

# Foreign Trade Statistics

*Security Guidelines for Federal Government Agencies*

Issued October 2007

FTD 07-SG



U S C E N S U S B U R E A U

*Helping You Make Informed Decisions*

U.S. Department of Commerce  
Economics and Statistics Administration  
U.S. CENSUS BUREAU

# Acknowledgments



**U.S. Department of Commerce**  
**Carlos M. Gutierrez,**  
Secretary

**Vacant,**  
Deputy Secretary



**Economics and Statistics Administration**  
**Cynthia A. Glassman,**  
Under Secretary for Economic Affairs



**U.S. CENSUS BUREAU**

**Charles Louis Kincannon,**  
Director

**Preston Jay Waite,**  
Deputy Director and  
Chief Operating Officer

**Thomas L. Mesenbourg,**  
Associate Director for  
Economic Programs

**William G. Bostic, Jr.,**  
Chief, Foreign Trade Division

The U.S. Census Bureau wishes to acknowledge the assistance of the following individuals and organizations in the preparation of this booklet:

**Judy Ward** of Computer and Hi-Tech Management was responsible for creating this booklet. The following Census Bureau employees contributed heavily toward the editing, content, and organization of the booklet: **Clifford Jordan, Bryant Turner, Jerome Greenwell, Dale Dickerson, Jacquelyn Mann, Samuel Jones, Diane Oberg,** and **Dorothy Brown** of the Foreign Trade Division; **Patrick Heelen** of the Legal Office; **Patricia Melvin** of the Policy Office; **Timothy P. Ruland,** Chief, of the IT Security Office; **Michael C. Cook** of the Customer Liaison and Marketing Services Office; **Lisa M. Blumerman,** Division Chief, and **Joanne Dickinson,** Chief, Marketing and Training Development Branch.

**Linda Chen** and **Monique Lindsay** of the Administrative and Customer Services Division, **Walter C. Odom,** Chief, provided publication and printing management, graphics design and composition, and editorial review for print and electronic media. General direction and production management were provided by **Wanda Cevis,** Chief, Publications Services Branch.

# Table of Contents

---

## Chapter

### **1 Introduction**

1.1	General .....	3
1.2	Legal and Regulatory Mandates .....	5
1.3	Overview of Publication .....	8

### **2 Requests for Confidential and Prerelease Data**

2.1	General .....	10
2.2	Requests for Confidential Data .....	10
2.3	Requests for Prerelease Data .....	11
2.4	Request Format .....	11

### **3 Documenting Need, Use, and Required Infrastructure**

3.1	General .....	12
3.2	Confidential Data Request Documents .....	13
3.3	Prerelease Data Request Documents .....	13
3.4	Need and Use .....	14
3.5	Coordinating Safeguards Within an Agency .....	14
3.6	Safeguard Review .....	14

### **4 Recordkeeping Requirements**

4.1	General .....	16
4.2	Tracking Log .....	16

### **5 Information and System Security, and Other Safeguards**

5.1	General .....	18
5.2	Physical Security .....	18
5.3	Logical Security .....	19
5.4	Incident Response and Reporting .....	21

### **6 Minimizing Access to Confidential and Prerelease Data**

6.1	General .....	22
6.2	Handling of Confidential and Prerelease Data .....	22

### **7 Other Safeguards**

7.1	General .....	24
7.2	Internal Inspections .....	24
7.3	Employee Awareness .....	25

<b>8</b>	<b>Reporting Requirements</b>	
8.1	General.....	27
8.2	Security Plan.....	27
8.3	Safeguard Procedure Report.....	28
8.4	Submission of Safeguard Procedure Report.....	29
8.5	Annual Safeguard Activity Report.....	30
8.6	Submission of Annual Safeguard Activity Report.....	31
<b>9</b>	<b>Disposal of Confidential or Prerelease Data After Completion of Use</b>	
9.1	General.....	32
9.2	Disposal of Paper Media .....	32
9.3	Disposal of Magnetic Media .....	33
<b>10</b>	<b>Publication/Release of Confidential or Prerelease Data</b>	
10.1	General.....	34
<b>11</b>	<b>Reporting Indications of Improper Disclosure</b>	
11.1	General.....	35
<b>Appendix A</b>		
A-1	Glossary .....	36
<b>Appendix B</b>		
B-1	Physical Access.....	37
B-2	Operating Systems Security .....	37
B-3	Security Incident Reporting.....	38
B-4	Encryption .....	39
<b>Appendix C</b>		
C-1	Checklist for Requesting Confidential or Prerelease Data.....	40
C-2	National Interest Determination Checklist .....	41
C-3	Memorandum of Understanding (MOU) Checklist .....	42
C-4	Nondisclosure Agreement.....	45
C-5	Checklist for Internal Safeguard Inspections.....	47



# INTRODUCTION

## 1.1 General

Foreign Trade Statistics (import and export data) compiled by the U.S. Census Bureau, Foreign Trade Division, are an economic indicator. The statistics are required to be collected and protected by legal mandate in Title 13, United States Code (USC) Chapter 9, Section 301, and Title 18, USC Section 1905 and by regulatory mandate in Title 15 Code of Federal Regulations (CFR), Part 30 (see *Section 1.2 Legal and Regulatory Mandates of this manual*). The foreign trade statistics are widely watched and heavily relied upon by both the private sector and the government. The private sector uses the foreign trade statistics to measure the impact of foreign competition, to conduct market share analysis and market penetration studies, and to develop various marketing policies. Government uses include the computation of the balance of payments for the United States,

setting economic and fiscal policy, the analysis of trends in international trade, multilateral trade negotiations, and assistance to U.S. exporters in locating markets for their merchandise.

The foreign trade statistics are based upon confidential individual business transactions between U.S. exporters/importers and their foreign customers. Because of the sensitivity of the commercial data collected, it is important to ensure this confidentiality. Any public release would place the exporter/importer at a serious competitive disadvantage in the world marketplace. Without the guarantee of confidentiality, exporters/importers may be inclined to withhold correct information

*The foreign trade statistics are based upon confidential individual business transactions between U.S. exporters/importers and their foreign customers. Because of the sensitivity of the commercial data collected, it is important to ensure their confidentiality.*

and, thereby, undermine the accuracy of the trade statistics.

Transaction-level data or aggregate-level export or import

information, from which one could determine individual business transactions, are defined as

**Confidential Data** for the purposes of these

guidelines. Confidential Data, whether commingled with nonconfidential data or kept pure, aggregated, or retained as transaction-level, are still Confidential Data. Once data are designated as Confidential, they and all their products, amalgamations, and changes remain Confidential Data and must be handled according to the guidelines presented in this handbook.

Additionally, for the purposes of these guidelines, aggregate trade data compiled, but not yet officially released to the public will be referred to as

**Prerelease Data.** In

very limited circumstances, federal government agencies may be authorized access to

Prerelease Data in order to meet programmatic requirements.

It is essential that Prerelease Data not

be released to the public prior to the official release date and time. The early release of such data could have a negative impact on trade negotiations and

stock markets around the world. The withholding of foreign trade statistics prior to official release is mandated by the Office of Management and Budget (OMB) Statistical Policy Directive Number 3 (see *Section 1.2 Legal and Regulatory Mandates of this manual*).

Prerelease Data must, therefore, be **kept confidential** and treated with the

same consideration as Confidential Data, *during the period of time between receipt of the information by the requesting agency and the official release of the data to*

*the public.* After the official release date and time, however, Prerelease Data no longer have to be kept confidential.

*Once data are designated as Confidential, they and all their products, amalgamations, and changes remain **Confidential Data.***

*Aggregate trade data compiled, but not yet officially released to the public will be referred to as **Prerelease Data.***

As a condition of receiving either Confidential or Prerelease Data, the receiving agency must show, to the satisfaction of the Census Bureau, the ability to protect the confidentiality of the data. Safeguards must be designed to prevent unauthorized access and uses. In addition to a written request, the Census Bureau may require a formal agreement that specifies, among other things, the purposes for which the data will be used and how it will be protected. An agency must ensure that its safeguards will be ready for immediate implementation upon the receipt of the data.

