

**U.S. Department of Commerce
U.S. Census Bureau**



**Privacy Impact Assessment for the
Foreign Trade Division Applications**

Reviewed by: _____ Byron A. Crenshaw, Bureau Chief Privacy Officer

- ☒ Concurrence of Senior Agency Official for Privacy/DOC Chief Privacy Officer
☐ Non-concurrence of Senior Agency Official for Privacy/DOC Chief Privacy Officer

BYRON CRENSHAW

Digitally signed by BYRON CRENSHAW
Date: 2021.06.29 17:00:52 -04'00'

Signature of Senior Agency Official for Privacy/DOC Chief Privacy Officer

Date

U.S. Department of Commerce Privacy Impact Assessment U.S. Census Bureau/ Field Systems Major Application System

Unique Project Identifier: 006-000400700

Introduction: System Description

Provide a description of the system that addresses the following elements:

The response must be written in plain language and be as comprehensive as necessary to describe the system.

The Foreign Trade Division Applications IT system collects, maintains, and processes Foreign Trade statistics to produce a press release called the U.S. International Trade in Goods and Services. The IT system also includes information about importers and exporters that are maintained in databases. A description of the Foreign Trade statistics and databases is provided below:

The Foreign Trade Statistics collected, processed and released as the FT900 are a principal economic indicator providing a complete count of American import and export transactions, based on official documents that shippers and receivers must file with the Department of Homeland Security (DHS), U.S. Customs and Border Protection (CBP). The data provide measures of the competitiveness and strength of domestic manufacturers and help measure the market for various goods; and allow computation of apparent consumption. They are essential for: economic policymaking; providing information used in the National Accounts; providing data essential for monitoring trade agreements and for measuring the impact of imports on the U.S. economy; providing data used for Civil and Criminal Enforcement activities.

The Importer Database provides both government and private sector users with information about the importing community including employment size, type of company, and major foreign markets. The Exporter Database provides both government and private sector users with information about the exporting community including employment size, type of company, and major foreign markets. The information is obtained from the FT900 and the Business Register (BR) and maintained in the Importer and Exporter Databases.

USA Trade Online (UTO) is an interactive online database for U.S. international trade data. It is the key dissemination tool for U.S. export and import statistics using the Harmonized System (HS) and North American Industry Classification System (NAICS) commodity classification system. This powerful tool allows users to create customized reports for port-level detail, state exports/imports, balance of trade, market level ranking, etc. Government agencies, businesses, and the academic community use this system at all times to advance their mission.

(a) Whether it is a general support system, major application, or other type of system

The Foreign Trade Division applications consists of major applications.

(b) System location

The Foreign Trade Division applications are located at the Census Bureau Headquarters, Suitland, MD.

(c) Whether it is a standalone system or interconnects with other systems (identifying and describing any other systems to which it interconnects)

IT systems covered by the Foreign Trade Division connect with the Automated Commercial Environment (ACE), which is managed and supported by the Department of Homeland Security Customs and Border Protection (DHS/CBP). Connections are also to internal Census Bureau IT systems covered by the Center for Enterprise Dissemination (CED), Data Communications systems, & Economic Census and Surveys and Special Processing Economic Census and Surveys and Special Processing systems. Connections are also to IT systems of the Canadian Exchange.

(d) The way the system operates to achieve the purpose(s) identified in Section 4

Following is a description of how the Foreign Trade Division applications operate to achieve the purpose(s) identified in Section 4.

FT900:

The electronic collection method for imports is the Automated Commercial Environment (ACE), which is managed and supported by the DHS/CBP.

Additional gas and electric import data are provided electronically to the Census Bureau's Economic Applications Division (EAD) via the Canadian Data Exchange (in coordination with Statistics Canada) and to the Foreign Trade Zones (FTZ). Each time import data is processed (five times for each statistical month), Canada receives micro data from the Census Bureau consisting of trade data detailed records showing imports from Canada to the US. Data includes Harmonized System (HS) code, district, port, method of transportation, foreign port, quantity, shipping weight, entry month, importer, etc. For each record, there are a total of 86 fields that are sent.

The Census Bureau's Governments and Trade Management Division (GTMD) has an office in Puerto Rico that processes import data keyed from paper documents via the Puerto Rico Data Capture System (PRDCS). Import documents are delivered to the Puerto Rico site via U.S. mail from each of the ports maintained by the DHS/CBP. The documents are secured in a locked file cabinet when not in use and eventually shredded.

