

Confidentiality and Security Guidelines

June 2007

The law requires the U.S. Census Bureau to maintain the confidentiality for all of the information that it collects. The Census Bureau takes its responsibility to protect the confidentiality of the information it collects very seriously. Respondents place their trust in the Census Bureau each time they complete a survey or an interview. This trust in confidentiality is critical to the success of the Census Bureau's mission to collect and report the most accurate data possible. To uphold the law, the Census Bureau requires that all individuals who work with the Census Bureau's confidential materials read, understand, and agree to abide by the confidentiality and security guidelines outlined below.

Why Address Information Is Protected

Title 13, United States Code (U.S.C.), provides for the confidential treatment of census-related information. Chapter 1, Section 9 of the code states:

"Neither the Secretary, nor any other officer or employee of the Department of Commerce or bureau or agency thereof, or local government census liaison, may, except as provided in section 8 or 16 or chapter 10 of this title...

- 1) *use the information furnished under the provisions of this title for any purpose other than the statistical purposes for which it is supplied; or*
- 2) *make any publication whereby the data furnished by any particular establishment or individual under this title can be identified; or*
- 3) *permit anyone other than the sworn officers and employees of the Department or bureau or agency thereof to examine the individual reports."*

Section 214 of the Code and the Uniform Sentencing Act of 1984 set the penalty for the wrongful disclosure or release of information protected by Title 13 at a fine of not more than \$250,000 or imprisonment for not more than 5 years, or both.

To implement this law, all Census Bureau employees (both temporary and permanent) take an oath to maintain the confidentiality of the census information they encounter in their work. Census information includes:

- Everything on a completed or partially completed questionnaire or obtained in a personal or telephone interview.
- Individual addresses maintained by the Census Bureau that Local Update of Census Addresses (LUCA) Program liaisons review.
- Maps that identify the location of individual housing units and/or group quarters ("structure points").

Title 13 of the U.S.C. does not protect generalized address information, such as the address range data available in the Census Bureau's digital shapefile products.

In 1994, the U.S. Congress amended Chapter 1 of Title 13 to allow local government designated census liaisons to review the Census Bureau's address list for their area. This amendment recognizes the important role that local knowledge and participation can play in building and updating an accurate, comprehensive census address list. In amending this chapter, the Congress reaffirmed the confidential nature of address information.

The Confidentiality Agreement

Each participating government must designate a primary liaison. The primary liaison, all reviewers, and anyone with access to Title 13, U.S.C. materials must understand and sign the Confidentiality Agreement. The Census Bureau considers all individuals who have access to the Census Bureau's address information and maps showing the location of housing units and group quarters, liaisons. Therefore, all Option 1 and Option 2 2010 Decennial Census LUCA Program liaisons, reviewers, and anyone with access to Title 13 materials must sign the Confidentiality Agreement.

Signatures on this form constitute an agreement by each individual to abide by the security guidelines outlined below. While access to Title 13 protected information is temporary, the commitment to keep the information confidential is permanent.

- **The Census Bureau will not deliver the address list materials to Option 1 and Option 2 participants until we have received a completed and signed Confidentiality Agreement and Self-Assessment Form.**
- **Although you may have prior confidentiality agreements on file at the Census Bureau, these will not fulfill the requirements of the 2010 Decennial Census LUCA Program**

Security Guidelines

The Census Bureau recognizes the fact that the implementation of these guidelines may vary slightly from one participant to another. Regardless, the result must be the same for each participant – nondisclosure of information protected by Title 13, U.S.C

The primary liaison accepts the responsibility for protecting and safeguarding the LUCA program materials covered by Title 13, U.S.C. This includes any list that shows individual Census Bureau addresses and any Census Bureau map or digital file that shows individual housing units and/or group quarters location ("structure points"). The primary liaison must restrict access to the Census Bureau's address information to those individuals who have signed the Confidentiality Agreement. The liaison, reviewers, and anyone with access to Title 13 materials must sign the Confidentiality Agreement.

As you read the Census Bureau's security requirements, keep in mind the important role security plays in the overall responsibilities of each LUCA program liaison, reviewers, and anyone with access to Title 13 materials. The Census Bureau must have your full cooperation and commitment to following these guidelines. Together, we will maintain the confidential information entrusted to the Census Bureau by the Congress and the American public.

