restricted-Use Data. Further, it is illegal to obtain restricted-use data under false pretenses.

WARNING
Violation of the NSF Act may result in a fine up to $10,000, imprisonment for a period of up to five (5) years, or both.

See http://www.nsf.gov/od/ogc/leg.jsp for the full text of the NSF Act, Section 1873(i) containing specific confidentiality-protection language.

1.3 Confidential Information Protection and Statistical Efficiency Act of 2002

On December 17, 2002, the President signed into law the Confidentiality Information Protection and Statistical Efficiency Act of 2002 (CIPSEA). A main function of the confidentiality sections of the Act is:

> "To ensure that information supplied by individuals or organizations to an agency for statistical purposes under a pledge of confidentiality is used exclusively for statistical purposes."

WARNING
Violation of the CIPSEA may result in a fine up to $250,000, imprisonment for a period of up to five (5) years, or both.

See http://www.eia.doe.gov/oss/CIPSEA.pdf for the full text of the CIPSEA.

Chapter 2: Licensing Procedures

2.1 Only Restricted-Use Data Are Licensed

Restricted-use data are collected under a pledge of confidentiality. Such data may contain individually identifiable information and are protected by law. Restricted-use data are only available under a license. (Note: Public-use data do not require licensing.)

The restricted-use data provided to the Licensee and all information derived from those data are subject to the License.

Information that could result in identifying individuals goes beyond the obvious personal identifiers (e.g., name, Social Security number, address, etc.). The survey data, even without personal identifiers, can provide identifiability based on:

- education,
- financial information,
- employment, and
- other data such as demographic characteristics.

Therefore, any file of survey data with such identification potential needs to be licensed for it to be used outside NCSES.

Appendix B contains a listing of both public-use and restricted-use data files available from NSF/NCSES.

2.2 Restricted-Use Data Procedures for NCSES Staff/Fellows and Contractors

Section 2.2.1 discusses restricted use procedures applying to NCSES staff. There are two vehicles used by NCSES to provide temporary, external access to restricted-use data away from NCSES: Contract and Licensing. Section 2.2.2 describes procedures specifically related to contracts.

2.2.1. Restricted-Use Data Procedures for NCSES Staff

NCSES staff and NCSES Fellows working on-site at NCSES are subject to all of the obligations and restrictions protecting restricted-use data. NCSES staff is not authorized to issue restricted-use data files—the NCSES Data Licensing Coordinator will assist in the process of obtaining a license. NCSES staff should refer all requests for licensing documents, affidavits, or restricted-use data to the NCSES Data Licensing Coordinator.

- Any in-house NCSES staff needing access to restricted-use data must sign a restricted-use data agreement.
- NCSES Fellows may have rules similar to those of NCSES staff or may have additional restrictions imposed as circumstances dictate as determined by the NCSES Confidentiality Officer and NCSES management.
- NCSES staff/Fellows working on-site in possession of restricted-use data must keep them under lock and key in an approved area (usually their office). These data may not be stored on a computer and the data files cannot be left open when not in use. (See **chapter 3, Security Procedures**, for full details.)

- The data may not be removed from the NCSES office area.
- These restricted-use data **must** be returned to the NCSES Data Licensing Coordinator prior to the departure of an NCSES staff or NCSES Fellow working on-site.

2.2.2. Restricted-Use Data Procedures for NCSES Contractors

When NCSES has a contract involving restricted-use data, the initial contract must contain the provisions of the License. However, this only applies to NCSES contracts that explicitly require the use of restricted-use data as part of the contractor's work for NCSES. Any new or additional need for restricted-use data by an NCSES contractor for NCSES work must be covered by a contract modification.

Note: Any NSF contractor who wishes to use restricted-use data for allowable statistical activities that are not part of NCSES-sponsored work must follow the regular license procedures as specified throughout this document.

2.3 What Is a License?

2.3.1 License Components

The License is the method used to provide access to restricted-use data to academic institutions and other qualified research organizations (e.g., non-Federal government agencies, non-regulatory Federal agencies, nonprofit organizations or research contracting firms). Appendix C contains a copy of the NSF/NCSES License Agreement. The License for Restricted-Use Data consists of the License Agreement and the 4 required attachments.

The License Agreement:

- specifies the information subject to the agreement,
- specifies the individuals who may have access to subject data (Principal researcher and collaborating researchers),
- specifies limitations on use and disclosure,
- specifies penalties for violations,
- specifies administrative requirements including
  - requires publications containing the Licensed data be sent to NCSES for review prior to publication,
  - requires the organization to contact the NCSES Confidentiality Officer in case of (suspected) breaches of security,
  - requires the organization to agree to unannounced and unscheduled inspections, and
- specifies the security requirements for the maintenance of, and access to, subject data.

2.3.2 Who Needs a License?

A license is held by an <u>organization</u>, not by an individual; therefore, all applications for a license must come from a requesting organization. The organization must have a license to authorize any individual access to restricted-use data. Note that restricted-use data cannot leave the United States and therefore organizations cannot apply for use outside the U.S. The principal researcher must officially be a member of the organization (e.g. an employee).

The following types of organizations within the United States are eligible to apply for a license:

- Non-regulatory Federal Agencies, including components of the NSF other than NCSES
- Non-governmental agencies/Groups/Organizations/Contractors

- State and Local Government Agencies
- Educational Institutions
- Research Laboratories

2.4 Applying for a License

The first step in this process is to contact the manager of the survey that the researcher is interested in using. The NCSES survey manager will help the researcher define the best data file(s) for the research, whether these data files are public use or restricted use, and whether the organization is eligible for a license. If restricted use data are required, the researcher's organization will need to apply for a license to use these data.

2.4.1. The License Application

The application for a restricted-use data license, consists of the following documents:

- Formal Letter of Request,
- Signed License Agreement (see appendix C),
- Data Requirements
- Research Plan,
- Security Plan (see chapter 3 and appendix D, and
- Executed Affidavits of Nondisclosure (see appendix E).

2.4.2. Formal Letter of Request

The Formal Letter of Request must be authorized by the organization and written on organization letterhead. The letter must provide specific items of information:

(a) The title of the data file(s) the organization wants to access.

(b) A short description of the statistical research project that necessitates accessing the survey data.

(c) The name and title of the Principal Researcher(s) (PR) who will oversee the daily operations. (The PR is the principal researcher, who must be formally employed by the organization, in charge of the day-to-day operations involving the use of the licensed restricted-use data and serves as liaison with NCSES for the organization.)

(d) The signature, name and title of the Senior Official of the organization having AUTHORITY to enter into a legal contract to bind the organization to the provisions of the license.

Note: The principal researcher should take into account the amount of time needed to obtain official institutional signatures in their scheduling.

2.4.3. License Agreement

An executed NSF/NCSES License for the Use of Restricted-Use Data, hereafter referred to as the License Agreement**,** is a legally binding agreement, and must be reviewed carefully. The License Agreement is signed by the Senior Official within the organization (educational institution, non-governmental entity, or government agency) as well as the Principal Researcher. See appendix C for a copy of the License Agreement. The License Agreement, along with its four required attachments, is referred to as the "License."

(a) Data Requirements (Attachment 1)

Attachment 1 to the License Agreement is the Data Requirements. This should include the name of the requested data file and a listing of the variables needed for the research.

(b) Research Plan (Attachment 2)

Attachment 2 to the License Agreement is the Research Plan. This Research Plan is a description of the statistical research project that necessitates accessing the requested survey data file(s). The description must fulfill the following conditions:

- explain why the public-use version of the data is insufficient;
- describe the final research objectives and uses, of the data;
- describe the sector(s) of the community that will be served by the product; and
- assure NCSES that the data will not be used for any administrative, regulatory, or commercial purpose in addition to, or instead of, the statistical purpose described.

(c) Security Plan (Attachment 3)

Attachment 3 to the License Agreement is the Security Plan that contains the detailed procedures for protecting the restricted-use data. All individuals having access to the licensed restricted-use data must be covered by the security plan.

