DS007: Safeguarding and Managing Information

PURPOSE

This policy ensures an integrated and consistent approach to information security management at the U.S. Census Bureau. It establishes Roles and Responsibilities and Information Handling Categories and guidelines, which apply to all information collected, acquired, or maintained by or on behalf of the Census Bureau in all forms (such as, paper copies, electronic files, or datasets) regardless of where they are stored (in Census Bureau facilities, on our local network, on third-party networks, or in the cloud). This policy applies to economic and demographic data used to generate statistical products (such as the results of censuses and surveys), administrative and third-party data acquired from other sources, other data collected for research or production purposes, personnel data, financial data, and data used to facilitate agency administration. It also establishes the Census Bureau's policy for managing unclassified information that requires safeguarding or dissemination controls pursuant to and consistent with laws, regulations, and Government-wide policies.

This policy does not provide information or guidelines for federally defined national security information; for information on the handling of classified data, please refer to Chapter S-10 of the Census Bureau *Policies and Procedures Manual*.

This policy replaces the version signed May 28, 2013.

BACKGROUND

One of the core objectives of the Census Bureau's Data Stewardship program is to effectively safeguard, while simultaneously facilitating legitimate access to, information through its entire lifecycle: generation, collection, transmission, processing, dissemination, storage, archiving, 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.

The Census Bureau has longstanding guidelines to properly categorize and handle information in accordance with the existing legal and regulatory framework under which the agency's Data Stewardship program was developed. More recently, Executive Order 13556 established *Controlled Unclassified Information* (CUI) as an umbrella designation for information that is controlled by law, regulation, or Government-wide policy but that is not classified national security information. Furthermore, on September 14, 2016, 32 CFR § 2002 established a uniform policy for federal agencies on designating, safeguarding, disseminating, marking, decontrolling, and disposing of CUI; self-inspection and oversight requirements; and other facets of the federal government's CUI program. While at its core, the CUI program is neither inconsistent, nor incompatible with the Census Bureau's historical information categorization and handling standards, this revised policy is the first step in a systematic approach to harmonizing them.

SCOPE

This policy applies to all Census Bureau employees, contractors, and special sworn status individuals.

This policy applies to controlled unclassified information (CUI), which is defined as any information the Census Bureau creates, acquires, or possesses, or that an entity creates, acquires, or possesses for or on behalf of the Census Bureau, that is required to be protected under law, regulation, or Government-wide policy. It also applies to administratively restricted information that is not controlled unclassified information.

This policy does not apply to classified information or information a non-executive branch entity possesses or maintains in its own systems that did not come from, or was not created or possessed by or for, the Census Bureau or an entity acting for the Census Bureau.

POLICY

The Census Bureau will safeguard and protect the information in its custody, consistent with federal statutes and regulations, and with a recognition that it is essential to the credibility of the agency and to the success of its mission. The roles, responsibilities, and standards to meet this critical obligation are outlined in this policy and in the Quick Reference Guide for Roles and Responsibilities (Attachment A). All information at the Census Bureau must be categorized and handled consistent with the guidance outlined below and in the Detailed Information Handling Guidelines (Attachment B). In addition to our legacy information handling categories and marking standards, the Census Bureau also recognizes the Controlled Unclassified Information (CUI) designations being implemented across federal agencies, and the agency is implementing CUI standards in line with the Department of Commerce, *CUI Policy and Guidelines*. As other agencies implement their CUI Programs and the Federal government-wide CUI Program is refined, Census Bureau personnel will encounter legacy designations and the new CUI markings and should look for updated guidance on the CUI Program in Attachment B of the policy and in the federal government-wide CUI Registry on the National Archives and Records Administration (NARA) website (https://www.archives.gov/cui).

The CUI categories identified in this policy reflect a government-wide approach to controlling data consistent with our longstanding practice of restricting access based on legal requirements as well as business need-to-know. Information about the major categories of CUI used at the Census Bureau, as well as handling requirements are contained in Attachment B. However, it is important to note that this is not an exhaustive list of CUI that may come into the possession of the agency.

While the use of CUI categorizations and labeling is being phased in and is not mandatory on digital and physical legacy materials remaining within the Department of Commerce (DOC)[1], program areas and individuals must be able to recognize CUI markings and standards and must incorporate them into their processes and documents.

All Census Bureau employees, contractors, and special sworn status individuals are required to identify and understand their role in safeguarding and managing information. All individuals are also required to adhere to the general requirements for Controlled Unclassified Information and the Detailed

[1] See *Waiver of Controlled Unclassified Information Marking Requirements for Legacy Information and Data* – https://ocio.commerce.gov/sites/default/files/media/files/2019/cui_legacy_waiver.pdf

Information Handling Guidelines that have been created to assist in the implementation of this policy. These guidelines are in Attachment B.

GENERAL REQUIREMENTS FOR CONTROLLED UNCLASSIFIED INFORMATION

The CUI Registry is the online repository for all information, guidance, policy, and requirements on handling CUI, including everything issued by the NARA, which is the Executive Agent overseeing the Federal government-wide CUI Program. Among other information, the CUI Registry identifies all approved CUI categories, provides general descriptions for each, identifies the basis for controls, establishes CUI markings, and includes guidance on handling procedures and safeguarding requirements.

Census Bureau employees and detailees, contractors, special sworn status collaborators, and other individuals associated with the Census Bureau must endeavor to recognize whether information is CUI by consulting CUI Markings, legacy markings, and, if it is unmarked, researching the origins of the information, consulting the legal authorities or agreements under which the information was created, collected, or otherwise acquired.

CUI Basic
CUI Basic is the subset of CUI for which the authorizing law, regulation, or Government-wide policy does not set out specific handling or dissemination controls. The Census Bureau and other federal agencies must handle CUI Basic according to the uniform set of controls set forth in 32 CFR § 2002 and the CUI Registry. CUI Basic is the minimum safeguarding requirement for all CUI and differs from CUI Specified (see definition for CUI Specified in this section), and CUI Basic controls apply whenever CUI Specified ones do not.

CUI Specified
CUI Specified is the subset of CUI in which the authorizing law, regulation, or Government-wide policy contains specific handling controls that require or permit agencies to use procedures and protections that exceed or differ from those for CUI Basic. The CUI Registry indicates which laws, regulations, and Government-wide policies include such specific requirements. CUI Specified controls may be more stringent than, or may simply differ from, those required by CUI Basic; the distinction is that the underlying authority spells out specific controls for CUI Specified information and does not for CUI Basic information.

Examples of CUI Specified information include Title 13 information, Title 26 information, Personnel Records, Title 5 Sensitive Personally Identifiable Information (PII), and information protected by the Confidential Information Protection and Statistical Efficiency Act (CIPSEA).

CUI BASIC CONTROLS

Safeguarding and Storage of CUI—Physical Controls
The objective of safeguarding is to prevent the unauthorized disclosure of or access to CUI. These guidelines in this subsection set forth the minimum standards for safeguarding CUI.

Unless different protections are specified by law, regulation, or policy, physical documents containing CUI must be stored in a locked office, locked drawer, or locked file cabinet whenever they are unattended. In addition, CUI stored on removable storage must be password protected. If cleaning or maintenance personnel are allowed into private offices after hours, CUI within those offices must be secured in a locked desk drawer or locked file cabinet.

Individuals working with CUI Specified Information must comply with the safeguarding standards outlined in the underlying law, regulation, or government-wide policy. The safeguarding requirements that apply to the specified categories of CUI most frequently used at the Census Bureau are outlined later in this policy.

Safeguarding During Working Hours. Persons working with CUI shall be careful not to expose CUI to unauthorized users or others who do not have a lawful government purpose to see it. Personnel must secure CUI documents in a locked location, such as a desk drawer, file cabinet, or office, when not in use or under observation, or filed for retention.

Other Precautions:

- Personnel must ensure that unauthorized individuals cannot access or observe CUI, or overhear conversations where CUI is discussed (ex. it may be necessary to hold conversations involving CUI in a private office or conference room).

- CUI should be kept in a controlled environment, which is defined as any area or space with adequate physical or procedural controls (that is, barriers and managed access controls, such as locked doors and guard stations) for protecting CUI from unauthorized access or disclosure.

- If authorized to remove CUI from a controlled environment, personnel must keep CUI under their direct control at all times or protect it with at least one physical barrier, like an envelope or file folder and reasonably ensure that they or the physical barrier protects the CUI from unauthorized access or observation.

Care While Traveling. All reasonable measures shall be taken (e.g., secure transmission, approved electronic USB or other method authorized) to mitigate risk and limit the necessity to hand carry CUI while in official travel status. CUI shall not be viewed while on public transportation where unauthorized individuals may be exposed to it. In hotel rooms, CUI shall be stored in a locked briefcase or room safe when not in use. CUI may be stored in a locked automobile only if it is in an envelope, briefcase, or otherwise covered from view. The trunk is the most secure location for storing CUI in an automobile.

Care During Foreign Travel. Specific instructions for handling and safeguarding of sensitive information, including CUI, while on approved foreign travel is contained in Chapter 35 of the DOC, *Manual of Security Policies and Procedures*.

Safeguarding and Storage of CUI on IT Systems

Information systems processing, storing, or transmitting CUI must meet the security and privacy protections at the moderate baseline as defined in *NIST Special Publication 800-53* and the Census Bureau's *IT Security Program Policy*. Like physical barriers for protecting CUI, barriers and access controls on IT systems should limit access only to those with a Lawful Government Purpose. Barriers include: dedicated network drives, restricted-access file folders or directories, or restricted-access intranet sites. On cloud services and external providers, they include meeting Federal Risk and Authorization Management Program (FedRAMP) controls.

The Census Bureau has additional IT security requirements on transmission of several categories of CUI Specified information.

Data Stewardship, IT Security, and CUI Training

All individuals with unsupervised access to Census Bureau facilities, or any access to the Census Bureau IT network or Census Bureau data will meet the training requirements as outlined in *DS017: Data Stewardship Awareness Training.* These training requirements address FISMA-required IT Security

Awareness training, as well as the requirements for general CUI awareness training required under DOC policy, and training on the categories of CUI Specified information most often and most widely handled at the Census Bureau. In addition, individuals with access CUI Specified information may be required to receive additional training on the specific handling requirements of the underlying law, regulation, or government-wide policy for that category of CUI.

Marking and Labeling of CUI

Consistent with the implementation guidance outlined in this policy, all new documents containing CUI must have a CUI marking denoting that the document contains CUI. Under this policy, the CUI marking must also contain category markings for all categories of CUI contained in the document. CUI markings listed in the CUI Registry are the only markings authorized to designate unclassified information that requires safeguarding or dissemination controls. Under federal regulations covering controlled unclassified information, "document" includes, but is not limited to, reports, computer files, tabulations, electronic matter, and data compilations from which information can be obtained, including materials used in data processing. Document also includes voice records, film, tapes, video tapes, emails, and memoranda in addition to the file, folder, exhibits, and containers, the labels on them, and any metadata, associated with each original or copy.[2] See Attachment B for more detailed information on how to apply a CUI marking.

The DOC issued and NARA approved, on August 14, 2019, a waiver allowing existing datasets and other documents to maintain "legacy" markings if the information remains within and under Departmental control. So long as that waiver is in place, personnel do not need to mark legacy materials. New information products and datasets and those information products and datasets that are shared with other federal partners must adhere to the new markings at the time of creation. All files and documents containing CUI that are leaving the DOC boundaries must be marked with a CUI marking or alternative bulk marking method as stipulated in the 32 CFR § 2002 and additional CUI Notices on alternative markings on the NARA CUI website. Approved alternate/bulk marking methods include but are not limited to user access agreements, information system log in screens, computer system digital splash screens, and signs in storage areas or on containers. Under all such methods the basic requirement remains—the person accessing CUI on a system or storage are, or the recipient of transmitted CUI must be made aware that the information is CUI and how it must be safeguarded.

New documents with CUI that are being stored and transmitted within the Census Bureau should also be marked with a CUI marking, or an approved alternate/bulk marking method.

