

## **DS007: Safeguarding and Managing Information**

### **INTRODUCTION**

For the U.S. Census Bureau, Safeguarding and Managing Information encompasses the Census Bureau's Data Stewardship program objectives while meeting its information security obligations. Safeguarding and Managing Information involves effectively safeguarding, while simultaneously facilitating legitimate access to, information through its entire life cycle: generation, collection, processing, dissemination, and disposal. Safeguarding and managing information is essential to the credibility of the Census Bureau and to the success of its mission. In working to provide relevant statistical products on the people and businesses of the United States, the Census Bureau must safeguard and protect the information in its custody, consistent with federal statutes and regulations. This policy replaces the prior DS007 policy, which was entitled, "Information Security Management Program", signed May 27, 2009.

This policy, *DS007: Safeguarding and Managing Information*, is intended to ensure an integrated and consistent approach to information security management. It establishes *Roles and Responsibilities* and *Information Handling Categories*, which apply to all information collected, acquired, or maintained by the Census Bureau in any and all forms (paper copies, computer systems, etc). Based on this policy Information Handling Guidelines have been created to assist in the implementation of this policy. These guidelines are in Attachment B. This policy applies to economic and demographic data used to generate statistical products (such as the results of censuses and surveys), data from administrative records acquired from other sources, and personnel or financial data used to facilitate agency administration. This policy is not intended to provide information or guidelines for federally defined classified data; please refer to Chapter S-10 of the Census Bureau Policies and Procedures Manual.

### **ROLES AND RESPONSIBILITIES**

This section identifies roles and responsibilities delegated to individuals who will directly implement this policy. These roles are modeled from the National Institute of Standards and Technology (NIST) and include, but are not limited to, the Data Stewardship Executive Policy Committee (DSEP), the Chief Information Officer, Senior Agency Information Security Officer, Chief Privacy Officer, Authorizing Officials, Information System Owners, Information Owners, and Data Stewards. (Please see Attachment A for a quick reference guide to the following Roles and Responsibilities.)

#### *Data Stewardship Executive Policy Committee*

The Data Stewardship Executive Policy Committee (DSEP) acts on behalf of the Director in setting policy and making decisions on policy-related matters related to privacy, security, confidentiality, and administrative records. The mission of DSEP is to ensure that the Census Bureau can effectively collect and use data about the nation's people and economy, while fully meeting the Census Bureau's legal and ethical obligations to respondents to respect privacy and protect confidentiality. This includes fully meeting the legal ethical and reporting obligations of the Census Act (Title 13), the Privacy Act, and other applicable statutes, including those of

governmental and other suppliers of data to the Census Bureau. DSEP is responsible for effectively safeguarding and facilitating legitimate access to information, including administrative information, required to fulfill the agency's mission. In any instance where an issue appears to fall outside of the scope of this policy, the issue should be brought to the attention of the DSEP.

*Chief Information Officer*

The Chief Information Officer is the organizational official responsible for: (i) designating a Senior Agency Information Security Officer; (ii) developing and maintaining information security policies, procedures, and control techniques to address all applicable requirements; (iii) overseeing personnel with significant responsibilities for information security and ensuring that the personnel are adequately trained; (iv) assisting senior organizational officials concerning their security responsibilities; (v) in coordination with other senior officials, reporting annually to the Director of the Census Bureau on the overall effectiveness of the organization's information security program, including progress on remedial actions; and (iv) ensuring that all DSEP policies are implemented for information technology (IT) security procedures. The Chief Information Officer is a member of the DSEP and is responsible for reporting to and updating the DSEP on a regular basis.

*Chief Privacy Officer*

The Chief Privacy Officer is the organizational official responsible for: (i) ensuring the agency's compliance with federal privacy laws, particularly those found under the Privacy Act, the E-Government Act, and the Federal Information Security Management Act (FISMA), (ii) influencing program decisions related to data collection, processing, and dissemination by advocating for strategies that enhance privacy protections, and (iii) managing and enhancing Privacy Impact Assessment program and System of Records Notices to ensure that the agency's privacy policies and principles are reflected in all operations. As a privacy expert knowledgeable of federal privacy laws, policies, regulations, and precedents applicable to the Census Bureau, the Chief Privacy Officer consults with the officials designated in this policy on issues of privacy and confidentiality. The Chief Privacy Officer is a member of the DSEP and is responsible for updating the DSEP on an as-needed basis.