The data collection mechanism for reporting exports is the ACE. ACE data transmissions occur daily. The information collected by the ACE is referred to as Electronic Export Information (EEI).

The Canadian Data Exchange also provides electronic data to the Census Bureau on

U.S. exports to Canada which is maintained by this IT system.

Importer and Exporter Databases:

Information used is matched with edited import and export data acquired from the ACE during the FT900 Press Release process; the Census Bureau's Business Register data, which contains Federal Tax Information (FTI); and Economic Census and Survey data.

USA Trade Online (UTO):

The following describes the UTO Update process. During the FT-900 Press Release closeout phase all ASCII files for the UTO data load and SQL cube creation are provided. The data provision process results in placing the UTO data on a server on Press Release day at 8:30AM. Upon completion, EAD programming staff verify that the UTO website is updated with the most recent statistical data.

The UTO is a web application that provides subscription users with U.S. trade data. It has two major components. One is the user authentication account management application, and the other provides users with a graphic user interface for searching the U.S. trade database and generating reports.

(e) How information in the system is retrieved by the user

The Foreign Trade Division FT900 component monthly produces the U.S. International Trade in Goods and Services press release. Regarding the Foreign Trade Importer and Exporter Databases components, during September/October of each year, final extracts are created for the current year and compiled into a final Report. General public users subscribe to the Foreign Trade Division UTO application by providing information; such as email address, city, country, locality, postal code, organization type, phone number and information required for selecting Security questions.. Once the subscription is completed, users can access U.S. trade data to generate customized reports.

(f) How information is transmitted to and from the system

For the FT900 please see the discussion above in section (d). For the Importer and Exporter Databases components, files are transmitted via Secure File Transfer Protocol (SFTP) from Foreign Trade Division servers to the Center for Enterprise Dissemination's server. General public users access UTO through a secured URL (https) using a browser.

(g) Any information sharing conducted by the system

Following is a description of how the Foreign Trade Division shares collected information.

FT900:

The FT900 is the U.S. official report on U.S. trade statistics and is used by U.S. and foreign government agencies, and private companies to establish business

trends and develop business plans.

Information from this IT system that is shared or made available with other agencies is secured through standardized language in Memorandums of Understanding (MOU) or Interagency Agreements as detailed in the Foreign Trade Statistics Security Guidelines for Federal Government Agencies handbook. An example of sharing conducted by this system are: Information shared monthly (bulk transfer) with the Bureau of Economic Analysis for the joint FT900 Press Release and with the Bureau of Industry and Security. In addition, there are several other federal agencies that enter into agreements to receive information from the Foreign Trade Division components on a case-by-case basis.

As previously mentioned, data is also shared with Canada via SFTP from the Census Bureau to Canada's servers.

Importer and Exporter Databases:

During September/October of each year, final extracts are created for the current year and compiled into a final Report. There are two reports comprising the final Report: One section of the report provides just the "highlights" of the report and, the other section is the full report. Before the final report is released, all tables containing disclosure must be reviewed and approved by the Census Bureau's Disclosure Review Board (DRB). All tables to be released are sent to the DRB Chairman for review.

The Profile of U.S. Exporters is partially sponsored by the Department of Commerce International Trade Administration (ITA). The profile is a set of aggregated exhibits showing industry and size characteristics of the companies that import and export goods. In return, the Census Bureau's Economic Statistical Methods Division, International Trade Evaluations Branch (formerly the Special Projects Branch in ITMD) tabulates an additional 26 tables for the ITA after the final Report is released to the public.

Information from this IT system shared within the Census Bureau is documented in the Data Management System. The data provided to the CEN13 server annually are edited transaction-level import and export data (Nets), the annual Exporter Database (EDB) and the annual Importer Database (IDB).

(h) The specific programmatic authorities (statutes or Executive Orders) for collecting, maintaining, using, and disseminating the information

The legal authority is 13 U.S.C. Chapter 9, Section 301(a), Foreign Trade Statistical Regulations or its successor document, the Foreign Trade Regulations, both in Title 15, CFR part 30; and Title 19, CFR 24.5, and Executive Order 13695.