Restricted-use data must be kept safe at all times. “Safe” means that the individually identifiable information is secure from unauthorized access, disclosure or modification. Security procedures are explained in detail in chapter 3; the Security Plan must be in compliance with those procedures. Appendix D is an approved format for the Security Plan. We recommend that you use this form, as all the information on the form is required in the Security Plan.

(d) Affidavits of Nondisclosure (Attachment 4)

Attachment 4 to the License Agreement will contain the Affidavits of Nondisclosure. An Affidavit of Nondisclosure must be executed for each person (researchers, employees or contractor staff) who may have data access or come in contact with the licensed data. NCSES allows up to seven (7) individuals per project to access the subject data. (NCSES may require that the supervisor of the applicant organization's computer facilities be one of those seven.)

Each Affidavit of Nondisclosure must be notarized and the originals sent to the NCSES Data Licensing Coordinator. Appendix E contains a copy of the Affidavit of Nondisclosure form.

The one-page Affidavit contains:

- an oath or affirmation never to disclose individually identifiable information covered by the License to any person not similarly sworn,
- the penalties for disclosure,
- the signature of the Principal Researcher and the Collaborating Researcher, and
- the signature and imprint of a notary public.

The Principal Researcher must also sign the Affidavit of Nondisclosure for each collaborating researcher. A new Affidavit of Nondisclosure must be submitted to NCSES for each new person given access to the restricted-use data by the license organization; organizations must promptly notify NCSES of any changes in project staff. (See section 2.8, Amending or Extending a License.)

2.5. NCSES Review/Approval of the License Application

The NCSES Data Licensing Coordinator and other relevant NCSES staff will review the submitted documents for content and completeness. In particular, the Formal Letter of Request and Research Plan must demonstrate that the proposed research meets the basic requirements, and the Security Plan must comply with the Security Procedures. In addition, all questions NCSES has about an organization's application must be resolved in writing prior to the formal granting of the license.

The NCSES Data Licensing Coordinator may request additional information regarding the proposed use of the data, the resources available to the researcher to perform the analysis, or other aspects of the project, as he/she deems necessary.

The NCSES Data Licensing Coordinator submits the original License (License Agreement and Attachments) to the NCSES Division Director for signature only after all required information has been received, the license application is complete, and all questions have been resolved.

The decision to grant a license is solely that of the NCSES. The authority granted in the license becomes effective on the date of the NCSES Division Director's signature.

2.6 After Approval of the License Request

After the license request has been approved by NCSES, the new Licensee receives the data package, including:

- copy of the approved signed License Agreement and all attachments,
- CD-ROM(s) with the requested restricted-use data file(s),
- Data file media materials and instructional materials to assist the project staff in the use of the data, and
- Warning/Restriction Labels (attached to all enclosures) and Loan Expiration Date Labels (attached to all enclosures).

NOTE: Under no circumstances may the original or duplicate of the restricted-use data file be removed or electronically transmitted from the Licensee's site!

2.7. Licensee and Principal Researcher (PR) Responsibilities

This section addresses the major administrative requirements of the licensee: maintain the License file, with copies of the Executed Affidavits; submit research publications; and be ready for on-site inspections at all times.

The security requirements are explained in detail in chapter 3.

2.7.1. Maintain the License File

The Licensee shall maintain a license file at the same facility where the Licensee stores the restricted-use data. The file is to contain, at a minimum, the following items:

- the License, including
  - License Agreement,
  - Data Requirements,
  - the Research Plan,
  - the licensee's Security Plan, and
  - a listing of all individuals who may have access to the data, along with copies of a notarized Affidavit of Nondisclosure for each individual;
- pertinent Federal laws governing the data confidentiality (provided by NCSES),
- list of changes in personnel accessing the restricted-use data, and
- all amendments to the License.

The Principal Researcher is accountable for having all pertinent information in this file.

In addition, all project staff with access to the restricted-use data shall sign statements that they have both READ and UNDERSTOOD the license requirements and procedures. All individuals who may have access to the restricted-use data must be fully aware of the required security precautions and procedures. (This is the parent institution and the Principal Researcher's responsibility.)

2.7.2. Submit Research Publications

Per Section III.A.1 of the License Agreement, the Principal Researcher (PR) must provide NCSES a copy of all or sufficient portions of each paper, report, or other data product containing information based on the NCSES restricted-use data at least forty-five (45) days prior to its submission for publication review (this includes before release to a reviewer), publication or other dissemination to anyone not listed on the license.

Licensee shall ensure that all printouts, tabulations, and reports are edited for any possible disclosures of subject data. In planning and producing analyses and tabulations, the general rule is not to publish a cell in which there are too fewrespondents or where the cell information could be obtained by subtraction. (In this case, complementary suppression techniques are required.)

The PR may not publicly release the publication until formally notified by NCSES that no potential disclosures were found. (NCSES generally clears allowable publications within a week.)

The PR shall cite the sources used and include the following statement in all publications or releases of research results using NSF restricted or unrestricted data: "The use of NSF data does not imply NSF endorsement of the research methods or conclusions contained in this report."

The PR shall forward a final copy of each publication containing information based on restricted-use data to the NCSES Data Licensing Coordinator.

2.7.3. Expect On-Site Security Inspections

The various confidentiality laws require NCSES to assure the security of the NCSES restricted use data. NCSES achieves this through on-site inspections (security audits). The license

(section III.E) gives NCSES Data Security Officials the right to conduct unannounced, unscheduled inspections of the Licensee's site to assess compliance with the provisions of the license, Security Procedures, and the Licensee's submitted Security Plan. The inspection procedures are described in chapter 4.

If an on-site inspection is conducted, NCSES will provide formal notification of any violations in the required security procedures and the Licensee must correct all identified security violations.

Any violation may subject the Licensee to immediate revocation of the license by NCSES. While all violations are serious, some may require reporting of the violation to the Inspector General of NSF and/or the U.S. Attorney.

2.7.4. Deny Outside Requests for Data

The Licensee may not provide the restricted-use data to anyone not covered by the license and not having a signed and notarized Affidavit of Nondisclosure. The Licensee shall notify NCSES Data Licensing Coordinator immediately when it receives any legal, investigatory or other demand for subject data, including any request or requirement to provide subject data to any State agency or State contractor, and shall keep a record of how the matter was resolved. Requests by institutional authorities must also be reported to NCSES.

2.8 Amending or Extending a License

NCSES shall be kept informed of any modifications in project operations throughout the span of the loan period. Amendments must be filed when there is:

- any change in the personnel (Principal Researcher or Collaborating Researcher or IT staff) accessing the data,
- a change in the format of the data file,
- a need for access to additional restricted-use data files or
- a request to extend the period covered by the License.

To change any of the terms and conditions in the License, the Licensee shall send a written request to the NCSES Data Licensing Coordinator. ALL SUCH CORRESPONDENCE SHALL BE SIGNED BY THE PRINCIPAL RESEARCHER (or the Senior Official in the PR's absence).

2.8.1. Additions to Project Staff

Affidavit(s) of Nondisclosure for new project staff should be submitted to the NCSES Data Licensing Coordinator along with a letter requesting an amendment to the licensing agreement. See appendix F for an example of the Amendment form that must be submitted along with the new Affidavit of Nondisclosure. An Amendment form must be filed for each new Collaborating Researcher (or other person gaining access to the restricted-use data).

The NCSES Data Licensing Coordinator will send a response letter to the Licensee indicating the action taken by NCSES on the request. This response is to be kept in the Licensee’s file.

2.8.2 Reduction of Project Staff

When a Collaborating Researcher or IT staff person no longer requires the use of the NCSES restricted-use data, NCSES must be informed in writing that the Licensee staff person is no longer accessing the restricted-use data. The NCSES Data Licensing Coordinator will note that

this person is no longer allowed access to the restricted-use data and will notify the NCSES Security contractor.

