International Trade Statistics Security Guidelines

United States Census Bureau
U.S. Department of Commerce
Economics and Statistics Administration
U.S. CENSUS BUREAU
census.gov

July 2019

Table of Contents

I. Introduction

The International trade statistics comprised of import and export data is compiled by the U.S. Census Bureau (Census Bureau) and published as an economic indicator. The international trade statistics are required to be collected and protected by legal mandate in Title 13, United States Code (U.S.C.) Chapter 9, § 301 and Title 18, U.S.C. § 1905, and by regulatory mandate in Title 15 Code of Federal Regulations (CFR), Part 30.

The international trade statistics are based upon confidential, business transactions between U.S. exporters/importers and their foreign customers. These transactions are reported in the Automated Commercial Environment (ACE) system maintained and operated by U.S. Customs and Border Protection (CBP). ACE was selected as the single portal system as a result of the February 19, 2014 issuance of Executive Order 13659 titled Streamlining the Export/Import Process for America's Businesses. Executive Order 13659 was written based on the International Trade Data System (ITDS) concept, which was established by the Security and Accountability for Every Port Act of 2006 (SAFE Port Act, Pub. L. 109-347). Pursuant to Section 405(d) of that Act, the purpose of the ITDS is to eliminate redundant information requirements, efficiently regulate the flow of commerce, and effectively enforce laws and regulations relating to international trade by establishing a single portal system, known as ACE.

Due to the sensitivity of the confidential business data collected, it is imperative to ensure the confidentiality of these data. Any public disclosure would place U.S. exporters/importers at serious competitive disadvantages in the world marketplace. Without the guarantee of confidentiality, U.S. exporters/importers may be inclined to withhold correct information and, thereby, undermine the accuracy of the trade statistics.

Federal agencies granted access to Confidential or Prerelease Data via direct access to ACE or a file transfer from the Census Bureau, are specifically responsible for exercising diligence in protecting the integrity, confidentiality, and sensitivity of the data. The Census Bureau created the International Trade Statistics Security Guidelines to ensure those U.S. Government Agencies (federal agencies) have the necessary information to properly safeguard and control the data.

II. The Data

A. Origin of Data

Access to the International Trade Statistics will either be provided by direct access to ACE or via a secure file from the Census Bureau.

Authorized filers use ACE to submit the import and export data required by federal agencies. Import filers report directly to ACE, whereas export filers report Electronic Export Information

(EEI) directly in the Automated Export System (AES) or AES*Direct* (a free Internet-based export data collection system and conduit to AES), which has been migrated into ACE. Export filers in AES use internal software or software certified by CBP of third party service providers to file EEI directly to AES. Export filers in AES*Direct* use the free Internet-based AES*Direct* within ACE to file EEI.

Only authorized federal agencies may access import and/or export data directly from ACE. For those agencies authorized, they will be provided access to ACE reports in the ACE portal. The portal allows federal agencies to download standard reports or create filtered or customized reports based on their authority. Additionally, a very limited number of authorized federal agencies will have access to user interfaces within ACE, giving them direct access to view real-time import and export transactions. Authorized federal agencies with this access generally have enforcement authority and gaining access to view data real time strengthens the agency's ability to seize or detain shipments before they occur.

On the other hand, agencies can request international trade statistics from the Census Bureau. The Census Bureau will prepare the data in a file(s) to be securely transmitted to the federal agency. The request by the federal agency will be granted upon the request being in the national interest. (See Section IV for more details).

B. Data Uses

The international trade statistics are widely watched and heavily relied upon by both the private sector and federal agencies. The private sector uses the international trade statistics to measure the impact of foreign competition, to conduct market share analysis and market penetration studies, to develop various marketing policies, and to measure compliance with export laws and regulations. Federal agencies use the statistics to compute the balance of payments for the United States, set economic and fiscal policy, analyze trends in international trade, support multilateral trade negotiations, assist U.S. exporters in locating markets for their merchandise, and investigate and enforce export laws and regulations.

