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

Privacy Impact Assessment
for the
eMenu

Reviewed by: Angenette Cash, 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

CATRINA PURVIS Digitally signed by CATRINA PURVIS
Date: 2020.09.21 17:21:02 -04'00' 06/06/2020

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

U.S. Department of Commerce Privacy Impact Assessment
International Trade Administration/eMenu

Unique Project Identifier: 2380

<u>Introduction</u>: 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 ITA eMenu System is based upon n-tier architecture for flexibility and reusability. Several servers are being used to support various layers of the system that include web (presentation), application, and database layer. The following section provides a brief description of each layer.

1) Presentation Layer: The topmost layer of the application that displays information related to the services provided by the information system. It communicates with the application layer and sends or displays information via web page (comprising static and dynamic content) to both authenticated and non-authenticated ITA end-users and external clients. The web servers used are IBM HTTP Server (Apache) and IBM Domino HTTP Server running on Windows 2016 platform.
2) Application Layer: Controls application's functionality. It utilizes authentication and authorization services from the infrastructure and communicates with the database and presentation layers. The application servers used are WebSphere Application Server (WAS) and IBM Domino Server running on Windows 2016 platform.
3) Database Layer: Provides data persistence and access layer. The back-end database DB2.

eMenu 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. EMenu system was used to track performances, leads & highlights until June 1st 2015, since then this module is rendered read-only. This also generates quality assurance surveys, and track results from clients. Locating an office, colleague or a foreign commercial officer capability is also available.

The system is located in AWS on ITA network (DMZ/internal).\

The System interconnects with Pay.gov for payment transactions and the Commerce Business System (CBS) for reconciliation of those payment transactions.

The Whitepages module is a repository of GM/OCIO employees contact information and employees emergency contact information (name/phone only). Whitepages is also used to on-board/off-board GM/OCIO employees.

Access to eMenu is available from the ITA network. Users must first connect/authenticate to Citrix or Cisco Any Connect an prior to gaining access to eMenu. At which point a user must authenticate into eMenu using their eMenu credentials.

The eMenu application provides access through a web page/browser and has distinct user base: End-Users (public users), Local Users and Local Administrators. The end-users have access to the public domain only. The local users and the local administrators have access to the application domain. Local administrators also have administrative access at the system level (i.e., Windows 2016). The rights, privileges, and accesses are different between distinct user groups. The end-users do not have access to the Windows domain and cannot use domain resources. Therefore, end-users are restricted from performing the functions of local user and/or a local Administrator.

SAs, DBAs, application developers, configuration managers, and database users' access rights and privileges are based on user specific administrative tasks/functions. Administrators in each distinct support function are given only the rights, privileges, and access necessary to perform their role-based functions.

eMenu implements least privilege principles using the ACL and group roles.

The information is transmitted through HTTPS or SFTP.

Any information sharing conducted by the Commerce Business System (CBS): The CBS is the Department of Commerce's enterprise financial management system. It is implemented in all Commerce operating units, except the U.S. Patent and Trademark Office (USPTO) and the National Technical Information Service (NTIS), which have their own systems.

Pay.gov: Pay.gov was developed to meet the U.S. Treasury Financial Management Service (FMS) commitment to process collections electronically using Internet technologies. Pay.gov satisfies agencies and consumers demands for electronic alternatives by providing the ability to complete forms, make payments and submit queries 24 hours a day electronically. Launched in October 2000, Pay.gov is a secure government-wide collection portal. Pay.gov provides a suite of services allowing agencies to obtain and process collections in an efficient and timely manner. The Pay.gov application is comprised of 4 services: Collections (ACH and Credit Card), Forms, Billing/Notification, and Reporting. ITA utilizes Pay.gov for processing financial transactions.

Refer to MOU/ISA. The system has established MOUs and ISAs for information sharing with the following external partner information systems using a secure IP tunnel, augmented with Secure File Transfer protocol(SFTP) and encryption.

The FIPS 199 security category for the system 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.

