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

Privacy Threshold Analysis
for the
Commerce USXPORTS Exporter Support System

U.S. Department of Commerce Privacy Threshold Analysis

BIS/CUESS

Unique Project Identifier: BIS022

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.*
The Commerce USXPORTS Exporter Support System (CUESS) program is a major application platform that resides on the BIS secure infrastructure.

b) *System location*
The system is located at the BIS data center in Manassas, VA.

c) *Whether it is a standalone system or interconnects with other systems (identifying and describing any other systems to which it interconnects)*
The Commerce USXPORTS Exporter Support System (CUESS) program interconnects with the following systems; These USXPORTS system interface enables partner agencies, associated with the Foreign national review process for Deemed exports, to support the license adjudication process for regulatory compliance.
The SNAP-R web application is a public facing website that is interconnected to the Internet for receiving export license applications and communicating updates with the exporter in compliance with the Export Administration Regulations.
The CUESS application platform resides on and executes within the BIS secure infrastructure environment. These systems work in tandem to provide a single integrated system view. CUESS back end modules run within the BIS secure infrastructure which has controlled and extremely limited-interconnections to the Internet. Besides daily synchronization of party coding and license determination data with extremely limited-interconnections to the Internet.

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. IMS-R implements daily synchronization of party coding and license determination data with the licensing review module of the system.

d) *The purpose that the system is designed to serve*
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.

e) *The way the system operates to achieve the purpose*
CUESS is running within the BIS secure infrastructure General Support System (GSS). Personally Identifiable Information (PII) would be shared electronically with specific external agencies for Foreign National review requirement deemed export licenses (CFR740.5: Civil End-users). For BIS Law enforcement, 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.

f) *A general description of the type of information collected, maintained, use, or disseminated by the system*
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 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 and BECCI process 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.
CUESS includes investigative, intelligence, and administrative data collected by BIS when

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. CUESS contains information that will either directly identify an individual (such as a name or Social Security number, passport number, visa status 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 CUESS Simplified Network Application Process (SNAP-R) module allows applicants to upload documents including their passport, resume and visa status as part of the Foreign National Review requirement for deemed exports licenses per the Export Administration Regulations (EAR), Section 734.2(b)(ii).

g) *Identify individuals who have access to information on the system*
Individuals that have access to CUESS includes export administration, export enforcement and interagency users authorized to review licenses for applicable regulatory compliance. 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, the BIS 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 can systematically track case progress, warn of approaching milestone dates, adjust resources when there are bottlenecks, and report various performance statistics.

h) *How information in the system is retrieved by the user*
Authorized Case Agents can retrieve case information using multi-factor authenticated access.

i) *How information is transmitted to and from the system*
All information is printed from the case file and manually input through data entry or scanned into the system by the agent assigned.

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.

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

Activities			
Audio recordings		Building entry readers	
Video surveillance		Electronic purchase transactions	
Other (specify): CUESS and BECCI process export investigative information, which is currently categorized as high-impact data.			

__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.)*

   ____ DOC employees
   ____ National Institute of Standards and Technology Associates
   ____ Contractors working on behalf of DOC
   ____ Other Federal Government personnel
   __X__ 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?

   __X__ 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. The system uses SSNs for individuals involved or identified in export transactions, export license applications, licenses, or individuals identified in BIS export enforcement proceeding or suspected of violating statutes, regulations, or Executive Orders administered, enforced, or implemented by BIS

Provide the legal authority which permits the collection of SSNs, including truncated form.
The Export Control Reform Act (ECRA) of 2018 (Section 1761(h)), formerly known 12c of the Export Administration Act (EAA) and the Denied Persons List or Export Enforcement laws and regulations are adhered to when collecting information for investigative purposes.

____ 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 USXPORTS Exporter Support System (CUESS) 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 USXPORTS Exporter Support System (CUESS) 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): Aleck Che-Mponda

Signature of ISSOor SO: ALECK CHE-MPONDA Digitally signed by ALECK CHE-MPONDA Date: 2021.07.28 18:46:06 -04'00' Date: 7-28-2021

Name of Information Technology Security Officer (ITSO): Ida Mix

Signature of ITSO: IDA MIX Digitally signed by IDA MIX Date: 2021.08.03 14:53:28 -04'00' Date: 08/03/2021

Name of Privacy Act Officer (PAO): Tiffany Daniel

Signature of PAO: TIFFANY DANIEL Digitally signed by TIFFANY DANIEL Date: 2021.08.03 15:15:12 -04'00' Date: 08/03/2021

Name of Authorizing Official (AO): Nagesh Rao

Signature of AO: G RAO Digitally signed by G RAO Date: 2021.08.03 17:03:10 -04'00' Date: 8/03/2021

Name of Bureau Chief Privacy Officer (BCPO): Carol Rose

Signature of BCPO: CAROL ROSE Digitally signed by CAROL ROSE Date: 2021.08.19 16:43:18 -04'00' Adobe Acrobat DC version: 2015.006.30527 Date: 08/19/2021