C. Data Types

i. Confidential Data

Transaction level or aggregate level export or import information, from which one could determine business confidential transactions, are defined as Confidential Data for these International Trade Statistics Security Guidelines. Confidential Data, whether commingled (see Section II.C.iii) with non-confidential 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 these International Trade Statistics Security Guidelines. The restrictions upon release of the specific data provided to the agency are detailed in National Interest Determinations (NIDs), Interagency Agreements (IAAs) and/or

Memorandums of Understanding (MOUs).

ii. Prerelease Data

Aggregate trade data that has been compiled, but not yet officially released to the public will be referred to as Prerelease Data. No request for public disclosure of Prerelease Data will be granted unless the federal agency has a current IAA or MOU with the Census Bureau, and the request has been approved by the Office of Management and Budget (OMB) (see Section III). In very limited circumstances, federal agencies may be authorized access to Prerelease Data in order to meet programmatic requirements. However, Prerelease Data must 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. The early release of such data could have a negative impact on trade negotiations and stock markets around the world. After the official release date and time, Prerelease Data no longer have to be kept confidential.

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. Federal agencies should handle Confidential and Prerelease Data 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 any unauthorized individuals.

iii. Commingled Data

If Confidential or Prerelease Data are stored with agency data, it should be protected as if it were entirely Confidential or Prerelease Data, and labeled accordingly (see Section VI.D). Such commingling should be avoided to the maximum extent possible. Federal agencies must ensure that Confidential or Prerelease Data cannot be extracted, such as by unsecure remote access from a computer during processing. When Information Technology (IT) equipment is used to process or store Confidential or Prerelease Data and the information is mixed with agency data, the commingled data must be treated with the same consideration as Confidential Data.

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, both physical and systemic must be maintained to prevent unauthorized disclosure of this information (see Section VI.D and E) for Physical and Logical Security respectively.

III. Legal and Regulatory Authorities

Title 13 U.S.C., Chapter 9, §301(a) directs the Secretary of Commerce to collect, compile, and publish trade statistics pertaining to exports, imports, trade and transportation to enable him/her to foster, promote, develop, and further the commerce, domestic and foreign of the United States and for other lawful purposes.

Title 13, Chapter 9, §301, of the U.S.C., 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 18 U.S.C., § 1905 governs that employees of the United States and any department or agency thereof who discloses confidential statistical information without authorization can be fined, imprisoned or removed from employment.

Title 18, of the U.S.C. § 1905, et seq.;
"an officer or employee of the United States or of any department or agency thereof,…publishes, divulges, discloses, or makes known in any manner or to any extent not authorized by law any information coming to him in the course of his employment or official duties…, which information concerns or relates to the trade secrets, processes, operations, style of work, or apparatus, or to the identity, confidential statistical data, amount or source of any income, profits, losses, or expenditures of any person, firm, partnership, corporation, or association;…except as provided by law; shall be fined under this title, or imprisoned not more than one year, or both; and shall be removed from office or employment."

Title 15 CFR, §§ 30.55 and 30.60 govern the access to confidential import and export data respectively, and the collection and publication of U.S. foreign commerce and trade statistics.

Title 15, CFR, Part 30, Subpart F:
"**§30.55 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 U.S. Customs and Border Protection…"

Title 15, Code of Federal Regulations, Part 30, Subpart G:

"**§30.60 Confidentiality of Electronic Export Information.**

(a) The Electronic Export Information (EEI) collected and accessed by the Census Bureau under 15 CFR Part 30 is confidential, to be used solely for official purposes as authorized by the Secretary of Commerce…Absent such authorization, information collected pursuant to this Part shall not be disclosed to anyone by any officer, employee, contractor, agent of the federal government or other parties with access to EEI other than to the U. S. Principal Party in Interest (USPPI) or the authorized agent of the USPPI."

The withholding of international trade statistics prior to the official release is mandated by OMB Statistical Policy Directive Number 3. This, along with these International Trade Statistics Security Guidelines, IAAs, MOUs and NIDs between the Census Bureau and specific federal agencies govern the access to Prerelease Data. OMB further defines 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 exemption must demonstrate…that the proposed exception is necessary and consistent with the purposes of the Directive."

Moreover, a NID is integral to the acceptance of a request for data, as dictated by both Titles 13 USC §301(g) and 15 CFR Part 30.60(e). No request for Confidential Data will be granted, unless it has been determined it is in the national interest. Additionally, in order for the Census Bureau to provide confidential import data to a requesting federal agency, that agency must have received written authorization from CBP.