The NCSES Data Licensing Coordinator will send a response letter to the Licensee acknowledging the revised personnel status. This response is to be kept in the Licensee's file.

Note: A change in the Principal Researcher requires close out of the license and issuance of a new license!

2.8.3. Requesting a Change in Data File Format

Only one copy of a given data file can be borrowed at a time, but the Licensee can request an exchange of data file formats. The data file product in the Licensee's possession must be returned to the NCSES Data Licensing Coordinator by certified mail before a replacement file can be sent.

2.8.4. Requesting an Additional Data File

A Licensee may request access to another data file in addition to those specified in the original license. See appendix F for an example of the Amendment to Add Additional Restricted-use Data form requesting additional data files.

If the data file request can be accommodated under the same License, then the applicant need only submit the following information to NCSES, in writing:

- Title of the file(s) requested
- Description of the research purpose which necessitates accessing the additional restricted-use data, and
- Names of the personnel who will have access to the additional data file(s). Include executed Affidavits of Nondisclosure for any new staff or for staff whom do not have the additional data file(s) listed on their original Affidavits.

The NCSES Data Licensing Coordinator will review the request and forward it for approval if judged complete. Once approved by the NCSES Division Director, the request for an additional data file will be included in the Licensee's file as an amendment to the License and the data file will be sent.

2.8.5 Extending a License

Per the License Agreement, the License may be extended by mutual written agreement between the Licensee and the NCSES Division Director. Such requests use the Amendment to Extend the License Time Period form (see appendix F). Any request for an extension must be signed by all parties to the original agreement or their assignees and is effective on the date that all required parties have signed the amendment. When asking for an extension, the licensee must provide a reason for the extension and plans for continued access of the restricted-use data. The NCSES Data Licensing Coordinator will process the request.

2.9. Closing-Out the License

The NCSES Data Licensing Coordinator shall be informed in writing by the Licensee when the project necessitating the use of the data has been completed. The Licensee shall return to

NCSES, by certified mail, the media containing the original restricted-use data and any additional materials and documentation sent to the licensee.

The Licensee shall also overwrite the restricted-use data from any computer used in their analyses, that is, totally obliterate erased (deleted) data so that it cannot be recovered by any means. (See Overwrite Data on Storage Media, in Section 3.4.2 (j).)

Chapter 3: Security Procedures

The security procedures used to protect individually identifiable information are based on the statutes described in Chapter 1. For both NCSES and licensee use of NCSES restricted-use data, the NCSES Division Director shall ensure that all personally identifiable information remain **confidential**, in accordance with the Privacy Act of 1974, the National Science Foundation Act of 1950, as amended, and when appropriate, the Confidential Information Protection and Statistical Efficiency Act of 2002. Other statutes may apply under certain circumstances, such as the Computer Fraud and Abuse Act of 1986, which makes it a felony to gain unauthorized access to a computer system containing Federal data, or to abuse the access one has, with the purpose of doing malicious destruction or damage.

Restricted-use data licenses are used to make more detailed federal information sources available to qualified organizations. A License for Restricted-Use Data is the legal agreement covering terms of use. Strict security procedures are required to protect the data on individuals who responded to Federal surveys; i.e., who provided individually identifiable information. The Licenses provide the assurances of confidentiality necessary to comply with the pertinent laws.

The Licensees are governed by the terms of the License and the security procedures, which are the minimum requirements for protecting the individually identifiable information (referred to as "subject data" in the License) while in the custody of the Licensee.

3.1 Risk Management

Individually identifiable information is often highly sensitive but even when not that sensitive, it requires high levels of confidentiality protection to prevent unauthorized disclosure or modification because respondents were promised confidentiality. Licensees shall ensure that required security measures are continuously in place so that the restricted-use data are safe at all times. “Safe” means that the subject restricted-use data are secure from unauthorized disclosure, use, or modification.

Note: The NCSES may inspect Licensee facilities (see chapter 4) and the inspection criteria are based on the minimum-security requirements specified in the following 3 sections on General Security, Physical Security, and Computer Security.

The Licensees with appropriate assistance from their organizational IT staff shall assess the security of the environment in which the data will be accessed, handled, and stored to determine if the minimum-security procedures, described herein, are adequate for their environment. Because facilities and computer capabilities vary considerably, there may be onsite conditions that necessitate additional protections. If so, the Licensees shall increase protections to make the environment safe.

Licensees must meet the spirit and intent of these protection requirements to ensure that the restricted-use data are in a safe environment at all times.

3.2 General Security Requirements

3.2.1. Assign Security Responsibilities

The Senior Official (SO), who signed the License Agreement, has full and final responsibility for the security of the restricted-use data.

The SO shall name a System Security Officer (SSO) in the Security Plan. Typically, the SSO is the network administrator (to verify the lack of network connectivity while using the data). The SSO shall be responsible for maintaining the day-to-day security of the system on which the licensed data reside. The SSO's assigned duties shall include the implementation, maintenance, and periodic update of the security plan to protect the data in strict compliance with statutory and regulatory requirements.

The Principal Researcher:

- also has responsibility for the security of the restricted-use data,
- is the most senior officer in charge of the day-to-day operations involving the use of restricted-use data,
- shall oversee the preparation and implementation of the restricted-use data security plan, and
- shall monitor and update the security requirements, as needed.

3.2.2. Develop and Implement Security Plan

Licensees shall develop and submit a Restricted-Use Data Security Plan as part of the License. Appendix D contains a sample security plan. The SO, PR, and SSO shall sign the implemented security plan and provide a copy to NCSES. The SSO, in signing the Security Plan, assures the inspection and integrity of the Licensee's Security Plan. (Note: NCSES advises that a draft of the security plan be sent for NCSES review early in the application process to avoid delays caused by needed security upgrades.)

After the license has been approved by NCSES, the security plan must be implemented before the licensee permits any access to the restricted-use data.

3.2.3. Restrict Access to Data

Access control at the research site is the process of determining WHO will have WHAT type of access to WHICH restricted-use data files.

- <u>WHO?</u> Only individuals who have signed an Affidavit of Nondisclosure (which requires reading and understanding the Security Procedures) as part of the license (e.g. PR, IT staff and Collaborating Researcher) may have access to the data, as stated in section 2.4.3.(d).
- <u>WHAT type of access?</u> User access to the original version of the restricted-use data shall be Read-Only. Restricted-use survey data files are not to be modified or changed in any way. Only statistical uses of the data are permitted. Trying to identify an individual or organizational respondent is strictly prohibited by law.
- <u>WHICH data?</u> Each individual's Affidavit of Nondisclosure lists the restricted-use data that can be accessed by that person.

3.2.4. Use Data at Licensed Site Only

Licensee shall retain the original version of the restricted-use data and all copies or extracts at the single licensed location, i.e., the licensed site.

Licensee shall not permit removal of any restricted-use data from the licensed site (i.e., the limited access space approved under the provisions of this license). Using restricted-use data at home or providing it to a contractor to use off-site is prohibited.

3.2.5. Response to Outside Request for Restricted-Use Data

Any researcher who requests access to restricted-use data held by the Licensee must sign an Affidavit of Nondisclosure and be approved by NCSES under the procedures for amending the License.

Licensee agrees to notify the NCSES Division Director immediately:

- of any attempt to access the data outside the terms of the license (such attempts are illegal); and,
- when Licensees receive any legal, investigative, or other demand for disclosure of restricted-use data, including any request or requirement to provide restricted-use data to any State agency or State contractor.

Such requests are inconsistent with requirements of this license. Time is of the essence in notifying NCSES of any such request or requirement. Licensee must also immediately inform the requestor or enforcer of the request or requirement that restricted-use data are protected under the law of the United States as specified in the License. Licensee authorizes NCSES to revoke the License, to take possession of or secure the restricted-use data, and take any other action necessary to protect the absolute confidentiality of the restricted-use data.