*Senior Agency Information Security Officer*

The Senior Agency Information Security Officer is an organizational official responsible for: (i) carrying out the Chief Information Officer's security responsibilities under the Federal Information Security Management Act (FISMA); and (ii) serving as the Chief Information Officer's primary liaison to the organization's Authorizing Officials, Information System Managers, Information System Owners, and Information System Security Officers. The Senior Agency Information Security Officer possesses professional qualifications, including training and experience required to administer the information security program functions, maintains information security duties as a primary responsibility, and heads an office with the mission and resources to assist in achieving FISMA compliance. It is also the responsibility of the Senior Agency Information Security Officer to work with the Chief Information Officer to jointly report and update the DSEP.

### *Authorizing Official*

The responsibilities of the Authorizing Official are generally defined in NIST SP 800-37 'Guide for the Security Certification and Accreditation of Federal Information Systems'. The Authorizing Official must have the authority to oversee the budget and business operations of the information system within the operating unit.

The Authorizing Official has the authority to assume responsibility for operating an information system at an acceptable level of: risk to operations, assets, or individuals by granting an Authorization to Operate, Interim Authorization to Operate or Denial of: Authority to Operate as defined in NIST SP 800-37. The Authorizing Official shall authorize system security requirements, System Security Plans (SSP), Interconnection System Security Agreements, and Memorandum of Agreements and/or Memorandum of Understandings.

With the increasing complexities of missions and organizations, it is possible that a particular information system may involve multiple Authorizing Officials. If so, agreements should be established among the Authorizing Officials and documented in the SSP system support plan. In most cases, it will be advantageous for a Lead Authorizing Official to represent the interests of the other Authorizing Officials. The Authorizing Officials can also delegate to an Authorizing Official Designated Representative to act on his or her behalf in carrying out and coordinating the required activities associated with security authorization.

### *Information Owner*

The Information Owner is an agency official with operational authority for specified information. The Information Owner is responsible for establishing the rules for appropriate use and protection of the subject information (e.g., rules of behavior) and retains that responsibility even when the information is shared with other organizations. The Information Owner of the information processed, stored, or transmitted by an information system may or may not be the same as the Information System Owner. Also, a single information system may contain information from multiple Information Owners.

The Information Owner is responsible for: (i) ensuring that the level of security required for the information is input into the requirements for appropriate security measures to be implemented by the proper Information System Owner of each applicable system; (ii) Privacy Impact Assessments are conducted to verify that appropriate IT security controls related to privacy and protection of data are deployed and (iii) approving or disapproving the use of information in their charge.

On May 3, 2012 the Data Stewardship Executive Policy (DSEP) Committee established the following guidelines for information ownership:

- Ownership is at the survey and program level.
- The Information Owner approves or disapproves use of the data for both production and research uses.
- Information that is co-mingled, i.e. from different programs, can have more than one owner.
- The Information Owner needs to be a grade GS14 or higher.

- Ownership and attending responsibilities can be delegated by the Information Owner for individual datasets.
- When ownership is delegated for a particular dataset, the delegated owner will approve or disapprove use.
- If use of a dataset is disapproved and after resolution is attempted at the appropriate division or directorate level, an appeal can be made to DSEP.

#### *Information System Owner*

The Information System Owner is an agency official responsible for the overall procurement, development, integration, modification, or operation and maintenance of an information system. The Information System Owner is responsible for the development and maintenance of the system security plan and ensures the system is deployed and operated according to the agreed upon security requirements. The Information System Owner is responsible for consulting with the Information Owner(s) to establish and implement the controls associated with information generation, collection, processing, dissemination, and disposal. Note that a single information system may process information from multiple Information Owners.

