Template Version Number: 01-2021

U.S. Department of Commerce
Bureau of Economic Analysis

Privacy Impact Assessment
for the
BEA's Estimation IT System (EITS)

Reviewed by: Donald Barnes, 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

Donald Barnes DONALD BARNES Digitally signed by DONALD BARNES Date: 2022.01.27 10:59:22 -05'00' 01/19/2022
Signature of Senior Agency Official for Privacy/DOC Chief Privacy Officer Date

U.S. Department of Commerce Privacy Impact Assessment
BEA's Estimation IT System (EITS)

Unique Project Identifier: 006-08-01-24-01-5252-00

Introduction: System Description

Provide a brief description of the information system.

BEA Estimation Information Technology System (BEA-EITS), encompasses all of BEA's information technology in support of its mission to promote a better understanding of the U.S. economy by providing the most timely, relevant, and accurate economic accounts data in an objective and cost-effective manner. The bureau, "produces some of the most closely watched U.S. economic statistics that influence critical financial decisions made by governments, businesses, and households."1 BEA-EITS is utilized in BEA's core business processes: data collection; analysis, tabulation, and estimation; and data dissemination.

Address the following elements:

(a) *Whether it is a general support system, major application, or other type of system*
The BEA Estimation IT System (BEA-EITS) is a major statistical application system.
System location
Suitland Federal Center, 2600 Silver Hill Rd, Suitland MD 20746; and Bowie Computer Center, 17101 Melford Blvd, Bowie MD 20715
Whether it is a standalone system or interconnects with other systems (identifying and describing any other systems to which it interconnects)
The BEA Estimation IT System (BEA-EITS) is made up of a portfolio of highly integrated and interdependent statistical and economic estimation subsystems.
The way the system operates to achieve the purpose(s) identified in Section 4
The BEA-EITS is a core statistical and economic processing system.
How information in the system is retrieved by the user
Information is retrieved by secure access to the system (user id, password, PIV. Card)
(b) *How information is transmitted to and from the system*
Bulk Transfers, Efile, Direct Access
(c) *Any information sharing conducted by the system*
BEA uses its survey data collected in compiling the national and international economic accounts. Aggregates derived from the reported data are also used by the agencies that are responsible for developing and implementing U.S. Government policies on international trade and investment. Business identifiable information collected by BEA is not shared with third parties.

(h) *The specific programmatic authorities (statutes or Executive Orders) for collecting, maintaining, using, and disseminating the information*
The International Investment and Trade in Services Survey Act (P.L. 94-472, 22 U.S.C. 3101-3108). BEA's authority is embodied in Title 15 of the U.S. Code, Section 171 et seq, which, provides for BEA's establishment and identifies its major functions and responsibilities. Section 1516 of Title 15 provides the Secretary of Commerce with authority to collect and disseminate statistical information. Departmental Organizational Order 35 further delegates this authority to the Director of BEA. Other laws and executive orders give BEA additional responsibility to perform specific functions. For example, the Bretton Woods Agreement Act (22 U.S.C. 286), as implemented by Executive Order No. 10033, requires that BEA make available balance of payments information, and the International Investment and Trade in Services Survey Act (22 U.S.C. 3101-3108) provides for collection of comprehensive data on international direct investment and trade in services.
(i) *The Federal Information Processing Standards (FIPS) 199 security impact category for the system*
Moderate - BEA complies with the Department's physical and environmental protection policy, as well as FIPS-201, which governs credentials and credential issuance. The purpose of BEA's Physical and Environmental controls is the physical protection of BEA's employees, data, facility, and IT infrastructure.

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.

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		g. Passport		k. Financial Transaction	
c. Employer ID		h. Alien Registration		l. Vehicle Identifier	
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:					

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		q. Military Service	
d. Gender		k. Telephone Number		r. Criminal Record	
e. Age		l. Email Address		s. Marital Status	
f. Race/Ethnicity		m. Education		t. Mother's Maiden Name	
g. Citizenship		n. Religion			
u. Other general personal data (specify):					

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	X	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):					

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

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		Online	
Telephone		Email			
Other (specify):					

Government Sources					
Within the Bureau	X	Other DOC Bureaus	X	Other Federal Agencies	X
State, Local, Tribal		Foreign			
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.

The accuracy of the information in the BEA-EITS is ensured by ensuring employees and contractors receive training on the uses and accuracy of the data collected by BEA. The information in the BEA-EITS is checked against source data by computer programs and methodology to check the accuracy of the data before the information is used.

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.
	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 (TUCPBNPD)			
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		To promote information sharing initiatives	
For litigation		For criminal law enforcement activities	
For civil enforcement activities		For intelligence activities	
To improve Federal services online		For employee or customer satisfaction	
For web measurement and customization technologies (single-session)		For web measurement and customization technologies (multi-session)	
Other (specify): Maximize U.S. competitiveness and enable economic growth for American industries, workers, and consumers.			

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).