(i) The Federal Information Processing Standards (FIPS) 199 security impact category for the system

The Federal Information Processing Standards (FIPS) 199 security impact category

is moderate.

Section 1: Status of the Information System

1.1 Indicate whether the information system is a new or existing system.

_____ This is a new information system.

_____ This is an existing information system with changes that create new privacy risks.
(Check all that apply.)

Changes That Create New Privacy Risks (CTCNPR)					
a. Conversions		d. Significant Merging		g. New Interagency Uses	
b. Anonymous to Non-Anonymous		e. New Public Access		h. Internal Flow or Collection	
c. Significant System Management Changes		f. Commercial Sources		i. Alteration in Character of Data	
j. Other changes that create new privacy risks (specify):					

_____ This is an existing information system in which changes do not create new privacy risks, and there is not a SAOP approved Privacy Impact Assessment.

X This is an existing information system in which changes do not create new privacy risks, and there is a SAOP approved Privacy Impact Assessment (version 01-2015 or 01-2017).

_____ This is an existing information system in which changes do not create new privacy risks, and there is a SAOP approved Privacy Impact Assessment (version 01-2019 or later).

Section 2: Information in the System

2.1 Indicate what personally identifiable information (PII)/business identifiable information (BII) is collected, maintained, or disseminated. (Check all that apply.)

Identifying Numbers (IN)					
a. Social Security*		f. Driver's License		j. Financial Account	
b. Taxpayer ID	X	g. Passport	X	k. Financial Transaction	
c. Employer ID	X	h. Alien Registration		l. Vehicle Identifier	X
d. Employee ID		i. Credit Card		m. Medical Record	
e. File/Case ID					
n. Other identifying numbers (specify):					
*Explanation for the business need to collect, maintain, or disseminate the Social Security number, including truncated form:					
In regards to Identifying Numbers,					

Collected from: U.S.
 Exporters/Importers
 Dissemination: This level of detail is only provided to other federal agencies for which it has been deemed can receive it based upon a National Interest Determination (NID) by the Census Bureau Director.

General Personal Data (GPD)

a. Name	X	h. Date of Birth		o. Financial Information	
b. Maiden Name		i. Place of Birth		p. Medical Information	
c. Alias		j. Home Address	X	q. Military Service	
d. Gender		k. Telephone Number	X	r. Criminal Record	
e. Age		l. Email Address	X	s. Physical Characteristics	
f. Race/Ethnicity		m. Education		t. Mother's Maiden Name	
g. Citizenship		n. Religion			

u. Other general personal data (specify):

In regards to General Personal Data,
 Collected from: U.S.
 Exporters/Importers
 Dissemination: This level of detail is only provided to other federal agencies for which it has been deemed can receive it based upon a National Interest Determination (NID) by the Census Bureau Director.
 Also Collected from: UTO users. Anyone can sign up for UTO, so this includes the general public, state and federal employees, and contractors. This information is not disseminated.

Work-Related Data (WRD)

a. Occupation		e. Work Email Address	X	i. Business Associates	
b. Job Title		f. Salary		j. Proprietary or Business Information	
c. Work Address		g. Work History		k. Procurement/contracting records	
d. Work Telephone Number	X	h. Employment Performance Ratings or other Performance Information			

l. Other work-related data (specify):

In regards to Work Related Data,
 Collected from: U.S. Exporters/Importers
 Dissemination: This level of detail is only provided to other federal agencies for which it has been deemed can receive it based upon a National Interest Determination (NID) by the Census Bureau Director.
 Also Collected from: UTO users. Anyone can sign up for UTO, so this includes the general public, state and federal employees, and contractors. This information is not disseminated.

Distinguishing Features/Biometrics (DFB)

a. Fingerprints		f. Scars, Marks, Tattoos		k. Signatures	
b. Palm Prints		g. Hair Color		l. Vascular Scans	
c. Voice/Audio Recording		h. Eye Color		m. DNA Sample or Profile	
d. Video Recording		i. Height		n. Retina/Iris Scans	
e. Photographs		j. Weight		o. Dental Profile	

p. Other distinguishing features/biometrics (specify):

System Administration/Audit Data (SAAD)

a. User ID	X	c. Date/Time of Access	X	e. ID Files Accessed	
b. IP Address	X	f. Queries Run		f. Contents of Files	
g. Other system administration/audit data (specify):					

In regards to System Administration Audit Data,
Collected from: UTO users. Anyone can sign up for UTO, so this includes the general public, state and federal employees, and contractors. This information is not disseminated.

