Version Number: 01-2019

U.S. Department of Commerce
International Trade Administration (ITA)

Privacy Threshold Analysis
for the
eMenu

U.S. Department of Commerce Privacy Threshold Analysis

ITA/eMenu

Unique Project Identifier: 2380

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 (in a way that a non-technical person can understand) of the information system that addresses the following elements:*

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*
Major Application.

b) *System location*
AWS (Gov Cloud).

c) *Whether it is a standalone system or interconnects with other systems (identifying and describing any other systems to which it interconnects)*
Emenu system interconnects with:
- Pay.gov to process Credit Card/ACH transactions
- NIST to reconcile Credit Card/ACH transactions on a daily basis

d) *The purpose that the system is designed to serve*
Emenu system is an ITA enterprise wide system supporting program units within the ITA primarily the Global Markets (Commercial Service). The system provides the capability to find the products/services GM posts/offices offer, track client participation in events & services, collect any fee (through Pay.gov), and monitor post/office financial transactions. This also generates quality assurance surveys, and track results from clients. Locating an office and/or colleague capability is also available.

e) *The way the system operates to achieve the purpose*
This is a web based thin client, available through ITA supported internet browser.

f) A general description of the type of information collected, maintained, use, or disseminated by the system

The information collected, maintained or disseminated in the system is mostly public in nature. Some PII, such as ITA employee full name, email address, contact details (business phone and address), location, etc. is available. Some BII, such as client's name, contact details (business address and phone), email address, electronic purchase transactions are also available.

g) Identify individuals who have access to information on the system

The access to system is role based and controlled through ITA Directory maintained in Lotus Dominos.

h) How information in the system is retrieved by the user

Information is retrieved through the web browser using HTTPS over port 443 (SSL).

i) How information is transmitted to and from the system

Information is transmitted through web browser using HTTPS over port 443 (SSL).

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		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. *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). *Continue to answer questions and complete certification.*

__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 01-2017 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.

_X__ Yes. *(Check all that apply.)*

Activities			
Audio recordings		Building entry readers	
Video surveillance		Electronic purchase transactions	X

____ 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.)."

__X_ Yes, the IT system collects, maintains, or disseminates BII.

____ No, this IT system does not collect any BII.

4. Personally Identifiable Information (PII)

4a. Does the IT system collect, maintain, or disseminate PII?

As per OMB 17-12: "The term PII refers to information that can be used to distinguish or trace an individual's identity either alone or when combined with other information that is linked or linkable to a specific individual."

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

_X__ DOC employees
____ National Institute of Standards and Technology Associates
__X_ Contractors working on behalf of DOC
____ Other Federal Government personnel
____ 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 Social Security numbers (SSNs), including truncated form?

____ Yes, the IT system collects, maintains, or disseminates SSNs, including truncated form.

Provide an explanation for the business need requiring the collection of SSNs, including truncated form.

Provide the legal authority which permits the collection of SSNs, including truncated form.

_X__ No, the IT system does not collect, maintain, or disseminate SSNs, including truncated form.

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

_X__ 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.

4d. 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.

__X_ 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, 4c, and/or 4d 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 ITA eMenu 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 ITA eMenu and as a consequence of this non-applicability, a PIA for this IT system is not necessary.

Name of System Owner (SO): Michael Hunt

Signature of SO: Michael Hunt Digitally signed by Michael Hunt Date: 2020.03.26 15:02:45 -04'00' Date: _____

Name of Information Technology Security Officer (ITSO): Joe Ramsey

Signature of ITSO: JOSEPH RAMSEY Digitally signed by JOSEPH RAMSEY Date: 2020.04.28 13:45:14 -04'00' Date: _____

Name of Privacy Act Officer (PAO): Angenette Cash

Signature of PAO: ANGENETTE CASH Digitally signed by ANGENETTE CASH Date: 2020.03.27 08:53:05 -04'00' Date: _____

Name of Authorizing Official (AO): Rona Bunn

Signature of AO: RONA BUNN Digitally signed by RONA BUNN Date: 2020.05.03 13:26:37 -04'00' Date: _____

Name of Bureau Chief Privacy Officer (BCPO): Angenette Cash

Signature of BCPO: ANGENETTE CASH Digitally signed by ANGENETTE CASH Date: 2020.03.27 08:53:28 -04'00' Date: _____