Version Number: 01-2017

U.S. Department of Commerce
Bureau of Industry and Security

Privacy Impact Assessment
for the
Commerce USXPORTS Exporter Support System (CUESS)

Reviewed by: Carol M. Rose, 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
DN: c=US, o=U.S. Government, ou=Department of Commerce, ou=Office of the Secretary, cn=CATRINA PURVIS, 0.9.2342.19200300.100.1.1=13001002875743
Date: 2018.04.19 15:47:41 -04'00'

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

U.S. Department of Commerce Privacy Impact Assessment
BIS/CUESS

Unique Project Identifier: 000552000

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.

(a) Whether it is a general support system, major application, or other type of system
The Commerce USXPORTS Exporter Support System (CUESS) program consists of components that were implemented to enable the Bureau of Industry and Security (BIS) to retire its costly mainframe system and support automated processes that were unique to Commerce/BIS. Interagency referrals are referred to the agencies through the Defense Technology Security Administration (DTSA USXPORTS system. Any licensing activity not supported by DTSA will transfer to CUESS. CUESS consists of the functionality of: Export Control Automated Support System (ECASS) Legacy and ECASS-Redesign that was not migrated to USXPORTS. CUESS also includes interfaces with other agencies not included in the USXPORTS system. These interfaces do not share PII with other agencies.
The CUESS server based components include Simplified Network Application Process (SNAP-R), Investigative Management System (IMS-R), System for Tracking Export License Applications (STELA) Web, Commodity Classifications (CCATS), Encryption Registration, License Determination (LD), Licensing Officer Access for Individual Validated License, BIS Automated Export System (BIS-AES), BIS Entity History System, Rubric, BIS Performance Reports, BECCI-2 (the secure infrastructure), and secure interagency data transfer between BIS and the inter-agencies that are not supported directly from the USXPORTS system (e.g. Department of Energy, DOD transfers, Customs Automated Export System (AES)) in support of the BIS export control licensing process. The Case Management Tool (CMT) was developed to replace the manual process for case notifications, tracking and reporting. Using CMT, OEE and OCC are able to systematically track case progress, warn of approaching milestone dates, adjust resources when there are bottlenecks, and report various performance statistics.
CUESS provides tools for BIS personnel to:

- *Perform data analysis and reporting,*
- *Automate many of the Export Enforcement lifecycle business processes,*
- *Make it easier to manage office workflow.*

CUESS carries export investigative information, which is currently categorized as high-impact data.

CUESS includes a case management solution for employees working for BIS to track and document export control-related investigation and outreach efforts. Specifically, IMS-R provides EE with the ability to manage export enforcement cases and leads electronically. IMS-R allows users to input data relating to investigations, including through the uploading of documents collected during an investigation.

IMS-R includes investigative, intelligence, and administrative data collected by BIS in the course of conducting its mission of advancing U.S. national security, foreign policy, and economic objectives by ensuring an effective export control and treaty compliance system and promoting continued U.S. strategic technology leadership. IMS-R includes information that will either directly identify an individual (such as a name or Social Security number, passport number and other law enforcement collected data as defined in Section 2) or that will indirectly identify an individual (such as date of birth and/or gender). Information about individuals may be input into structured fields or it may be included in areas in IMS-R where users can enter free text. In addition, documents uploaded onto the system may contain information about an individual (such as religious affiliation) that is not intentionally or systematically collected. In support of BIS's law enforcement function, IMS-R allows search and reporting capabilities to help uncover links between investigations. Information may be about U.S. citizens, legal permanent residents, or foreign nationals.

The purpose of this system is to maintain records that are related to the administration, enforcement, and implementation of the laws and regulations under the jurisdiction of BIS. Included in these records are individuals involved or identified in export transactions, export license applications, licenses, or other authorizations from BIS, and individuals identified in BIS export enforcement proceedings or suspected of violating statutes, regulations, or Executive Orders administered, enforced, or implemented by BIS.

(b) System location

The system is located in the HCHB.

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

The SNAP-R web application is a public facing website that is interconnected to the internet for the purpose of receiving export license applications and communicating updates with the exporter in compliance with the Export Administration Regulations.

CUESS back end modules run within the BECCI-2 General Support System (GSS) which is not interconnected to the internet. Besides daily synchronization of party coding and license determination data with CUESS which does not share information with any internal/external system. IMS-R is a component of CUESS used to manage cases and leads, establish unique entity codes for parties to a transaction, conduct party screening to monitor potential violations, and submit License Determination requests to the Licensing officers.