Other Information (specify)

2.2 Indicate sources of the PII/BII in the system. *(Check all that apply.)*

Directly from Individual about Whom the Information Pertains					
In Person		Hard Copy: Mail/Fax	X	Online	X
Telephone	X	Email	X		
Other (specify):					

Government Sources					
Within the Bureau	X	Other DOC Bureaus	X	Other Federal Agencies	X
State, Local, Tribal		Foreign	X		
Other (specify):					

Non-government Sources					
Public Organizations		Private Sector	X	Commercial Data Brokers	
Third Party Website or Application			X		
Other (specify):					

2.3 Describe how the accuracy of the information in the system is ensured.

Data on U.S. exports of merchandise from the U.S. to all countries, except Canada, is compiled from the Electronic Export Information (EEI) filed by the USPPi or their agents through ACE. The EEI is unique among Census Bureau data collection methods since it is not sent to respondents soliciting responses as in the case of surveys. Each EEI represents a shipment of one or more kinds of merchandise from one exporter to one foreign importer on a single carrier. Filing the EEI is mandatory under Chapter 9, Title 13, United States Code. Qualified exporters or their agents submit EEI data by automated means directly to the U.S. Census Bureau.

Published data on U.S. imports of merchandise is compiled primarily from automated data submitted through ACE. Data are also compiled from import entry summary forms, warehouse withdrawal forms and Foreign Trade Zone documents as required by law to be filed with the U.S. Customs and Border Protection. Data on imports of electricity and natural gas from Canada are obtained from Canadian sources.

The export and import data collected via ACE, have upfront edits and response messages that are sent to the filer of the data to confirm accuracy of the reported information. Certain error messages, such as missing or inaccurate information, will not allow the

import or export data to be reported and submitted to the U.S. Government, until the error is resolved. Furthermore, Census Bureau staff contacts importers and exporters to verify erroneous data.

Pertaining to UTO, upon the creation of a new account, users get an email to verify the email address entered is their own. They have access to their account if they would like to update any of the information that is collected about themselves. In order to ensure their account is their own, users answer three security questions.

2.4 Is the information covered by the Paperwork Reduction Act?

X	Yes, the information is covered by the Paperwork Reduction Act. Provide the OMB control number and the agency number for the collection. The OMB control number is 0607-0152
	No, the information is not covered by the Paperwork Reduction Act.

2.5 Indicate the technologies used that contain PII/BII in ways that have not been previously deployed. *(Check all that apply.)*

Technologies Used Containing PII/BII Not Previously Deployed (TUCBPNPD)			
Smart Cards		Biometrics	
Caller-ID		Personal Identity Verification (PIV) Cards	
Other (specify):			

X	There are not any technologies used that contain PII/BII in ways that have not been previously deployed.
---	--

Section 3: System Supported Activities

3.1 Indicate IT system supported activities which raise privacy risks/concerns. *(Check all that apply.)*

Activities			
Audio recordings		Building entry readers	
Video surveillance		Electronic purchase transactions	
Other (specify):			

X	There are not any IT system supported activities which raise privacy risks/concerns.
---	--

Section 4: Purpose of the System

- 4.1 Indicate why the PII/BII in the IT system is being collected, maintained, or disseminated.
(Check all that apply.)

Purpose			
For a Computer Matching Program		For administering human resources programs	
For administrative matters	X	To promote information sharing initiatives	
For litigation		For criminal law enforcement activities	X
For civil enforcement activities	X	For intelligence activities	
To improve Federal services online	X	For employee or customer satisfaction	X
For web measurement and customization technologies (single-session)		For web measurement and customization technologies (multi-session)	X
Other (specify): For Statistical Purposes			

Section 5: Use of the Information

- 5.1 In the context of functional areas (business processes, missions, operations, etc.) supported by the IT system, describe how the PII/BII that is collected, maintained, or disseminated will be used. Indicate if the PII/BII identified in Section 2.1 of this document is in reference to a federal employee/contractor, member of the public, foreign national, visitor or other (specify).