## 1.2 Legal and Regulatory Mandates

Several laws and policy documents govern the confidentiality of and access to Confidential and Prerelease Data: Title 13 USC, Chapter 9; Title 15 CFR, Sections 30.90–30.91; and Title 18 USC, Section 1905 govern the access to Confidential Data. The Foreign Trade Division’s statistical guidelines, Memorandums of Understanding (MOU) between the U.S. Census Bureau and specific agencies, and OMB’s Statistical Policy Directive, Number 3, govern the access to Prerelease Data.

The legal authority for the collection and publication of U.S. foreign commerce and trade statistics is established by Title 13, USC Chapter 9 and Title 18, USC Section 1905.

**Title 13, Chapter 9, §301,**  
**of the United States Code,**

**Paragraph (a):**

*“The Secretary [of Commerce] is authorized to collect information from all persons exporting from, or importing into, the United States and the noncontiguous areas over which the United States exercises sovereignty, jurisdiction, or control . . .”*

Title 13 directs the Secretary of Commerce to collect, compile, and publish foreign trade statistics on a monthly and cumulative basis. Title 13 is implemented by regulations contained in Title 15 of the CFR, Part 30. These regulations define the **confidentiality** of the trade data:

**Title 15 Code of Federal  
Regulations, Part 30,**

**Subpart H:**

**“§30.91 Confidential  
information, Shipper’s Export  
Declarations.**

(a) Confidential status.

*The shipper’s Export Declaration is an official Department of Commerce form prescribed jointly by the Census Bureau and the Bureau of Industry and Security. Information required thereon is **confidential**, whether filed electronically or in any other approved format, for use solely for official purposes authorized by the Secretary of Commerce. Use for unauthorized purposes is not permitted. Information required on the Shipper’s Export Declarations may not be disclosed to anyone except the exporter or his agent . . .”*

**Title 15 Code of Federal  
Regulations, Part 30,**

**Subpart H:**

**“§30.90 Confidential  
information, import entries  
and withdrawals.**

*The contents of the statistical copies of import entries and withdrawals on file with the Census Bureau are treated as **confidential** and will not be released without authorization by the U.S. Customs Service . . .”*

OMB further defines both the limits imposed, in order to keep Prerelease Data confidential and the burden placed upon the party making the request:



**Office of Management  
and Budget Statistical Policy  
Directive Number 3:**

**Section 3:**

*“(a) The [Census Bureau] head must establish whatever security arrangements are necessary and impose whatever conditions on the granting of access are necessary to ensure that there is no unauthorized dissemination or use.*

*“(b) The [Census Bureau] head shall ensure that any person granted access has been fully informed of and agreed to these conditions.*

**Section 7:**

*Any agency requesting an exception must demonstrate . . . that the proposed exception is necessary and is consistent with the purposes of the Directive.”*

Moreover, a National Interest Determination (NID) is integral to the acceptance or refusal of a request for data, as dictated by both Titles 13 USC and 15 CFR:

**Title 13, Chapter 9,  
§301, of the United States  
Code, Paragraph (g):**

*“[Trade data], wherever located, shall be exempt from public disclosure unless the Secretary [of Commerce] determines that such exemption would be contrary to the **national interest.**”*

**Title 15 Code of Federal  
Regulations, Subpart H,  
§30.92:**

*“In recommendations regarding any other requests for access to official copies, a judgment in the light of circumstances will be made as to whether it is contrary to the national interest to apply the exception, keeping in view that the maintenance of confidentiality has in itself an important element of national interest.”*

**No request for Confidential Data will be granted, unless the Census Bureau Director determines it is in the *national interest* to do so. Also, no request by a federal agency for advance access to Prerelease data will be granted unless the agency enters into a Memorandum of Understanding (MOU) with the U.S. Census Bureau's Foreign Trade Division. Additionally, no request for public disclosure of Prerelease Data will be granted unless approved by OMB.**

Penalties for unauthorized disclosure of Confidential Data are defined under Title 18:

**Title 18, USC Section**

**1905, et seq.:**

*The penalty for unlawful disclosure is a fine under this title and/or imprisonment for not more than 1 year, or removal from office or employment.*

Because of the sensitivity of this information, requests for and usage of Confidential or Prerelease Data are restricted and controlled as specified in the body of this document.


## 1.3 Overview of Publication

This Foreign Trade Statistics Security Guidelines handbook is directed towards any federal agency granted access to data considered by the Census Bureau as Confidential or Prerelease Data. Its purpose is to make a requesting agency aware of their responsibility for protecting the confidentiality and security of these data. A federal agency accessing Confidential or Prerelease Data must exercise diligence in adhering to the controls and safeguards set in place to protect the integrity, confidentiality, and sensitivity of the data.

This handbook is divided into 11 chapters. Chapter 2, immediately following this section, addresses the preliminary steps for submission of a request to receive data. Chapter 3 discusses the documents used to specify the need and use of the Confidential Data, as well as, the security infrastructure required prior to receiving Confidential or Prerelease Data. Chapters 4 through 8 contain information regarding the necessary safeguards and recordkeeping requirements for the data once they are received from the Census Bureau. Chapter 9 outlines proper disposal of

Confidential and Prerelease Data, while Chapters 10 and 11 detail the inherent confidentiality and acceptable use of the data, and the requirements for reporting of any improper disclosures. Finally, the appendices following the body of this booklet contain procedures, checklists, and additional instructions designed to help ensure that any agency receiving Confidential or Prerelease Data protects and uses them appropriately.

This publication, as well as other information including the Foreign Trade Statistics Regulations, is available on our Web site <[www.census.gov/foreign-trade/reference/guides/index.html](http://www.census.gov/foreign-trade/reference/guides/index.html)>.



## REQUESTS FOR CONFIDENTIAL AND PRERELEASE DATA

### 2.1 General

Export data are compiled based upon information reported on the Shipper's Export Declaration (SED) or through the Automated Export System (AES). These documents/records have enforcement, as well as statistical purposes and may only be released to authorized agencies for specific, authorized purposes if the Director of the Census Bureau, as the designee of the Secretary of Commerce, determines that it is in the ***national interest*** to do so.

### 2.2 Requests for Confidential Data

As detailed in *Section 1.2, Legal and Regulatory Mandates*, Title 13 USC, Chapter 9, Section 301(g), and 15 CFR, Sections 30.90–30.91 govern the confidentiality of and access to Confidential Data. Except for requests by an exporter/importer for its own data, only Congress and U.S. government agencies with statistical

or trade-related responsibilities may be granted access to Confidential Data. Trade-related responsibilities include: enforcement of export/import laws and regulations; monitoring of trade agreements; official, legal, or regulatory needs by the exporter/importer or their agent as authorization for proof of export/import; and U.S. Department of Agriculture requirements for proof of export in connection with subsidy payments. Access can only be granted if it is determined to be in the ***national interest*** to do so. To receive Confidential Data for statistical purposes, the agency must have requirements that cannot be met with aggregate, published data. Those requirements must be explained in a written request.

All requests for export or import Confidential Data must be made in writing to:

Director  
U.S. Census Bureau  
Washington, DC 20233

The guidelines presented in the subsequent sections of this handbook apply to all Confidential Data.

## 2.3 Requests for Prerelease Data

Because export and import data are considered one of the leading economic indicators, it is only under very rare circumstances that agencies are authorized to receive a restricted amount of Prerelease Data. To receive Prerelease Data for extraordinary purposes, the agency must have unique requirements that cannot be met with published data released publicly at preordained intervals. Those requirements must be explained in a written request.