____ 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).
__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).

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	X
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	X
b. Maiden Name		i. Place of Birth		p. Medical Information	

c. Alias		j. Home Address		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):					

Work-Related Data (WRD)					
a. Occupation		e. Work Email Address	X	i. Business Associates	
b. Job Title	X	f. Salary		j. Proprietary or Business Information	
c. Work Address	X	g. Work History			
d. Work Telephone Number	X	h. Employment Performance Ratings or other Performance Information			
k. Other work-related data (specify):					

Distinguishing Features/Biometrics (DFB)					
a. Fingerprints		d. Photographs		g. DNA Profiles	
b. Palm Prints		e. Scars, Marks, Tattoos		h. Retina/Iris Scans	
c. Voice Recording/Signatures		f. Vascular Scan		i. Dental Profile	
j. 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		d. Queries Run	X	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	X
Telephone		Email			
Other (specify):					

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

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

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

The PII/BII information such as employee name, telephone number, email address, Job Title is entered through eMenu White pages during onboarding process through New User Request and is verified by OCIO Customer Support. Financial transactions are reconciled by CBS on daily basis.

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. OMB Number 0625-0217
	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	X
Other (specify):			

	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	
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):			

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 general personal data and work-related data is collected from federal employee/contractor (including foreign service nationals) as PII in the Whitepages module. The Whitepages module serves as the system of record for user profile management. The BII (private/public sector company information) is collected for providing business services to facilitate trade/exports to meet the bureau’s mission.

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.)

All the information is collected over SSL connection using RSA 2048 bit/SHA 256 encryption. The data is stored in IBM DB2 database that resides on internal ITA Network behind ITA NOC approved firewall. All this application data must be retained as is for the operations and continuity of the Information System.

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
DOC bureaus	X	X	
Federal agencies	X		
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 Indicate whether the IT system connects with or receives information from any other IT systems authorized to process PII and/or BII.

X	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: **Pay.gov** system – the communication is conducted over SSL using PKI certificates.
	No, this IT system does not connect with or receive information from another IT system(s) authorized to

	process PII and/or BII.

6.3 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	X	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: https://emenuapps.ita.doc.gov/ePublic/Privacy_Act_Notice.htm .	
	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: The OMB approved form is used for financial transactions
	No, individuals do not have an opportunity to decline to provide PII/BII.	Specify why not:

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: The OMB approved form is used for financial transactions
	No, individuals do not have an opportunity to consent to particular uses of their PII/BII.	Specify why not:

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: The information collected using OMB approved form is available in read-only mode, upon submission.

	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.)*

	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: The information is accessible through the application to authorized ITA internal users. Only authorized DB admin can access the Database.
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): __5/31/2019__________ □ 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).*

The database is behind the firewall (internal network)
Access to the database is limited to the Application Development team and system administrator(s) only.
Access to the Web application is limited to internal application users over SSL connection using RSA 2048 bit/SHA 256 encryption only. Users are required to authenticate themselves. User roles are set up based on least privilege principle.

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. *(list all that apply)*: ITA-7 Export.gov; COMMERCE/DEPT-23 Information Collected Electronically in Connection with Department of Commerce Activities, Events, and Programs; COMMERCE/DEPT-2 Accounts Receivable; and COMMERCE/DEPT-18 Employees Personnel Files Not Covered by Notices of Other Agencies. http://www.osec.doc.gov/opog/PrivacyAct/PrivacyAct_SORNs.html
	Yes, a SORN has been submitted to the Department for approval on (date).
	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: DAA-GRS2013-0003-0001 36
	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	
Other (specify): Data is not deleted within eMenu database. Items marked by deleting are flagged as deleted but are not removed from system.			

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 levels. *(Check all that apply.)*

X	Identifiability	Provide explanation: Search is limited to name only.
X	Quantity of PII	Provide explanation: Collectively, the number of records collected generate an enormous amount of PII.
X	Data Field Sensitivity	Provide explanation: Name, email address, address, telephone numbers, and financial transactions.
X	Context of Use	Provide explanation: The use is limited to ITA employees/ contractors only. Tracking client participating, collection of fees, and monitor financial transactions.
	Obligation to Protect Confidentiality	Provide explanation:
X	Access to and Location of PII	Provide explanation: Limited to employees and contractors internal to ITA.
	Other:	Provide explanation:

<u>Section 12</u>: 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 is not planned method for the disposal of PII collected by the system if a user is removed, or if the system were to be disposed/retired.

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.