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

CUESS is running within the BIS Export Control Cyber Infrastructure V2 (BECCI-2) General Support System (GSS). Besides daily synchronization of party coding and license

determination data with CUESS, Personally Identifiable Information (PII) is not shared electronically with any external system. PII Data may be shared manually through court order or for law enforcement purposes. OMB M-01-05, Guidance on Inter-Agency Sharing of Personal Data

(e) The specific programmatic authorities (statutes or Executive Orders) for collecting, maintaining, using, and disseminating the information
Export Administration Act of 1979 (Pub L. 96-72, 50 U.S.C. 4601-4623)
Export Administration Regulations (EAR) (15 CFR Parts 730-774)
The Security Assistance Act of 2002 (13 U.S.C. § 305) and the Foreign Trade Regulations (15 CFR §§ 30.60 and 30.73)
International Emergency Economic Powers Act (IEEPA) as amended (50 U.S.C. §§ 1701-1706)
5 U.S.C. 301, 22 U.S.C. 401, 22 U.S.C. 8544, 28 U.S.C. 533-535, 44 U.S.C. 3101
United States Additional Protocol Implementation Act (Pub. L. 109-401)
Chemical Weapons Convention Implementation Act of 1998 (22 U.S.C. § 6701 et seq.)
Defense Production Act of 1950, as amended (50 U.S.C. § 4501 et seq.)
Fastener Quality Act, as amended (15 U.S.C. § 5401 et seq.).

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

The system is rated high as documented in the system security categorization memorandum, dated 09/29/15.

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

__x__ 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.

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*	x	e. File/Case ID	x	i. Credit Card	x
b. Taxpayer ID	x	f. Driver's License	x	j. Financial Account	x
c. Employer ID	x	g. Passport	x	k. Financial Transaction	x
d. Employee ID	x	h. Alien Registration	x	l. Vehicle Identifier	x
m. Other identifying numbers (specify):					

*Explanation for the need to collect, maintain, or disseminate the Social Security number, including truncated form: Law Enforcement agents collect and aggregate information on individuals involved or identified in export transactions, export license applications, licenses, or other authorizations from BIS, and individuals identified in BIS export enforcement proceedings or suspected of violating statutes, regulations, or Eos administered, enforced or implemented by BIS.

General Personal Data (GPD)					
a. Name	x	g. Date of Birth	x	m. Religion	x
b. Maiden Name	x	h. Place of Birth	x	n. Financial Information	x
c. Alias	x	i. Home Address	x	o. Medical Information	x
d. Gender	x	j. Telephone Number	x	p. Military Service	x
e. Age	x	k. Email Address	x	q. Physical Characteristics	x
f. Race/Ethnicity	x	l. Education	x	r. Mother's Maiden Name	x
s. Other general personal data (specify):					

As stated in the introduction, for purposes of this PIA, BIS does not distinguish between information collected on U.S. citizens and information collected on non-U.S. citizens. As part of its law enforcement activities, BIS may obtain and upload onto IMS-R documents on individuals that contain some categories of information that are not systematically collected but nevertheless become searchable through IMS-R's general search function.

Work-Related Data (WRD)					
a. Occupation	x	d. Telephone Number	x	g. Salary	x
b. Job Title	x	e. Email Address	x	h. Work History	x
c. Work Address	x	f. Business Associates	x		
i. Other work-related data (specify):					

Distinguishing Features/Biometrics (DFB)					
a. Fingerprints	x	d. Photographs	x	g. DNA Profiles	
b. Palm Prints	x	e. Scars, Marks, Tattoos	x	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	x
b. IP Address	x	d. Queries Run	x	f. Contents of Files	x
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	x	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	x	Foreign	x		
Other (specify):					

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

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

The information is actually tracked and confirmed by the case file and multiple requests from the applicant themselves. IMS-R provides two major auditing related functions. (i) First, for each IMS object such as Lead, Case, Organization, etc., a list of audit records can be displayed that tracks users' actions performed against the object, e.g. adding, viewing, and modifying the object. (ii) Secondly, IMS-R employs system level auditing records that track the changes of object data and is only accessible from a system management interface. This second type of auditing function uses raw database field names in the audit log table requires the assistance of database or system administrators to properly decipher