All requests from federal agencies for export/import Prerelease Data must be directed in writing to the Director of the Census Bureau (see *Section 2.2* for address).

## 2.4 Request Format

All written requests for Confidential or Prerelease Data must:

- Be written on requesting agency letterhead.
- Specify precisely what data (i.e., net import/export record layout fields, country of destination/origin, port of export/import) are being requested.
- Stipulate why the requested data are required.
- Cite the legislative authority supporting the request.
- Demonstrate why data aggregated to the agency's specifications will not suffice, if requesting Confidential Data.
- Substantiate and justify the early access, if requesting Prerelease Data.

For complete information, see *Appendix C, Section C-1*, for a *Checklist for Requesting Confidential or Prerelease Data*.



# DOCUMENTING NEED, USE, AND REQUIRED INFRASTRUCTURE

## 3.1 General

### National Interest Determination

When a request for Confidential Data is received, the Director of the Census Bureau, under Title 13 USC, 301 (g), makes a *National Interest Determination* (NID) that results in the granting or denial of the request. NIDs can be made for: (1) specific (one time) export/import or commodity detail file requests, or (2) more complex requests for data covering specific export/import or commodity information over a specified time period. The granting of a request results in the drafting of a Memorandum of Understanding (MOU). (See *Memorandum of Understanding* below.) The MOU will include the NID as a cover memorandum, attachment, or enclosure. Also, the MOU will have an NID statement included in the body of the document.

A checklist for the information included in a National Interest Determination is available in *Appendix C, Section C-2*.

### Memorandum of Understanding

For each approved request for Confidential or Prerelease Data, the Census Bureau's Foreign Trade Division works with the requesting agency to develop the MOU. This document, after being approved and ratified with an authorized signature of the agency, will be returned and retained in Census Bureau files for a period of 3 years. Included in the MOU will be security provisions tailored to both the information security requirements for the requested data and the system security infrastructure of the requesting agency.

*Included in the MOU will be security provisions tailored to both the information security requirements for the requested data and the system security infrastructure of the requesting agency.*

The MOU will detail, among other things, the data to be released, the purposes for which they may be used, who may have access to the data, the restrictions on use of the data, how the data will be protected from unauthorized disclosure, and the ultimate disposition of the data.

A checklist for the information included in an MOU is available in *Appendix C, Section C-3*.

### 3.2 Confidential Data Request Documents

To ensure compliance with Census Bureau disclosure requirements, the MOU for export/import Confidential Data will specifically prohibit receiving agencies from publishing data compiled from Confidential Data without the express, written consent of the Census Bureau. The receiving agency, in cooperation with the Census Bureau, must detail how the data will be protected from unauthorized disclosure. In addition, the receiving agency must restrict Confidential Data access to authorized personnel only and ensure that neither the data, nor any information based upon the data, are made available to any other agency or third party without a need to know and prior written approval from the Census Bureau.

### 3.3 Prerelease Data Request Documents

In those rare instances when a request for Prerelease Data is granted, the requester will be permitted early access to export/import data. The MOU developed in such an instance will detail the data to be provided, the purposes for which the data are being provided, and the restrictions on use of the data. In addition, it will prohibit any further distribution of the data beyond the approved parties prior to the Census Bureau's official release of the trade statistics, and will also detail strict provisions for the handling of the data.

The receiving agency, in cooperation with the Census Bureau, must also detail how the data will be protected from unauthorized disclosure. As with Confidential Data, the receiving agency must restrict access to nonconfidential Prerelease Data only to authorized personnel with a need to know. It is the requesting agency's responsibility to ensure that none of these data, nor any information based upon the data—including inferences regarding the level of trade (for example, that imports went up or down)—are made available prior to the data's official release.

### 3.4 Need and Use

In all instances, the requested data must be used exclusively for the authorized purpose. If an agency's needs extend beyond the purpose for which the data were originally authorized, a new request must be submitted explaining the reason for the additional use. Written approval is required before the data provided may be used for any additional purpose.

Any unauthorized disclosure may result in denial of future access and imposition of penalties on the responsible officials, as authorized Under Title 18 USC, Section 1905.

*The penalty for unlawful disclosure is a fine under this title and/or imprisonment for not more than 1 year, or removal from office or employment.*

### 3.5 Coordinating Safeguards Within an Agency

Confidential or Prerelease Data may only be disbursed to those employees within an agency who have a need to know and have been authorized to have access under the provisions of the MOU.

The agency should designate a specific individual to be responsible for establishing and maintaining safeguard standards consistent with the Census Bureau guidelines. The official assigned these responsibilities must have adequate authority in the agency's organizational structure to ensure compliance with the agency's safeguard standards and procedures. The selected official should be responsible for conducting internal inspections (see *Section 7.2*), for submitting safeguard reports to the Census Bureau (see *Section 8.3*), and for any necessary liaison with the Census Bureau.

### 3.6 Safeguard Review

A Safeguard Review is an onsite evaluation of the receiving agency by the Census Bureau to determine if Confidential or



Prerelease Data are being used according to the specifications detailed in the MOU, and to observe the measures implemented to protect the data. Census Bureau security staff will also verify that security policies and procedures are in place to protect the Confidential or Prerelease Data.

The initial onsite Safeguard Review will occur before the initial provision of Confidential or Prerelease Data and then at least every 3 years thereafter. As a condition of granting access the Census Bureau's Foreign Trade Division has the option to regularly conduct onsite reviews of agency safeguards. The onsite reviews will be conducted by a Census Bureau safeguard team comprised of persons from the following areas: Foreign Trade Division Regulations and Outreach Branch; Foreign Trade Division Commodity Analysis Branch; Foreign Trade Division Information Security Staff; and staff from the Census Bureau IT Security Office. Several factors will be considered when determining the need for and the frequency of a review. In each instance, the Census Bureau will

provide a written review plan. The plan will include:

- A list of records to be reviewed (e.g., Title 13, Nondisclosure Agreements, internal inspection reports, and agency awareness program).
- The scope and purpose of the review.
- A list of the specific areas to be reviewed.
- A list of agency personnel to be interviewed.

Need and use will be evaluated and actual operations will be observed. Agency employees may be interviewed during the onsite review, generally to clarify procedures or to determine employee awareness of security requirements and Titles 13 and 18 penalty provisions.

Safeguard Reviews are conducted to determine the adequacy of safeguards, as opposed to an evaluation of the agency's programs. The Census Bureau will issue a Safeguard Review Report. The agency will have the opportunity to provide comments that will be included in the report.



## RECORDKEEPING REQUIREMENTS

### 4.1 General

The Census Bureau requires that all agencies granted access to Confidential or Prerelease Data establish a permanent system for tracking the flow of data within the agency. The tracking system must begin with the expected date of receipt and must be maintained until:

- The completion of use, in the case of Confidential Data, where the data are either destroyed or returned to the Census Bureau as described in *Chapter 9* of this manual.
- Until their official release, in the case of Prerelease Data.

The tracking record of all Confidential or Prerelease Data received must remain on file for a period of 2 years after the date the data are destroyed, returned, or released to the public.

### 4.2 Tracking Log

The tracking log for Confidential or Prerelease Data should include the following sections:

#### **Receipt of Data**

- Description of data to be received (i.e., export/import, prerelease, net export/import record layout fields, country of destination/origin, port of export/import, month/year).
- Expected date of receipt, if data are to be delivered to the receiving agency. (If the data are not received by the scheduled due date and the agency was not informed of a delay, the agency must immediately notify the Census Bureau contact person identified in the MOU.)
- Actual date of receipt (or pickup from the Census Bureau).
- Name of authorized person receiving the data.
- Location where data are stored or filed.