#### *Information System Security Officer*

The Information System Security Officer is the individual responsible to the authorizing official, Information System Owner and the Senior Agency Information Security Officer for ensuring that appropriate security controls are implemented and operating as intended for an information system. The Information System Security Officer typically has the detailed knowledge and expertise required to manage the security aspects of an information system and, in many cases, is assigned responsibility for the day-to-day security operations of the system. This responsibility may include, but is not limited to, tasks required to fulfill information security management security responsibilities, as agreed to by the Information Owners and System Owner. The Information System Security Officer may be called upon to assist in the development of the system security policy and to ensure compliance with that policy on a routine basis. In close coordination with the Information System Owner, the Information System Security Officer often plays an active role in developing and updating the system security plan, as well as in managing and controlling changes to the system and assessing the security impact of those changes. The Information System Security Officer coordinates and manages the security requirements of the system with the Information System Owner and the Information Owners, as necessary, and facilitates implementation of those requirements through system administration and operational support staff.

#### *Data Steward*

All Census Bureau employees, and individuals with Special Sworn Status, are Data Stewards. Data Stewards are responsible for adhering to all regulatory requirements and internal data policies and standards. This includes fully meeting the legal and reporting obligations levied by the Census Act, the Privacy Act, and other applicable statutes, including the requirements of governmental and other suppliers of data to the Census Bureau. Data Stewards are responsible for following all security controls mandated by the Census Bureau.

## **INFORMATION HANDLING CATEGORIES**

This section establishes Information Handling Categories. These categories are intended to assist all Census Bureau Data Stewards in effectively implementing this policy. Moreover, they are the foundation of the Census Bureau Information Handling Guidelines, which provide general guidance to Census Bureau Data Stewards for ensuring that information is handled correctly. The information handling categories reflect policies and regulations that apply to the Census Bureau. (Please note this policy does not apply to classified information; for further information refer to the Census Bureau Policies and Procedures Manual-Chapter S-10.)

The Census Bureau's Information Handling Categories are intended to provide an effective means of addressing the agency's data stewardship obligations. All of the information categories, with the exception of 'Public Information', are either legally protected or have restricted access. Data that fall within these categories, if released, can have detrimental impacts on individuals, businesses, markets, and the Census Bureau's integrity. Information in the 'Public Information' is fully available to the public.

### **Title 13**

Title 13, U.S.C. protects information collected from or on behalf of a respondent and prohibits disclosure of this information to anyone who is not sworn to uphold the oath of non-disclosure and who does not have a need to know. The information protected includes response data and some types of paradata (For additional guidance on the protections afforded paradata, please see the 'Policy on the Collection and use of Paradata'.) The following is a list of information protected by Title 13:

- Individual census or survey responses.
- Microdata or paradata containing original census or survey respondent data and/or administrative records data that do not meet the disclosure avoidance requirements.
- Address lists and frames including the Master Address File (MAF).
- Aggregate statistical information produced for internal use or research that do not meet the Disclosure Review Board disclosure avoidance requirements or that have not been reviewed and approved for release.
- Administrative records from other agencies (not including the IRS and Federal Tax Information)
- NOTE: All information collected on behalf of another federal agency, under the authority of CIPSEA, should be treated as Title 13 information.

### **Title 26**

All information protected by Title 26, U.S.C. is Federal Tax Information (FTI) including Fact of Filing information. This information is provided through agreements with the Internal Revenue Service and includes:

- The Business Register;
- All files containing federal and state tax forms;
- Record layouts for datasets that are protected by Title 26;
- Any dataset that is commingled with data that is protected by Title 26.

## **Title 5**

Title 5 protects the personally identifiable information, or PII, of both Federal employees and members of the public. PII is information that can be used to distinguish an individual's identity. Some PII is considered sensitive and requires special handling and other PII is considered non-sensitive and does not require special handling. All PII that is part of survey microdata, paradata, or the MAF is considered Title 13. The following are examples of non-sensitive PII:

- Work, home, and cell phone numbers
- Work and home addresses
- Work and personal e-mail addresses
- Resumes that do not include an SSN or where the SSN is redacted
- General background information about individuals found in resumes and biographies
- Position descriptions and performance plans without ratings.