The Census Bureau will continue to label all information protected under Title 13 U.S.C. (hereafter referred to as Title 13) with a label stating that disclosure is prohibited and that it is protected under Title 13. However, that label must be separated and distinguishable from the CUI marking.

The lack of a CUI marking on information that qualifies as CUI does not exempt anyone accessing or receiving that information from abiding by applicable CUI marking and handling requirements as described in this policy and the CUI Registry.

Marking CUI: Only for a Lawful Government Purpose

Information may only be designated and marked as CUI to further a lawful government purpose and only if the information is protected by a law, regulation, or government-wide policy. See Attachment B for the CUI markings for the categories of CUI most commonly handled at the Census Bureau.

[2] 32 CFR § 2002.4(w)

CUI Designation Indicator
The CUI Designation Indicator shows the agency, office, or person that identified that the information is CUI. It must appear on the first page or cover page of all documents containing CUI. The CUI Designation Indicator might only identify the agency at a minimum, but preferably it should identify the person, or office, that designated the CUI (the designator). The agency designator indicator requirement may be met through use of Census Bureau letterhead and email signatures. Designator indicators of an office or person may be accomplished by adding a line saying a "Controlled by" and then stating the office or person.

Portion Marking
Portion markings are a means to provide information about the sensitivity of a specific section of text, paragraph, bullet, picture, chart, etc. They consist of an abbreviation enclosed in parentheses, usually at the beginning of a sentence or title.

Portion marking is not required, but it is permitted to facilitate information sharing, information tracking, and proper handling. Portion marking also assists Freedom of Information Act (FOIA) reviewers in identifying the CUI within a large document that may contain other information suitable for public release.

Note: If portion markings are used in any portion of a document, they must be used throughout the entire document. All portions or sections must be portion marked, even those that do not contain CUI. Sections that do not contain CUI should be marked with as Uncontrolled Unclassified Information, designated with a [U].

Misuse of CUI
Misuse of CUI is when an individual uses CUI in a manner not in accordance with this policy, E.O. 13556, 32 CFR Part 2002, the CUI Registry or the applicable law, regulation, or Government-wide policy that govern the affected information. This may include intentional violations or unintentional errors in safeguarding or disseminating CUI that results in unauthorized sharing of, or access to, that information in any form. This may also include designating or marking information as CUI when it does not qualify as CUI.

Misuse of CUI may result in administrative or disciplinary action, up to and including removal from federal service. Some misuses of CUI may also result in criminal penalties as outlined in the underlying law, regulation, or Government-wide policy governing protection of the information. Any disciplinary action shall be guided by Department Administrative Order (DAO) 202-751. Discipline and authorities listed therein is set forth in E.O. 9830, as amended, and chapters 43 and 75 of Title 5, U.S. Code and the DOC *CUI Guidelines*, Section 36. Disciplinary actions relative to misuse of CUI are considered as "Violation of a security regulation" as listed in Appendix B, Table of Offenses and Penalties of DAO 202-751. In the event a contractor misuses CUI, the matter must be referred to the contracting officer to determine whether remedies should be imposed under the contract.

Information may not be designated as CUI:

- To conceal violations of law, inefficiency, or administrative error;
- To prevent embarrassment to the U.S. Government, any U.S. official, organization, or agency;
- To improperly or unlawfully interfere with competition;
- To prevent or delay the release of information that does not require such protection;
- If it is required by law, regulation, or government-wide policy to be made available to the public; or,
- If it has been released to the public under proper authority.

Reporting Misuse of CUI
Suspected or confirmed misuse of CUI must be reported via the Bureau of the Census-Computer Incident Response Team (BOC-CIRT) response process as soon as possible but no later than one hour after discovery. Incident handlers shall obtain the details of the situation, coordinate with a subject matter expert regarding the severity of the incident and report the results of the investigation in accordance with *DS022: Personally Identifiable Information (PII) Breach Policy* and the Office of the Chief Information Officer's *Cyber Incident Response Policy*.

Incident handlers should coordinate mitigation measures as appropriate within their incident response and management structures. Investigations also must be reported to the Census Bureau's CUI Point of Contact (CUI POC), who will report on incidents to the DOC CUI Program Manager (CUI PM) in accordance with procedures developed with the DOC CUI Program. Depending on the severity of an incident of misuse of CUI, the CUI POC will report the incident to the CUI PM within 48 hours of discovery and provide regular status reports to the CUI PM until mitigation efforts are complete.

Decontrol of CUI
When control is no longer needed, and as permitted by law, regulation, or government-wide policy, the Census Bureau should decontrol any CUI that it designates. This means the information should be removed from the protection of the CUI program as soon as practicable when the information no longer requires safeguarding or dissemination controls, unless doing so conflicts with the underlying law, regulation, or government-wide policy. An example of such a conflict is in Title 13, which prohibits the Census Bureau from releasing any information from a Title 13 data collection from which it would be possible to distinguish an individual or entity's information.

CUI may be decontrolled automatically for all or limited purposes upon the occurrence of one of the conditions below, or through an affirmative decision by the designator:

- When laws, regulations or government-wide policies no longer require its control as CUI and the authorized holder, designated by the Census Bureau as the Information Owner[3] has the appropriate authority under the authorizing law, regulation, or government-wide policy
- When the agency that designated it as CUI decides to release the CUI to the public by making an affirmative, proactive disclosure. (Note that CUI collected or acquired by the Census Bureau under the authority of Title 13 becomes Title 13 information even if it was designated as another category of CUI by another agency.)
- When the Census Bureau discloses it in accordance with an applicable information access statute, such as the Freedom of Information Act (FOIA) or the Privacy Act (when legally permissible), provided the designator's agency incorporates such disclosures into its public release processes
    - Disclosures of CUI under FOIA constitute CUI decontrol for all purposes.
    - Disclosures under the Privacy Act constitute decontrol only with respect to the limited purpose of disclosure to the individual who requested access to their records maintained in a system of records (not for other purposes).
- When a predetermined event or date occurs, as described in the authorizing regulations listed in the CUI Registry.

When indicated by a decontrol marking specifying a decontrol date or event, CUI is decontrolled without further review by the originator.

[3] See "*Information Owner"* as defined in the Roles and Responsibilities section of this policy.

The Census Bureau may also decontrol CUI:

In response to a request from an authorized holder to decontrol it, and

Concurrently with any declassification action under E.O. 13556 or any predecessor or successor order, as long as the information also appropriately qualifies for decontrol as CUI.

As permitted under DOC *CUI Policy*, the Census Bureau may designate, in this and other policies, which personnel it authorizes to decontrol CUI, consistent with law, regulation, and government-wide policy. For example, the Census Bureau's Disclosure Review Board is authorized to decontrol statistical aggregations of Title 13, Title 26[4], and Title 5 information in manners consistent with those statutes.

Decontrolling CUI for purposes other than FOIA disclosure relieves the requirement to handle the information under the CUI Program but does not constitute authorization for public release.

Once decontrolled, any public release of information that was formerly CUI must be in accordance with applicable law and policies on the public release of information.

Authorized holders may request that the designating agency decontrol CUI that they believe should be decontrolled. See section 35, Challenges to Designation of Information as CUI in the DOC *Controlled Unclassified Information Guidelines*.

If an authorized holder publicly releases CUI in accordance with the designating agency's (not DOC) authorized procedures, the release constitutes decontrol of the information.

Unauthorized disclosure of CUI does not constitute decontrol.

Personnel must not decontrol CUI to conceal, or to otherwise circumvent accountability for, an unauthorized disclosure.

When laws, regulations, or government-wide policies require specific decontrol procedures, personnel must follow such requirements.

Records Management Note: The Archivist of the United States may decontrol records transferred to the National Archives and Records Administration (NARA) in accordance with 32 CFR § 2002.34, absent a specific agreement to the contrary with the Census Bureau or another agency that designated it as CUI and from whom the Census Bureau received the CUI.

Decontrolling CUI differs from declassification of information because Classified Information is part of a separate system and declassification of a document that contains CUI does not mean that it has been decontrolled or is releasable to the public

Sharing of CUI with Other Federal Agencies, Other Entities, and Non-Census Bureau Employees
The Census Bureau will disseminate and permit access to CUI, provided that such access or dissemination:

- Abides by the laws, regulations, or Government-wide policies that established the CUI category;
- Furthers a lawful Government purpose;

[4] Census is only permitted to decontrol statistical products created from FTI. All other decontrol of FTI is solely within the purview of the Internal Revenue Service per the guidance in IRS PUB-1075.

- Is not restricted by an authorized limited dissemination control established by the CUI Executive Agent; and,
- Is not otherwise prohibited by law.
    - Note: *DS006: Controlling Non-employee Access to Title 13 Information* and *DS001B: Handbook for Administrative Data Projects* provide more information on requirements and processes for lawfully permitting access to Title 13 and Title 26 information.

Destruction of CUI

CUI may be destroyed:

- When the information is no longer needed, and
- When records disposition schedules, published or approved by NARA or other applicable laws, regulations, or government-wide policies, no longer require retention.

Destruction of CUI, including in electronic form, must be accomplished in a manner that makes it unreadable, indecipherable, and irrecoverable. CUI may not be placed in office trash bins or recycling containers. CUI must be destroyed according to any specific directives regarding the information. If the authority does not specify a destruction method, one of the following methods must be used:

- Guidance for destruction in Census Bureau, *Policies and Procedures Manual Chapter K-3 Records Management*; NIST SP 800-53, *Security and Privacy Controls for Federal Information Systems and Organizations*; NIST SP 800-88, *Guidelines for Media Sanitization;* NARA, *CUI Notice 2017-02: Controlled Unclassified Information (CUI) and Multi-Step Destruction Process;* or NARA*, CUI Notice 2019-03: Destroying Controlled Unclassified Information (CUI) in Paper Form.*
- Any method of destruction approved for Classified National Security Information, as delineated in 32 CFR 2001.47, *Destruction*, or any implementing or successor guidance.
- National Security Agency approved product for device sanitation.

Legacy Materials and Agencies that Have Not Implemented the CUI Program Yet

As a natural consequence of federal agencies not implementing the CUI program at the same time, legacy markings, or any markings that were previously used to identify information that should be designated as CUI, and CUI markings will exist at the same time.

Handling instructions must be included for CUI sent to another agency that has not implemented the CUI Program yet or for CUI Specified information sent to any authorized recipient.

CUI and the Freedom of Information Act and the Whistleblower Protection Act

This policy is not intended to supersede or conflict with existing DOC policy and practice in responding to requests for information under the Freedom of Information Act (FOIA). The marking of CUI does not exempt information from being considered responsive to a request under FOIA, nor is information deemed exempt from release under the FOIA inherently CUI.

There may be circumstances in which CUI may be disclosed to an individual or entity, including through a FOIA or Privacy Act request and response, but such disclosure does not always constitute public release as defined by the CUI Program. Although disclosed via a FOIA response, the CUI may still need to be controlled while the Census Bureau continues to hold the information, despite the disclosure, unless it is otherwise decontrolled (or the Census Bureau FOIA Officer indicates that FOIA disclosure results in public release and the CUI does not otherwise have another legal requirement for its continued control).

Similarly, the CUI Program does not change or affect existing legal protections for whistleblowers under the Whistleblower Protection Act. The fact that information is designated or marked as CUI does not determine whether an individual may lawfully disclose that information under a law or other authority and does not preempt or otherwise affect whistleblower legal protections provided by law, regulation, E.O. or directive.

Reporting on IT Systems with CUI

As directed by the DOC Chief Information Officer (DOC CIO), the Census Bureau will inventory its IT systems to determine which ones contain CUI and whether they meet the required security requirements for CUI. The Census Bureau will report the results following the form and schedule requested by the DOC CIO.