### **Receipt of Data from AES (Interactive)**

When agencies request access to AES data in an interactive mode the following applies:

Pursuant to an NID and establishing an MOU with the Census Bureau, the receiving agency must enter into an Interconnection Security Agreement (ISA) with U.S. Customs and Border Protection (CBP). Computers used to access the data are to have an operating system (Windows XP or Vista) that is in compliance, or will comply with OMB M-07-11 “Plans for Managing Security Risk by Using Common Security Configurations.” The operating system must also allow for automatic auditing. Auditing is to track the person accessing the data, as well as the time and date of the access. The downloading of data (i.e. print screens, transposing the data into a spreadsheet, etc.) accessed in this manner is prohibited unless specified in the MOU.

### **Receipt of Data from AES (Data Transfer)**

For requested AES data that is downloaded by the Census Bureau and provided to an agency, upon approval of the request pursuant to an NID, the receiving agency must enter into an MOU with the Census Bureau. These documents will detail the

transfer mechanism and related security measures for the transfer and data access. As previously discussed, automatic auditing is to be performed on the computer accessing the data. Security controls must be in place for the media (hard drive, removable media) used to store the data after it is downloaded. This will be outlined in the MOU.

*Note:* The agency must establish accounts through U.S. Customs for every employee designated to access AES data. When agency employees depart or no longer have a need to access AES data their accounts are to be terminated. Agency employee AES accounts will be further addressed in the MOU.

### **Access to Data (Audit Trail)**

- A. Documents and listings
  - Name and signature of authorized user.
  - Date and time logged “Out/In.”

*Note:* The agency must account for any lost or misplaced data by documenting search efforts and notifying the responsible official noted in the MOU.

- B. Operating System/Application
  - Name of authorized user.
  - Date of computer access.

### **Disposal of Data**

- A. Name and signature of authorized person disposing of data.
- B. Date and method of destruction or date and method of return to the Census Bureau.

For disposal guidelines see *Chapter 9*.



# INFORMATION AND SYSTEM SECURITY, AND OTHER SAFEGUARDS

## 5.1 General

Agencies receiving Confidential or Prerelease Data must take appropriate actions to ensure that the data are protected against unauthorized possession and use. Possession and use of Confidential or Prerelease Data must be in accordance with

*Use of Confidential or Prerelease Data must be in accordance with the provisions of the MOU between the Census Bureau and the agency authorized to receive the data.*

the provisions of the MOU between the Census Bureau and the agency authorized to receive the data. In addition, all systems and applications that receive, transmit, process,

manipulate, or store Confidential or Prerelease Data must meet minimum security requirements as set forth in the MOU. The Census Bureau reserves the right to view and approve any measures utilized by the receiving agency to secure the data. The receiving agency should submit a security certification and accreditation, in accor-

dance with NIST SP 800-37 and SP 800-53, of the system or application, and make available for viewing a copy of its current security plan to document the measures implemented for securing Confidential or Prerelease Data. During Safeguard Reviews and any subsequent inspections, the Census Bureau or its representative may use these submitted documents or request to review other pertinent documentation to include plans, policies, standards, procedures, and approvals related to information and system security in implementing the MOU and authorizing the release of Confidential or Prerelease Data to the receiving agency. Several areas will be addressed during this Inspection and Review as described below.

## 5.2 Physical Security

Receiving agencies must identify and document measures to control physical access to equipment, media, and work areas where Confidential or Prerelease

Data are housed to ensure against eavesdropping, theft, vandalism, or accidents that may occur. Physical controls shall be employed to secure the facility of the receiving agency in accordance with agency security standards.

#### **Work Area and Desktop**

All computer and work areas containing Confidential or Prerelease Data must be protected with key locks, cipher locks, or other suitable access controls. Such areas must be kept locked when not occupied by staff. Computer terminals must be capable of locking to prevent unauthorized use or viewing of the data. Such terminals must be kept locked when not occupied by staff.

#### **Mobile Computers and Other Electronic Equipment**

Confidential or Prerelease Data are not to be placed onto laptop, handheld, or mobile computers of any kind. Further, Confidential or Prerelease Data shall not be placed, stored, or processed on personally owned equipment or media of any kind. Confidential or Prerelease Data are not for use over the Internet, on an intranet, with unsecured facsimile machines, or with computers containing modems unless appropriate and authorized security

procedures are in place. All Confidential or Prerelease Data files transmitted from the Census Bureau to the receiving agency will be in accordance with the ratified and approved MOU. All such transmissions require the specific written approval of the Census Bureau. **UNENCRYPTED TRANSMISSION OF CONFIDENTIAL OR PRERELEASE DATA SHALL NOT BE ALLOWED VIA ELECTRONIC MAIL OR MESSAGING SYSTEMS, EVEN AMONG AUTHORIZED USERS.**

#### **Removable Media**

The receiving agency shall not use removable media without written authorization from the Census Bureau. Authorized removable media must be kept locked and stored securely when in, or removed from, designated equipment.

### **5.3 Logical Security**

Receiving agencies must identify and document measures to control logical access to systems, applications, media, and data where Confidential or Prerelease Data are housed to ensure against eavesdropping, theft, vandalism, or accidents that may occur.

### **Data Integrity**

Prior to releasing Confidential or Pre-release Data to the receiving agency, the data are scanned to ensure their content is protected against malicious and/or destructive programs or scripts. Furthermore, Confidential or Prerelease Data are verified for accuracy and integrity prior to release. The receiving agency shall implement virus detection and eradication efforts, as well as integrity verification efforts, to ensure continued security of the data. The Census Bureau uses encryption software that meets current National Institute of Standards (NIST) and Federal Information Processing Standards (FIPS) requirements. The receiving agency shall also use software that meets current NIST and FIPS guidelines.

### **Data Confidentiality**

Prior to releasing Confidential or Pre-release Data to the receiving agency, the data are encrypted to secure their content against unauthorized access. The Foreign Trade Division, Information Security Officer oversees encryption policies, procedures, and practices, and oversees the provision of encryption keys and passphrases to the authorized representative of the receiving agency. Encryption keys and passphrases

will be changed periodically to further ensure data security and access control. The receiving agency must appoint a contact person to receive these keys and passphrases and implement efforts to ensure their continued security. The Census Bureau uses encryption software that meets current NIST and FIPS requirements. The receiving agency shall be informed by the Information Security Officer as to the software required.



*Encryption keys and passphrases will be changed periodically to further ensure data security and access control.*

### **Information Sharing and Interconnecting Systems Controls**

The receiving agency must identify and document any sharing of information or interconnected system that impacts the security of Confidential or Prerelease Data. It is required that written authorization be obtained prior to connection with other systems and/or sharing Confidential or Prerelease Data.

### **Operational Controls**

The receiving agency must describe the controls used for receiving, identifying, handling, processing, storing, and disposing of input and output data and its media.

In addition, the controls used to monitor the installation of, and updates to, hardware and software for the system shall be documented. It is required that written authorization be obtained prior to release or distribution of Confidential or Prerelease Data.


### **Technical Controls**

The receiving agency must describe the controls used for identifying and authenticating users, limiting and restricting user access, tracking and auditing user activities, deterring and detecting unauthorized use, preventing undesired use, and protecting data integrity and availability. It is required that written authorization be obtained prior to accessing Confidential or Prerelease Data.

## **5.4 Incident Response and Reporting**

The receiving agency must appoint a representative to respond to incidents, serve as the contact person for the Information Security Officer, and report any incidents to the Information Security Officer. A security incident, as it relates to the possession and use of Confidential or Prerelease Data, is any violation, or suspected violation, of standards, policies, procedures, and practices governing the data as set forth in the MOU. Examples of security incidents may include, but are not limited to:

- Unauthorized use of Confidential or Prerelease Data.
- Use of unauthorized accounts to access Confidential or Prerelease Data.
- Misused, stolen, or compromised passwords.
- Lost or stolen Confidential or Prerelease Data.
- Duplication or distribution of Confidential or Prerelease Data.