Title 13, Chapter 9, §301, of the U.S.C., Paragraph (g):

Shipper's Export Declarations (or any successor document), 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, CFR, Part 30, Subpart G:

§30.60(e) Confidentiality of Electronic Export Information.

"In determining whether, under a particular set of circumstances, it is contrary to the **national interest** to apply the exemption, the maintenance of confidentiality and national security shall be considered as important elements of the **national interest**."

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.

IV. National Interest Determination (NID)

Export data may only be released to authorized federal agencies for specific, authorized purposes if the Director of the Census Bureau, as the designee of the Secretary of Commerce, determines that is in the national interest to do so. Except for requests by an exporter for its own data, the Director of the Census Bureau must determine that it is in the national interest for federal agencies to access the data.

There are three types of NIDs: a One-Time NID, a NID for an IAA/MOU, and a Comprehensive NID. In all instances, the requested data must be used exclusively for the authorized purpose. Requests for NIDs should be written on requesting agency letterhead and submitted to:

Chief, Economic Management Division
U.S. Census Bureau, 4600 Silver Hill Road – Room 6K064
Suitland, MD 20746 (Courier) or Washington, DC 20233 (regular mail)

If a federal agency's needs extend beyond the purpose for which the data were originally authorized, the federal agency must submit a new request explaining the reason for the additional use. Written approval is required before the data provided may be used for any additional purpose. Additionally, any unauthorized disclosure may result in denial of future access and imposition of penalties on the responsible officials, as authorized Under Title 18 U.S.C., Section 1905. (See Section III).

Requests for import data will not require a NID (see Section V.B). However, when CBP provides import data to a federal agency directly, CBP authorization is required. Requests to CBP for import data should be submitted to CBP's privacy office at privacy.cbp@cbp.dhs.gov.

A. One-Time NID

One-Time NIDs are generally for investigations and involve the request from a federal agency for specific export information related to specific shipments or parties to the transaction for a specified "one-time" period. These requests are typically related to investigations of possible violations of U.S. export laws and regulations. Refer to *Appendix A* for a Checklist for Requesting Confidential or Prerelease Data through a NID.

B. NID for an IAA/MOU

NID requests for an IAA/MOU occur when the federal agency submits an initial request or a renewal request for an IAA/MOU with the Census Bureau. These requests typically cover a specific time-period and include the specific export information that the agency has the authority to receive. Refer to *Appendix A* for a Checklist for Requesting Confidential or Prerelease Data through a NID.

An IAA involves the requesting agency to compensate the Census Bureau for the costs associated with the collection, preparation and delivery of the data. The Census Bureau does not use IAAs for agreements that do not involve the transfer of funds. Whereas, a MOU is typically an exchange of data between the Census Bureau and a federal agency in order to ensure accurate reporting of data and improved accuracy of published statistics. The MOU does not involve a financial agreement since both agencies are engaging in an equitable apportionment of costs. The IAA/MOU furthers the mission of both parties in a way that could otherwise not be achieved.

For each approved request for recurring access to Confidential Data, the Census Bureau works with the requesting agency to develop an IAA/MOU. Upon an executed IAA/MOU, the agreement will usually be in place for a three-year period.

An IAA/MOU will be created in conjunction with the NID and generally include language regarding the federal agency holding the data confidential, including safeguarding the data, system controls, employee accountability and assign point of contact for data security (see Section VI and *Appendix C* for the Checklist for Internal Safeguard Inspections). In addition, the IAA/MOU will include requirements regarding disclosure, commingling of data, disposal of data, and penalty provisions, also explained in this document.

C. Comprehensive NID

As a result of Executive Order 13659 (See Section I), the Secretary of Commerce issued a NID which lists specific federal agencies who have been authorized to access export data in ACE based on the agency's statutory authority. This NID is referred to as the comprehensive NID. An amendment to the comprehensive NID is required when a federal agency is added to the list or a current approved federal agency adds or modifies their statutory or regulatory authority.

In addition to the Checklist for Requesting Confidential or Prerelease Data through a NID request found in *Appendix A*, federal agencies must satisfy either or both of the following prerequisites to gain permitted access to EEI collected and stored in ACE:

- An Information Collection Request approved by OMB for export information collected in, stored in, or accessed through ACE; and/or
- Statutory and legal obligations that require access to that information which is relevant to all the EEI data elements to which they are seeking access.