CUI Self-Inspection Program

The Census Bureau will implement a CUI Self-Inspection Program as follows:

- Following technical guidance from the DOC CUI Program, the Census Bureau will conduct reviews and assessments of its CUI Program, at least annually, and report the results to the CUI PM as required by NARA.
- The self-inspection and reporting of the results will be on a schedule determined by the DOC CIO.
- The Census Bureau will include in the self-inspection any contractors that are under their purview by on-site inspections or by examining any self-inspections conducted by the contractors.
- Following guidance and inspection materials received from the DOC CUI PM, self-inspection methods, reviews, and assessments shall serve to evaluate program effectiveness, measure the level of compliance, and monitor the progress of CUI implementation.
- The DOC CUI PM shall provide to the bureaus formats for documenting self-inspections and recording findings and provide advice for resolving deficiencies and taking corrective actions.
- Results from the DOC-wide self-inspections will inform updates to the CUI training provided to the Census Bureau.

INFORMATION HANDLING CATEGORIES

The Census Bureau's Information Handling Guidelines assist all Census Bureau employees, contractors, and SSS individuals in safeguarding and managing information. Federal laws, regulations, and standards are the foundation of the Census Bureau Information Handling Guidelines. The guidelines break down types of information handled at the Census Bureau according to whether they are protected by law, regulation, or government-wide policy (CUI), whether they are subject to administrative controls, or whether they are suitable for public release. CUI and administratively restricted information, if released, can have detrimental impacts on individuals, businesses, markets, and the Census Bureau's reputation. Conversely, "Public Information" is fully releasable to the public through business processes outlined elsewhere (examples: Freedom of Information Act (FOIA) requests, Custom Tabulations, Press Releases, etc.). See Attachment B for Detailed Information Handling Guidelines.

ROLES AND RESPONSIBILITIES

This section identifies roles and responsibilities delegated to individuals who will directly implement this policy. These roles are modeled on Special Publications and Federal Information Processing Standards created by the National Institute of Standards and Technology (NIST) and the DOC *Controlled Unclassified Information (CUI) Policy*. These roles include, but are not limited to, the Data Stewardship Executive Policy Committee (DSEP), the Chief Information Officer, Chief Information Security Officer,

Chief Privacy Officer, Authorizing Officials, Information System Owners, Information Owners, the Controlled Unclassified Information Point of Contact (CUI POC), Data Security Stewards, and all employees, contractors, and special sworn status individuals. (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) sets policy and makes decisions on policy-related matters related to privacy, security, confidentiality, administrative data, and data management. 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 (Title 5), 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 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; (vi) assessing all Census Bureau IT systems that contain CUI and ensuring that they have the appropriate CUI Markings, and meet all required security controls for Federal information systems that process, store, and transmit CUI; (vii) ensuring the Census Bureau applies NIST SP 800-171 when establishing security requirements to protect CUI's confidentiality on non-federal information systems unless the information involved prescribes specific safeguarding requirements or unless the agreement establishes requirements to protect CUI at higher than moderate confidentiality; and (viii) 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 Modernization 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.

Chief Information Security Officer
The Chief Information Security Officer is the 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. The Chief Information Security Officer has the responsibility of working 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, *Risk Management Framework for Information Systems and Organizations.* 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 Memoranda of Agreement and/or Memoranda of Understanding.

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 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.

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 (*ex*, rules of behavior) and retains that responsibility even when the information is shared with other organizations or transferred across system boundaries. 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.

DSEP established the following guidelines for information ownership:

- Ownership is at the survey, program, or project level.
- The Information Owner approves or disapproves use of the data for both production and research uses and can revoke the use of their data.
- New Information Owners review every project using their data whenever the Information Owner changes.
- Information that is co-mingled (sourced from multiple programs) can have more than one owner.
- The Information Owner must be a grade GS14 or higher.
- Ownership and attending responsibilities can be delegated by the Information Owner.
- When ownership is delegated, 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 Owners are responsible for registering all the data assets within their purview in the Census Bureau's Enterprise Data List (i.e., the Data Management System, or DMS). This step ensures proper use and reporting, and it enhances the coordination of corporate information sharing across the Census Bureau. By registering their data assets, the Information Owner consents to curation activities, including but not limited to cleaning and standardizing the data. The Information Owner retains the responsibility and authority to approve or disapprove further uses of a curated dataset.

CUI Point of Contact (CUI POC)
The CUI Point of Contact is a Census Bureau official designated by the DSEP to oversee implementation of the Controlled Unclassified Program at the Census Bureau. The CUI POC's responsibilities are defined in the DOC *Controlled Unclassified Information Guidelines*. They include: (i) conducting oversight actions to ensure compliance within their area of responsibility and report findings at least annually to the DOC CUI Program Manager (DOC CUI PM); (ii) serving as the Census Bureau's CUI subject matter expert, responding to most inquiries from their organizations and consulting with the CUI PM on questions beyond their expertise; (iii) ensuring all personnel within the Census Bureau complete initial and annual

training as required and reporting the progress of training to the DOC CUI PM; (iv) conducting annual Census Bureau self-inspections of the CUI Program, according to guidance provided by the DOC CUI PM, to reflect the progress of implementation and reporting those self-inspections to the DOC CUI PM; (v) providing input from the Census Bureau on all other reporting requirements to the DOC CUI PM to enable a DOC-wide response to the National Archives and Records Administration (NARA); (vi) working with offices delegated by the CIO on reporting instances of potential CUI misuse, violation or infractions in accordance with the DOC Computer Incident Response Plan and keeping track of violations for reporting purposes, the DOC CUI PM will be notified through the incident response process; (vii) reporting to DSEP on the status of the Census Bureau's CUI Program; and (viii) confirming their status as a CUI POC with the DOC CUI PM on a semi-annual basis (by the dates designated by the CUI PM) and providing notification within five business days if their status changes.

CUI Implementation Team
The CUI Implementation Team with representation from most directorates and OCIO will be responsible (i) for helping the CIO and the CUI POC establish the Census Bureau's CUI Program (ii) ensuring it is being implemented within their respective directorates, (iii) helping the CIO and CUI POC report to the DOC CUI PM, (iv) conducting an inventory of categories of CUI handled by their respective directorates and how they are labeled; (v) making their directorates aware of new categories of CUI if their directorates handle that CUI; and (iv) investigating CUI incidents (BOC-CIRT) for categories of CUI handled predominantly by their area.

Data Security Steward
Each Division must designate a Data Security Steward (DSS) that is responsible for being the point of contact for: the Policy Coordination Office (PCO) for privacy and confidentiality concerns; for the CUI POC for CUI implementation milestones and annual self-inspections of their respective divisions; IRS Safeguard Reviews, Office of Security (OSY) for physical security reviews. The DSS is responsible for monitoring all print and disposal logs in their designated area as required by IRS Publication 1075, Tax Information Security Guidelines for Federal, State and Local Agencies and Entities. Logs of Title 26 information printed must be placed at every printer and reviewed monthly and maintained by the DSS for 5 years. Disposal logs for Title 26 information are placed on compliant shredders, reviewed monthly and maintained by the DSS for 5 years. Disposal logs are placed on locked blue bins, reviewed on the 1st and 15th of the month and are collected and maintained by ACSD for 5 years. In addition, DSSs must ensure that proper signage related to Title 26 compliance is in place, including replacing missing or defaced signs. Additionally, DSS must help conduct oversight actions at the request of the CUI POC to ensure CUI compliance within their division and report findings at least annually to the CUI POC for reporting to the DOC.

DSSs must work with their Division Chief to disseminate information provided by OSY or PCO related to Title 26 compliance, physical security, the CUI Program, privacy compliance, and other Data Stewardship issues as needed. Training and update meetings are held three times per year and DSSs are required to attend. Management should identify a backup for each DSS as well to ensure proper coverage since this work is required to be performed while physically in the building.

Contracting Officers, Contracting Officer Representatives (CORs) and Agreement Managers
All contracting officers, contracting officer representatives, and agreement managers will (i) include the applicable privacy FAR clauses and applicable SORNS, security clauses and standards in their assigned contracts; (ii) identify the types of CUI the agreement contains; (iii) include the appropriate CUI requirements of the DOC *CUI Policy* in all agreements; and (iv) ensure contractors receive training on CUI before reporting to work as part of their Data Stewardship and IT Security Awareness Training and any needed targeted trainings on specified categories of CUI they will be handling.

Authorized Holder of CUI
An authorized holder of CUI is an individual, agency, organization, or group of users who have a lawful government purpose to handle or designate CUI. Being an authorized holder is a result of Federal employees, contractors, or those with another type of lawful government purpose conducting their official duties. There is no formal process for appointment, though agency policies, contracts, and information sharing agreements may specify who under those authorities may handle or designate particular categories of CUI. Only authorized holders may apply [NARA] ISOO-approved Limited Dissemination Controls to agency information and they may apply them only for a lawful government purpose.

Supervisors and Managers
All supervisors and managers will (i) review and ensure that all documents within their area's purview containing CUI are properly marked in accordance with this policy; (ii) verify that all physical safeguarding measures for individual workspaces are adequate for the protection of CUI (i.e., prevent unauthorized access) annually; (iii) verify that all electronic and paper safeguarding measures are adequate for the protection of CUI (i.e., prevent unauthorized access) annually; (iv) ensure that all personnel under their purview receive Data Stewardship and IT Security Training to make them aware of information handling for categories handled by their office that are not major categories at the Census Bureau; and (v) comply with CUI Guidance provided by DOC and the Census Bureau.

All Staff
All Census Bureau employees, contractors, and individuals with Special Sworn Status are responsible for adhering to all regulatory requirements and internal data stewardship 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. This also includes managing, marking, and protecting CUI in accordance with applicable laws, regulations and government-wide policies. Staff are responsible for following all security controls mandated by the Census Bureau and all procedures laid out in the Information Handling Guidelines and for reporting information security incidents and incidents where CUI markings have been misapplied or misused.

EFFECTIVE DATE

This policy is effective upon signature.

LEGAL AUTHORITIES

Title 5, U.S.C., *Government Organization and Employees*

Title 13, U.S.C., *Census*

Title 26, U.S.C., *Internal Revenue Code*

Confidential Information Protection and Statistical Efficiency Act (CIPSEA)

Federal Information Security Modernization Act (FISMA)

32 CFR Part 2002, "Controlled Unclassified Information"

OMB Memorandum M-01-05, *Guidance on Inter-Agency Sharing of Personal Data - Protecting Personal Privacy* (December 20, 2000)

OMB Memorandum M-14-06, *Guidance for Providing and Using Administrative Data for Statistical Purposes* (February 14, 2014)

OMB Memorandum M-16-04, *Cybersecurity Strategy and Implementation Plan (CSIP) for Federal Civilian Government* (Oct. 30, 2015),

OMB Memorandum M-16-24, *Role and Designation of Senior Agency Officials for Privacy* (September 15, 2016)

OMB Memorandum M-17-12, *Preparing for and Responding to a Breach of Personally Identifiable Information* (January 3, 2017)

OMB Circular A-108, *Federal Agency Responsibilities for Review, Reporting, and Publication under the Privacy Act* (December 23, 2016)

OMB Circular A-123, *Management's Responsibility for Enterprise Risk Management and Internal Control* (July 15, 2016)

OMB Circular No. A-130, *Managing Information as a Strategic Resource* (July 28, 2016)

Executive Order 13556, *Controlled Unclassified Information*, November 4, 2010

IMPLEMENTATION

Individuals and program areas are responsible for implementation of this policy. With the signing of this policy, trained staff within the program areas may begin applying CUI markings. However, as the Census Bureau transitions to the new labeling schema, staff may also continue using legacy markings as appropriate. Program areas should begin planning to revise procedures and systems to come into compliance.

Staff are not permitted to use CUI markings on Federal Tax Information until the Census Bureau receives approval from the Internal Revenue Service (IRS) and updates are made to IRS PUB-1075. Additionally, staff should consult any applicable agreements as well as the sponsoring agency before applying CUI markings to information collected on behalf of another agency under CIPSEA.

The Policy Coordination Office and the Census Bureau's CUI Implementation Team will develop additional guidance and training on CUI marking and safeguards. Upon the roll out of further revisions to this policy, as well as a comprehensive CUI training, CUI markings will be made mandatory. Staff with questions can find more information on the Policy Coordination Office's CUI SharePoint page [redacted] or by sending an email to pco.cui@census.gov

RELATED DOCUMENTS

Department of Commerce, *Controlled Unclassified Information (CUI) Policy*

Department of Commerce, *Controlled Unclassified Information (CUI) Guidelines*

Department of Commerce, *Waiver of Controlled Unclassified Information Marking Requirements for Legacy Information and Data* (August 14, 2019)

National Institutes of Standards and Technology, *NIST Special Publication 800-171 Rev. 2: Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations* (February 2020)

Internal Revenue Service Publication 1075.