## MINIMIZING ACCESS TO CONFIDENTIAL AND PRERELEASE DATA

### 6.1 General

Only authorized employees whose duties and responsibilities require access may use the Confidential and Prerelease Data. An employee's background should be considered when designating authorized personnel. Access to and use of Confidential and Prerelease Data must be within the restrictions of the MOU.

Access granted to authorized employees must be on a need-to-know basis, where no employee is granted more information than is needed to perform

his or her duties. Each employee granted access to Confidential and Prerelease Data is required to sign a Nondisclosure Agreement (see *Appendix C, Section C-4*).

*Good safeguard practice dictates that access to Confidential or Prerelease Data must be strictly on a need-to-know basis.*

### 6.2 Handling of Confidential and Prerelease Data

Confidential and Prerelease Data should be handled in such a manner that ensures they do not become misplaced or made available to unauthorized personnel. To the maximum extent possible, Confidential

and Prerelease Data should not be copied to agency files, separate listings, or tables, in order to avoid inadvertent disclosure. Likewise, Confidential and Prerelease Data

should not be transmitted in any form to anyone, except as prescribed in the MOU. Any file, listing, table, or other material on any media containing such data must be clearly labeled, "Disclosure Prohibited-Title 13 USC, Authorized Personnel Only," and remain so labeled until the release date,



if Prerelease Data, or until destroyed or returned to the Census Bureau, if Confidential Data.

### **Commingling**

If Confidential or Prerelease Data are recorded on CD-ROM or any other electronic media with agency data, it should be protected as if it were entirely Confidential or Prerelease Data, and labeled as described above. Such commingling on a single media should be avoided to the maximum extent possible. When data processing equipment is used to process or store Confidential or Prerelease Data and the information is mixed with agency data, the agency must ensure that Confidential or Prerelease Data cannot be extracted from the computer during processing, such as by a remote terminal or remote access, and the commingled data must be handled as if it were all Confidential Data. Confidential or Prerelease Data access must be controlled by:

- Systemic means, including server protection, password protection, and labeling. (See *Chapter 5, Information and System Security and Other Safeguards* for additional information.)
- Restricting access to the data

processing equipment to only those personnel authorized to see Confidential or Prerelease Data.

- Removing all Confidential or Prerelease Data from all resident files, databases, and programs after the data have served their authorized purpose.

Commingled data in shared facilities present additional security risks that must be addressed. If your agency shares physical and/or computer facilities with other agencies, departments, or individuals not authorized to have access to Confidential or Prerelease Data, strict controls—physical and systemic—must be maintained to prevent unauthorized disclosure of this information (see *Appendix B*).

The restrictions imposed upon use of Prerelease Data end once the Census Bureau has officially released the data. A listing of the press release dates and times are provided with the MOU authorizing access to the data. However, the restrictions upon access to Confidential Data are permanent. The restrictions upon release of the specific data provided to the agency are detailed in the MOU.



## OTHER SAFEGUARDS

### 7.1 General

Title 15 CFR, Subpart H, §30.91 requires agencies receiving Confidential or Prerelease Data to provide other safeguard measures as appropriate to ensure the confidentiality of the data. Internal inspections and a good employee security awareness program can provide effective, yet inexpensive, protection against unauthorized disclosure of Confidential or Prerelease Data.

*Internal inspections and a good employee security awareness program can provide effective, yet inexpensive, protection against unauthorized disclosure of Confidential or Prerelease Data.*

citing compliance with security provisions outlined in the MOU, as well as any deficiencies and corrective actions taken.

The inspection records should be filed in a separate folder in a designated area and retained on file for 4 years. They should

be available for the Safeguard Review outlined in Section 3.6.

Safeguard Inspections should include the following items:

1. A review of the storage and handling of Confidential or Prerelease Data.
2. A review of how access to Confidential or Prerelease Data is granted to authorized employees.
3. An assessment of facility security features.

### 7.2 Internal Inspections

Agencies receiving Confidential or Prerelease Data must conduct inspections once a year to ensure that safeguards are adequate. These Safeguard Inspections should be done according to written specifications detailed in the MOU. A complete record must be made of each inspection,

4. Verification that Confidential or Prerelease Data has not been commingled with other information in such a way that confidentiality could be inadvertently compromised.
5. A review of after-hours security measures.
6. A review of access to secure storage containers or areas and of responsibility for changing keys.
7. An analysis of security procedures and instructions to employees.
8. A review of the data processing operations, including computer systems.
9. A review of the control and storage of magnetic and paper media.
10. An audit of the file room activity.
11. Interviews of those charged with security responsibilities.
12. A review of planned organizational changes to assure that security consideration is covered.
13. A review of procedures for and documentation of, returning, disposing of, or destroying Confidential or Prerelease Data no longer needed by the recipient.

These inspections should be conducted by authorized personnel who are not directly responsible for the use of the data. The inspections should be subject to formal follow-up procedures and reporting for any necessary corrective actions.

A checklist for internal inspections is available in *Appendix C, Section C-5*.

### 7.3 Employee Awareness

All agency employees granted access to Confidential or Prerelease Data must be thoroughly briefed on security procedures and instructions requiring their awareness. As part of the awareness program, a copy of the MOU developed between the Census Bureau and the agency must be provided to each authorized employee. In addition, a copy of this Security Guidelines booklet must also be provided.

Before being granted access to Confidential or Prerelease Data and each year thereafter, all authorized employees are required to sign a Nondisclosure Agreement (see *Appendix C, Section C-4*).

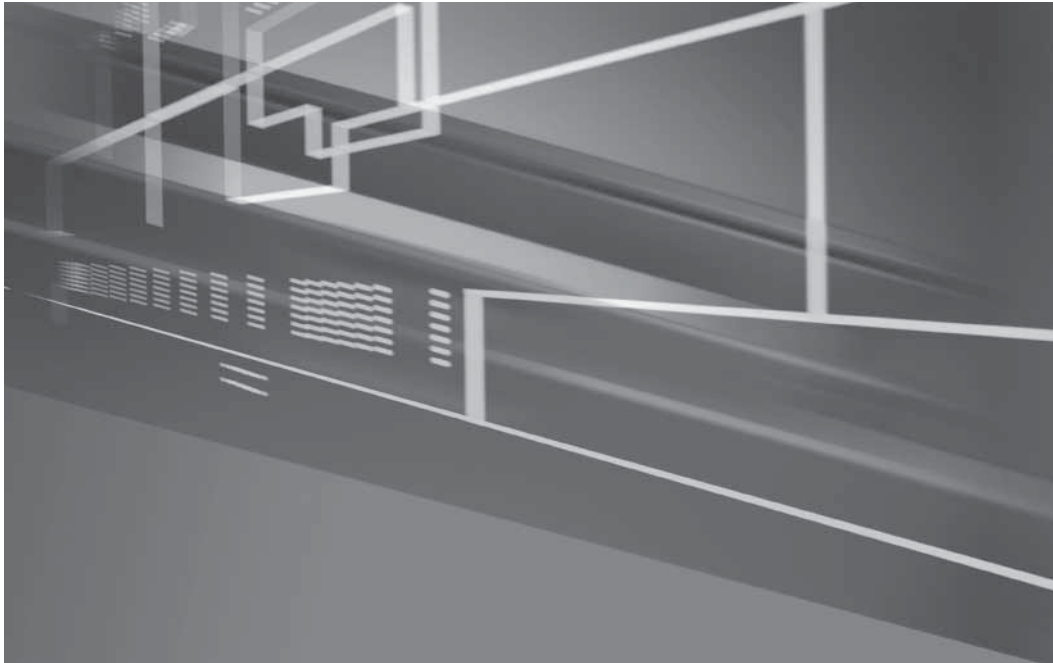
*Before being granted access to Confidential or Prerelease Data and each year thereafter, all authorized employees are required to sign a Nondisclosure Agreement.*

The receiving agency must inform the employees of this requirement.