3.2.6. Return Original Data to NCSES

Licensee shall return to NCSES the original restricted-use data when the research that is the subject of the License Agreement has been completed or the license expires or is revoked, whichever occurs first. All other individually identifiable information (e.g., the one backup copy, working notes) shall be destroyed under NCSES supervision or by approved NCSES procedures. The NCSES Data Licensing Coordinator will assist in determining the appropriate procedures.

3.3 Physical Security (Handling, Storage, and Transportation)

3.3.1. Machine-Readable Media and Printed Material

Portable machine-readable storage media (such as CD-ROMS, USB drives, floppy diskettes, and removable hard disk drives) containing restricted-use data must be secure at all times.

(Note: Securing data stored on fixed hard drives is addressed in section 3.4.1 in Stand-alone Computers.)

(a) Lock Up Media. Restricted-use data on machine-readable media shall always be secured from unauthorized access (e.g., locked in a secure cabinet when not in use).

(b) Label/Catalog/Track Media. To avoid exceeding License expiration dates, all portable media from NSF are labeled with the expiration date of the license. If the user changes

the media, or develops subsets, new labels with the license expiration date must be affixed. Additionally, the Licensees should use a cataloging/tracking system to know who has possession and responsibility for what media at all times. Anyone having possession of the restricted-use data must have executed an Affidavit of Nondisclosure and keep the data at a site approved in the License. This applies to computer personnel who load data on the system. Restricted-use data shall not be in a computer facility library unless all who have access to the library media have executed Affidavits of Nondisclosure.

(c) Lock Up Printed Material. Printed material containing individually identifiable information shall always be secured from unauthorized access (e.g., locked in a secure cabinet when not in use).

(d) Only One Backup Copy. The Licensee is permitted to make ONLY ONE BACKUP COPY OF THE ENTIRE DATA FILE at the beginning of the loan period. The Licensee shall protect this backup copy and all copies of files developed during analysis under the same Security Procedures as the original data file. If the Licensee plans to make a backup copy of the restricted-use data, the Licensee must state that in the Security Plan.

The Licensee is accountable for any copies of the restricted-use data, including subsets and intermediate files made during the conduct of research. The Licensee shall ensure that all such datasets are:

- Made only when necessary for performing the licensed statistical research;
- Protected at the same level as the original confidential data;
- Kept only at the approved work site as stated in the License Document,
- Made available only to those persons authorized to access the restricted-use data; and
- Destroyed upon completion of the purpose for which the copy was created.

3.3.2. Limit Transporting of Data

Restricted-use data are licensed for one site only (see section 3.2.4), and only the following methods shall be used for transporting the data from that site to a new license site as approved by NCSES, or to and from NCSES:

- NCSES employee;
- A "bonded courier," who must sign for the sealed package, and who is responsible for the data during transport; or
- By certified mail (normal for transporting data between NCSES and the Licensee).

3.4. Computer Security Requirements

3.4.1. Stand-Alone Computers

The National Institute of Standards and Technology (NIST) issued the *Federal Information Processing Standard Publication (FIPSPUB) 41, Computer Security Guidelines for Implementing the Privacy Act of 1974.* This 1975 publication provides the basic guidance for protecting Privacy Act data, which includes individually identifiable information.

The minimum-security requirements for the SAFE use of restricted-use data are described in the context of a stand-alone computer, the only type of computer permitted. Licensees shall meet all the minimum-security requirements for a stand-alone computer before restricted-use data can be processed on that system.

A stand-alone computer is one that is in no way connected to another computer or networked device, such as a switch, hub, or router (with the possible exception of a printer), or to the Internet or a local area network (LAN). The stand-alone computer can be running Windows 2000/XP client or server, Linux, or Mac OS X. Because the stand-alone computer is not connected to the Internet or a local or wide area network, the emphasis for securing the data is placed on physical security of the computer and controlling access to the data. (Note: Portable computers (e.g. notebook or laptop computers) are not allowed and will not be approved.) The computer may be configured for a single user or for multiple users. If configured for multiple users, all users must be named in the license and have signed an Affidavit of Nondisclosure.

If a prospective Licensee cannot meet computer security requirements, a License will not be granted.

3.4.2. Minimum Security Requirements

(a) Limit room/area access. The data must always be secured from unauthorized access. Computer rooms/areas that process individually identifiable data must be secure during business hours and locked after close of business.

(b) Passwords. When passwords are used, they shall be unique, at least 6-8 characters in length, contain at least one non-alphanumeric character (e.g., ?, &, +), and be changed at least every three months. See sections below on “Lock Computer and/or Room,” and “Automatic 'Shutdown' of Inactive Computer” for other password requirements. (For additional details on passwords, see FIPSPUB 112, *Password Usage*, Section 4.3, “Password System for High Protection Requirements.”

In the absence of an automated password generator, user-selected passwords should be unique, easy to memorize, and NOT dictionary words. One good way to select a password is to make up an easy to remember phrase-My Favorite Lake Is Superior-and use the first letter in each word plus a non-alphanumeric character (e.g., ?, +, *) as your password. The result is MFL?IS.

(c) Notification (warning screen). During the login or boot-up process, a warning statement should appear on the screen before access is permitted. This statement should remain on the screen until the user takes action allowing boot-up to continue (preferable), or for at least ten seconds to ensure sufficient time for the warning to be read. The following statement should be used on the access screen; alternative statements need to be approved by NCSES.

WARNING
FEDERAL RESTRICTED-USE DATA
UNAUTHORIZED ACCESS TO LICENSED INDIVIDUALLY IDENTIFIABLE INFORMATION IS A VIOLATION OF FEDERAL LAW AND WILL RESULT IN PROSECUTION.
DO YOU WISH TO CONTINUE? (Y)es ___ or (N)o ___

If it is not feasible for this statement to appear on the screen, the statement must be printed and attached to the monitor in a prominent location.

(d) Read-only Access. User access authorization to the original data shall be Read-Only. Restricted-use survey data files are not to be modified or changed in any way.

(e) No Connections. The computer on which the restricted-use data are loaded must not be connected to any other computer or network through any means. It must truly be configured as a stand-alone machine.

(f) Lock Computer and/or Room. When the authorized user (or users) is away from the computer, protect the restricted-use data by locking the computer. For example, physically lock the computer with its exterior key lock and/or shut down the computer and enable its power-on password. When out of the room, lock the room to prevent an unauthorized individual from gaining access to the computer.

(g) Automatic "Shutdown" of Inactive Computer. Computers can automatically shutdown, logout, or lockup (e.g., password-protected screen-savers) when a period of defined inactivity is detected. This feature may be used in addition to locking the computer and/or room. The defined period of inactivity shall be three to five minutes.

(h) Do Not Backup Restricted-Use Data. Licensees shall not make routine or system backups (e.g., daily, weekly, incremental, partial, full) of restricted-use data (one backup copy of the entire restricted-use data file may be made). (Also see section 3.3.1.(d).) Intermediate research subsets may be backed up, but such data shall be kept as secure and at the same site as the original data.

(i) Staff Changes. Change passwords when staff changes are made.

(j) Overwrite Data on Storage Media. Deleting files from a storage device does not ensure that the data cannot be later recovered and read using alternate means. To help ensure that restricted-use data cannot be read after being erased, drives and other storage devices must be completely overwritten. Overwriting places new data in storage locations, making the previous data unreadable. Overwriting is necessary when a computer containing restricted-use data is no longer used for the NCSES license work (e.g., reallocated to other projects or the project ends) or when the computer needs to be repaired (e.g., hard drive crashes).

Chapter 4: On-Site Inspections

The License authorizes representatives of NCSES to make unannounced and unscheduled inspections of the Licensee's facilities, including any associated computer center, to evaluate compliance with the terms of the License and security procedures.

4.1. On-Site Inspection Procedures

Under the provisions of the License, NCSES may conduct **unannounced** and **unscheduled** inspections of the license site to assess compliance with the terms of the license.

