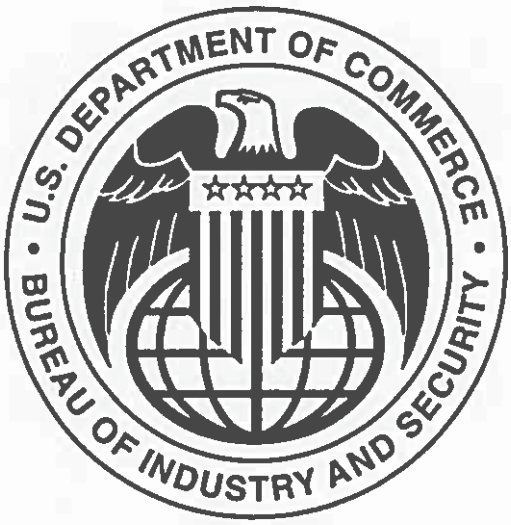
U.S. Department of Commerce
Bureau of Industry and Security



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 system. This PTA is primarily based from the Office of Management and Budget (OMB) privacy guidance and the Department of Commerce (DOC) privacy policy. If questions arise or further guidance is needed in order to complete this PTA, please contact your bureau Information Technology Security Officer (ITSO).

Description of the information system and its purpose:

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.

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).

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	X	d. Significant Merging	X	g. New Interagency Uses	X
b. Anonymous to Non-Anonymous		e. New Public Access		h. Internal Flow or Collection	X
c. 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. *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. *Please describe the activities which may raise privacy concerns.*

The mere possession of PII/BII raises privacy concern. Others activities: who has access to the data; unauthorized disclosure of the data; how is the data protected at rest, during transit, and processing;

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

___ **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 about: *(Check all that apply.)*

_X__ Companies
_X__ 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..."

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

____ DOC employees
____ Contractors working on behalf of DOC
_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 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.

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.

_X__ 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 CUESS and as a consequence of this applicability, I will perform and document a PIA for this system.

____ I certify the criteria implied by the questions above do not apply to the CUESS and as a consequence of this non-applicability, a PIA for this system is not necessary.

Name of Information Systems Security Officer (ISSO): Jawayne Davis

Signature of ISSO: Jawayne D [illegible] Date: 3/15/2018

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

Signature of ITSO: Ida M. Mix Date: 3/15/2018

Name of System Owner: Aleck Che-Mponda for

Signature of System Owner: Eddy Date: 4/17/18