Security guidelines should periodically be a topic of discussion with agency employees. Upon request, the Census Bureau, Foreign Trade Division, Regulations, Outreach, and Education Branch will be available to conduct briefings for agencies on Confidential or Prerelease Data security measures. Requests for security

briefings should be made in writing to the Chief of the Foreign Trade Division.

Agency employees are to be made aware of the provisions in Title 18 USC, Section 1905 which makes unauthorized disclosure of Confidential Data a crime, punishable under this title, and/or by imprisonment for not more than 1 year, or removal from office or employment.



## 8.1 General

Agencies receiving Confidential or Prerelease Data must file a report containing a description of the procedures established and used by the agency for ensuring the confidentiality of the information received from the Census Bureau. The Safeguard Procedures Report is a record of how Confidential or Prerelease Data is used by the agency and how the data are protected from unauthorized disclosure by that agency.

Annually thereafter, the agency must file a Safeguard Activity Report. This report advises the Census Bureau of any changes to the procedures or safeguards described in the Safeguard Procedures Report, no matter how minor. It also:

- Advises the Census Bureau of future actions that will affect the agency's safeguard procedures.

- Summarizes the agency's current efforts to ensure the confidentiality of Confidential or Prerelease Data.
- Certifies the agency is protecting Confidential or Prerelease Data pursuant to the security requirements specified in the MOU and the agency's own security requirements.
- Failure to submit either the Safeguard Procedures Report or the Annual Safeguard Activity Report by the designated date may result in discontinuance of the provision of Confidential or Prerelease Data to the receiving agency.

## 8.2 Security Plan

Any changes to the agency's Security Plan or security procedures, during the period of Confidential or Prerelease Data usage, must be documented and reported to the security contact designated in the

MOU, or to the Foreign Trade Division's Computer Security Team Leader. Census Bureau security staff will determine if the protection provided for Confidential or Prerelease Data has been modified in any way. The security policies, procedures, and practices outlined in the MOU are essential to the nondisclosure requirements mandated in Title 13 of the USC, Title 15 of the CFR, and OMB Circular A-130.

### 8.3 Safeguard Procedure Report

All agencies receiving Confidential or Prerelease Data must provide a report to the Chief of the Foreign Trade Division describing the Safeguard Procedures used to protect the confidentiality of the data. The report is to be submitted by March 1<sup>st</sup> and cover the preceding calendar year. The head of the agency must sign the report, unless otherwise specified in the MOU.

The Safeguard Procedure Report will contain the following information:

1. Name, title, and telephone number of the official responsible for implementing safeguard procedures.
2. Description of the data covered by the report.
3. A chart or description of the flow of Confidential or Prerelease Data through the organization, from receipt to return to the Census Bureau or their destruction.
4. A determination whether Confidential or Prerelease Data are commingled with or transcribed into data kept by the agency.
5. If applicable, a description of automated data processing (ADP) system(s) as they relate to maintaining or processing Confidential or Prerelease Data, including system configuration, what data are processed, files/records created when processing Confidential or Prerelease Data and which of these files/records contain such data, timesharing, internal system security (access controls, audit trails, and so forth), equipment and area physical security, and networks to remote terminals and/or other computers. Also, include any planned changes to the agency's system (equipment, safeguards, or processes).
6. Copies of all other written procedures and other related memoranda concerning the safeguards afforded

to the Confidential or Prerelease Data. The procedures should, at a minimum, describe the physical security afforded Confidential or Prerelease Data, the access allowed to Confidential or Prerelease Data by authorized agency employees, and the manner in which access is controlled. The procedures will also describe in detail the manner in which Confidential or Prerelease Data are disposed of upon completion of use, to include the methods of destruction, the place of destruction, the time schedule for disposal, and the names and titles of agency employees who are responsible for supervising destruction or disposal of Confidential or Prerelease Data. In addition, the procedures will describe the agency's security awareness program and the controls used to restrict visitors, janitorial help, and unauthorized employees in areas where Confidential or Prerelease Data are maintained.

7. Copies of all signed Nondisclosure Agreements and access logs.
8. Detailed description of significant changes in safeguard procedures or

authorized access to Confidential or Prerelease Data, and any changes or enhancements to physical and computer security measures utilized to safeguard Confidential or Prerelease Data.

9. Copy of reports of internal inspections conducted by the agency to assure that the written procedures are being adhered to by all authorized agency employees.
10. Copy of records of the disposal of Confidential or Prerelease Data. The information should be adequate to identify the material destroyed, include the control number of the data destroyed, and the date and manner of destruction.

## 8.4 Submission of Safeguard Procedure Report

The Safeguard Procedure Report is to be submitted to:  
Chief, Foreign Trade Division  
U.S. Census Bureau  
4600 Silver Hill Rd.  
Room 6K032  
Washington, DC 20233

## 8.5 Annual Safeguard Activity Report

Agencies should submit an annual Safeguard Activity Report by March 1<sup>st</sup> each year; the report should cover the preceding calendar year. The report must be on agency letterhead and be signed by the head of the agency or delegate. The report should contain the following information:

### **Changes to Information or Procedures Previously Reported**

- Responsible Officers or Employees.
- Functional Organizations Using the Confidential or Prerelease Data.
- Computer Facilities or Equipment and System Security—Changes or Enhancements.
- Physical Security—Changes or Enhancements.
- Retention or Disposal Policy or Methods.

### **Current Annual Reporting Period Safeguard Activities**

- Agency Disclosure Awareness Program—

Describe the efforts to inform all employees having access to Confidential or Prerelease Data

of the confidentiality requirements, the security requirements, and the sanctions imposed for unauthorized disclosure of Confidential or Prerelease Data.

- Reports of Internal Inspections—

Copies of a representative sampling of the Safeguard Inspections Reports and a narrative of the corrective actions taken (or planned) to correct any deficiencies should be included with the annual Safeguard Activity Report.

- Disposal of Confidential or Prerelease Data—

Report the disposal of the Confidential or Prerelease Data to the Census Bureau. The information should be adequate to identify the material destroyed/returned, and the data and manner of destruction (see *Chapter 9, Disposal of Confidential or Prerelease Data*).

**Note:** Including Confidential or Prerelease Data in the disposal record is not necessary, and should be avoided. Alternative identification methods should be employed in order to avoid unintended disclosure during communication of disposal information.



### **Actions on Safeguard Review Recommendations**

The agency should report all actions taken, or being initiated, regarding recommendations in the Final Safeguard Review Report issued as a result of the latest Safeguard Review.

### **Planned Actions Affecting Safeguard Procedures**

Any planned agency action that would create a major change to current procedures or safeguard considerations should be reported. Such major changes would include, but are not limited to, new computer equipment, facilities, or systems.