POLICY OWNER

The Policy Coordination Office owns this policy.

SIGNATURE

RON JARMIN Digitally signed by RON JARMIN
Date: 2021.10.05 08:49:15
-04'00'

Ron Jarmin
Chair, Data Stewardship Executive Policy Committee
U.S. Census Bureau

Summary Information	
Policy Title:	DS007: Safeguarding and Managing Information
Date Signed:	See Signature Date
Last Reviewed:	9/28/2021
Intended Audience:	All Staff
Policy Owner:	Policy Coordination Office
Office Responsible for Implementation:	All Offices
Office Responsible for Dissemination:	All Offices
Stakeholder Vetting:	CUI Cross-Directorate Implementation Team, DSEP, Bargaining Unit

Quick Reference Guide for Roles and Responsibilities

Role Title	Responsibilities	Agency Level
Data Stewardship Executive Policy Committee (DSEP)	• Makes policy decisions on issues related to privacy, security, and confidentiality. • Ensures the methods of collection and uses of data adhere to legal, ethical, and reporting obligations.	• **Chair:** Deputy Director/ Chief Operating Officer • **Members:** Designated Associate and Assistant Directors, Chief Privacy Officer, and other Senior Officials (see charter) • **Staff:** Policy Coordination Office
Chief Privacy Officer (CPO)	• Ensures compliance with privacy laws • Works with program areas to ensure privacy protections in data collection, processing, and dissemination • Consults with all agency officials in this policy on issues of privacy and confidentiality	• Chief, Policy Coordination Office
Chief Information Officer (CIO)	• Designates Senior Agency Security Officer • Develops and maintains information security policies, procedures and techniques to address requirements. • Ensures information security personnel are adequately trained. • Assists senior officials in their security related responsibilities. • Reports annually to the Director of the Census Bureau on the state of its security program. • Assesses all Census Bureau systems that contain CUI and ensures they meet all required security controls from FIPS PUB 199 and 200 and NIST SP 800-53 for Federal information systems that process, store, and transmit CUI. • Ensures the Census Bureau applies NIST SP 800-171 when establishing security requirements to protect CUI's privacy and confidentiality on non-federal information systems. • Ensures DSEP policies are implemented in IT security procedures.	• Chief Information Officer

Role Title	Responsibilities	Agency Level
Chief Information Security Officer (CISO)	• Carries out CIO's security responsibilities under FISMA. • Serves as the CIO's liaison to the organization's Authorizing Officials, Information System Owners, and Information System Security Officers.	• Chief Information Security Officer
Authorizing Official	• Assumes responsibility for operating a system at an acceptable level of risk. • Designates the Information System Owner(s) and the Information Owner(s). • Ensures that the Information System Owner(s) and the Information Owner(s) are adhering to all applicable policies.	• Associate Director (1 per system)
Information System Owner	• Responsible for the overall procurement, development, integration, modification and/or operation and maintenance of an information system. • Develops and maintains system security plans. • Consults with the Information Owner(s) to gather requirements needed to establish and implement controls for information generation, collection, processing, dissemination, and disposal.	• Division Chief or Assistant Division Chief (1 per system)
Information System Security Officer (ISSO)	• 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. • Manages day-to-day security of an information system. • Assists in developing and assessing system security policies and plans, and ensuring compliance.	• Technical Representative for a system, a system may have one or more Information System Security Officers
Information Owner	• Establishes rules for lifecycle use and protection of specified information (such as datasets, systems of records, etc.). • Retains responsibility for information even when shared with other organizations. • Has input to the requirements to ensure the correct level of required security measures are implemented by the appropriate Information System Owner. • Ensures Privacy Impact Assessments are conducted.	• Staff member of grade 14 or higher

Role Title	Responsibilities	Agency Level
CUI Point of Contact (CUI POC)	• Conducts oversight actions to ensure compliance within their area of responsibility and report findings at least annually to the Department of Commerce CUI Program Manager (DOC CUI PM). • Serves as the Census Bureau's CUI subject matter expert, responding to most inquiries from their organizations and consulting with the CUI PM on questions beyond their expertise. • Ensures all personnel within the Census Bureau complete initial and annual training as required and reports the progress of training to the DOC CUI PM. • Conducts annual Census Bureau self-inspections of the CUI Program, according to guidance provided by the DOC CUI PM, to reflect the progress of implementation and reporting those self-inspections to the DOC CUI PM. • Working with CIO delegated offices to report instances of potential CUI misuse, violation, or infractions in accordance with the DOC Computer Incident Response Plan and keep track of violations for reporting purposes, the DOC CUI PM will be notified through the incident response process. • Confirms their status as a CUI POC with the DOC CUI PM on a semi-annual basis (by the dates designated by the CUI PM) and provides notification within five business days if their status changes.	• Staff member designated by DSEP.
Contracting Officers, Contracting Officer Representatives (CORs) and Agreement Managers	• Include the applicable security clauses and standards in their assigned contracts as well as privacy FAR clauses and applicable SORNs. • Identify the types of CUI the agreement contains. • Include the appropriate CUI requirements on the DOC *CUI Policy* in all agreements. • Ensure contractors receive training on CUI and privacy requirements prior to beginning work.	• Staff members assigned by divisions.

Role Title	Responsibilities	Agency Level
CUI Implementation Team	• Help the CIO and the CUI POC establish the Census Bureau's CUI Program. • Ensure it is being implemented within their respective directorates. • Help the CIO and CUI POC report to the DOC CUI PM. • Conduct an inventory of categories of CUI handled by their respective directorates and how they are labeled. • Make their directorates aware of new categories of CUI if their directorates handle that CUI. • Investigate CUI incidents for categories of CUI handled predominantly by their area.	• Chair – CUI POC • Representatives from program areas and OCIO
Data Security Steward	• Serves as point of contact for: the Policy Coordination Office (PCO) for privacy and confidentiality concerns; the CUI POC for CUI implementation milestones and annual self-inspections of their respective divisions; IRS Safeguards Reviews; as well as the Office of Security (OSY) for physical security reviews. • Monitors, reviews, and maintains all print and disposal logs in their designated area as required under IRS Pub 1075, other statutes. • Disseminates information from OSY, the CUI POC, and PCO on Title 26, the Privacy Act (Title 5), the CUI Program, physical security, and data stewardship. • Helps conduct oversight actions to ensure compliance within their division and report findings at least annually to the CUI POC for CUI reporting to the DOC	• Staff member designated by Division Chief
Supervisors and Managers	• Review and ensure that all documents within their area containing CUI are properly marked in accordance with this policy, as needed. • Verify that all physical safeguarding measures for individual workspaces are adequate for the protection of CUI (i.e., prevent unauthorized access) annually. • Verify that all electronic and paper safeguarding measures are adequate for the protection of CUI (i.e., prevent unauthorized access) annually.	• All Census Bureau managers and supervisors

Role Title	Responsibilities	Agency Level
	• Ensure that all personnel under their purview receive CUI training as required by this policy along with the required Data Stewardship and IT Security Training • Comply with CUI Guidance provided by DOC and the Census Bureau.	
All Staff	• Are responsible for knowing, applying, and following all appropriate security controls deemed necessary and mandated by the U.S. Census Bureau and Federal Government. • Complete all initial, recurring Data Stewardship and IT Security Awareness Trainings and CUI Specified trainings within the required timeframes. Additionally, the Privacy in Small Bites modules are highly recommended. • Manage, mark, and protect CUI in accordance with this policy and national directives. • Ensure that sensitive information currently stored as legacy material that is annotated as For Official Use Only (FOUO), Sensitive But Unclassified (SBU), or that contains other legacy security markings is re-marked as CUI before the information leaves the DOC. Only markings that are contained in the NARA CUI Registry may be used to annotate CUI. • Report information security and incidents CUI misuse and mismarking as needed to BOC-CIRT.	• All Census Bureau employees, contractors, and other Special Sworn Status individuals

Detailed Information Handling Guidelines

This attachment provides detailed descriptions for identifying which law or administrative restrictions protect various kinds of information, and it provides specific guidelines for handling each information type commonly in use at the Census Bureau. For each information type, it discusses marking, printing, managing paper copies, mailing and shipping, email, faxing, other forms of electronic transmission/online collaboration, teleworking, scanning, electronic storage, and disposing of the information.

Most of the information types are controlled unclassified information (CUI) and require CUI safeguards and markings under Federal CUI regulations. This document is not intended to be a comprehensive source for all CUI and program areas are encouraged to reference: (1) Department of Commerce (DOC), *Controlled Unclassified Information (CUI) Policy*, dated August 2019; and (2) DOC, *Controlled Unclassified Information (CUI) Guidelines*, dated August 2019, or contact the CUI POC in the Policy Coordination Office for specific questions on any CUI categories not referenced here.

Definitions:

CUI Basic is the subset of CUI for which the authorizing law, regulation, or Government-wide policy does not set out specific handling or dissemination controls. Agencies handle CUI Basic according to the uniform set of controls set forth in 32 CFR § 2002 and the CUI Registry. CUI Basic differs from CUI Specified (see definition for CUI Specified in this section), and CUI Basic controls apply whenever CUI Specified ones do not cover the involved CUI.

CUI Specified is the subset of CUI in which the authorizing law, regulation, or Government-wide policy contains specific handling controls that requires or permits agencies to use procedures and protections that exceed those for CUI Basic. The CUI Registry indicates which laws, regulations, and Government-wide policies include such specific requirements. CUI Specified controls may be more stringent than, or may simply differ from, those required by CUI Basic; the distinction is that the underlying authority spells out specific controls for CUI Specified information and does not for CUI Basic information. CUI Basic controls apply to those aspects of CUI Specified where the authorizing laws, regulations, and Government-wide policies do not provide specific guidance. Title 13 information, Title 26 information, Title 5 Personnel Records, Title 5 Sensitive Personally Identifiable Information (PII), and CIPSEA information are CUI Specified.

Document: Under federal regulations covering controlled unclassified information, 32 CFR § 2002.4(w), “document” includes but is not limited to reports, computer files, tabulations, electronic matter, and data compilations from which information can be obtained, including materials used in data processing. Document also includes voice records, film, tapes, video tapes, emails, and memoranda, in addition to the file, folder, exhibits, and containers, the labels on them, and any metadata, associated with each original or copy.

Marking CUI

As of the issuance of this policy, staff and program areas may begin marking CUI and replacing legacy markings where appropriate and with guidance from their managers. Personnel will receive additional notice and instruction at which point all new files and documents containing CUI, as well as legacy materials that are leaving the DOC boundaries must be marked with a CUI banner marking or alternative bulk marking method as stipulated in the 32 CFR § 2002 and additional CUI Notices on alternative markings on the NARA CUI website.

Elements of a CUI Banner Marking: In general, a CUI banner marking consists of the CUI control marking, which is the abbreviation CUI, followed by two slashes (//) and the category markings for every category of CUI in the file or other document, and then two slashes and the limited dissemination control marking if a limited dissemination control has been applied to the information. Any time a document or file comingles multiple categories of CUI, the labeling and

handling requirements are cumulative. The banner marking must include CUI category markings for all the categories of CUI in the document. Multiple category markings in a banner marking must be separated by a single forward slash (/), and the category markings for specified information must come first and be alphabetized by category marking. Then the banner marking must include category markings for all categories of CUI basic information also alphabetized by category marking. For example, the header of a comingled Title 13 and Title 26 dataset would read CUI//SP-CENS/SP-TAX; and the filename, where feasible, could include an indication that the file contains CUI for example, dataextract__CUI_SP-CENS__SP-TAX.csv.