The Census Bureau International Trade Management Division has the primary responsibility for the collection and compilation, while the Economic Indicators Division is responsible for the dissemination of data on U.S. exports, imports, and merchandise trade balances that are essential in formulating basic policy decisions affecting the economy.

For Statistical Purposes:

The Foreign Trade statistics collected from information obtained from importers and exporters are processed and released as the FT900. They are a principal economic indicator providing a complete count of American import and export transactions based on information that importers and exporters must file with the DHS/CBP. The data provide measures of the competitiveness and strength of domestic manufacturers help measure the market for various goods; and allow computation of apparent consumption. They are essential for economic policymaking, providing information used in the National Accounts and provide data essential for monitoring trade agreements and for measuring the impact of imports on the U.S. economy.

The Importer Database is information collected from importers to the U.S. that provides both government and private sector users with information about the importing community including employment size, type of company, and major foreign markets. The Exporter Database is data collected from U.S. exporters to the U.S. that provide both government and

private sector users with information about the exporting community including employment size, type of company, and major foreign markets.

The PII/BII collected by UTO is being used to create accounts for access to already published international merchandise trade data and is in reference to federal employee/contractor, member of the public, foreign national, and DOC employee. This application provides users the ability to save their customized reports.

For Civil and Criminal Enforcement activities Purposes (performed by Federal agencies receiving the Foreign Trade Statistics per a National Interest Determination):

- Improving compliance with U.S. export laws and regulations;
- Detecting and preventing violations of export, census, customs, homeland security, national resource, and other laws, regulations and treaties;
- Analysis to assess threats to U.S. and international security such as money laundering, and other potential violations of U.S. and foreign criminal laws;
- Enforcement of U.S. export-related laws and regulations;
- Investigation and prosecution of possible violations of U.S. export-related laws and regulations.

- 5.2 Describe any potential threats to privacy, such as insider threat, as a result of the bureau's/operating unit's use of the information, and controls that the bureau/operating unit has put into place to ensure that the information is handled, retained, and disposed appropriately. (For example: mandatory training for system users regarding appropriate handling of information, automatic purging of information in accordance with the retention schedule, etc.)

As we move towards a "single window" under the Automated Commercial Environment, as a result of Executive Order 13659 "Streamlining the Export/Import Process for America's Businesses", which moves import and export reporting and accessibility into a single window, data sharing challenges may arise. More federal agencies will have visibility to import and export data, which may lead to the possibility of confidential information being shared.

Privacy concerns also pertain to unauthorized access to importer and exporter company information. Census Bureau employees utilizing Foreign Trade systems must annually complete Data Stewardship Awareness and Title 26 Awareness training. They also must annually read and sign Rules of Behavior documents. Foreign Trade related information are purged in accordance with the Census record schedule N1-029-11-1.

The DHS/CBP ACE system uses a multitude of security controls mandated by the Federal Information Security Management Act of 2002 (FISMA) and various other regulatory control frameworks including the National Institute of Standards and Technology (NIST) special publication 800 series. These security controls include, but are not limited to the use of

mandatory HTTPS for public facing websites, access controls, anti-virus solutions, enterprise auditing/monitoring, encryption of data at rest, and various physical controls at DHS facilities that house Information Technology systems.

Only authorized government/contractor personnel are allowed to access PII/BII within a system. Authorizations for users occur yearly, at a minimum in accordance with applicable Bureau, Agency, and Federal policies/guidelines. In addition to system processes that handle PII/BII, all manual extractions for PII/BII are logged and recorded per Department of Commerce Policy, the NIST 800- 53 Appendix J Privacy Control Catalog, and specifically NIST control AU-03, Content of Audit records.

Section 6: Information Sharing and Access

- 6.1 Indicate with whom the bureau intends to share the PII/BII in the IT system and how the PII/BII will be shared. *(Check all that apply.)*

Recipient	How Information will be Shared		
	Case-by-Case	Bulk Transfer	Direct Access
Within the bureau		X	X
DOC bureaus	X	X	
Federal agencies	X	X	
State, local, tribal gov't agencies			
Public			
Private sector			
Foreign governments	X	X	
Foreign entities			
Other (specify):			

<input type="checkbox"/>	The PII/BII in the system will not be shared.
--------------------------	---

- 6.2 Does the DOC bureau/operating unit place a limitation on re-dissemination of PII/BII shared with external agencies/entities?