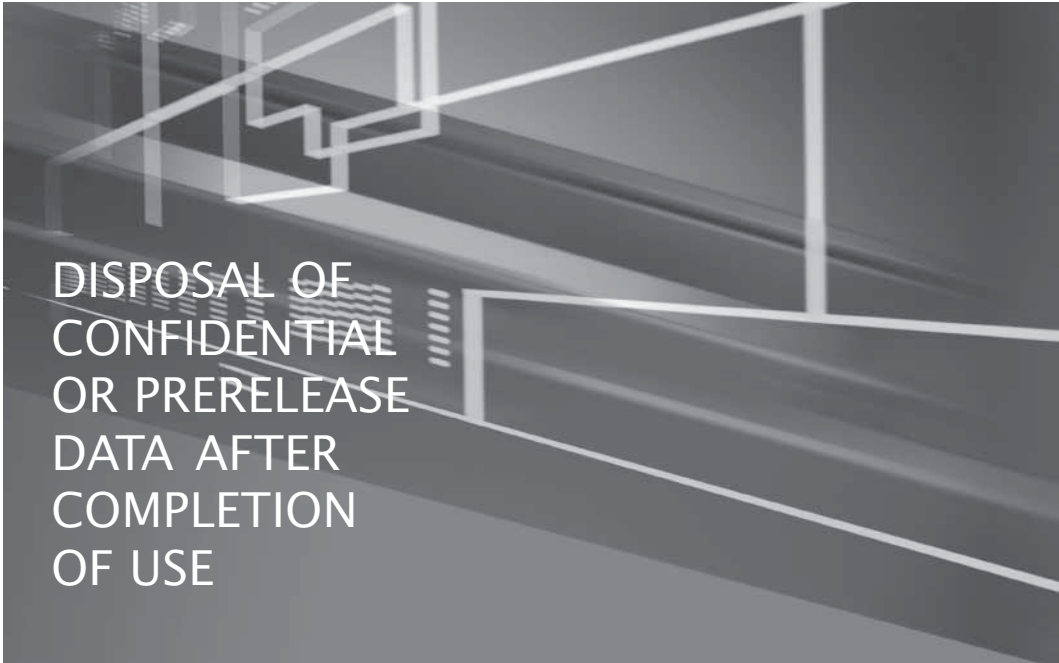
### **Agency Use of Contractors**

Agencies employing contractors, who require access to Confidential or Prerelease Data, must ensure the contractor's adherence to the mandates discussed in this Guideline.

## **8.6 Submission of Annual Safeguard Activity Report**

Annual Safeguard Activity Reports are to be submitted to:

Chief, Foreign Trade Division  
U.S. Census Bureau  
4600 Silver Hill Rd.  
Room 6K032  
Washington, DC 20233



## DISPOSAL OF CONFIDENTIAL OR PRERELEASE DATA AFTER COMPLETION OF USE

### 9.1 General

If use of Prerelease Data is completed prior to the official release date, the data must be destroyed, otherwise the data should continue to be secured by the receiving agency as outlined in the MOU.

Conversely, in order to continue to protect their confidentiality through the completion of their life cycle, Confidential Data, including the original data provided by the Census Bureau and any working files containing Confidential Data, must **always** be destroyed or returned to the Census Bureau according to the following guidelines after they have served their authorized purpose. The timeframe indicating when such actions must be performed will be detailed in the MOU between the U.S. Census Bureau and the receiving agency. The destruction process must prevent recognition of the information. Outlined below are the required methods of destruction for both paper and magnetic media containing Confidential Data.

### 9.2 Disposal of Paper Media

The following methods must be used to destroy Confidential Data:

- Burning—Use Environmental Protection Agency (EPA) approved public incinerators. When burning sensitive material, examine ash residue, if possible. If there are any large pieces of unburned material, reburn it until totally destroyed.
- Shredding—Use shredders that reduce residue particle size to 3/16 of an inch or less in width for destruction of sensitive paper and nonpaper products containing Confidential or Prerelease Data. All material should be shredded in such a manner that recognition or reconstruction is impossible by feeding material into the shredder vertically or diagonally to chop up sentences. Shredded materials must be recycled or thrown

in the trash and must not be used for other purposes, such as packaging.

- Return to Census Bureau—If the receiving agency does not have the facilities to properly destroy the paper media, then the documents must be returned to the Census Bureau to the office from which they were originally obtained.

Additionally, paper documents jammed in copying equipment, unusable copied documents, and tables, including listings or other documents prepared from the data provided by the Census Bureau, must be destroyed using one of the above methods.

### 9.3 Disposal of Magnetic Media

Magnetic media, such as cartridges, disks, e-mail drop boxes, and hard drives containing sensitive Confidential or Prerelease Data, must be cleared prior to reuse. To clear, overwrite all Confidential or Prerelease Data a minimum of three times with a commercial disk utility program. Then, for additional confidence, degauss using a commercial degausser. Destroy CD-ROMs by breaking into pieces so that they are completely unusable. The broken pieces should be discarded in the trash.



## PUBLICATION/ RELEASE OF CONFIDENTIAL OR PRERELEASE DATA

### 10.1 General

As stated earlier, foreign commerce and trade statistics are based upon confidential data, individual business transactions between U.S. exporters/importers and their foreign customers. Because of the sensitivity of the commercial data collected, it is important to ensure their confidentiality. Any

*The agency must ensure that **neither the Confidential or Prerelease Data, nor any information based upon the Confidential or Prerelease Data, including inferences that would disclose individual business transactions, are made available to any other agency or third party without prior written permission from the Census Bureau's Foreign Trade Division.***

public release would place the exporter/importer at a serious competitive disadvantage in the world marketplace. Without the security of confidentiality, exporters/importers may be inclined to withhold correct information and, thereby, undermine the accuracy of the trade statistics.

It is also essential that trade statistics are not released to the public prior to the official release date and time.

The prerelease of such data could have a negative impact on trade negotiations and stock markets around the world.

To ensure compliance with Census Bureau disclosure requirements, agencies that receive Confidential or Prerelease Data are specifically prohibited from publishing data compiled from Confidential or Prerelease Data without the express, written consent of the Census Bureau. The agency must ensure that neither the Confidential or Prerelease Data, nor any information based upon the Confidential or Prerelease Data, including inferences that would disclose individual business transactions, are made available to any other agency or third party without prior written permission from the Census Bureau's Foreign Trade Division.

Penalties for failure to adhere to these requirements are detailed in the provisions of Title 18 USC, Section 1905, which makes unauthorized disclosure of Confidential Data a crime, punishable by a fine under this title, and/or imprisonment for not more than 1 year, or removal from office or employment.



## REPORTING INDICATIONS OF IMPROPER DISCLOSURE

### 11.1 General

Both the Information Security Officer of the Census Bureau's Foreign Trade Division and the Chief of the Foreign Trade Division should be contacted upon discovery of any possible improper disclosure of Confidential or Prerelease Data by an agency employee or any other person.

The individual making the observation or receiving the information should communicate the security incident via telephone, fax, or paper mail. Faxed information should include only minimum detail,

and avoid using words that would alert the violator. Words like "hackers," "incident," or the suspected person's name would probably alert the suspected party or someone who has knowledge of the suspected party. Faxed information should be followed up with a detailed written report. If e-mail must be used, like faxed information, details that could possibly alert the violator should be avoided. Sensitive details should be written to a file and encrypted as an e-mail attachment (see *Section 5.3*).

# APPENDIX A

## A-1 Glossary

ADP	Automated Data Processing
AES	Automated Export System
CFR	Code of Federal Regulations
DES	Data Encryption Standard
EIN	Employer Identification Number
EPA	Environmental Protection Agency
FIPS	Federal Information Processing Standard
IT	Information Technology
MOU	Memorandum of Understanding
NID	National Interest Determination
OMB	Office of Management and Budget
SED	Shipper's Export Declaration
USC	United States Code

## **APPENDIX B**

### **B-1 Physical Access**

Guidelines:

1. Protect all offices, computer rooms, and work areas containing Confidential or Prerelease Data with key locks, cipher locks, magnetic card door locks, or other suitable access controls.
2. Employees, while passing through doors, gates, and other entrances to access-controlled areas, must not permit unknown or unauthorized persons to pass through at the same time.
3. Limit the number of entrances to the office space. Place the computer system away from the main entrances. Position work stations so there is control over who gains access to the computer system area. If a theft does occur, report it to the appropriate authority.
4. Properly secure computer systems to prevent theft, misuse, and abuse.
5. Supervise or challenge unauthorized personnel whenever they are in a restricted area containing Confidential or Prerelease Data.