If applicable, the last portion of the CUI banner marking will be the limited dissemination control marking. The National Archives and Records Administration (NARA) has published a list of limited dissemination control markings that can be applied. These markings appear in the CUI Registry and include such controls as FED ONLY (Federal Employees Only), NOCON (No dissemination to contractors), and DL ONLY (Dissemination authorized only to those individuals or entities on an accompanying distribution list). Limited dissemination control markings are preceded by a double forward slash (//). The only limited dissemination control markings allowed in a CUI banner marking are those approved by NARA and listed in the CUI Registry.

CUI Basic -- Minimum Safeguarding Requirements for All CUI

This section outlines the minimum safeguarding requirements for all forms of CUI which includes all categories of CUI Basic information. CUI Specified information has additional safeguarding requirements beyond those covered here. These additional requirements are covered later in this document.

All CUI must be protected from access, overhearing, or observation by unauthorized persons. That is--persons without a business need to know the information; persons who are not authorized by a law, regulation, or government-wide policy to access it; or persons who are prohibited from accessing it by law, regulation, or policy or dissemination control.

In the Census Bureau's open office environments, personnel should be aware of CUI being viewed on a computer screen and should find a private area for CUI-related discussions. A CUI cover sheet may be used to protect printed material while in use, but CUI must be locked away when unattended.

Storage

CUI documents must be secured in a locked location (ex: locked office, locked cabinet, locked drawer, locked storage room) when not in use. This applies to CUI in hard copies and electronic media.

CUI stored on removable storage must be password protected.

Any cabinets or other storage devices containing CUI information must be labeled as containing CUI. Where it is not feasible to place signs/labels on all cabinets or boxes in a storage area, signage may be placed on the nearest access-controlled door.

Electronic Documents:
Information systems processing, storing, or transmitting CUI must meet the security and privacy protections at the moderate baseline as defined in NIST Special Publication 800-53 and the Census Bureau’s IT Security Program Policy.

Electronic documents containing CUI Basic information must have a CUI banner marking CUI followed by the relevant CUI category marking(s) in the document and centered in the header and separated from any other text.

Electronic Transmission and Online Collaboration
Unless otherwise specified, O365 is approved for transmitting CUI Basic information internally between Census Bureau users. Approved encryption methods, such as Kiteworks or WinZip, should be used to send CUI to external agencies or third parties permitted to receive that CUI.

When faxing, care must be taken to ensure the intended recipient receives the information, and their receipt should be verified.

Microsoft Teams is the only platform authorized for video conferencing and screen sharing with CUI.

Mailing and Shipping:
When mailing or shipping CUI Basic information, the media must be double wrapped.

The outer wrapping must specify that the package or envelope is for delivery only to a specific recipient, preferably an individual where possible. The outer wrapping should be opaque and NOT indicate that the package or envelope inside it contains CUI.

The inner wrapping must be opaque, tamper-evident, and be labeled as follows:

CUI//Category Marking
To be opened by addressee only

Disposal:
Dispose of hard copies of CUI Basic information in a locked blue bin designated for sensitive materials if you are working at Census Bureau HQ, or in an approved bin for multi-step destruction in other Census Bureau facilities.

If you are in a facility without one of the above and if shredding is the only step being used in destruction, the document must be shredded to pieces no larger than 1mm by 5 mm. Otherwise, the CUI documents must be sent securely to another authorized Census Bureau facility for destruction.

Information Handling Guidelines for Major Categories of CUI Handled at the Census Bureau

Title 13 Information

Marking:

CUI//SP-CENS
Disclosure Prohibited: Title 13 U.S.C.

Legacy Marking:

Disclosure Prohibited: Title 13 U.S.C. (or similar)

Description:
Title 13 information is a category of CUI Specified Information also known as Census Information. Historically, this information may have also been referred to as "Census Confidential Information." Title 13, U.S.C. protects information collected from or on behalf of a respondent, as well as information the Census Bureau acquires from administrative sources, and information in our address lists and sampling frames. Title 13 prohibits disclosure of this information to anyone who is not sworn to uphold the oath of non-disclosure (also known as special sworn status individuals) and who does not have a need to know. Title 13 information should remain exclusively in possession of the Census Bureau and may not be transmitted to another federal agency, contractor, or other entity except as permitted under the *DS006 – Controlling Non-Employee Access to Title 13 Information* Policy. 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 non-exhaustive list of information protected by Title 13:

- All respondent personally identifiable information (PII) and business identifiable information (BII);
- All individual census or survey responses;
- Respondent contact information;
- Address lists and frames including the Master Address File (MAF);
- Administrative data from other agencies (not including the Federal Tax Information from the IRS) or Third-party data acquired by the Census Bureau under the authority of Title 13;
- Any aggregation of statistical information (including geographic products) based on a Title 13 protected source that has not been approved for release by the Census Bureau's Disclosure Review Board process.

Electronic Documents:
Electronic documents containing Title 13 information must have a CUI banner marking (or appropriate alternative or bulk marking) with CUI//SP-CENS centered in the header and separated from any other text. They will also still have the label Disclosure Prohibited--Title 13 U.S.C. below the CUI marking.

The filename, where feasible, could include CUI_SP-CENS at the end of the filename immediately preceding the file extension. Examples: presentation_CUI__SP-CENS.pptx OR eclipse_ CUI__SP-CENS _2017-08-21.pptx

Paper Documents:
Printed documents as well as any handwritten documents containing Title 13 information must have the CUI//SP-CENS banner marking in the header on every page of the document.

Paper documents must also have the label Disclosure Prohibited--Title 13 U.S.C. below the CUI marking.

Title 13 information must be kept locked in a desk or file cabinet when not in use.
Access must be restricted to only those Census Bureau staff, contractors, or other special sworn status individuals with a business need to know.

Hard copies must not be removed from secure Census Bureau facilities, even for teleworking.

Printing:
Title 13 information may only be printed via private (secure) printing, and printouts must be removed immediately from the printer.

Mailing and Shipping:
When mailing or shipping Title 13 information, the media (paper documents, hard drives, DVDs, etc.) must be double wrapped and shipped using an approved traceable carrier.

The outer wrapping must specify that the package or envelope is for delivery only to a specific recipient, preferably an individual where possible. The outer wrapping should be opaque and NOT indicate that the package or envelope contains Title 13 information.

The inner wrapping must be opaque, tamper-evident, and be labeled as follows:

Legacy Labeling:

Disclosure Prohibited--Title 13 U.S.C.
To be opened by addressee only.

CUI Labeling:

CUI//SP-CENS
Disclosure Prohibited--Title 13 U.S.C.
To be opened by addressee only.

The CUI marking CUI//SP-CENS must be distinguishable from other information in the label.

To prevent loss when the outer wrapping/packaging is damaged, the inner wrapping also must be addressed to a specific recipient, preferably to an individual wherever possible.

Electronic Transmission and Online Collaboration:

Email:
The Census Bureau Office 365 email system is not approved for use with Title 13 information. Title 13 information may not be included in the body of an email, subject line, or as an unencrypted attachment. It must be encrypted with an approved encryption method before transmission, even to another user on the Census Bureau network. Send the file using an approved encryption method such as Kiteworks (https://sfc.doc.gov/). Do not include Title 13 information in the subject line of a Kiteworks message, or in the body unless you enable message protection. The attachment may also be encrypted and password protected via WinZip and attached to an email sent from the Outlook Web App.

Faxing:
When faxing Title 13 information, ensure that someone is at the machine to receive it. Do not fax to an electronic fax service that delivers the fax to the final recipient by email.

When a transmittal document such as a FAX cover page accompanies Title 13 information, the transmittal document must indicate that CUI is attached or enclosed. The transmittal document must also include conspicuously on its face, the following instructions:

"When attachment/enclosure is removed, this document is Uncontrolled Unclassified Information" or

"When attachment/enclosure is removed, this document does not contain CUI."

Other Forms of Electronic Transmission:
Microsoft Teams is the only platform authorized for video conferencing and screen sharing with Title 13 data. See the guidance on *Using Microsoft Teams to Share Title 13 Data, Title 26 Data, and Sensitive PII* for more instructions.

[redacted]

Note: The transmission of a document containing CUI, by a means that is not accredited to hold that CUI, is an unauthorized disclosure. Such disclosures must be reported to the Bureau of the Census Computer Incident Response Team (BOC CIRT) at 301-763-3333 or 866-300-7063 as soon as possible but no later than 1 hour after discovery.

Document Sharing/Collaboration:
Documents may be shared using network drives, sent securely to other individuals on the Census Bureau network using Kiteworks or shared via restricted access on-premises SharePoint sites. If you have questions about using a secure SharePoint site for this purpose, contact your Site Collection Admin.

Other forms on online collaboration with sponsoring agencies of Title 13 information collections may be allowed if they have been authorized by OIS and the corresponding information security offices at the other agency, as well as the Policy Coordination Office.

Teleworking*:*
During telework or working remotely, only access Title 13 information through approved Census Bureau remote access technology (such as VDI or VPN) at your approved telework location(s) or place of performance (for contractors). Do not email or use any file-sharing technology to send Title 13 information to yourself for use on personally owned equipment.

Do not remove hardcopies of Title 13 protected information from a secure Census Bureau facility for use in telework.

Scanning:
Title 13 information should only be scanned using a scanner that is approved for use with controlled information. Typically, this will be a scanner that is physically connected to a workstation, or a networked scanner that can save files directly in a file share. Do not use a scanner that delivers scanned documents by email.

Electronic Storage:
Information systems require an Authority To Operate (ATO) signed by the Chief Information Officer that permits the storage and processing of Title 13 information.

In addition to authorized research and production systems, Title 13 information may be also be stored on:

Microsoft Windows file share drives (e.g., H:\, M:\ and others)

Microsoft SharePoint on-premises servers (also known as, On-Prem SharePoint and sites that begin with [redacted]) operated within the Census Bureau.

While Microsoft Windows C:\ drives are secure enough to store/process Title 13 data, good business practice, as far as recoverability, dictates they should be kept in the shared file drives listed above.[5]

It is **prohibited** to store or share Title 13 information on Office365 Services. These include SharePoint Online, OneDrive, Office 365 Collaboration Groups, MS Teams[6], and the Outlook Web Application (OWA).

Physical Space for Access:
With the exception of individuals performing authorized field activities, access Title 13 information only from approved restricted access space (These include Census Bureau Headquarters North building above the second floor, Census Bureau Regional Offices, the Bowie Computing Center, Federal Statistical Research Data Centers (FSRDCs), Off-site Locations approved by the Data Stewardship Executive Policy Committee (DSEP), approved telework sites, and contractor remote place of performance sites approved by DSEP.)

It is prohibited to access Title 13 information from public spaces, including the first floor of the Census Bureau headquarters and second floor training rooms.

Disposal:
At headquarters, dispose of hard copies in a locked blue bin designated for sensitive materials.

Dispose of electronic copies (tapes, CDs, disks, etc.) in a locked blue bin or contact the Records Management Branch at 301-763-2282 for instructions.

Field staff should follow guidance on shipping materials to the Regional Office for destruction.

Title 13 Controlled Unclassified Information and Limited Dissemination Control Markings

Description:
Some Title 13 information requires additional handling controls because of its sensitivity. Such information is restricted within the Census Bureau to individuals that have a specific "need to know" in order to perform their official duties. Such information should be marked with the appropriate limited dissemination control marking (LDCM) and stored with additional access controls to assure that the information will be restricted to appropriate individuals, offices, or organizations. Controls can include file storage areas that are restricted with access control lists and documents encrypted with document-specific encryption passphrases.

The National Archives and Records Administration (NARA) has published LDCMs and only those approved by NARA and published in the CUI Registry are allowed as part of the CUI Banner Marking. Most typically Census Bureau program areas will use the LDCM "DL ONLY" which means that the dissemination is authorized only to those individuals or

[5] Note: Acceptable Use Policy for Census Bureau Information Technology Resources (IT AUP) states "work related files are not to be stored on any workstation's hard drive (the C:\ drive)" because such files are not backed up. However, the operation of Microsoft Windows inherently stores information from documents on the C:\ drive in the form of downloaded files, temporary files, and virtual memory page files. As such, any computer that is used to process controlled information should use drive-level encryption for all fixed storage, such as the Windows C:\ drive. Linux systems should be configured to use the Linux Unified Key Setup-on-disk-format (OUKS) to encrypt all Linux partitions, including partitions used for file systems and for virtual memory.