Once the Director of the Census Bureau approves the NID request, the federal agency requesting the NID will receive a courtesy copy of the approval letter that the Census Bureau sends to CBP. CBP must have the approval letter from the Census Bureau in order to prepare a MOU between CBP and the federal agency for access to data on ACE. Along with the approved NID to CBP, the Census Bureau will provide attachments that identify specific data elements and commodities that the agency has legal authority to access. CBP uses these attachments to program ACE to restrict access to the data that the agency is authorized to view or retrieve.

V. Requests for Prerelease and Confidential Data

A. Requests for Export Data

To receive Confidential Export Data for statistical purposes, the agency must have requirements that cannot be met with aggregate or published data. To receive Confidential Export Data for uses consistent with an agency's statutory or legal obligations not collected in accordance with an agency's independent OMB-approved Information Collection Request, the agency's uses shall include, but not be limited to:

- Improve compliance with U.S. export laws and regulations;
- Detect and prevent violations of export, census, customs, homeland security, national resource, and other laws, regulations and treaties;
- Analyze to assess threats to U.S. and international security such as money laundering, and other potential violations and U.S. and foreign criminal laws;
- Enforce U.S. export-related laws and regulations;
- Investigate and prosecute possible violations and U.S. export-related laws and regulations;
- Provide proof of export for enforcement of laws relating to exemption from or refund, drawback or other return of taxes, duties, fees, or other charges;
- Analyze and monitor trade agreements and the impact of proposed and implemented trade agreements and fulfill U.S. obligations under such agreements; or
- Prepare statistics consistent with an agency's statutory mission.

Refer to *Appendix A* for the Checklist for Requesting Confidential or Prerelease Data through a NID.

B. Request for Import Data

CBP collects import data through ACE. As a result, the Census Bureau may only provide raw or edited transaction level confidential and/or prerelease import data after the requesting agency has received written authorization from CBP. These requests will not require a NID. The requesting agency must provide the written authorization from

CBP along with the formal request for Confidential or Prerelease Data. The granting of a request may result in the drafting of an IAA/MOU. The IAA/MOU will include the CBP authorization as a cover memorandum, attachment, or enclosure. In addition, the IAA/MOU will have a CBP authorization statement included in the body of the document.

C. Request 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, the agency must have unique requirements that cannot be met with published data released on the official release date.

In those rare instances when a request for Prerelease Data is granted, the requester will be permitted early access to export/import data. The IAA/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 the use of 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. 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. The receiving agency, in cooperation with the Census Bureau, must also detail how the data will be protected from unauthorized disclosure. (See Sections VII.B and C).

VI. Safeguarding the Data

A. Coordinating Safeguards within a Federal Agency

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 provide information regarding the security certification and accreditation or Authorization to Operate, in accordance with National Institute of Standards and Technology (NIST) Special Publication (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. Confidential or Prerelease Data access must be controlled by:

- Systemic means, including server protection, password protection, and labeling (see Section VI.E).
- Restricting access to the IT 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.

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 IAAs/MOUs and authorizing the release of Confidential or Prerelease Data to the receiving agency. Several areas will be addressed during this Inspection and Review.

i. Authorized Employees

Confidential or Prerelease Data may only be accessed/utilized by those employees within a federal agency who have an official need to know and have been authorized to have access under the provisions of NID, IAA, and/or MOU. An employee's background should be considered when designating authorized personnel. Employees must be thoroughly briefed on security procedures and instructions requiring their awareness. As part of the awareness program, a copy of the NID, IAA or MOU developed between the Census Bureau and the federal agency and an electronic or physical copy of this International Trade Statistics Security Guidelines handbook must be made available to each authorized employee. These International Trade Statistics Security Guidelines should periodically be a topic of discussion with agency employees.

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 B*). The receiving agency must inform the employees of this requirement. By signing the Nondisclosure Agreement, employees are committing to not disclosing Confidential or Prerelease data for any unauthorized reason and committing to being good stewards of the data at all times.

