U.S. Department of Commerce
Bureau of Economic Analysis

Privacy Threshold Analysis
for the
Bureau of Economic Analysis
Introduction: This Privacy Threshold Analysis (PTA) is a questionnaire to assist with determining if a Privacy Impact Assessment (PIA) is necessary for this IT system. This PTA is primarily based from the Office of Management and Budget (OMB) privacy guidance and the Department of Commerce (DOC) IT security/privacy policy. If questions arise or further guidance is needed in order to complete this PTA, please contact your Bureau Chief Privacy Officer (BCPO).

Description of the information system and its purpose: Provide a general description of the information system in a way that a non-technical person can understand.

The E-Government Act of 2002 defines “information system” by reference to the definition section of Title 44 of the United States Code. The following is a summary of the definition: “Information system“ means a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information. See: 44 U.S.C. § 3502(8).

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.

b) System location
Suitland Federal Center, 2600 Silver Hill Rd, Suitland MD 20746 and Bowie Computer Center, 17101 Melford Blvd, Bowie MD 20715

c) 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.

d) The purpose that the system is designed to serve
The BEA-EITS is the core economic processing system and is the primary tool used to produce the production of the BEA’s economic accounts.

e) The way the system operates to achieve the purpose
The BEA-EITS is a core statistical and economic processing system.

f) A general description of the type of information collected, maintained, use, or disseminated by the system
The information collected is statistical data from US and foreign base companies. The BEA-EITS produces critical national (GDP), international, industry, and regional economic statistic accounts that enable the government, business decision-makers, and the public to understand the performance of the Nation’s economy.

g) Identify individuals who have access to information on the system
BEA employees and government contractors.

h) How information in the system is retrieved by the user
   Information is retrieved by secure access to the system (user id, password, PIV Card)

i) How information is transmitted to and from the system
   Bulk Transfers, Efile, Direct Access

Questionnaire:

1. What is the status of this information system?

   ___ This is a new information system. Continue to answer questions and complete certification.

   ___ This is an existing information system with changes that create new privacy risks. Complete chart below, continue to answer questions, and complete certification.

   Changes That Create New Privacy Risks (CTCNPR)

   a. Conversions  
   b. Anonymous to Non-Anonymous  
   c. Significant System Management Changes  
   d. Significant Merging  
   e. New Public Access  
   f. Commercial Sources  
   g. New Interagency Uses  
   h. Internal Flow or Collection  
   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. Continue to answer questions and complete certification.

   ____ 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 later). Skip questions and complete certification.

2. Is the IT system or its information used to support any activity which may raise privacy concerns?

   NIST Special Publication 800-53 Revision 4, Appendix J, states “Organizations may also engage in activities that do not involve the collection and use of PII, but may nevertheless raise privacy concerns and associated risk. The privacy controls are equally applicable to those activities and can be used to analyze the privacy risk and mitigate such risk when necessary.” Examples include, but are not limited to, audio recordings, video surveillance, building entry readers, and electronic purchase transactions.

   ___ Yes. Please describe the activities which may raise privacy concerns.

   ___ No
3. Does the IT system collect, maintain, or disseminate business identifiable information (BII)?

As per DOC Privacy Policy: “For the purpose of this policy, business identifiable information consists of (a) information that is defined in the Freedom of Information Act (FOIA) as “trade secrets and commercial or financial information obtained from a person [that is] privileged or confidential.” (5 U.S.C. 552(b)(4)). This information is exempt from automatic release under the (b)(4) FOIA exemption. "Commercial" is not confined to records that reveal basic commercial operations but includes any records [or information] in which the submitter has a commercial interest and can include information submitted by a nonprofit entity, or (b) commercial or other information that, although it may not be exempt from release under FOIA, is exempt from disclosure by law (e.g., 13 U.S.C.).”

____ Yes, the IT system collects, maintains, or disseminates BII about: (Check all that apply.)

___ Companies
___ Other business entities
___ No, this IT system does not collect any BII.

4. Personally Identifiable Information

4a. Does the IT system collect, maintain, or disseminate personally identifiable information (PII)?

As per OMB 07-16, Footnote 1: “The term ‘personally identifiable information’ refers to information which can be used to distinguish or trace an individual’s identity, such as their name, social security number, biometric records, etc... alone, or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, mother’s maiden name, etc...”

____ Yes, the IT system collects, maintains, or disseminates PII about: (Check all that apply.)

___ DOC employees
___ Contractors working on behalf of DOC
___ Members of the public
___ No, this IT system does not collect any PII.

If the answer is "yes" to question 4a, please respond to the following questions.

4b. Does the IT system collect, maintain, or disseminate PII other than user ID?

____ Yes, the IT system collects, maintains, or disseminates PII other than user ID.
___ No, the user ID is the only PII collected, maintained, or disseminated by the IT system.
4c. Will the purpose for which the PII is collected, stored, used, processed, disclosed, or disseminated (context of use) cause the assignment of a higher PII confidentiality impact level?

Examples of context of use include, but are not limited to, law enforcement investigations, administration of benefits, contagious disease treatments, etc.

____ Yes, the context of use will cause the assignment of a higher PII confidentiality impact level.

____ No, the context of use will not cause the assignment of a higher PII confidentiality impact level.

*If any of the answers to questions 2, 3, 4b, and/or 4c are “Yes,” a Privacy Impact Assessment (PIA) must be completed for the IT system. This PTA and the approved PIA must be a part of the IT system’s Assessment and Authorization Package.*
CERTIFICATION

___X___ I certify the criteria implied by one or more of the questions above apply to the BEA-EITS and as a consequence of this applicability, I will perform and document a PIA for this IT system.

_____ I certify the criteria implied by the questions above do not apply to the [IT SYSTEM NAME] and as a consequence of this non-applicability, a PIA for this IT system is not necessary.

Name of Information System Security Officer (ISSO) or System Owner (SO): Greg Lower

Signature of ISSO or SO: GREGORY LOWER

Digitally signed by GREGORY LOWER
Date: 2019.06.25 08:08:30 -04'00'

Date: __________

Name of Information Technology Security Officer (ITSO): Fredrick Carlson

Signature of ITSO: FREDERICK CARLSON

Digitally signed by FREDERICK CARLSON
Date: 2019.06.25 08:25:41 -04'00'

Date: __________

Name of Authorizing Official (AO): Brian Callahan

Signature of AO: BRIAN CALLAHAN

Digitally signed by BRIAN CALLAHAN
Date: 2019.06.25 07:57:44 -04'00'

Date: __________

Name of Bureau Chief Privacy Officer (BCPO): Janice Townsend

Signature of BCPO: JANICE TOWNSEND

Digitally signed by JANICE TOWNSEND
Date: 2019.06.24 15:26:40 -04'00'

Date: __________