[6] Except as permitted per: [redacted]

entities on an accompanying distribution list. For example, a person creating a decision document on a new disclosure avoidance practice might mark it CUI//SP-CENS//DL ONLY and the accompanying list would either say it is restricted to the Disclosure Review Board or to listed individuals.

Title 26 Information

Special Note: Use of CUI markings on Federal Tax Information will not go into effect until the Census Bureau receives guidance from the Internal Revenue Service based on implementation of its own CUI program. Until further guidance is issued, staff should continue to use legacy markings as outlined in the Title 26 Awareness Training and other related documents in accordance with IRS PUB 1075. Aside from the document marking guidance below, the other handling requirements outlined in this section are consistent with current IRS guidelines and should be followed.

Marking:

CUI//SP-TAX
Disclosure Prohibited—Federal Tax Information Protected by Title 26 U.S.C.

Legacy Marking:

Disclosure Prohibited –Federal Tax Information Protected by Title 26 U.S.C.

Description:
Federal Tax Information (FTI) is a category of CUI Specified Information. All Federal Tax Information (FTI) is protected by Title 26, U.S.C. It is also called Federal Taxpayer Information. This information is provided to the Census Bureau through agreements with the Internal Revenue Service and includes:

- Fact of Filing information;
- All files containing information from federal tax forms, the forms themselves, and some data from state tax forms;
- Record layouts for datasets that are protected by Title 26;
- Flags derived solely from FTI;
- Any dataset that is commingled with data that is protected by Title 26;
    - Ex. The Business Register;
- Any aggregation of statistical information (including geographic products) based on a Title 26 protected source that has not been approved for release by the Census Bureau's Disclosure Review Board process.

Electronic Documents:
Access must be restricted to only those Census Bureau staff, contractors, or other special sworn status individuals working on an approved Title 26 project and with a business need to know.

Electronic documents containing Title 26 information must have a CUI banner marking (or appropriate alternative or bulk marking) CUI//SP-TAX centered in the header and separated from any other text. They will also still have the label Disclosure Prohibited—Federal Tax Information Protected by Title 26 U.S.C.

The filename, where feasible, could include CUI_SP-TAX at the end of the filename immediately preceding the file extension. Examples: presentation_CUI__SP-TAX.pptx OR eclipse_ CUI__SP-TAX _2017-08-21.pptx

Paper Documents:
Restrict access to only those Census Bureau staff or individuals with special sworn status with a business need to know who are on an approved Title 26 project.

Keep locked in a desk or file cabinet when not in use. The file cabinet must be labeled as containing Title 26 information.

Do not remove hard copies from secure Census Bureau facilities, even for teleworking. Printed documents as well as any handwritten documents containing Federal Tax Information must have the label Disclosure Prohibited—Federal Tax Information Protected by Title 26 U.S.C. below any CUI marking for other CUI in the document.

Printing:
Title 26 information may only be printed via private (secure) printing, and printouts must be removed immediately from the printer. Log any printed document containing Title 26 information in the print log next to the printer used to ensure tracking of hard copies.

Mailing and Shipping:
When mailing or shipping Title 26 information, the media (paper documents, hard drives, DVDs, etc.) must be double wrapped and shipped using an approved traceable carrier.

The outer wrapping must specify that the package or envelope is for delivery only to a specific recipient, preferably an individual where possible. The outer wrapping should be opaque and NOT indicate that the package or envelope inside it contains Title 26 information.

The inner wrapping must be opaque, tamper-evident, and be labeled as follows:

Legacy Labeling:

Disclosure Prohibited—Federal Tax Information Protected by Title 26 U.S.C.
To be opened by addressee only.

CUI Labeling:

CUI//SP-TAX
Disclosure Prohibited—Federal Tax Information Protected by Title 26 U.S.C

To be opened by addressee only.

To prevent loss when the outer wrapping/packaging is damaged, the inner wrapping also must be addressed to a specific recipient, preferably to an individual wherever possible.

Electronic Transmission and Online Collaboration:

Email:
The Census Bureau Office 365 email system is not approved for use with Title 26 information. Title 26 information may not be included in the body of an email, subject line, or as an unencrypted attachment. It must be encrypted with an approved encryption method before transmission, even to another user on the Census Bureau network. Send the file using an approved encryption method such as the DOC Kiteworks software (https://sfc.doc.gov/). Do not include Title 26 information in the subject line of a Kiteworks message, or in the body unless you enable message protection. The attachment may also be encrypted and password protected via WinZip and attached to an email sent from the Outlook Web App.

Faxing:
When faxing Title 26 and other controlled information, ensure that someone is at the machine to receive it. Do not fax to an electronic fax service that delivers the fax by email.

When a transmittal document such as a FAX cover page accompanies Title 26 information, the transmittal document must indicate that CUI is attached or enclosed. The transmittal document must also include conspicuously on its face, the following instructions:

"When attachment/enclosure is removed, this document is Uncontrolled Unclassified Information" or

"When attachment/enclosure is removed, this document does not contain CUI."

Other Forms of Electronic Transmission:
Microsoft Teams is the only platform authorized for video conferencing and screen sharing with Title 26 data. See the guidance on *Using Microsoft Teams to Share Title 13 Data, Title 26 Data, and Sensitive PII* for more instructions.

[redacted]

Note: The transmission of a document containing CUI, by a means that is not accredited to hold that CUI, is an unauthorized disclosure. Such disclosures must be reported to the Bureau of the Census Computer Incident Response Team (BOC CIRT) at 301-763-3333 or 866-300-7063 as soon as possible but no later than 1 hour after discovery.

Document Sharing/Collaboration:
Documents may be shared using network drives or sent securely to other individuals on the Census Bureau network using Kiteworks or another approved encryption solution.

Teleworking:
Only Census Bureau employees and specifically authorized Special Sworn Status individuals and contractors[7] may access Title 26 information while teleworking or working remotely. Staff may only access Title 26 information through approved Census Bureau remote access technology (such as VDI or VPN) at their approved telework location(s). Staff may not email or use any file sharing technology to send Title 26 information to themselves for use on personally owned equipment.

Do not remove hardcopies of Title 26 information from a Census Bureau facility for use while teleworking.

Scanning:
Title 26 information should only be scanned using a scanner that is approved for use with controlled information. Typically, this will be a scanner that is physically connected to a workstation, or a networked scanner that can save files directly in a file share. Do not use a scanner that delivers scanned documents by email.

Electronic Storage:
Information systems require an Authority To Operate (ATO) signed by the Chief Information Officer before they may be used to store Title 26 information

In addition to authorized research and production systems, Title 26 information may be also be stored on:

Microsoft Windows file share drives (ex H:\, M:\ and others)

[7] Subject to approval by the Internal Revenue Service.

While Microsoft Windows C:\ drives are secure enough to store/process Title 26 data, good business practice, as far as recoverability, dictates they should be kept in the shared file drives listed above.

It is **prohibited** to store or share Title 26 information on Office365 Services. These include SharePoint Online, OneDrive, Office 365 Collaboration Groups, MS Teams[8], and the Outlook Web Application (OWA). It is also prohibited to store Title 26 information on On-Prem SharePoint.

Physical Space for Access:
With the exception of individuals performing authorized field activities, access Title 26 information only from restricted access space (These include Census Bureau Headquarters above the second floor, Census Bureau Regional Offices, the Bowie Computing Center, Federal Statistical Research Data Centers (FSRDCs),), Off-site Locations approved by the Data Stewardship Executive Policy Committee (DSEP) and the IRS, approved telework sites, and contractor remote place of performance sites approved by DSEP and the IRS.

It is prohibited to access Title 26 information from public spaces, including the first floor of the Census Bureau headquarters and second floor training rooms.

Disposal:
Dispose of hard copies of Title 26 information in a locked blue bin designated for sensitive materials.

Log disposal and destruction of all hard copies using disposal logs located in printing rooms.

Dispose of electronic copies (tapes, CDs, disks, etc.) in a locked blue bin or contact the Records Management Branch at 301-763-2282 for instructions.

Field staff should follow guidance on shipping materials to the Regional Office for destruction.

---

[8] Except as permitted per [redacted]

CIPSEA Information

Special Note: Most CIPSEA information at the Census Bureau is collected through surveys sponsored by other statistical agencies. The Census Bureau will defer to the sponsoring statistical agency on labeling and safeguarding requirements for information we collect on their behalf. Eventually we anticipate that these agencies will adopt the CUI program as well and we will transition accordingly.

Where specific safeguarding requirements are not otherwise specified by the sponsoring agency or through an agreement, or in unique circumstances where we use CIPSEA to collect data on behalf of a non-statistical agency and therefore are the designated agent responsible for safeguarding the information, the guidelines below should be followed.

Marking:

CUI//SP-STAT

Description:
The *Confidential Information Protection Statistical Efficiency Act of 2002* ensures that information supplied by individuals or organizations to an agency for statistical purposes under a pledge of confidentiality is used exclusively for statistical purposes. It also ensures that individuals or organizations who supply information under a pledge of confidentiality to agencies for statistical purposes will neither have that information disclosed in identifiable form to anyone not authorized by CIPSEA nor have that information used for any purpose other than a statistical purpose.

In general, CIPSEA protects information collected when the Census Bureau conducts surveys and data collections for other statistical agencies or statistical units of non-statistical agencies and the data collection does not depend on a Title 13 sampling frame.

Examples of CIPSEA data include:

--Data collected by and for the National Hospital Ambulatory Medical Care Survey (NHAMCS)

--Data collected by and for the National Ambulatory Medical Care Survey (NAMCS)

--Data collected by and for the National Health Interview Survey (NHIS)

--Certain information shared with the Census Bureau by the Bureau of Labor Statistics and the Bureau of Economic Analysis for the purposes of improving North American Industry Classification System codes (NAICS codes)

In some cases, though, data for reimbursable projects are protected by confidentiality provisions or information handling requirements in the sponsoring agency's laws and not Title 13 **or** CIPSEA. Staff should consult the sponsoring agency with questions about safeguarding requirements for these data.

Handling Guidelines for CIPSEA Information:
Data from a reimbursable survey or data collection that uses a non-Census Bureau frame are to be securely transmitted to the sponsoring statistical agency and then are subject to handling guidelines and marking requirements from the sponsoring agency since the data are protected under a legal authority other than Title 13.

Electronic Documents:
Electronic documents containing CIPSEA information must have a CUI banner marking (or appropriate alternative or bulk marking) CUI//SP-STAT centered in the header and separated from any other text.

The filename, where feasible, could include CUI_SP-STAT at the end of the filename immediately preceding the file extension. Examples: presentation_CUI__SP-STAT.pptx OR eclipse_ CUI__SP-STAT _2017-08-21.pptx

Paper Documents:
Printed documents as well as any handwritten documents containing CIIPSEA information must have the CUI//SP-STAT banner marking in the header on every page of the document.

CIPSEA information must be kept locked in a desk or file cabinet when not in use.

Hard copies must not be removed from secure Census Bureau facilities, even for teleworking.

Printing:
CIPSEA information may only be printed via private (secure) printing, and printouts must be removed immediately from the printer.

Mailing and Shipping:
When mailing or shipping CIPSEA Controlled information, the media (paper documents, hard drives, DVDs, etc.) must be double wrapped and shipped using an approved traceable carrier.

The outer wrapping must specify that the package or envelope is for delivery only to a specific recipient, preferably an individual where possible. The outer wrapping should be opaque and NOT indicate that the package or envelope contains CIPSEA information.

The inner wrapping must be opaque, tamper-evident, and be labeled as follows:

CUI SP-STAT

To be opened by addressee only.

To prevent loss when the outer wrapping/packaging is damaged, the inner wrapping also must be addressed to a specific recipient, preferably to an individual wherever possible.