Protecting Census Bureau Address Information

The Census Bureau will conduct training workshops covering all aspects of the LUCA program. In addition, the workshops will provide the participating governments with an opportunity to review the security guidelines and safeguards to protect against illegal use of Census Bureau address information. Census Bureau staff conducting the workshops will provide information to help you decide who in your organization needs to have access to the Census Bureau's Address List and will review the civil and criminal penalties for improper or illegal use of the data.

Onsite Visits

To ensure that participating entities or organizations are maintaining adequate security safeguards, the Census Bureau may make on-site visits to review your government or organization's security procedures. The Census Bureau will strive not to disrupt your office operations. A typical visit would include a review of:

- Storage and handling of Census Bureau address information.
- Employee access to Census Bureau address information.
- The physical safeguard of the computers, rooms, and buildings where the Census Bureau address information is stored.
- Instructions to employees about security.
- Data processing operations (including use of passwords).
- Employee awareness of their responsibilities to protect the confidentiality of Census Bureau addresses.

Protecting Paper Copies of Census Bureau Address Information and Maps

- Keep all Census Bureau address information in a locked room during non-work hours. If possible, store the Census address materials and maps showing structure points in locked desks or cabinets.
- During work hours, do not leave a room unattended where Census Bureau address information is stored. Lock the room whenever you leave.
- Do not leave Census Bureau address information unattended at your desk. Return any Title 13 data to secure storage when you are not using it.

- Only make copies of the information necessary to complete your task. Do not leave the copying machine unattended while making copies. All copied material containing Title 13 information must bear the statement:

“This document contains information, the release of which is prohibited by Title 13, U.S.C., and is for U.S. Census Bureau official use only. Wrongful disclosure or release of information can be punished by fine or imprisonment (Public Law 99-474).”

- To FAX a document containing Census Bureau address information to a Census Bureau location, make sure the document is properly labeled with the disclosure statement: **“DISCLOSURE PROHIBITED BY Title 13, U.S.C.”**, verify the FAX number before sending, and arrange for a Census Bureau employee to be at the FAX machine to receive it and acknowledge receipt.
- Do not disclose precise or even anecdotal information about Census Bureau addresses or locations to anyone who has not signed the Confidentiality Agreement Form or is not a Census Bureau employee.

Protecting Computer-Readable Census Bureau Address Information and Maps

Operating systems, programs, applications, and data related to the review of Census Bureau addresses must be accessible only to LUCA program liaisons and reviewers. The automated data processing (ADP) system should restrict the read, write, delete, and execute functions applicable to the Census Bureau's addresses.

The ADP system must use log-on routines that require a user-ID and password that conform to the following guidelines:

- Assign a unique user-ID and password for liaisons, reviewers, and anyone with access to Title 13 materials.
- Passwords must consist of at least 8, nonblank characters consisting of at least one alphabet letter and either one number or one special character (\$, *, &). No more than six consecutive characters (AAAAAA) may appear in the password, and then only once.
- Reject passwords that are the same as the user-ID or that have been used within the last 6 months.
- Encrypt passwords.
- Disable passwords after three bad attempts.
- Do not display passwords on terminals or printers.
- Change passwords every 90 days (more frequent change is optional) or immediately, if compromised.
- On new accounts, the user must change the assigned password to a unique password the first time they log on.

The ADP system must display a warning log-on feature. Computer screens must display a warning that states:

****WARNING*WARNING*WARNING****
YOU HAVE ACCESSED A COMPUTER SYSTEM CONTAINING UNITED STATES GOVERNMENT INFORMATION. USE OF THIS COMPUTER WITHOUT AUTHORIZATION OR FOR PURPOSES FOR WHICH AUTHORIZATION HAS NOT BEEN EXTENDED IS A VIOLATION OF FEDERAL LAW AND CAN BE PUNISHED BY FINE OR IMPRISONMENT (Public Law 99-474). ALL USE MAY BE INTERCEPTED, MONITORED, RECORDED, COPIED, AUDITED, INSPECTED, AND DISCLOSED TO AUTHORIZED LAW ENFORCEMENT OFFICIALS. REPORT SUSPECTED VIOLATIONS TO YOUR AGENCY SECURITY OFFICER. USE OF THIS SYSTEM INDICATES YOU CONSENT TO THIS WARNING. LOG OFF IMMEDIATELY IF YOU DO NOT AGREE TO THE CONDITIONS OF THIS WARNING.
****WARNING*WARNING*WARNING****

If Census Bureau address information is placed on a shared computer system, construct electronic security profiles to allow only LUCA program liaisons, reviewers, and anyone with access to the Census Bureau's address information. Test your security to ensure that only LUCA liaisons and reviewers are permitted access to the Census Bureau's address information.