Agency employees are to be made aware of the provisions in Title 18 U.S.C., Section 1905 which make 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. (See Section III).

ii. Employee Responsibilities

The agency should designate a specific individual to be responsible for establishing and maintaining safeguard standards consistent with these International Trade Statistics Security Guidelines. The specific individual assigned these responsibilities must have adequate authority in the agency's organizational structure to ensure compliance with the federal agency's safeguard standards and procedures. The selected official should be responsible for conducting internal inspections (see Section VI.C) for

submitting safeguard reports to the Census Bureau (Section VII.B and C), and for any necessary liaison with the Census Bureau. In addition, the federal agency official shall report to the Census Bureau Information Security Officer any security incidents that are in violation, or suspected violation, of standards, policies, procedures, and practices governing the data as set forth in the IAA/MOU. (See Section VII.D). Examples of security incidents may include, but are not limited to:

- Unauthorized use of Confidential or Prerelease Data, including use when working teleworking;
- Use of unauthorized accounts to access Confidential or Pre-release Data;
- Misused, stolen, or compromised passwords;
- Lost or stolen Confidential or Prerelease Data (in hard copy, on removable media, and/or portable computer (laptop, tablet)); and/or
- Duplication or distribution of Confidential or Prerelease Data.

B. Census Bureau Safeguard Reviews

A Safeguard Review is an on-site 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 IAA/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 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 Trade Regulations Branch of the Economic Management Division, Information Security Staff and Programming Branch staff of the Economic Applications Division. 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, Non-disclosure Agreements, internal inspection reports, and agency awareness program);
- The scope and purpose of the review; and
- A list of the specific areas to be reviewed.

The safeguard review team will evaluate the data need and use, and observe the actual operations. In addition, the safeguard review team may interview federal agency employees during the onsite review, generally to clarify procedures or to determine employee awareness of security requirements of Title 13 and Title 18 penalty provisions.

The Census Bureau conducts safeguard reviews 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 at the conclusion of the safeguard review which the federal agency will have the opportunity to provide comments that will be included in the report. See Section VII.B and C.

C. Internal Safeguard Reviews

Title 15 CFR, Subpart G, §30.60 requires agencies receiving Confidential or Prerelease Data to provide safeguard measures as appropriate to ensure confidentiality of the data. Internal safeguard reviews can provide effective, yet inexpensive protection against unauthorized disclosure of Confidential or Prerelease Data.

Agencies receiving Confidential or Prerelease Data must conduct internal safeguard reviews once a year to ensure that safeguards are adequate. These safeguard reviews should be done to written specifications detailed in the IAA/MOU. A complete record must be made of each inspection, citing compliance with security provisions outlined in the IAA/MOU, as well as any deficiencies and corrective actions taken.

The internal safeguard review records should be retained in a designated area or saved on file for four years. They should be available for the Census Bureau Safeguard Review outlined in Part B of this section.

Internal safeguard inspections should include the following items:

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

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

D. 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. The following physical security guidelines should be implemented:

- 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.
- 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.
- 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.
- Properly secure computer systems to prevent theft, misuse, and abuse.
- Supervise or challenge unauthorized personnel whenever they are in a restricted area containing Confidential or Prerelease Data.
- 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.

i. 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. Computers must be capable of locking to prevent unauthorized use or viewing of the data. Such computers must be kept locked when not utilized by staff.

ii. Mobile Computers and Other Electronic Equipment

Confidential or Prerelease Data are not to be placed on personally owned equipment or media of any kind. Confidential or Prerelease Data are not for use over the Internet, on an intranet, or with offsite computers, including laptops and tablets 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 IAA/MOU. All such transmissions require the specific written approval of the Census Bureau.

iii. 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.

E. 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.

i. Systems Security

The following guidelines should be implemented to protect unauthorized access to systems that contain Confidential of Prerelease data:

- 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.
- 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 IAA/MOU to overwrite erased data to ensure data cannot be recovered.
- All vendor-supplied default passwords must be changed before any computer or communications system is used for processing Confidential or Prerelease Data.
- Password protect those utilities that are required only by the installation Local Area Network manager to maintain security files.
- Mask, suppress, or otherwise obscure the password display, such that unauthorized parties will not be able to observe or subsequently recover them.

ii. Data Integrity

Prior to releasing Confidential or Prerelease 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 NIST and Federal Information Processing Standards (FIPS) requirements. The

receiving agency shall also use software that meets current NIST and FIPS guidelines.

iii. Data Confidentiality

Prior to releasing Confidential or Prerelease Data to the receiving agency, the data are encrypted to secure their content against unauthorized access. Use only encryption software that utilizes FIPS-approved Data Encryption Standard. Unencrypted transmission of Confidential or Prerelease data shall not be allowed via electronic mail or messaging systems, even among authorized users. The Economic Applications Division's 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 also use software that meets current NIST and FIPS guidelines

iv. 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.

v. 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.

vi. 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.