Electronic Transmission and Online Collaboration:

Email:
The Census Office 365 email system is not approved for use with CIPSEA information. CIPSEA information may not be included in the body of an email or as an attachment. It must be encrypted with an approved encryption method before transmission. Send the file using an approved encryption method such as DOC Kiteworks (https://sfc.doc.gov/). Do not include CIPSEA information in the subject line or body of a Kiteworks message unless you enable message protection. The attachment may also be encrypted, and password protected via WinZip and attached to an email sent from the Outlook Web App.

Faxing:
When faxing CIPSEA and other controlled information, ensure that someone is at the machine to receive it. Do not fax to an electronic fax service that delivers the fax by email.

When a transmittal document such as a FAX cover page accompanies CIPSEA information, the transmittal document must indicate that CUI is attached or enclosed. The transmittal document must also include conspicuously on its face, the following instructions:

"When attachment/enclosure is removed, this document is Uncontrolled Unclassified Information" or

"When attachment/enclosure is removed, this document does not contain CUI."

Other Forms of Electronic Transmission:
Microsoft Teams is the ONLY platform authorized for video conferencing and screen sharing with CIPSEA data. You should treat it the same as you would Title 13 information in the guidance in *Using Microsoft Teams to Share Title 13 Data, Title 26, and Sensitive PII*.
[redacted]

Note: The transmission of a document containing controlled information, by a means that is not accredited to hold that controlled information, is an unauthorized disclosure. Such disclosures must be reported to the Bureau of the Census Computer Incident Response Team (BOC CIRT) at 301-763-3333 or 866-300-7063 as soon as possible but no later than 1 hour of discovery.

Document Sharing/Collaboration:
Documents may be shared using network drives, sent securely to other individuals on the Census Bureau network using Kiteworks or shared via on-premises SharePoint sites. If you have questions about using a secure SharePoint site for this purpose, contact your Site Collection Admin.

Other forms on online collaboration with sponsoring agencies of CIPSEA information may be allowed if they have been authorized by OIS and the corresponding information security offices at the other agency.

Teleworking*:*
During telework or working remotely, only access CIPSEA information through approved Census Bureau remote access technology (such as VDI or VPN) at your approved telework location(s) or place of performance (for contractors). Do not email or use any file-sharing technology to send CIPSEA information to yourself for use on personally owned equipment.

Do not remove hardcopies of CIPSEA protected information from a Census Bureau facility for use in telework.

Scanning:
CIPSEA information should only be scanned using a scanner that is approved for use with controlled information. Typically, this will be a scanner that is physically connected to a workstation, or a networked scanner that can save files directly in a file share. Do not use a scanner that delivers scanned documents by email.

Electronic Storage:
Information systems require an Authority To Operate (ATO) signed by the Chief Information Officer before they may be used to store CIPSEA information

In addition to authorized research and production systems, Title 13 information may be also be stored on:

Microsoft Windows file share drives (ex H:\, M:\ and others)

Microsoft SharePoint on-premises servers (also known as On-Prem SharePoint and sites that begin with [redacted]) operated within the Census Bureau.

While Microsoft Windows C:\ drives are secure enough to store/process CIPSEA data, good business practice as far as recoverability dictates they should be kept in the shared file drives listed above.[9]

It is **prohibited** to store or share CIPSEA information on Office365 Services. These include SharePoint Online, OneDrive, Office 365 Collaboration Groups, MS Teams[10], and the Outlook Web Application (OWA).

Physical Space for Access:
With the exception of individuals performing authorized field activities, access CIPSEA information only from restricted access space (These include Census Bureau Headquarters above the second floor, Census Bureau Regional Offices, the Bowie Computing Center, Federal Statistical Research Data Centers (FSRDCs), or locations approved by the sponsoring agency (or DSEP if applicable)).

It is prohibited to access CIPSEA information from public spaces, including the first floor of the Census Bureau headquarters and second floor training rooms.

Disposal:
At headquarters, dispose of hard copies in a locked blue bin designated for sensitive materials.

Dispose of electronic copies (tapes, CDs, disks, etc.) in a locked blue bin or contact the Records Management Branch at 301-763-2282 for instructions.

Field staff should follow guidance on shipping materials to the Regional Office for destruction.

---

[9] Note: Acceptable Use Policy for Census Bureau Information Technology Resources (IT AUP) states "work related files are not to be stored on any workstation's hard drive (the C:\ drive)" because such files are not backed up. However, the operation of Microsoft Windows inherently stores information from documents on the C:\ drive in the form of downloaded files, temporary files, and virtual memory page files. As such, any computer that is used to process controlled information should use drive-level encryption for all fixed storage, such as the Windows C:\ drive. Linux systems should be configured to use the Linux Unified Key Setup-on-disk-format (OUKS) to encrypt all Linux partitions, including partitions used for file systems and for virtual memory.

[10] Except as permitted per [redacted]

Title 5 Information: Sensitive Personally Identifiable Information (SPII)

Markings:

CUI//SP-PRVCY

Description:
Title 5 protects the personally identifiable information (PII) of members of the public and Federal employees. OMB Memorandum M-17-12 describes PII as follows:

> The term PII refers to information that can be used to distinguish or trace an individual's identity, either alone or when combined with other information that is linked or linkable to a specific individual. Because there are many different types of information that can be used to distinguish or trace an individual's identity, the term PII is necessarily broad.[11]

Some PII is sensitive and is considered CUI, 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, even if it is in the category of non-sensitive PII below, is protected under Title 13 in addition to being subject to provisions for reporting breaches involving PII. 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 a Social Security Number (SSN) or where the SSN is redacted
- General background information about individuals found in resumes and biographies
- Position descriptions and performance plans without ratings.

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 business need to know; keeping it away from public view when in use; keeping it secured when not in use; and encrypting it when sent by email. In addition, the information listed above in combination with PII considered sensitive must be given special handling. Some examples of **sensitive PII** (CUI//SP-PRVCY) include:

- SSNs, even if it is just the final four digits of an SSN
- 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 and is therefore not CUI, 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.

[11] OMB Memorandum M-17-12, *Preparing for and Responding to a Breach of Personally Identifiable Information*, January 3, 2017.

Electronic Documents:
Access to SPII must be restricted to only federal employees, contractors, or other individuals with a business need to know.

Electronic documents containing sensitive PII must have a CUI banner marking (or appropriate alternative or bulk marking) of CUI//SP-PRVCY centered in the header and separated from any other text.

The filename, where feasible, could include CUI__SP-PRVCY. Example: extract_CUI__SP-PRVCY.txt

Paper Documents:
Printed documents as well as any handwritten documents containing SPII must have the appropriate CUI banner marking in the header CUI//SP-PRVCY.

Sensitive PII must be kept locked in a desk or file cabinet when not in use.

Do not remove hard copies from secure Census Bureau facilities, even for teleworking.

Printing:
Sensitive PII may only be printed via private (secure) printing. Non-sensitive PII information may be printed with everyday printing.

Immediately remove printouts from the printer.

Mailing and Shipping:
Address packages and parcels that contain Title 5 information for delivery only to a specific recipient, wherever possible address it to an individual. Do not put CUI markings on the outside of an envelope or package, or otherwise indicate on the outside that the item contains CUI.

When mailing sensitive PII, it must be doubled wrapped. The inner wrapping must be labeled as follows:

Legacy Labeling

Disclosure Prohibited--Title 5 U.S.C.
To be opened by addressee only.

CUI Labeling

CUI//SP-PRVCY
Disclosure Prohibited--Title 5 U.S.C.
To be opened by addressee only

The inner packaging must be tamper-evident packaging. To prevent loss when the outer wrapping/packaging is damaged, the inner wrapping also must be addressed to a specific recipient, preferably to an individual wherever possible.

Electronic Transmission

Email:

The Census Bureau Office 365 email system is not approved for use with SPII. SPII may not be included in the body of an email, subject line, or as an unencrypted attachment. It must be encrypted with an approved encryption method before transmission, even to another user on the Census Bureau network. Send the file using

an approved encryption method such as Kiteworks (https://sfc.doc.gov/). Do not include SPII in the subject line of a Kiteworks message, or in the body unless you enable message protection. The attachment may also be encrypted and password protected via WinZip and attached to an email sent from the Outlook Web App.

Faxing:
When faxing SPII, ensure that someone is at the machine to receive it. Do not fax to an electronic fax service that delivers the fax by email.

Other Forms of Electronic Transmission or Online Collaboration:
Only Microsoft Teams is authorized for teleconferencing with Sensitive PII. See the guidance on *Using Microsoft Teams to Share Title 13 Data, Title 26 Data, and Sensitive PII* for more instructions.
[redacted]

Note: The transmission of a document containing controlled information, by a means that is not accredited to hold that controlled information, is an unauthorized disclosure. Such disclosures must be reported to the Bureau of the Census Computer Incident Response Team (BOC CIRT) at 301-763-3333 or 866-300-7063 as soon as possible but no later than 1 hour of discovery.

Teleworking*:*
If teleworking or working remotely, staff may only access Sensitive PII through approved Census Bureau remote access technology (such as VDI or VPN) at their approved telework location(s). Do not email Sensitive PII to yourself for use on personally owned equipment.

Scanning:
Sensitive PII should only be scanned using a scanner that is approved for use with controlled information. Typically, this will be a scanner that is physically connected to a workstation, or a networked scanner that can save files directly in a file share. Do not use a scanner that delivers scanned documents by email.

Electronic Storage:
Information systems require an Authority To Operate (ATO) signed by the Chief Information Officer before they may be used to store Sensitive Personally Identifiable Information.

In addition to authorized production systems, Sensitive PII may be stored on the following systems:

Microsoft Windows file share drives (ex H:\, M:\ and others)

Microsoft SharePoint on-premises servers (also known as, On-Prem SharePoint and sites that begin with [redacted]) operated within the Census Bureau.

While Microsoft Windows C:\ drives are secure enough to store/process Sensitive PII, good business practice as far as recoverability dictates they should be kept in the shared file drives listed above. [12]

[12] Note: Acceptable Use Policy for Census Bureau Information Technology Resources (IT AUP) states “work related files are not to be stored on any workstation’s hard drive (the C:\ drive)” because such files are not backed up. However, the operation of Microsoft Windows inherently stores information from documents on the C:\ drive in the form of downloaded files, temporary files, and virtual memory page files. As such, any computer that is used to process controlled information should use drive-level encryption for all fixed storage, such as the Windows C:\ drive. Linux systems should be configured to use the Linux Unified Key Setup-on-disk-format (OUKS) to encrypt all Linux partitions, including partitions used for file systems and for virtual memory.

It is **prohibited** to store Sensitive PII on SharePoint Online, OneDrive, Office365, and Outlook Web Application (OWA).

Physical Space for Access:
Personnel records and sensitive PII may only be accessed electronically from restricted access space including approved telework sites, and authorized contractor remote place of performance sites.

Sensitive PII may only be accessed where at least one barrier prevents observation of that CUI by someone without a business need to know. That barrier may include the authorized individual accessing the CUI.

For example, Census Bureau security guards may view sensitive PII at guard stations at entrances.

Personnel records and sensitive PII may only be accessed electronically from restricted access space. (These include Census Bureau Headquarters above the second floor, Census Bureau Regional Offices, the Bowie Computing Center, approved telework sites, and authorized contractor remote place of performance sites.

Disposal:
At headquarters, dispose of hard copies in a locked blue bin designated for sensitive materials.

Dispose of electronic copies (tapes, CDs, disks, etc.) in a locked blue bin or contact the Records Management Branch at 301-763-2282 for instructions.

Field staff should follow guidance on shipping materials to the Regional Office for destruction.

Personnel Records

Markings:

CUI//SP-PERS

Description:
The Code of Federal Regulations (5 CFR § 293.106) protects personnel records. Federal personnel records are any records concerning an individual which are maintained and used in the personnel management or personnel policy setting process. These include records that relate to the supervision over, and management of, Federal civilian employees; records on the general administration and operation of human resource management programs and functions; as well as records that concern individual employees.

Examples include:

- Position classification correspondence
- The Official Personnel Folder/eOPF
- Adverse action case file
- Performance plans with ratings
- Results of background investigations
- Disciplinary action history

Electronic Documents:
Electronic documents containing federal personnel records must have a CUI banner marking (or appropriate alternative or bulk marking) of CUI//SP-PERS centered in the header and separated from any other text.