All PII **not included** in the list above should be considered sensitive and requires special handling. This special handling includes only accessing when there is a need to know; keeping it away from public view when in use; keeping it secured when not in use; and encrypting it when sent in an email. In addition, the information listed above in combination with PII considered sensitive must be given special handling. Some examples of sensitive PII include:

- Social Security Numbers
- Financial account numbers, such as credit card and bank account numbers
- Medical and insurance account numbers
- Performance plans with ratings
- Results of background investigations
- Disciplinary action history

Even though some PII is considered non-sensitive, this does not mean that it can be publicly released. The determination to publicly release any information can only be made by an official authorized to make such a determination. At the Census Bureau, the Policy Coordination Office should be contacted if there are questions about whether PII can be released to the public.

## **Administratively Restricted Information**

Administratively restricted information is information that is not intended as a public information product. While administratively restricted information may not be protected by Federal statute, this does not mean that it does not require special handling. This information should be considered sensitive and handled accordingly. The following types of information are considered administratively restricted:

- For Official Use Only information such as internal documentation (contracting, financial, budget, legal, policy documents)
- Embargoed data or reports that have not been released but meet DRB requirements for public release
- Proprietary contractor information (cost proposal and labor rates)
- All information subject to restrictions but not protected by statutory restrictions, such as valid agreements with government agencies or other entities
- Internal use methodological documentation in support of statistical products such as the PSA
- Pre-release Principal Economic Indicators and Demographic Time-Sensitive Data.

### **Public Information**

Consists of information that is released to the public, such as statistical products, metadata, schedules, program descriptions, and risk plans, as well as information released under the Freedom of Information Act (FOIA) requirements.

### **EFFECTIVE DATE**

This policy is effective upon signature.

### **LEGAL AUTHORITIES**

Title 13, U.S.C.

Title 5, U.S.C.

Title 26, U.S.C.

Confidential Information Protection and Statistical Efficiency Act (CIPSEA)

### **IMPLEMENTATION**

Individual program areas are responsible for implementation of this policy.

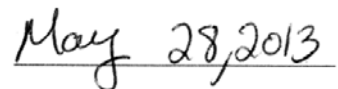
### **POLICY OWNER**

The Policy Coordination Office is the owner of this policy.

### **SIGNATURE**

A handwritten signature in black ink, appearing to read "Nancy A. Potok", written over a horizontal line.

Nancy A. Potok, Deputy Director

A handwritten date "May 28, 2013" in black ink, written over a horizontal line.

Date

### Quick Reference Guide for Roles and Responsibilities

Role Title	Responsibilities	Agency Level
Data Stewardship Executive Policy Committee (DSEP)	<ul style="list-style-type: none"> <li>• Make policy decisions on issues related to privacy, security, and confidentiality.</li> <li>• Ensure the methods of collection and uses of data adhere to legal, ethical, and reporting obligations.</li> </ul>	<ul style="list-style-type: none"> <li>• Chair: Deputy Director</li> <li>• Members: Designated Associate Directors, Senior Advisor for Data Management, Chief Privacy Officer</li> <li>• Staff: Policy Coordination Office</li> </ul>
Chief Privacy Officer	<ul style="list-style-type: none"> <li>• Ensures compliance with privacy laws</li> <li>• Works with program areas to ensure privacy protections in data collection, processing, and dissemination</li> <li>• Consults with all agency officials in this policy on issues of privacy and confidentiality</li> </ul>	<ul style="list-style-type: none"> <li>• Office of the Deputy Director</li> </ul>
Chief Information Officer	<ul style="list-style-type: none"> <li>• Designate Senior Agency Security Officer</li> <li>• Develop and maintain information security policies, procedures and techniques to address requirements.</li> <li>• Ensure information security personnel are adequately trained.</li> <li>• Assist senior officials in their security related responsibilities.</li> <li>• Report annually to the Director of the Census Bureau on the state of its security program.</li> <li>• Ensure DSEP policies are implemented in IT security procedures.</li> </ul>	<ul style="list-style-type: none"> <li>• Associate Director for Information Technology</li> </ul>
Senior Agency Information Security Officer	<ul style="list-style-type: none"> <li>• Carry out CIO's security responsibilities under FISMA.</li> <li>• Serve as the CIO's liaison to the organization's Authorizing Officials, Information System Owners, and Information System Security Officers.</li> </ul>	<ul style="list-style-type: none"> <li>• Chief, Office of Information Security</li> </ul>
Authorizing Official	<ul style="list-style-type: none"> <li>• Assumes responsibility for operating a system at an acceptable level of risk.</li> <li>• Designates the Information System Owner(s) and the Information Owner(s).</li> <li>• Ensures that the Information System Owner(s) and the Information Owner(s) are adhering to all applicable policies.</li> </ul>	<ul style="list-style-type: none"> <li>• Associate Director (1 per system)</li> </ul>