### **B-2 Operating Systems Security**

Guidelines:

1. Control access to Confidential or Prerelease Data according to the user's authorization. The system must be able to allow or deny access based on the profile of the user.
2. Prevent unauthorized access by clearing all Confidential or Prerelease Data from systems before relocating the data to another system. Use software approved by the security contact identified in the MOU to overwrite erased data to ensure nonrecoverability.

3. All vendor-supplied default passwords must be changed before any computer or communications system is used for processing Confidential or Prerelease Data.
4. Password protect those utilities that are required only by the installation LAN manager to maintain security files.
5. Mask, suppress, or otherwise obscure the password display, such that unauthorized parties will not be able to observe or subsequently recover them.

## B-3 Security Incident Reporting

### Guidelines:

1. Report all suspected IT Confidential or Prerelease Data security problems or violations to the Chief, Foreign Trade Division and the Information Security Officer of the Foreign Trade Division.
2. Communicate the security incident via telephone or paper mail. If e-mail or facsimile must be used, avoid revealing phrases in the subject. Words like "hackers," "incident," or suspect names can be dead giveaways to unauthorized, interested parties. The details should be written to a file and encrypted as an e-mail attachment.
3. Ensure that every password is changed on a system that has been involved in a successful attack by a hacker or by some other system penetrator.



## B-4 Encryption

### Guidelines:

1. Use only encryption software that utilizes FIPS-approved Data Encryption Standard (DES).
2. Ensure that Confidential or Prerelease Data are not sent through e-mail.
3. Develop management procedures involving key distribution, key storage, and key destruction, and submit them to the Chief, Foreign Trade Division and the Information Security Officer of the Foreign Trade Division for review and approval prior to implementation.
4. Provide appropriate physical security for the protection of all encryption keys.

## **APPENDIX C**

### **C-1 Checklist for Requesting Confidential or Prerelease Data**

- Written on receiving agency letterhead
- Cites the legislative authority that supports the request
- Identifies the requester and agency employee(s) primarily responsible for data security
- Specifies precisely what data (i.e., net export/import fields off net record layout, country of destination/origin, port of export/import) are being requested
- Defines what period of time the requested data spans, if applicable
- Details how the data will be used (i.e., in what investigation, or as input to what type of statistical analysis)
- Identifies all users of the requested information
- If requesting Confidential Data, demonstrates why data aggregated to the agency's requirements will not suffice
- If requesting Prerelease Data, justifies the early access
- Specifies what time increment is being requested between installments (i.e., monthly, biweekly), if applicable
- If a company is involved in a court case or investigation, includes the company's federal Employer Identification Number (EIN)

## C-2 National Interest Determination Checklist

- Description of requested or affected export data, including timeframe(s) (i.e., Shipper's Export Declarations or detail files)
- Statement of the primary purpose(s) of agency data use, including statutory and regulatory citations
- Descriptions of the kinds of activities or operations for which data use is requested or authorized
- Statement that data received will be used and maintained under strictly secure conditions
- Description of the purposes, activities, or operations for which use is *not* authorized, if applicable
- Statement of export/import law enforcement, statistical, or other NID policy justification
- Explanation of how the agency use, as requested, is in the national interest
- Statement of time period for which the determination is effective, up to 3 years
- Statement that agency must designate employee(s) primarily responsible for data security (i.e., Agency Contact Person)
- Statement that specific conditions apply to agency receipt, use, and security of data (Foreign Trade Security Manual)
- Statement of whether there is or may be a related interagency agreement, if applicable
- States Census Bureau will conduct safeguard review at agency site to evaluate both the use of Confidential or Prerelease Data and the measures employed by the receiving agency to protect that data
- Statement of whether Census Bureau actions do, or may, require agency reimbursement, if applicable
- Statement as to how the affected agency may request a renewal of the NID

### C-3 Memorandum of Understanding (MOU) Checklist

- Includes NID statement
- Identifies parties involved in the agreement
- States objective of the MOU
- States specific purpose to which the data are being applied
- Includes confidentiality statement
- Cites legal and regulatory authority under which the data are being released
- Specifies effective dates for data release/expiration date of MOU, if Prerelease Data
- Particularizes data to be provided:
  - Codes/Field names
  - Formats/Layouts
  - Time periods
- Specifies method of data transmittal
- States access control procedures will be updated/changed at least every quarter
- States Census Bureau will conduct safeguard review at agency site to evaluate both the use of Confidential or Prerelease Data and the measures employed by the receiving agency to protect that data

- Itemizes any specific conditions applicable to agency receipt, use, and security of data (Foreign Trade Security Manual)
  - Held and managed only under strictly secure conditions
  - Used only for purposes, activities, and operations as authorized in the NID
  - Accessed and used only by named agency employees or agents with a need to know
  - Not used for any specifically unauthorized purpose, activity, or operation, if applicable
  - Returned or destroyed when use is complete or determination expires
- Outlines detailed data protection security measures specific to the receiving agency's systems, usage requirements, and environment
- Identifies a Census Bureau Information Security Officer as the contact for key/access control transmittal and general security oversight
- Identifies the agency employee(s) to serve as the contact for key/access control transmittal and general security oversight
- Specifies that anyone who might come in contact with Confidential or Prerelease Data must annually renew and sign a Census Bureau Nondisclosure Agreement
- States necessity for continuing data integrity monitoring
- Prohibits receiving agencies from publishing data compiled from Confidential Data without the express, written consent of the Census Bureau; and prohibits any further distribution of the data, or information based upon the data, beyond the approved parties prior to the Census Bureau's official release of the trade statistics, if Prerelease Data, or permanently, if Confidential Data

- States data are not to be released to third parties without prior written approval
- Stipulates MOU is internal government document and does not confer rights or benefits on any private person or party
- Defines termination terms
- Specifies MOU needs to be updated/renewed after 3 years, and procedure for doing so
- Cites that any unauthorized disclosure may result in denial of future access and imposition of penalties on the responsible officials, as authorized by Title 18 USC, Section 1905

## C-4 Nondisclosure Agreement

**This Agreement will be reratified annually by anyone receiving, using, or having access to Confidential or Prerelease Data.**

**U.S. Census Bureau Nondisclosure Agreement for CY/FY\_\_\_\_\_**  
**with \_\_\_\_\_** (agency/dept name)

I will not disclose any of the confidential foreign commerce or trade statistics obtained for or prepared by the Census Bureau to any person or persons either during or after my employment. I know such disclosure through publication, or any other communication method, could result in a fine and/or imprisonment, or removal from office or employment. I will use these data only for the purposes authorized in the governing Memorandum of Understanding (MOU) and will abide by the terms and conditions of that document.

This commitment to confidentiality as detailed in Title 13, USC forms the basis of our bond of trust with the public. Respondents entrust to us personal and financial information that we need to produce aggregate data. In turn, we promise not to disclose any of our data in such a way that respondents can be identified.

In addition, I acknowledge receipt of a copy of the MOU and the Foreign Trade Statistics Security Guidelines handbook.

Name	Signature	Date
_____	_____	_____
_____	_____	_____
_____	_____	_____
_____	_____	_____
_____	_____	_____
_____	_____	_____

## C-5 Checklist for Internal Safeguard Inspections

- Review storage and handling of Confidential or Prerelease Data
- Review how access to Confidential or Prerelease Data is granted to authorized employees
- Assess facility security features
- Verify that Confidential or Prerelease Data have not been commingled with other information in such a way that confidentiality could be inadvertently compromised
- Review after-hours security measures
- Review access to secure storage containers or areas and of responsibility for changing keys
- Analyze security procedures and instructions to employees
- Review data processing operations, including computer systems
- Review the control and storage of magnetic and paper media
- Audit the file room activity
- Interview those charged with security responsibilities
- Review planned organizational changes to assure that security considerations are covered
- Review procedures for and records of returning, disposing of, or destroying Confidential or Prerelease Data no longer needed by the recipient