The on-site inspection will include a tour of the Licensee's computer facilities. Specifically, Data Security Officials will visit the Licensee's facilities to evaluate compliance in the following two areas, which are explained in detail in this section.

- Operational Procedures
- Security Procedures and Security Plan

Licensee shall cooperate with NCSES representatives to facilitate such compliance audits.

4.1.1. Operational Procedures

Data security officials will review the project operations with the Principal Researcher, or the Senior Official, at the Licensee's facility. This review will focus on the agreements set forth in the actual License or NCSES contract. This includes an inspection of the current status of the project, as discussed below.

- Record of License. Data Security Officials will review the Licensee's file for a copy of the License Agreement and its attachments along with copies of all of the Affidavits of Nondisclosure.
- Affidavits of Nondisclosure. Data Security Officials will review the names and status of all project personnel. All project personnel must have an executed Affidavit of Nondisclosure, and the original Affidavits must be on file at NCSES. This review is to confirm that NCSES has the most current information on file for those individuals who have the authority to access the restricted-use data.
- The Project Staff. Data security officials will investigate whether all members of the project staff have reviewed a copy of the License and a copy of the Security Procedures. This is to ensure that all members of the project team are aware of the procedures required for accessing restricted-use data.

4.1.2. Security Procedures and Security Plan

Data Security Officials will review with the Licensee:

- all aspects of the Licensee's security procedures for the restricted-use data, as documented in the Licensing Agreement and Chapter 3 of this Guide,
- the Licensee's submitted Security Plan, which is the on-site implementation document for the Security Procedures, and
- the procedures for compliance as stated in the License Agreement and in this License Guide.

4.2. Violations, Penalties, and Prosecution

4.2.1. Violations

- Statement of Warning. If during the security review or otherwise, NCSES finds the Licensee to be in noncompliance in a manner that has not yet resulted in unauthorized disclosure, NCSES will send a Statement of Warning to the Senior Official within six weeks (30 working days) with the finding (often they are provided at the conclusion of the inspection). More serious violations may result in License revocation or criminal prosecution. (See below.)

  The Licensee has one month (20 working days) from receipt of a Statement of Warning to provide NCSES a letter detailing what procedures have been implemented to restore compliance.

- Revocation of License. As stated in the License Agreement (Section VI, Penalties), any violation of the terms and conditions contained in the License may subject the Licensee to immediate revocation of the License by the NCSES Division Director. NCSES will notify the Licensee, in writing, of the factual basis and grounds for revocation. Data are to be removed from Licensee computers immediately and returned to NCSES within two business days of notification of revocation.

  The Licensee has six weeks (30 working days) to submit a written argument and evidence to NCSES indicating why the License should be reinstated. NCSES shall provide written notice of a decision to the Licensee within nine weeks (45 working days) after receipt of the Licensee's written argument. The NCSES Division Director may extend the time period for good cause, at the Director’s discretion. If reinstated, the NCSES Data Licensing Coordinator will work with the Licensee to return the data.

4.2.2. List of Most Common Problems and Violations

- No three to five-minute shutdown when the computer is left on
- Lack of warning statement when restricted-use data are brought up on the screen
- Accessing restricted-use data from an off-site location
- PR not maintaining control over the restricted-use data
- PR neglecting to inform NCSES of project personnel changes
- Neglecting to return restricted-use data to the NCSES Data Licensing Coordinator
- Neglecting to destroy all subsets of the data at the end of the project (the NCSES Data Licensing Coordinator must be informed that this has taken place)
- Restricted-use data leaving the licensed site
- Making a copy of the restricted-use data and allowing it to leave the licensed site
- Removing the warning label with the expiration date from the restricted-use data
- Not labeling any copies or sub-sets of the data with the warning label
- Sending correspondence not signed by the PR

4.2.3. Prosecution and Penalties

Alleged violations of the Privacy Act of 1974, CIPSEA, or NSF-specific laws are subject to prosecution by the United States Attorney.

Penalties, fines and imprisonment, may be enforced for each occurrence of a specific violation.

APPENDIX A

DEFINITION OF TERMS

Definition of Terms

The following are definitions of terms associated with the access to restricted-use information and are used within this *Guide*.

Access - The term for the privilege accorded to a Licensee to see and utilize the restricted-use data covered by an approved NSF/NCSES License for Restricted-Use Data.

Affidavit of Nondisclosure - A one-page form that is completed by any person (Principal Researcher, Collaborating Researcher, or IT staff) who may have access to individually identifiable information. This form contains: (1) the name of the data file(s) to be accessed, (2) the wording of an oath not to disclose such information to persons not similarly sworn, (3) a description of the penalties for such disclosure, and (4) the imprint of a notary public.

Collaborating Researcher (CR) – A CR, under the supervision of a Principal Researcher (PR), may conduct the research, or conduct any analysis, for which the License is issued. Only seven (7) CR or IT staff may have password access to restricted-use data unless NCSES provides written authorization for a larger number of CRs. Each CR must complete an Affidavit of Nondisclosure.

Disclosure - The availability or release of restricted-use data to anyone other than the individuals duly authorized in the License Agreement and Affidavits of Nondisclosure. Such disclosure is unlawful.

Individually Identifiable Information - Any item, collection, or grouping of information pertaining to an individual including, but not limited to, the individual's education, financial transactions, or employment history, and especially when containing the name, or an identifying number, such as Social Security number.

License - This term applies to a method that is utilized by NCSES to authorize access to a data file, or a subset of a data file, containing restricted-use data. As used in this Guide, “License” refers to the License Agreement and its required 4 attachments (Data Requirements, Research Plan, Security Plan and Affidavits of Nondisclosure.) The "License" specifies the obligations imposed on the Licensee and the procedures that must be followed in the maintenance of the restricted-use data.

License Agreement – This refers to the legal document signed by the requesting institution and the NCSES to allow the institution access to the requested restricted-use data. It includes eight Sections. As used in the Guide, the signed License Agreement along with the 4 required attachments is collectively referred to as “the License.”

Licensee – The organization that applied for and was granted the License.

Maintain - To collect, store, use or have available for dissemination when used in connection with the term "record"; and to have control over, or responsibility for, a system of records when used in connection with the term "System of Records."

Personal/Individual Identifier - An identifying element associated with an individual, including the individual's name, or Social Security number, which is assigned to or directly correlates with the individual.

Principal Researcher (PR) - The PR is the researcher in charge of the day-to-day operations involving the use of the restricted-use data and is responsible for the liaison with NCSES. Graduate students are not permitted to be a PR, but may work under the supervision of a PR as a Collaborating Researcher. The PR must complete an Affidavit of Nondisclosure.

Public Use - This describes any survey data that are disseminated through NCSES that are publicly available without restriction. Such survey data have been coded or aggregated to remove any individually identifiable information and thus do not require restrictions for access.

Restricted-Use Data - This is a descriptor of any data set that contains individually identifiable information (with or without individual identifiers). Special procedures are taken to protect this information, and it can be issued only to Licensees on loan.

Routine Use - The description in the Privacy Act of 1974 of the permissible uses of individually identifiable information in a system of records. Except for the use of data for statistical purposes, these routine uses are not permitted for NCSES data files.

Senior Official (SO) - The SO is the individual who has the authority to bind the organization to the License. The SO is responsible for signing the License, and with his/her signature certifies that: (1) the organization has the authority to undertake the commitments in the License, and (2) he/she has the authority to bind the organization to the provisions of the License.

Subject Data - These are all data containing individually identifiable information collected by, or on behalf of, NCSES that are provided to the Licensee and are protected under the terms presented in the executed License. This includes all data/information derived from these data. (see Restricted-Use Data.)

System of Records - Any group of records under the control of a federal agency or its contractors, from which information is retrieved by the name of the individual, or by some identifying number, symbol, or other personal identifier. A notice in the Federal Register publishes the maintenance of a System of Records. Single records or groups of records, which are not retrieved by a personal identifier, are not part of a system of records.