VII. Reporting Requirements

Agencies receiving Confidential or Prerelease Data must file the following plan and reports containing descriptions of the procedures established and used by the federal agency for ensuring the confidentiality of the information received from the Census Bureau.

A. 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 Economic Applications Division's Information Security Staff or to the security contact designated in the IAA/MOU. 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 IAA/MOU are essential to the nondisclosure requirements mandated in Title 13 of the U.S.C., Title 15 CFR, and OMB Circular A-130.

B. Safeguard Procedure Report

All agencies receiving Confidential or Prerelease Data must provide a Safeguard Procedures Report. This report is a record of how Confidential or Prerelease Data are used by the agency and how the data are protected from unauthorized disclosure by that agency. The report is to be submitted to the following address by March 1st and cover the preceding calendar year. The head of agency must sign the report, unless otherwise specified in the IAA/MOU.

Chief, Economic Applications Division
U.S. Census Bureau, 4600 Silver Hill Road – Room 6K062
Suitland, MD 20746 (Courier) or Washington, DC 20233 (regular mail)

The Safeguard Procedure Report will contain the following information:

- Name, title, and telephone number of the official responsible for implementing safeguard procedures;
- Description of the data covered by the report;
- 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;
- A determination whether Confidential or Prerelease Data are commingled with or transcribed into data kept by the agency;
- If applicable, a description of Information Technology 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);

- 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 upon completion of use, to include the methods 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;
- Copies of all signed Nondisclosure Agreements and access logs;
- 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;
- Copy of reports of internal inspections conducted by the agency to assure that all authorized agency employees are adhering to the written procedures; and
- Copy of records detailing 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.

C. Annual Safeguard Activity Report

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 Safeguards 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; and
- Certifies that agency is protecting Confidential or Pre-release Data pursuant to the security requirements specified in the IAA/MOU and the agency's own security requirements.

Agencies should submit an annual Safeguard Activity report by March 1st each year; the report should cover the preceding year. The report must be on agency letterhead and be signed by the head of the agency or delegate. Annual Safeguard Activity Reports are to be submitted to:

Chief, Economic Applications Division
U.S. Census Bureau, 4600 Silver Hill Road – Room 6K062
Suitland, MD 20746 (Courier) or Washington, DC 20233 (regular mail)

The report should contain the following information:

i. Changes to Information of Procedures Previously Reported

- Responsible officers or employees;
- Functional organizations using the Confidential or Prerelease Data;
- Changes or enhancements to computer facilities or equipment and system security; and
- Retention or disposal policy or methods.

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

iii. 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.

iv. 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.

v. 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 these

International Trade Statistics Security Guidelines.

D. Reporting Incidents of Improper Disclosure

If an incident occurs, an incident disclosure report must also be filed. Any agency employee or any other person should contact both the Information Security Officer of the Census Bureau's the Economic Applications Division's Information Security Staff upon discovery of any possible improper disclosure of Confidential or Prerelease Data.

The individual making the observation or receiving the information should communicate 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. In addition, the designated authorized employee of the federal agency should 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.

Failure to submit a Security Plan, and the Safeguard Procedures Report or the Annual Safeguard Activity Report by the designated date, or Incident Disclosure Report may result in discontinuance of the provision of Confidential or Prerelease Data to the receiving agency.

VIII. Recordkeeping Requirements

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 (see Section VIII.B); and/or 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.

A. Tracking Log

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

i. Receipt of Census Bureau 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 identified in the IAA/MOU.
- Actual date of receipt.
- Name of authorized person receiving the data.
- Location where the data are stored or filed.
- Documentation including search efforts and notification to responsible officials in the IAA/MOU whenever any data is lost or misplaced.

ii. User Interface Access in the Automated Export System (AES) or Access to the Automated Commercial Environment (ACE) Reports (Interactive)

When agencies request data in ACE through a user interface or ACE reports, the following applies:

Pursuant to a NID with the Census Bureau, the receiving agency must enter into a MOU and an Interconnection Security Agreement with U.S. CBP. Computers used to access the data are to have an operating system 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 IAA/MOU.