2.4 Is the information covered by the Paperwork Reduction Act?

	Yes, the information is covered by the Paperwork Reduction Act. Provide the OMB control number and the agency number for the collection.
x	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	x	To promote information sharing initiatives	x
For litigation	x	For criminal law enforcement activities	x
For civil enforcement activities	x	For intelligence activities	x
To improve Federal services online	x	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 purpose of this system is to maintain records that are related to the administration, enforcement, and implementation of the laws and regulations under the jurisdiction of BIS. Included in these records are members of the public and foreign nationals; individuals involved or identified in export transactions, export license applications, licenses or other authorizations form BIS, and individuals identified in BIS export enforcement proceedings or suspected of violating statutes, regulations or Eos administered, enforced or implemented by BIS:
Records may be disclosed to the general public, Federal, State, Local or International agencies in furtherance of BIS' mission, regarding individuals and entities whose export privileges have been denied or limited. This includes disclosure of information to the general public regarding individuals and entities that have been denied export privileges by BIS, or who are subject to additional restrictions and license requirements. This encompasses publishing this information in the Federal Register, in the Code of Federal Regulations on BIS' website, and by other means. Individuals and entities on the Denied Persons List are generally designated based on authorities denying or restricting their export privileges because of identified threats to the national security, foreign policy, and/or economy of the United States. Generally, the personal identifier information provided on the Denied Persons List may include, but is not limited to, names and aliases, addresses, dates of birth, citizenship information, and at times, identification numbers associated with government issued documents. It is necessary to provide this identifier information in a publicly available format so that listed individuals and entities can be identified and prevented from engaging in conduct otherwise prohibited by the Export Administration Regulations (EAR). The release of detailed identifier information of individuals is also important in helping protect other individuals from being improperly identified as the prohibited party. Because the Denied Persons List are posted on BIS' public website and published in the Federal Register and Code of Federal Regulations, a designated individual's identifier can be accessed by any individual or entity with access to the internet, the Federal Register, or the Code of Federal Regulations. Thus, the impact on the individual's privacy will be substantial, but this is necessary in order to make targeted denial orders and restrictions effective. Designated individuals can file an appeal or petition to request their removal from these lists. If such an appeal is granted, the individual's name and all related identifier information may be removed from the Denied Person's List.

5.2 Describe any potential threats to privacy 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.)

Individuals that handle the PII/BII receive annual refresher training on PII/BII and NSI. However, the CUESS back end modules are not interconnected to the internet nor does it share information with any internal/external systems and is only shared manually when requested by a court order for law enforcement requirements.

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		
Federal agencies	x		
State, local, tribal gov't agencies	x		
Public	x		
Private sector			
Foreign governments	x		
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.

	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.

6.3 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.	
	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: Privacy Statement Banners are included upon login where applicable.
x	No, notice is not provided.	Specify why not: Individuals whose information is collected as part of law enforcement investigations are not given specific notice of such collection as it could jeopardize the law enforcement investigation or reveal classified information such as sources and methods of collection.

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: For operational information individuals do not have an opportunity and/or right to decline to provide information.

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

	Yes, individuals have an opportunity to consent to particular uses of their PII/BII.	Specify how:
x	No, individuals do not have an opportunity to consent to particular	Specify why not: For operational information, individuals do not have an

	uses of their PII/BII.	opportunity to consent to particular uses of the information. Section 12(c) of the Export Administration Act provides procedures for the use and release of certain information, including information obtained for the purpose of consideration or concerning, license applications.

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 individual assigned as the account administrator can act on behalf of the company to review/update information. This is further detailed in the SNAP-R FAQs.
x	No, individuals do not have an opportunity to review/update PII/BII pertaining to them.	Specify why not: Individuals whose information is collected as part of an enforcement investigation are not given an opportunity to review or update information pertaining to them as it may jeopardize the law enforcement investigations or reveal classified information such as sources and methods of collection, including revealing to individuals that they are targets or potential targets of investigations.

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.
	Access to the PII/BII is being monitored, tracked, or recorded. Explanation:
x	The information is secured in accordance with FISMA requirements. Provide date of most recent Assessment and Authorization (A&A): 07/31/2017 ☐ 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).
	A security assessment report has been reviewed for the supporting 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 ownership rights over data including PII/BII.
	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).*

Paper records and discs are maintained in secure office areas with access limited to screened personnel whose official duties require access. Automated records are maintained on protected servers in data centers where data is encrypted at rest and access is limited to screened personnel whose official duties require access on a need to know basis which require a user ID and Password. Each user is required to log on to the system and log out, hence locking the system upon completion.

Section 9: Privacy Act

9.1 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)*: Commerce/BIS1 (Individuals Identified in Export Transactions and Other Matters http://www.osec.doc.gov/opog/PrivacyAct/SORNs/bis-1.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.)*

	There is an approved record control schedule. Provide the name of the record control schedule:
x	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: Retention and disposal practices are IAW NARA's General Records Schedule (GRS). Generally, records are retained for periods of 5-15 years unless a longer period is deemed necessary for investigative purposes or for permanent archival retention.
	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		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 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.
	Moderate – the loss of confidentiality, integrity, or availability could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals.
x	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: See Section 2
x	Quantity of PII	Provide explanation: See Section 2
x	Data Field Sensitivity	Provide explanation: See Section 2
x	Context of Use	Provide explanation:
x	Obligation to Protect Confidentiality	Provide explanation: PII confidentiality impact level of moderate
x	Access to and Location of PII	Provide explanation: See Section 6.1
	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 Export Administration Act 12c, provides procedure for the use and release of certain information obtained for the purpose of consideration concerning license applications; and The Denied Persons List or Export Enforcement laws and regulations are adhered to when collecting information for investigative purposes.

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.