System Security Officer - The SSO is the person responsible for maintaining the day-to-day security of the system on which the licensed data reside. The SSO's assigned duties shall include the implementation, maintenance, and periodic update of the security plan to protect the data in strict compliance with statutory and regulatory requirements.

APPENDIX B

NSF/NCSES SCIENTISTS AND ENGINEERS SURVEY DATA

NSF/NCSES Scientists and Engineers Survey Data

The National Center for Science and Engineering Statistics (NCSES) of the National Science Foundation (NSF) produces and disseminates a wide variety of publications and data releases. Their content ranges from survey documents that present little more than tabular data to sophisticated studies that present more complex analysis of raw data. The analysis documents tend to contain more textual information with occasional tabular data or graphic presentations.

The NCSES Web site (http://www.nsf.gov/statistics/) provides access to a wide range of publications and data sets about scientific and engineering education, workforce, facilities, and research & development in the United States. Each survey description states the series of reports in which data from that series are published.

NSF/NCSES Restricted-Use Data

Data on scientists and engineers from the following sources are currently available under license agreement:

- Survey of Earned Doctorates (SED) - the population for this survey consists of all individuals receiving a research doctorate from a U.S. academic institution. For additional information contact: Mark Fiegener at mfiegene@nsf.gov or 703 292-4622.

- Survey of Doctorate Recipients (SDR) - the population for this survey consists of all individuals under the age of 76 who received a research doctorate in science or engineering from a U.S. institution and were residing the U.S. on the survey reference date. For additional information contact: Lynn Milan at lmilan@nsf.gov or 703 292-2275.

- National Survey of Recent College Graduates (NSRCG) - the population for this survey consists of all individuals under the age of 76 who received a bachelor's or master's degree in science or engineering during the reference periods from a U.S. institution. This survey is designed in part to cover individuals excluded from the NSCG because they did not have a college degree at the time of the NSCG. For additional information contact: John Finamore at jfinamor@nsf.gov or 703 292-2258.

- SESTAT Integrated Database (http://www.nsf.gov/statistics/sestat/) - contains about 100,000 records of persons with a science engineering degree and/or occupation, weighted to represent an estimated 13 million persons in the U.S. educated or working as scientists or engineers during the survey reference weeks. Data from three surveys (Survey of Doctorate Recipients, National Survey of College Graduates, and the National Survey of Recent College Graduates) are integrated into this combined database to provide information about the employment, education and demographic characteristics of scientists and engineers in the United States. This public database contains variables that were created to protect the confidentiality of individuals. For additional information contact: Steve Proudfoot at sproudfo@nsf.gov or 703 292-4434.

NSF/NCSES Public-Use Data

NCSES makes public-use survey data electronically available in three ways:

- Integrated S&E Resources Data system (WebCASPAR)
- Scientists and Engineers Statistical Data System (SESTAT)
- Microdata files

WebCASPAR (http://webcaspar.nsf.gov/)

WebCASPAR is a database system containing information about academic science and engineering resources and is available on the World Wide Web. Included in the database is information from several of NCSES's academic surveys: the Survey of Graduate Students and Postdoctorates in Science and Engineering, Survey of Earned Doctorates, and Survey of Research and Development Expenditures at Universities and Colleges; plus, information from a variety of other sources, including the National Center for Education Statistics. The system is designed to provide multi-year information about individual fields of science and engineering at individual academic institutions. The system provides the user with opportunities to select variables of interest and to specify whether and how information should be aggregated. Information can be output in hard copy form or in Lotus, Excel, or SAS formats for additional manipulation by the researcher.

Scientists and Engineers Statistics Data System (SESTAT) (http://www.nsf.gov/statistics/sestat/)

SESTAT is a comprehensive and integrated system of information about the employment, education, and demographic characteristics of scientists and engineers in the United States and is intended for both policy analysis and general research, having features for both the casual and more intensive data user.

SESTAT contains data from three NSF-sponsored sample surveys: the Survey of Doctorate Recipients, the National Survey of College Graduates, and the National Survey of Recent College Graduates. The NSF surveys provide compatible data, which have been merged into a single integrated data system. For additional information about the SESTAT system and the data it contains see *SESTAT: A Tool for Studying Scientists and Engineers in the United States* (NSF 99-337), available through the Web at http://www.nsf.gov/statistics/nsf99337/start.htm.

Microdata Files

NCSES also develops public-use files for some survey data. The individual survey descriptions on the NCSES web site (http://www.nsf.gov/statistics/) indicate whether a public-use file is available for the survey and whom to contact for more information.

APPENDIX C

NSF/NCSES LICENSE FOR RESTRICTED-USE DATA

Note: This is a legal document and cannot be changed without prior consultation with the NSF's Office of General Counsel.

LICENSE FOR RESTRICTED-USE DATA

Survey files requested:

WHEREAS, the Science Resources Statistics Division (NCSES) of the National Science Foundation (NSF) has collected individually identifiable information in the above named survey(s), the confidentiality of which is protected by the Confidential Information Protection and Statistical Efficiency Act of 2002 (CIPSEA), 44 U.S.C. 3501 et. sec.; section 14(i) of the National Science Foundation Act of 1950, as amended, 42 U.S.C. 1873(i); and/or the Privacy Act of 1974 as amended, 5 U.S.C. 552a; and

WHEREAS, NCSES wishes to make the data available for use by qualified and capable researchers collaborating with NCSES and/or other divisions of the NSF exclusively for statistical purposes so long as the data are appropriately used and protected in accordance with the terms and conditions stated in this License and all prevailing laws and regulations;

IT IS HEREBY AGREED BETWEEN

___,
Principal Researcher (the most senior researcher for this License Agreement who has the authority to manage the day-to-day statistical operations),

and

___,
Parent Institution of the Principal Researcher,
Hereinafter referred to as the "Licensees,"

and NCSES that:

I. <u>INFORMATION SUBJECT TO THIS AGREEMENT</u>

A. All data containing individually identifiable information collected by or on the behalf of NSF that are provided by NCSES to the Licensees and all information derived from those data which contains individually identifiable information or from which individual identity could be deduced are subject to this License and

are referred to in this License as "Subject Data." (Data requirements provided under the terms of this License are to be included as Attachment No. 1.)

B. Subject Data under this License may be in the form of computer tapes, diskettes, CD-ROMS, hard copy, etc. The Principal Researcher may only use the Subject Data in a manner and for a purpose consistent with:

(1) the exclusively statistical purpose for which the data were supplied, which statement of purpose is set forth in a research plan and attached as part of this License in Attachment No. 2;

(2) the limitations imposed under the provisions of this License; and,

(3) the Federal laws referenced in the first paragraph of Page 1 and related NSF regulations and procedures.

II. LIMITATIONS ON USE AND DISCLOSURE

A. Principal Researcher shall not use Subject Data for other than statistical purposes. Principal Researcher shall not use Subject Data in any manner to change the status, condition, or public perception of any individual with regard to whom Subject Data are maintained. Principal Researcher shall not use or disclose Subject Data for any administrative purpose.

B. Principal Researcher shall not merge or match Subject Data with any data without advance written approval of NCSES.

C. Principal Researcher shall not disclose Subject Data to anyone, including other employees of the Principal Researcher's institution, except the Collaborating Researcher (s) listed below:

The Principal Researcher shall not disclose Subject Data to the above named Collaborating Researchers until they have completed an Affidavit of Nondisclosure and such Affidavit is included in Attachment No. 4.

The Principal Researcher may not disclose or allow Collaborating Researchers to disclose any information containing or derived from Subject Data at levels of

refinement that would enable the identities of individuals whose information is contained in Subject Data to be deduced. The Principal Researcher shall ensure that the Collaborating Researchers shall have the same responsibilities and observe the same requirements respecting the Subject Data that are set forth herein as to the Principal Researcher and Licensees.