Information Owner	<ul style="list-style-type: none"> <li>• Establishes rules for lifecycle use and protection of specified information (such as datasets, systems of records, etc.).</li> <li>• Retains responsibility for information even when shared with other organizations.</li> <li>• Has input to the requirements to ensure the correct level of required security measures are implemented by the appropriate Information System Owner.</li> <li>• Ensures Privacy Impact Assessments are conducted.</li> </ul>	<ul style="list-style-type: none"> <li>• Staff member of grade 14 or higher</li> </ul>
Information System Owner	<ul style="list-style-type: none"> <li>• Responsible for the overall procurement, development, integration, modification and/or operation and maintenance of an information system.</li> <li>• Develops and maintains system security plans.</li> <li>• Consults with the Information Owner(s) to gather requirements needed to establish and implement controls for information generation, collection, processing, dissemination, and disposal.</li> </ul>	<ul style="list-style-type: none"> <li>• Division Chief or ADC (1 per system)</li> </ul>
Information System Security Officer	<ul style="list-style-type: none"> <li>• Responsible to the Authorizing Official, Information System Owner, and the Senior Agency Information Security Officer to ensure security controls are implemented and operation for an information system.</li> <li>• Manages day-to-day security of an information system.</li> <li>• Assists in developing and assessing system security policies and plans, and ensuring compliance.</li> </ul>	<ul style="list-style-type: none"> <li>• Technical Representative for a system, a system may have one or more Information System Security Officers</li> </ul>
Data Steward	<ul style="list-style-type: none"> <li>• Responsible for knowing, applying, and following all appropriate security controls deemed necessary and mandated by the U.S. Census Bureau and Federal Government</li> </ul>	<ul style="list-style-type: none"> <li>• All Census Bureau employees and Special Sworn Status individuals</li> </ul>