X	Yes, the external agency/entity is required to verify with the DOC bureau/operating unit before re-dissemination of PII/BII.
<input type="checkbox"/>	No, the external agency/entity is not required to verify with the DOC bureau/operating unit before re-dissemination of PII/BII.
<input type="checkbox"/>	No, the bureau/operating unit does not share PII/BII with external agencies/entities.

6.3 Indicate whether the IT system connects with or receives information from any other IT systems authorized to process PII and/or BII.

X	<p>Yes, this IT system connects with or receives information from another IT system(s) authorized to process PII and/or BII. Provide the name of the IT system and describe the technical controls which prevent PII/BII leakage:</p> <p>The connected system is the Automated Commercial Environment (ACE), which is managed and supported by the Department of Homeland Security Customs and Border Protection (DHS/CBP). The DHS/CBP ACE connectivity for the receipt of data by the Census Bureau is established through a secure VPN between the Census Bureau and the Department of Homeland Security Redundant Trusted Internet Connection. In addition, the Foreign Trade Division receives Business Register information from the Economic Applications Division and authentication information from the Data Communications IT system.</p> <p>The Foreign Trade Division uses a multitude of security controls mandated by the Federal Information Security Management Act of 2002 (FISMA) and various other regulatory control frameworks including the National Institute of Standards and Technology (NIST) special publication 800 series. These security controls include, but are not limited to the use of mandatory HTTPS for public facing websites, access controls, anti-virus solutions, enterprise auditing/monitoring, encryption of data at rest, and various physical controls at the Census Bureau facilities that house Information Technology systems. The Census Bureau also deploys an enterprise Data Loss Protection (DLP) solution as well.</p>
	No, this IT system does not connect with or receive information from another IT system(s) authorized to process PII and/or BII.

6.4 Identify the class of users who will have access to the IT system and the PII/BII. (*Check all that apply.*)

Class of Users			
General Public		Government Employees	X
Contractors	X		
Other (specify):			

Section 7: Notice and Consent

7.1 Indicate whether individuals will be notified if their PII/BII is collected, maintained, or disseminated by the system. (*Check all that apply.*)

X	Yes, notice is provided pursuant to a system of records notice published in the Federal Register and discussed in Section 9.	
X	Yes, notice is provided by a Privacy Act statement and/or privacy policy. The Privacy Act statement and/or privacy policy can be found at: http://www.census.gov/about/policies/privacy/privacy-policy.html	
	Yes, notice is provided by other means.	Specify how:
	No, notice is not provided.	Specify why not:

7.2 Indicate whether and how individuals have an opportunity to decline to provide PII/BII.

X	Yes, individuals have an opportunity to decline to provide PII/BII.	Specify how: For UTO, users are consenting to providing PII/BII by signing up for access to the system. Users are not required to sign into UTO to gain access to international trade data as it is available in other formats on the Census Bureau website.
X	No, individuals do not have an opportunity to decline to provide PII/BII.	Specify why not: For FT900 the data collection is mandatory. For the Importer and Exporter databases there is no direct data collection.

7.3 Indicate whether and how individuals have an opportunity to consent to particular uses of their PII/BII.

X	Yes, individuals have an opportunity to consent to particular uses of their PII/BII.	Specify how: For UTO, there is a notice and consent warning when users log in.
X	No, individuals do not have an opportunity to consent to particular uses of their PII/BII.	Specify why not: For FT900 the data collection is mandatory. For the Importer and Exporter databases there is no direct data collection.

7.4 Indicate whether and how individuals have an opportunity to review/update PII/BII pertaining to them.

X	Yes, individuals have an opportunity to review/update PII/BII pertaining to them.	Specify how: Individuals have access to reports generated by Census Bureau staff containing their transactions and these transactions must be updated if an error is identified. For UTO, users have the ability to change their own information within the system.
	No, individuals do not have an opportunity to review/update PII/BII pertaining to them.	Specify why not:

Section 8: Administrative and Technological Controls

8.1 Indicate the administrative and technological controls for the system. *(Check all that apply.)*

X	All users signed a confidentiality agreement or non-disclosure agreement.
X	All users are subject to a Code of Conduct that includes the requirement for confidentiality.
X	Staff (employees and contractors) received training on privacy and confidentiality policies and practices.
X	Access to the PII/BII is restricted to authorized personnel only.
X	Access to the PII/BII is being monitored, tracked, or recorded. Explanation: Only authorized government/contractor personnel are allowed to access PII/BII within a system. Authorizations for users occur yearly, at a minimum in accordance with applicable Bureau, Agency, and Federal policies/guidelines. In addition to system processes that handle PII/BII, all manual extractions for PII/BII are logged and recorded per Department of Commerce Policy, the NIST 800-53 Appendix J Privacy Control Catalog, and specifically NIST control AU-03, Content of Audit records.
X	The information is secured in accordance with the Federal Information Security Modernization Act (FISMA) requirements. Provide date of most recent Assessment and Authorization (A&A): <u>July 6, 2020</u> <input type="checkbox"/> This is a new system. The A&A date will be provided when the A&A package is approved.

X	The Federal Information Processing Standard (FIPS) 199 security impact category for this system is a moderate or higher.
X	NIST Special Publication (SP) 800-122 and NIST SP 800-53 Revision 4 Appendix J recommended security controls for protecting PII/BII are in place and functioning as intended; or have an approved Plan of Action and Milestones (POA&M).
X	A security assessment report has been reviewed for the information system and it has been determined that there are no additional privacy risks.
X	Contractors that have access to the system are subject to information security provisions in their contracts required by DOC policy.
	Contracts with customers establish DOC ownership rights over data including PII/BII.
	Acceptance of liability for exposure of PII/BII is clearly defined in agreements with customers.
X	Other (specify): Publications are approved by the Disclosure Review Board

- 8.2 Provide a general description of the technologies used to protect PII/BII on the IT system. *(Include data encryption in transit and/or at rest, if applicable).*

The Census Bureau Information technology systems employ a multitude of layered security controls to protect BII/PII at rest, during processing, as well as in transit. These NIST 800-53 controls, at a minimum, are deployed and managed at the enterprise level including, but not limited to the following:

- Intrusion Detection | Prevention Systems (IDS | IPS)
- Firewalls
- Mandatory use of HTTP(S) for Census Bureau Public facing websites
- Use of trusted internet connection (TIC)
- Anti-Virus software to protect host/end user systems
- Encryption of databases (Data at rest)
- HSPD-12 Compliant PIV cards
- Access Controls

The Census bureau Information technology systems also follow the National Institute of Standards and Technology (NIST) standards including special publications 800-53, 800-63, 800-37 etc. Any system within the Census Bureau that contains, transmits, or processes BII/PII has a current authority to operate (ATO) and goes through continuous monitoring on a yearly basis to ensure controls are implemented and operating as intended. The Census Bureau also deploys a Data Loss Prevention solution as well.

Section 9: Privacy Act

- 9.1 Is the PII/BII searchable by a personal identifier (e.g, name or Social Security number)?

 X Yes, the PII/BII is searchable by a personal identifier.

 No, the PII/BII is not searchable by a personal identifier.

- 9.2 Indicate whether a system of records is being created under the Privacy Act, 5 U.S.C. § 552a. *(A new system of records notice (SORN) is required if the system is not covered*

by an existing SORN).

As per the Privacy Act of 1974, "the term 'system of records' means a group of any records under the control of any agency from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual."

X	Yes, this system is covered by an existing system of records notice (SORN). Provide the SORN name, number, and link. <i>(list all that apply):</i> COMMERCE/CENSUS-12 Foreign Trade Statistics: http://osec.doc.gov/opog/PrivacyAct/SORNs/census-12.html
	Yes, a SORN has been submitted to the Department for approval on <u>(date)</u> .
	No, this system is not a system of records and a SORN is not applicable.