D. The Principal Researcher may disclose Subject Data to designated NCSES employees working in the course of their employment. Such designation will be requested of and made by the Director of NCSES.

E. Principal Researcher and Collaborating Researchers shall not make any publication or other release that lists Subject Data information regarding specific individuals even if individual identifiers have been removed.

F. Principal Researcher may publish the results, analysis or other information developed as a result of any research based on Subject Data made available under this License, but only in summary or statistical form such that the identity of individuals contained in the Subject Data are not revealed, nor able to be deduced. Principal Researcher and Collaborating Researchers must apply techniques for disclosure avoidance and submit the research for NCSES disclosure review as described in Section III.A.below.

III. <u>ADMINISTRATIVE REQUIREMENTS</u>

A. Publications made available to NCSES.

1. Principal Researcher shall provide NCSES a copy of all or sufficient portions of each paper, report, or other data product containing information based on Subject Data at least forty-five (45) days prior to its submission for publication review, publication or other dissemination to anyone not listed in this License.

2. In developing information for publication or other release of research results, if any material could raise reasonable questions regarding disclosure of individually identifiable information contained in the Subject Data, Principal Researcher shall provide NCSES a copy of the material intended for use before any disclosure is made, so that NCSES may advise whether the disclosure is allowed or prohibited under this License and the laws cited in the first paragraph of this License. Principal Researcher shall not publish or otherwise release research results provided to NCSES, if NCSES advises such disclosure is not authorized.

3. Principal Researcher shall cite the sources used and include the following statement in all publications or releases of research results using NSF restricted (or unrestricted) data.

"The use of NSF data does not imply NSF endorsement of the research, research methods, or conclusions contained in this report."

4. Principal Researcher shall send copies of published reports to NCSES.

B. Principal Researcher shall notify NCSES immediately upon receipt of any legal, investigative, or other demand for disclosure of Subject Data.

C. Principal Researcher shall notify NCSES immediately upon discovering any breach or suspected breach of security or any disclosure of Subject Data to unauthorized parties or agencies.

D. The Licensees shall indemnify and hold harmless NCSES and their contractors, their employees and agents against any and all claims for damages, demands, and all other actions, including any penalties imposed as well as payment of all expenses and costs arising from any such penalty resulting from the disclosure by the Principal Researcher or Collaborator of the Subject Data or statistical data derived from and/or based upon Subject Data, or resulting from the failure of the Principal Researcher or the Collaborator to comply with any of the terms or conditions of this License.

E. The Licensees agree that representatives of NSF have the right to make unannounced and unscheduled inspections of the Licensees' facilities, including any associated computer center, to evaluate compliance with the terms of this License and the requirements of 5 U.S.C. 552a.

IV. SECURITY REQUIREMENTS

A. The Principal Researcher shall retain the original version of the Subject Data at a single location and may make no copies or extracts of the Subject Data available to anyone except as permitted by Part II, Limitation on Use and Disclosure, of this License.

B. The Licensees shall maintain Subject Data including printed or other material in a space that is limited to access by authorized personnel.

C. The Licensees shall ensure that access to Subject Data maintained in computer memory is controlled by password protection. The Licensees shall maintain all print-outs, diskettes, personal computers with subject data on hard disk, or other physical products containing individually identifiable information derived from Subject Data in locked cabinets, file drawers, or other secured locations when not in use.

D. The Licensees shall ensure that all printouts, tabulations, and reports are edited for any possible disclosures of Subject Data using generally accepted methods.

E. The Licensees shall establish procedures to ensure that Subject Data cannot be extracted from a computer mainframe, remote terminals or separate PCs by unauthorized individuals.

F. The Licensees shall not permit removal of any Subject Data from the limited access space protected under the provisions of this Agreement as required in the attached SECURITY PLAN (Attachment No. 3), without first notifying, and obtaining written approval from NSF.

V. RETENTION OF SUBJECT DATA

A. The Licensees shall return to NSF all Subject Data or destroy those data under NSF supervision or by approved NSF procedures when the research that is the subject of this agreement has been completed, or when this License has expired, or been revoked, or terminated.

B. The Licensees shall comply with the SECURITY PLAN (Attachment No. 3) attached to this Agreement.

VI. PENALTIES

A. Any violation of the terms and conditions of this License may result in immediate revocation of the License by NCSES.

B. Any violation of this License may also be a violation of Federal criminal law under the Confidential Information Protection and Statistical Efficiency Act of 2002 (CIPSEA), 44 U.S.C. 3501, et sec., and section 14(i) of the National Science Foundation Act of 1950, as amended, 42 U.S.C. 1873(i). Violation of the CIPSEA may result in a fine up to $250,000, imprisonment for a period of up to five (5) years, or both; and for section 14(i) a fine up to $10,000, imprisonment for a period of up to five (5) years, or both. A violation of this License may also violate the Privacy Act of 1974, 5 U.S.C. 552a, which carries potential criminal sanctions.

VII. TERM OF THE LICENSE

A. This License is in effect until _____, unless amended, extended, revoked, or terminated.

B. This License may be unilaterally revoked or terminated by the Director of NCSES at any time.

C. This License may be amended or extended by mutual written agreement between the Licensees and the Director of NCSES. Any amendment must be signed by all

parties to the original agreement or their assignees and is effective on the date that all required parties have signed the amendment.

VIII. PROCESSING OF THE LICENSE

A. The institutional signatory to this agreement must have the authority to bind the parent institution to the terms of the License and so signify by his/her signature below that the parent institution has the authority to undertake the commitments set forth in this License.

_____ Signature of the Senior Official (Parent Institution of Principal Researcher)	___ Date
___ Typed/Printed Name of the Senior Official Title: ___ Name of Parent Institution: ___	___ Telephone

B. The Principal Researcher shall sign this License below to indicate agreement to undertake the commitments set forth in this License. The Principal Researcher is the most senior researcher for this License Agreement who has the authority to manage the day-to-day statistical operations. The Senior Official cannot also sign as the Principal Researcher.

_____ Signature of Principal Researcher	_____ Date
_____ Typed/Print Name of Principal Researcher Title:	_____ Telephone

C. The Director and the Confidentiality Liaison of the National Science Foundation, National Center for Science and Engineering Statistics, issue this License.

_____ Signature of Confidentiality Liaison, National Center for Science and Engineering Statistics, National Science Foundation	_____ Date
_____ Typed/Printed Name of Confidentiality Liaison	
_____ Signature of Director, National Center for Science and Engineering Statistics, National Science Foundation	_____ Date
_____ Typed/Printed Name of Director	

REQUIRED LICENSE AGREEMENT ATTACHMENTS

Attachment 1: Data Requirements (to be provided by the requestor)

Attachment 2: Research Plan (to be provided by the requestor)

Attachment 3: Security Plan (use form from Appendix D of the License Guide)

Attachment 4: Affidavits of Nondisclosure (use form from Appendix E of the License Guide)

APPENDIX D

SECURITY PLAN FORM
(Attachment # 3 to License Agreement)

SECURITY PLAN

Name of Institution/Organization: _____

Security Procedures for: **Researcher:** New License ☒ License Amendment ☐
Contractor: ☐

Restricted-Use Data Holder Information:

Name of Principal Researcher (PR): _____

Mailing Address: _____

_____

_____

Office Phone: _____

Office Fax Number: _____

Email Address: _____

Person(s) having access to the Restricted-Use Data:

Name	Office Location	Office Phone

Note: Access must be limited ONLY to those who have signed an Affidavit of Nondisclosure.

Storage Information: *Note: Whether being used or not, the restricted-use data must be stored in this office.*

Exact Data Location: Location of computer (include room number), where all work must be done: _____

_____

_____

Office Phone at this location: _____

Page 1 of 4 PR Initials_____

Computer Security Requirements

- Description of Computer System *(All work must be done on this system.)*

Note: The restricted-use data must be run on a stand-alone computer. Use of laptop computers is prohibited. All modes of communication with the computer (e.g. modem, cable, network, wireless) must be disconnected when the Restricted-Use Data are being used. The residual Restricted-Use Data must be purged from the system immediately after each use and before reconnecting to a network.