### Data Handling Guidelines

Data Type	Hard Copies	Electronic Transmission	Printing	Disposal
<b>Title 13</b>	<ul style="list-style-type: none"> <li>• Keep locked in desk or file cabinet when not in use.</li> <li>• Restrict access to only those Census Bureau staff or individuals with special sworn status with a need to know.</li> <li>• Do not remove hard copies from the Census Bureau building, even if teleworking.</li> </ul>	<ul style="list-style-type: none"> <li>• Encrypt before transmission using an approved encryption method, such as SecretAgent or Safeboot encryption.</li> <li>• If teleworking, only access Title 13 information in VDI – do not email Title 13 information to yourself in iNotes for use at home.</li> <li>• Do not scan.</li> <li>• If faxing, ensure someone is at the machine to receive it and confirm receipt after sending.</li> </ul>	<ul style="list-style-type: none"> <li>• Either use private printing or use a cover sheet.</li> <li>• Pick up print outs immediately from the printer.</li> </ul>	<ul style="list-style-type: none"> <li>• Dispose of hard copies in a locked blue bin designated for sensitive materials.</li> <li>• Dispose of electronic copies (tapes, cds, disks, etc.) in locked blue bin or by contacting the Records Office at 3-2282.</li> </ul>
<b>Title 26</b>	<ul style="list-style-type: none"> <li>• Keep locked in desk or file cabinet when not in use. File cabinet should be labeled as having Title 26 information.</li> <li>• Restrict access to only those Census Bureau staff or individuals with special sworn status with a need to know who are on an approved Title 26 project.</li> <li>• Do not remove hard copies from the Census Bureau building, even if teleworking.</li> </ul>	<ul style="list-style-type: none"> <li>• Encrypt before transmission using an approved encryption method, such as SecretAgent or Safeboot encryption.</li> <li>• If teleworking, only access Title 26 information in VDI – do not email Title 26 information to yourself in iNotes for use at home.</li> <li>• Do not scan.</li> <li>• If faxing, ensure someone is at the machine to receive it and confirm receipt after sending.</li> </ul>	<ul style="list-style-type: none"> <li>• Either use private printing or use a cover sheet.</li> <li>• Pick up print outs immediately from the printer.</li> <li>• Log printing in print logs to ensure tracking of hard copies.</li> </ul>	<ul style="list-style-type: none"> <li>• Dispose of hard copies in a locked blue bin designated for sensitive materials.</li> <li>• Log disposal and destruction of all hard copies using disposal logs located in printing rooms.</li> <li>• Shred documents using only approved cross-cut shredders provided in copy rooms.</li> <li>• Dispose of electronic copies (tapes, cds, disks, etc.) in locked blue bin or by contacting the Records Office at 3-2282.</li> </ul>

Version 2.1

<b>Data Type</b>	<b>Hard Copies</b>	<b>Electronic Transmission</b>	<b>Printing</b>	<b>Disposal</b>
<b>Title 5</b>	<ul style="list-style-type: none"> <li>• Keep locked in desk or file cabinet when not in use.</li> <li>• Restrict access to only those Census Bureau staff or individuals with special sworn status with a need to know.</li> </ul>	<ul style="list-style-type: none"> <li>• Encrypt before transmission using an approved encryption method, such as SecretAgent or Safeboot encryption.</li> <li>• If teleworking, only access Title 5 information in VDI – do not email Title 13 information to yourself in iNotes for use at home.</li> <li>• Do not scan.</li> <li>• If faxing, ensure someone is at the machine to receive it.</li> </ul>	<ul style="list-style-type: none"> <li>• Use private printing or a cover sheet.</li> <li>• Pick up print-outs immediately from the printer.</li> </ul>	<ul style="list-style-type: none"> <li>• Dispose of in locked blue bin, not regular recycling.</li> <li>• Dispose of electronic copies (tapes, cds, disks, etc.) in locked blue bin or by contacting the Records Office at 3-2282.</li> </ul>
<b>Administratively Restricted</b>	<ul style="list-style-type: none"> <li>• Keep hidden from view when members of the public are present.</li> <li>• Keep locked when not in use if warranted; check with your supervisor if unsure of the sensitivity of a particular item.</li> <li>• Label ‘for internal use only’ or something similar to designate it as a non-public document.</li> </ul>	<ul style="list-style-type: none"> <li>• Encrypt if the sensitivity level is high; check with your supervisor.</li> <li>• Transmit with care if not encrypting – ensure that the individual receiving the email is aware of the sensitive nature of the document.</li> <li>• If faxing, ensure someone is at the machine to receive it.</li> <li>• Scan with care and take into account the sensitivity of the material - scanning is not secure.</li> </ul>	<ul style="list-style-type: none"> <li>• Can print without restrictions but treat print-outs as you would hard copies.</li> </ul>	<ul style="list-style-type: none"> <li>• Dispose of in locked blue bin, not regular recycling.</li> <li>• Dispose of electronic copies (tapes, cds, disks, etc.) in locked blue bin or by contacting the Records Office at 3-2282.</li> </ul>
<b>Public Use</b>	No handling restrictions – Do not release to the public without permission from your supervisor.	No handling restrictions – Do not send to the public without permission from your supervisor.	No handling restrictions.	<ul style="list-style-type: none"> <li>• Dispose in regular recycle bins.</li> </ul>