There is a small sub-component of the BEA-EITS that involves a survey data collection program. This program covers U.S. direct investment abroad, foreign direct investment in the United States, and U. S. international trade in services. These surveys collect company confidential data only and have been approved by OMB under the PRA. BEA's economic statistics are regularly disseminated to the public. The BEA-EITS supports the production of approximately 15,000-time series estimates each month and thousands of other data produced quarterly and annually. BEA's economic data are of utmost importance to government and business decision-makers and to ensure the integrity and reliability of this data the privacy of identifiable information must be protected. The sensitive data processed in the BEA-EITS is company confidential, not personally sensitive. BEA-EITS does not include personally identifiable information.

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.)

BEA complies with the Department's physical and environmental protection policy, as well as FIPS-201, which governs credentials and credential issuance. BEA employees are required to complete mandatory security and privacy training regarding appropriate handling of information. Any potential threat, internal and external, to privacy as a result to the small amount of BII the agency collects is low and would have limited adverse effect on BEA's operations or individuals.

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	X
DOC bureaus			
Federal agencies			
State, local, tribal gov't agencies			
Public			
Private sector			
Foreign governments			
Foreign entities			
Other (specify):			

	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?

	Yes, the external agency/entity is required to verify with the DOC bureau/operating unit before re-dissemination of PII/BII.
	No, the external agency/entity is not required to verify with the DOC bureau/operating unit before re-dissemination of PII/BII.
X	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.

	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:
X	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.)*

	Yes, notice is provided pursuant to a system of records notice published in the Federal Register and discussed in Section 9.	
	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: _____.	
X	Yes, notice is provided by other means.	Specify how: The following statement is provided to all respondents to BEA surveys: The [International Investment and Trade in Services Survey] Act provides that your report to this Bureau is CONFIDENTIAL, and may be used only for analytical or statistical purposes.
	No, notice is not provided.	Specify why not:

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

	Yes, individuals have an opportunity to decline to provide PII/BII.	Specify how:
X	No, individuals do not have an opportunity to decline to provide PII/BII.	Specify why not: These data are as mandated by the International Investment and Trade in Services Survey Act (P.L. 94-472, 22 U.S.C. 3101-3108).

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: Without your prior written permission, the information filed in your report CANNOT be presented in a manner that allows it to be individually identified. Your report CANNOT be used for purposes of taxation, investigation, or regulation. Copies retained in your files are immune from legal process.
	No, individuals do not have an opportunity to consent to particular	Specify why not:

	uses of their PII/BII.	

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: Individual have the opportunity to review resubmit information by contacting the Bureau.
	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:
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): __02/14/2021_____ ☐ 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.
X	Contracts with customers establish DOC ownership rights over data including PII/BII.
X	Acceptance of liability for exposure of PII/BII is clearly defined in agreements with customers.
	Other (specify):

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).*

BEA uses PIV cards for secure access to the BEA-EITS. The process ensures PIV cards are provided only to authorized, identity-proofed individuals. GSA controls access at all physical access points, including the lobby entrance and exit, the loading doc. BEA controls work areas containing IT workstations and displays. Facility access is controlled through a physical access control system (PACS). Facility access is further controlled at entrance and exit points by security guards at the lobby and by mailroom staff at th e loading dock. Further security is provided by intrusion detection systems and closed-circuit television, which are monitored by the security guards. The Department of Homeland Security Federal Protective Service Mega Center provides 24 -7 response capability. Access to the lockup area during production of GDP and personal income estimates requires the approval of the Director or Deputy Director. Access to the Computer Center requires the approval of the Chief Information Officer or the Deputy Chief Information Officer. BEA controls access to media displaying sensitive material using locked offices, unshared printers, and timed screensaver lockout. Cipher locks and key locks are employed on individual offices as needed to secure sensitive material. BEA requires a building occupant with a valid PIV card to authorize visitors into the facility. Signage informs visitors that compliance with Title 18 U.S.C. and Title 41 CFR is required. Visitors must present a valid photo ID and manually sign a log, as well as submit to X-ray and magnetometer screening. During green, blue, and yellow DHS Threat Advisories, visitors who present a valid PIV card from a federal agency are exempt from X-ray and magnetometer screening. During visitor screening, the visitor's ID is scanned into the visitor management system (VMS), which retains the visitor's picture, name, contact information, and information about the ID.

Section 9: Privacy Act

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

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

__X__ 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."

	Yes, this system is covered by an existing system of records notice (SORN). Provide the SORN name, number, and link. *(list all that apply)*:
	Yes, a SORN has been submitted to the Department for approval on (date).
X	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: BEA's records control schedule is approved and is in compliance with NARA's Appraisal Archivist.
	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		Overwriting	
Degaussing		Deleting	X
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.)*

X	Low – the loss of confidentiality, integrity, or availability could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals.
	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:
	Quantity of PII	Provide explanation:
	Data Field Sensitivity	Provide explanation:
	Context of Use	Provide explanation:

	Obligation to Protect Confidentiality	Provide explanation:
	Access to and Location of PII	Provide explanation:
X	Other:	Provide explanation: Small amount BII collected, limited access through IT system.

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.)

There are no know threats to privacy that exist from the information collected by BEA. BEA does not collect PII on individuals. BEA collects a small amount of BII for survey purpose, the information is collected from the source of the information. The type and quantity of information collected is mandated by the International Investment and Trade in Services Survey Act. We consider the threat level to be low for this category and we have implemented controls.

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.