The system security officer* for the work site must initial below to indicate that the following security measures are in place:

- Anti-Virus software installed on computer **Initials: ____**
- Limit room/area access by locking office when away from computer **Initials: ____**
- Passwords: unique, 6-8 characters with one non-alphanumeric **Initials: ____**
- Change password at least every 3 months **Initials: ____**
- Read-only access to original data **Initials: ____**
- Enable automatic "password screensaver" within 5 minutes of inactivity **Initials: ____**
- No routine backups of restricted-use data **Initials: ____**
- Remove data by overwriting at the end of the project **Initials: ____**
- Notification (Warning Statement): During the login process the following statement will appear on the screen before access is granted. If it is not feasible to have the warning appear on the screen, it will be typed and attached to the monitor in a prominent location. **Initials: ____**

W A R N I N G
Federal Restricted-Use Data
Unauthorized Access To Licensed Individually Identifiable Information Is A Violation Of Federal Law And Will Result In Prosecution.

DO YOU WISH TO CONTINUE? (Y)es or (N)o

* **System Security Officer (SSO)** - The SSO is the person responsible for maintaining the day-to-day security of the system on which the licensed data reside. The SSO's assigned duties shall include the implementation, maintenance, and periodic update of the security plan to protect the data in strict compliance with statutory and regulatory requirements.

Page 3 of 4 PR Initials_____

Review and Approval

I have reviewed the requirements of the license security procedures and the contents of this security plan, which describes the protection measures for the requested restricted-use data files. I have also instructed the collaborating researchers on the requirements of the security plan.

I hereby certify that this system meets all requirements of the license security procedures and that the in-place security safeguards adequately protect the restricted-use data.

Principal Researcher Signature Date

Principal Researcher (type/print) Name

System Security Officer Signature Date

System Security Officer (type/print) Name

APPENDIX E

NSF/NCSES AFFIDAVIT OF NONDISCLOSURE FORM
(Attachment #4 to the License Agreement)

NSF/NCSES AFFIDAVIT OF NONDISCLOSURE

I, _____ , do solemnly swear (or affirm) that I have read and understand the content of the NSF/NCSES LICENSE FOR RESTRICTED-USE DATA are protected under the Confidential Information Protection and Statistical Efficiency Act of 2002, 44 U.S.C. 3501 et. sec.; section 14(i) of the National Science Foundation Act of 1950, as amended, 42 U.S.C. 1873(i); and/or the Privacy Act of 1974 as amended, 5 U.S.C. 552a and when given access to the restricted use data (hereinafter referred to as the subject file) from the Survey of Doctorate Recipients, the Survey of Earned Doctorates, the National Survey of Recent College Graduates and/or the SESTAT Integrated Database:

- I will not use the data in the subject file for any purpose other than statistical reporting and analysis. Information from the file will be released only in statistical summaries that do not disclose information about any individual.
- I will not release the subject file or any part of it to any other person or organization.
- I will not use the subject file to attempt to learn the identity of, or to gain information concerning, any person included in the data set; unless such identification is directly related to survey administrative tasks or quality control, arising from a comparison with NIH administrative data.

If the identity of any individual in the file should be discovered inadvertently, then a) I will make no use of this knowledge, (b) I will advise the Director, NCSES, of the incident, (c) the information about the individual will be safeguarded, and (d) no one else will be told of the information discovered.

_____
Notary Public/Seal/Date

_____
Signature of Collaborating Researcher

___
Typed/Printed Name of Collaborating Researcher

_____
Date signed by Collaborating Researcher

_____
Signature of Principal Researcher

___
Typed/Printed Name of Principal Researcher

_____
Date signed by Principal Researcher

VIOLATION OF THIS AGREEMENT IS PUNISHABLE UNDER THE PRIVACY ACT OF 1974 AND OTHER LAWS NAMED ABOVE, AND MAY RESULT IN THE RESEARCHER AND THE RESEARCHER'S INSTITUTION BEING INELIGIBLE FOR FEDERAL GRANTS.

APPENDIX F

AMENDMENT FORMS TO
NSF/NCSES LICENSE FOR RESTRICTED-USE DATA

AMENDMENT TO ADD ADDITIONAL RESTRICTED-USE DATA

AMENDMENT TO ADD COLLABORATING RESEARCHER

AMENDMENT TO EXTEND LICENSE TIME PERIOD

NSF/NCSES LICENSE FOR RESTRICTED-USE DATA

AMENDMENT TO ADD ADDITIONAL RESTRICTED-USE DATA

This is an amendment to the agreement between the National Science Foundation (NSF), National Center for Science and Engineering Statistics (NCSES),

the **Principal Researcher**, _____, and

_____, the **Parent Institution** of the Principal

_____

Researcher granting access to the following additional restricted use data file:

(additional data file name)

The Principal Researcher is still authorized to continue using the files already obtained under the original license and any previous amendments to add additional restricted data.

All stated security requirements are still in compliance as stated in the previous License Agreement signed and dated, _____.

The Collaborating Researcher(s) confirm that they have read and understand the terms of the original license and that they will abide by such terms for the full term of the original license which shall be in effect until _____.

_____	_____
Signature of Principal Researcher	Date
_____	_____
Signature of Collaborating Researcher	Date
_____	_____
Signature of Senior Official from Parent Institution	Date

_____	_____
Signature of Director, NSF/NCSES	Date
_____	_____
Signature of Chief Statistician, NSF/NCSES	Date

NSF/NCSES LICENSE FOR RESTRICTED-USE DATA

AMENDMENT TO ADD COLLABORATING RESEARCHER

This is an amendment to add a Collaborating Researcher to the License agreement between the National Science Foundation (NSF), National Center for Science and Engineering Statistics (NCSES),

_____, and

Principal Researcher

_____.

Parent Institution of the Principal Researcher

Approval is granted for _____

(**Collaborating Researcher)**

under the direction of the Principal Researcher, to be added to the above-mentioned License agreement for access to the restricted use data file specified in the License agreement. All security requirements as stated in the previous License Agreement signed,

remain in effect.

_____

Date

The Collaborating Researcher confirms that he/she has read and understood the terms of the original License and will abide by such terms for the full term of the original and any subsequent extensions.

_____	_____
Signature of Principal Researcher	Date
_____	_____
Signature of Collaborating Researcher	Date
_____	_____
Signature of Senior Official from Parent Institution	Date

_____	_____
Signature of Director, NSF/NCSES	Date
_____	_____
Signature of Chief Statistician, NSF/NCSES	Date

NSF/NCSES LICENSE FOR RESTRICTED-USE DATA

AMENDMENT TO EXTEND LICENSE TIME PERIOD

IT IS HEREBY AGREED BETWEEN

_____, and
Principal Researcher

_____,
Parent Institution of Principal Researcher

Hereinafter referred to as the "Licensees,"
and the National Science Foundation, National Center for Science and Engineering Statistics

___

(NCSES) that the License between them for the Licensees' use of the data (file name) specified in the License originally expiring on _____, is extended until _____ unless amended, extended, or revoked.

All of the provisions of the original License, except for the termination date, will remain in effect during the extension and the institution shall advise the Principal Researcher and the Collaborating Researchers of the extension and continuing terms of their nondisclosure **agreements.**

_____ Name of Principal Researcher	
_____ Signature of Principal Researcher	_____ Date
_____ Name of Senior Official/Parent Institution	
_____ Signature of Senior Official	_____ Date
_____ Title of Senior Official	_____ Telephone

_____ Signature, Director, NSF/NCSES	_____ Date
_____ Signature, NSF/NCSES Chief Statistician	_____ Date