ZIP and password protect Title 13 Census Bureau address information.

Lock all rooms containing computers with Title 13 Census Bureau address information and all associated media during non-work hours.

Do not leave computers with Census Bureau address information unattended during work hours. Log-off the computer/system or lock the room whenever you leave.

Label any computer diskettes, CD-ROMs, DVDs, tapes, cartridges or other computer storage media containing Census Bureau address information with the following:

“This document contains information, the release of which is prohibited by Title 13, U.S.C., and is for U.S. Census Bureau official use only. Wrongful disclosure or release of information can be punished by fine or imprisonment (Public Law 99-474).”

If backup is necessary, do not send the tapes, cartridges, or disks off-site. Store them in a secured area. **Do not mix, store, or back-up LUCA data with other data.**

Clear magnetic media (tapes, disks, hard drives) containing Census Bureau address information before reuse. To clear magnetic media, overwrite all Title 13 data three times at a minimum using a commercial disk utility program or degauss using a commercial degausser.

Program any software you develop for displaying the Census Bureau addresses to label each affected page of a printout containing Census Bureau address information with the following:

“This document contains information, the release of which is prohibited by Title 13, U.S.C., and is for U.S. Census Bureau official use only. Wrongful disclosure or release of information can be punished by fine or imprisonment (Public Law 99-474).”

Returning Census Bureau Title 13 Materials

Once you have completed your initial review and update of the LUCA materials, return only those materials with updates to the Census Bureau’s Regional Office responsible for your jurisdiction. Make a copy of all updated pages to keep for your records. Retain all non-annotated Title 13 materials until you receive your feedback materials. Keep all retained address lists and copies in a secure location.

Use the following guidelines to ship the updated materials:

- Ship all Census Bureau confidential material in two opaque sealed envelopes that are durable enough to prevent someone from viewing or tampering with the enclosed materials.
- Label both sides of the inner envelope or wrapping with the disclosure notice:

“DISCLOSURE PROHIBITED BY Title 13, U.S.C.”

- **DO NOT** label the outer envelope with the **“DISCLOSURE PROHIBITED BY Title 13, U.S.C.”** notice.
- Address the outer envelope to:

ATTN: Geography
Regional Director
US Census Bureau
Regional Office name and address
- Use shipping contractors that provide tracking services, such as U.S. Postal Service certified or registered mail, FedEx, United Parcel Service, or similar service.

Return or Destruction of Census Bureau Confidential Materials

After the appeals process has concluded, **all** Title 13, U.S.C., Census Bureau address lists and maps containing structure points **must be returned or destroyed** according to the Census Bureau's specific guidelines for returning or destroying confidential material.

The liaison is required to verify the return or destruction of any remaining Title 13 materials, both paper and computer-readable including all paper copies, backup files, etc. The liaison must sign and return to the Census Bureau the "Return or Destruction of Title 13, U.S.C. Materials" form. In addition, all LUCA program reviewers and anyone with access to Title 13 materials who signed the Confidentiality Agreement are required to sign this form once their participation in the LUCA program has ended. Should any liaison, reviewer, or anyone leave before the end of the LUCA program, they are required to "sign-out" of the program by signing and dating this form.

Only those individuals who signed the Confidentiality Agreement are permitted to destroy Title 13, U.S.C. materials.

- Never deposit Census Bureau confidential materials in a trash or recycle container before destruction.
- Store the materials in a secure area in a container labeled "document destruction container" until they are destroyed.
- The destruction process must prevent recognition or reconstruction of the paper or computer-readable information. Use one of the following methods to destroy census confidential materials:
 - o Shredding
 - o Chemical decomposition
 - o Pulverizing (such as, hammer mills, choppers, etc.)
 - o Burning (only in a facility approved by the Environmental Protection Agency)
 - o Clear magnetic media (tapes, disks, hard drives) containing Census Bureau address information before reuse. To clear, overwrite all Title 13 data a minimum of three times, using a commercial disk utility program or degauss using a commercial degausser.
 - o Clear diskettes by running a magnetic strip of sufficient length to reach all areas of the disk over and under each surface a minimum of three times. If the information cannot be destroyed as suggested, damage the disk in an obvious manner to prevent use in any disk drive unit and discard.
Note: Hand tearing or burying information in a landfill are unacceptable methods of disposal before destruction.
 - o Destroy CD-ROMs and DVDs using a commercial grade shredder, suitable for rendering them un-usable, or cut them up with scissors in an obvious manner to prevent use in a drive unit.