The filename, where feasible, could include CUI__SP-PERS. Example: extract_CUI__SP-PERS.txt

The filename where feasible could include CUI_PRVCY. Exs: download_CUI_PRVCY.csv

Access to personnel records must be restricted to only those Census Bureau employees, contractors, or other individuals with a business need to know.

Paper Documents:
Printed documents as well as any handwritten documents containing personnel records must have the appropriate CUI banner marking in the header--CUI//SP-PERS.

Personnel records must be kept locked in a **metal** filing cabinet or storage room with appropriate signage when not in use.

Do not remove hard copies from secure Census Bureau facilities, even for teleworking.

Printing:
Personnel records without sensitive PII in them may be printed with everyday printing. Personnel records with sensitive PII should be printed using private printing.

Immediately remove printouts from the printer.

Before printing, ensure that it has the appropriate label CUI//SP-PERS.

Mailing and Shipping:
Address packages and parcels that contain personnel records for delivery only to a specific recipient, wherever possible address it to an individual. Do not put CUI markings on the outside of an envelope or package, or otherwise indicate on the outside that the item contains CUI.

When mailing information from personnel records, it must be doubled wrapped. The inner wrapping must be labeled as follows:

CUI Labeling

CUI//SP-PERS
Disclosure Prohibited--Title 5 U.S.C.
To be opened by addressee only.

The inner packaging must be tamper-evident packaging. To prevent loss when the outer wrapping/packaging is damaged, the inner wrapping also must be addressed to a specific recipient, preferably to an individual wherever possible.

Electronic Transmission

Email:
The Census Office 365 email system is approved for personnel records if they do not contain sensitive PII. Sensitive PII information may not be included in the body of an email or as an attachment. It must be encrypted with an approved encryption method before transmission. Send the file using an approved encryption method such as Kiteworks (https://sfc.doc.gov/). Do not include SPII in the subject line of a Kiteworks message, or in the body unless you enable message protection. The attachment may also be encrypted and password protected via WinZip and attached to an email sent from the Outlook Web App.

Faxing:
When faxing personnel records, ensure that someone is at the machine to receive it. Do not fax to an electronic fax service that delivers the fax by email.

Other Forms of Electronic Transmission or Online Collaboration:
Only Microsoft Teams is authorized for teleconferencing with Sensitive PII. See the guidance on *Using Microsoft Teams to Share Title 13 Data, Title 26 Data, and Sensitive PII* for more instructions.
[redacted]

Note: The transmission of a document containing controlled information, by a means that is not accredited to hold that controlled information, is an unauthorized disclosure. Such disclosures must be reported to the Bureau of the Census Computer Incident Response Team (BOC CIRT) at 301-763-3333 or 866-300-7063 as soon as possible but no later than 1 hour after discovery.

Teleworking*:*
If teleworking or working remotely, staff may only access personnel records through approved Census Bureau remote access technology (such as VDI or VPN) at their approved telework location(s). Do not email personnel records information to yourself for use on personally owned equipment or remove printed copies from the building.

Scanning:
Personnel records should only be scanned using a scanner that is approved for use with controlled information. Typically, this will be a scanner that is physically connected to a workstation, or a networked scanner that can save files directly in a file share. Do not use a scanner that delivers scanned documents by email.

Electronic Storage:
Information systems require an Authority To Operate (ATO) signed by the Chief Information Officer before they may be used to store Title 5 information.

In addition to authorized production systems, personnel records may be stored on the following systems:

Microsoft Windows file share drives (ex H:\, M:\ and others)

Microsoft SharePoint on-premises servers (also known as, On-Prem SharePoint and sites that begin with [redacted]) operated within the Census Bureau.

While Microsoft Windows C:\ drives are secure enough to store/process personnel records, good business practice as far as recoverability dictates they should be kept in the shared file drives listed above. [13]

It is **prohibited** to store personnel records with sensitive PII on SharePoint Online, OneDrive, Office365, and Outlook Web Application (OWA).

Physical Space for Access:
Personnel records and sensitive PII may only be accessed electronically from restricted access space including approved telework sites, and authorized contractor remote place of performance sites.

To the extent feasible, entry into personnel records storage areas shall be limited to only employees whose official duties require access to that information in whatever form or media the records might appear. Hardcopies of personnel records must be kept in a lockable metal filing cabinet. Documentation of removal of personnel records from storage areas must be kept so that adequate control procedures can be established to assure that removed records are returned on a timely basis.

It is prohibited to access personnel records and sensitive PII from public spaces, including the first floor of the Census Bureau headquarters and second floor training rooms.

Disposal:
At headquarters, dispose of hard copies in a locked blue bin designated for sensitive materials.

Dispose of electronic copies (tapes, CDs, disks, etc.) in a locked blue bin or contact the Records Management Branch at 301-763-2282 for instructions.

Field staff should follow guidance on shipping materials to the Regional Office for destruction.

---

[13] Note: Acceptable Use Policy for Census Bureau Information Technology Resources (IT AUP) states “work related files are not to be stored on any workstation’s hard drive (the C:\ drive)” because such files are not backed up. However, the operation of Microsoft Windows inherently stores information from documents on the C:\ drive in the form of downloaded files, temporary files, and virtual memory page files. As such, any computer that is used to process controlled information should use drive-level encryption for all fixed storage, such as the Windows C:\ drive. Linux systems should be configured to use the Linux Unified Key Setup-on-disk-format (OUKS) to encrypt all Linux partitions, including partitions used for file systems and for virtual memory.

Other Categories of Controlled Unclassified Information

In addition to the categories of CUI most used at the Census Bureau and outlined above, the Census Bureau generates, stores or processes about 40 other categories of CUI (both basic and specified). Many categories of information received from other federal agencies may be subject to controls detailed in the Federal Government's CUI Registry and agreements with that agency. Furthermore, information received from non-federal agencies may be subject to additional controls agreed to with that entity.

Many categories of information the Census Bureau uses, acquires, or generates while conducting its day-to-day business are also CUI. The Census Bureau used to treat some of these categories of CUI as Administratively Restricted Information. but all information for which a law, regulation, or governmentwide policy says it must be controlled is CUI. This includes but is not limited to:

- Procurement and Acquisition information used in Source Selection (CUI//SP-SSEL)
- Non-public Financial and Budget information concerning the federal budget, including authorizations and estimates of income and expenditures (CUI//SP-BUDG)
- Other Proprietary Business Information, such as cost proposals and labor rates (CUI//PROPIN)
- Attorney-client privileged information (CUI//PRIVILEGE)
- Information Systems Vulnerability Information (CUI//ISVI)

Note: The term "For Official Use Only" (FOUO) and "Sensitive But Unclassified" (SBU) were previously used to describe some of these categories however they have been replaced by the term Controlled Unclassified Information in accordance with *Executive Order (EO) 13556, Controlled Unclassified Information*. Staff and Program areas must cease using FOUO and SBU consistent with implementation guidance included in this policy.

If you have questions on what information you work with is included within one of these categories of CUI, please speak with your supervisor. {see also contract and memoranda of understanding

If the law, regulation, or government-wide policy stipulates handling requirements that exceed those of CUI Basic information, personnel must follow those requirements. Otherwise, they must follow the handling requirements for CUI Basic information.

Information Handling Guidelines for Non-CUI Information

Administratively Restricted Information

Description and Markings:
Information at the Census Bureau may be restricted for reasons other than controls in Titles 13, 26, or 5, or other laws, regulations, or government-wide policies that rise to the level of classifying the information as CUI.

Information that is administratively restricted, but which is not covered under the CUI program may include:

- Pre-decisional policy documents.
- Information subject to restrictions but not protected by statutory restrictions, such as valid agreements with government agencies or other entities if they do not contain CUI.
- Internal use methodological documentation in support of statistical products.
- Administrative email messages and memoranda.
- Individual employee work schedules.
- Documents that are not intended for public release or are still in the clearance process.

Documents providing background, options, and/or recommendations about a topic that do not yet reflect an accepted policy can be marked “PREDECISIONAL" Those that capture internal decision-making processes can be marked “DELIBERATIVE.” Documents that contain both may use a combination of these two supplemental administrative markings “PREDECISIONAL/DELIBERATIVE".

Documents may also be labeled “Draft,” “For Internal Use Only,” or “Not Cleared for Public Dissemination” as appropriate.

> **IMPORTANT NOTE:** Pre-release Principal Economic Indicators and Demographic Time-Sensitive Data, as well as embargoed data releases, have unique restrictions. For more details, see especially the Policy on Pre-release of Information.

Labeling (electronic and hardcopy):
These labels may not appear as part of a CUI banner marking or in a place where it may be mistaken for a CUI banner marking. Options include off-center headers, including the label in the document footer, or as a watermark.

Printing:
Administratively restricted information may be printed without restrictions.

Managing Paper Copies:
Administratively restricted information should be kept hidden from view when members of the public are present.

It should be kept away locked when not in use if warranted. Employees, contractors, and other SSS should check with their supervisor, task manager, or SSS sponsor if unsure of the sensitivity of a particular item.

Mailing and Shipping:
No restrictions.

Electronic Transmission
Administratively restricted information should be encrypted if the sensitivity level is high. Employees, contractors, and other SSS should check with their supervisor, task manager, or SSS sponsor if unsure of the sensitivity of a particular item. They should also ensure the individual receiving the email is aware of the sensitive nature of the document.

Email:
No restrictions, other than sending only to those individuals authorized to receive it.

Faxing:
No restrictions, other than sending only to those individuals authorized to receive it, and, if appropriate, ensure someone authorized to receive it is at the machine to retrieve it.

Other Forms of Electronic Transmission:
No restrictions on video/teleconferencing with administratively restricted information, other than sending only to those individuals authorized to receive it.

Teleworking:
No restrictions, other than ensuring material cannot be viewed by those not authorized to see it.

Scanning:
No restrictions.

Electronic Storage:
Administratively restricted information may be stored on the following systems:

SharePoint Online, OneDrive, Office365, and Outlook Web Application (OWA)
Microsoft Windows file share drives (ex H:\, M:\ and others)

SharePoint on-premise servers operated within the Census Bureau.

While Microsoft Windows C:\ drives are secure enough to store/process administratively restricted information, good business practice as far as recoverability dictates they should be kept in the shared file drives listed above. [14]

Physical Space for Access:
No restrictions.

Disposal:
At headquarters dispose of hard copies in a locked blue bin designated for sensitive materials.

Dispose of electronic copies (tapes, CDs, disks, etc.) in a locked blue bin or contact the Records Management Branch at 301-763-2282 for instructions.

[14] Note: Acceptable Use Policy for Census Bureau Information Technology Resources (IT AUP) states “work related files are not to be stored on any workstation’s hard drive (the C:\ drive)” because such files are not backed up. However, the operation of Microsoft Windows inherently stores information from documents on the C:\ drive in the form of downloaded files, temporary files, and virtual memory page files. As such, any computer that is used to process controlled information should use drive-level encryption for all fixed storage, such as the Windows C:\ drive. Linux systems should be configured to use the Linux Unified Key Setup-on-disk-format (OUKS) to encrypt all Linux partitions, including partitions used for file systems and for virtual memory.

Public Information

Marking: Optional but it may be marked as Uncontrolled Unclassified Information (UUI).

Description:
Consists of information that is released to the public, such as statistical products, approved metadata, schedules, program descriptions, and risk plans, as well as information released under the Freedom of Information Act (FOIA) requirements. Public information has gone through a clearance process.

Printing:
Public information may be printed with regular printing.

Managing Paper Copies:
No handling restrictions but public information should not be released to the public without permission from a supervisor, task manager, or SSS sponsor.

Mailing and Shipping:
No restrictions.

Electronic Transmission:
No handling restrictions but public information should not be sent to the public without permission from a supervisor, task manager, or SSS sponsor.

Teleworking*:*
No restrictions.

Scanning:
No restrictions.

Electronic Storage:
No restrictions.

Physical Space for Access:
No restrictions.

Disposal:
Dispose of in regular recycling bins.