Note: The agency must establish accounts through CBP for every employee designated to access ACE data. When agency employees depart or no longer have a need to access ACE data, their accounts are to be terminated. Agency employee's ACE accounts will be further addressed in the IAA/MOU.

iii. Transfer of Data from ACE (Data Transfer)

When a federal agency requests access to data from the Census Bureau, in which the source of the information is ACE, the Census Bureau must approve that access request via a NID. Whether the request is for transaction-level or aggregate level data, the receiving agency most likely will be required to enter into an IAA/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 the Census Bureau provides the data. This will be outlined in the IAA/MOU.

iv. Access to Data (Audit Trail)

Each federal agency with access to Confidential or Prerelease data must have an audit trail of the authorized users of the data. The name and signature of the authorized user and the date and time when the user logged in and out must be recorded.

In addition, when accessing a computer system that warehouses the Confidential or Prerelease data, the federal agency must record the name and signature of the authorized user and the date of user's access to the computer system. Recording of such access information can be documented on a Nondisclosure Agreement (see *Appendix B*).

B. Disposal of Data

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 IAA/MOU. According to the following disposal guidelines, once the data have served their authorized purpose, they must be destroyed or returned to the Census Bureau. In doing so, the confidentiality of data, including the original data provided by the Census Bureau and any working files containing confidential data are protected through the completion of their life cycle. The timeframe indicating when such actions must be performed will be detailed in the IAA/MOU between the 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.

i. Disposal of Paper Media

The following methods must be used to destroy Confidential or Prerelease Data on paper media:

- Burning - Use Environmental Protection Agency approved public incinerators. When burning sensitive material, examine ash residue, if possible. If there are any large pieces of unburned metal, re-burn it until it is completely destroyed.
- Shredding – Use shredders that reduce particle size to 3/16 of an inch or less in width for destruction of sensitive paper and non-paper products. All material should be shredded in 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 the Census Bureau – If the receiving agency does not have the facilities listed above to properly destroy 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 listing or other documents prepared from the data provided by the Census Bureau, must be destroyed using one of the above methods.

ii. Disposal of Magnetic Media

Magnetic media, such as cartridges, disks (CD/DVD), 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.

Whenever disposing of the data occurs, the following shall be recorded by the agency and retained with other records.

- Name and signature of Authorized person disposing of data.
- Date and method of destruction or date and method of return to the Census Bureau.
- The information disposed of, in adequacy to identify the material destroyed/returned.

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.

IX. Appendices

Appendix A

Checklist for Requesting Confidential or Prerelease Data through a National Interest Determination

- ☐ Written on federal agency letterhead
- ☐ Cite the legal and regulatory authority supporting the request
- ☐ If requesting Confidential Data, demonstrate why data aggregated to the agency's specifications will not suffice
- ☐ If requesting Prerelease Data, justify the early access
- ☐ Stipulate the details of how the data will be used (i.e. investigation, enforcement, statistical analysis, etc.)
- ☐ Specify if the requested data will be commingled and/or published in any detail
- ☐ Identify the requestor and agency employee(s) primarily responsible for data security
- ☐ Identify all users of the requested information
- ☐ Specify precisely what data are being requested (i.e., import/export data elements)
- ☐ Define what period of time the requested data spans, if applicable
- ☐ Identify the preferred format for receiving the data records (i.e., Microsoft Excel file, AES printouts, etc.)
- ☐ If the data is requested to be printed, specify if documents need to be certified
- ☐ Specify what time increment is being requested between installments (i.e. annually, monthly, biweekly) if applicable
- ☐ If data is being used in an investigation or court case specify:
    - Company's Employer Identification Number
    - Name of Party for which records are requested or
    - Internal Transaction Numbers for specific shipments

Appendix B

Nondisclosure Agreement

This Agreement will be re-ratified annually by anyone receiving, using, or having access to Confidential or Prerelease Data.

U.S. Census Bureau Non-Disclosure Agreement for CY/FY

With_____

Agency/Department 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 who does not have an official need to know and has not signed the Nondisclosure Agreement 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 of employment. I will use these data only for the purposes authorized in the governing IAA/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 IAA/MOU and the International Trade Statistics Security Guidelines handbook.

NAME	SIGNATURE	DATE

Appendix C

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 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 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