Section 10: Retention of Information

10.1 Indicate whether these records are covered by an approved records control schedule and monitored for compliance. *(Check all that apply.)*

X	There is an approved record control schedule. Provide the name of the record control schedule: Census Bureau Schedule N1-029-11-1; GRS 3.1: General Technology Management Records; GRS 3.2: Information Systems Security Records; 4.1: Records Management Records; 4.2: Information Access and Protection Records; and GRS 4.3: Input Records, Output Records, and Electronic Copies
	No, there is not an approved record control schedule. Provide the stage in which the project is in developing and submitting a records control schedule:
X	Yes, retention is monitored for compliance to the schedule.
	No, retention is not monitored for compliance to the schedule. Provide explanation:

10.2 Indicate the disposal method of the PII/BII. *(Check all that apply.)*

Disposal			
Shredding	X	Overwriting	
Degaussing	X	Deleting	
Other (specify):			

Section 11: NIST Special Publication 800-122 PII Confidentiality Impact Level

11.1 Indicate the potential impact that could result to the subject individuals and/or the organization if PII were inappropriately accessed, used, or disclosed. *(The PII Confidentiality Impact Level is not the same, and does not have to be the same, as the Federal Information Processing Standards (FIPS) 199 security impact category.)*

	Low – the loss of confidentiality, integrity, or availability could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals.
--	---

X	Moderate – the loss of confidentiality, integrity, or availability could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals.
	High – the loss of confidentiality, integrity, or availability could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals.

11.2 Indicate which factors were used to determine the above PII confidentiality impact level.
(Check all that apply.)

	Identifiability	Provide explanation: PII/BII collected can be indirectly used to identify individuals or if combined with other data elements may uniquely identify an individual.
	Quantity of PII	Provide explanation: The collection is for Foreign Trade collections, therefore, a serious or substantial number of individuals would be affected if there was loss, theft or compromise of the data.
	Data Field Sensitivity	Provide explanation: The PII/BII, alone or in combination, may be relevant in some other contexts and may, in those contexts, make the individuals or the Census Bureau vulnerable to harm.
	Context of Use	Provide explanation: Disclosure of the act of collecting and using the PII/BII in this IT system or the PII/BII itself may result in serious harm to the individual or organization.
	Obligation to Protect Confidentiality	Provide explanation: PII/BII is protected under 13 U.S.C. 9 Sections.
	Access to and Location of PII	Provide explanation: The PII/BII is located on computers and on a network, and IT systems controlled by the Census Bureau. Access is limited to those with a need-to-know. Access is only allowed by Census Bureau-owned equipment outside of the physical locations owned by the Census Bureau only with a secure connection. Backups are stored at Census Bureau-owned facilities. Paper documents are secured in locked cabinets with access limited to Census Bureau with a need-to-know.
	Other:	Provide explanation:

Section 12: Analysis

12.1 Identify and evaluate any potential threats to privacy that exist in light of the information collected or the sources from which the information is collected. Also, describe the choices that the bureau/operating unit made with regard to the type or quantity of information collected and the sources providing the information in order to prevent or mitigate threats to privacy. (For example: If a decision was made to collect less data, include a discussion of this decision; if it is necessary to obtain information from sources other than the individual, explain why.)

The Census Bureau is responsible for collecting, compiling, and publishing export trade statistics for the United States under the provisions of Title 13, United States Code (U.S.C.), Chapter 9, Section 301. The EEI collected via the ACE is the primary source used for collecting export trade data, and the Census Bureau uses such data for statistical purposes only. The EEI is also used for export control purposes under Title 50, U.S.C., Export Administration Act, to detect and prevent the export of certain items by unauthorized parties or to unauthorized destinations or end users. Other Federal Agencies use the EEI to evaluate the impact of trade agreements and to monitor compliance with such agreements.

As we move towards a "single window" under the Automated Commercial Environment, as a result of Executive Order 13659 "Streamlining the Export/Import Process for America's Businesses", which moves import and export reporting and accessibility into a single window, data sharing challenges may arise. More federal agencies will have visibility to import and export data, which may lead to the possibility of confidential information being shared.

Under Title 13 U.S.C., Chapter 9 301(g), the Secretary of Commerce has the authority to disclose the export information, if he or she determines it is the best interest of the Nation. The Census Bureau, the Secretary's delegate for issuing National Interest Determinations (NIDs), has not authorized the DHS to share the export data with any foreign governments or for purposes beyond the enforcement of U.S. export laws and regulations.

12.2 Indicate whether the conduct of this PIA results in any required business process changes.

	Yes, the conduct of this PIA results in required business process changes. Explanation:
X	No, the conduct of this PIA does not result in any required business process changes.

12.3 Indicate whether the conduct of this PIA results in any required technology changes.

	Yes, the conduct of this PIA results in required technology changes. Explanation:
X	No, the conduct of this PIA does not result in any required technology changes.