Template Version Number: 01-2021

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

Privacy Impact Assessment
for the
Compliance Application and Reporting System (CARS)

Reviewed by: Keven Valentin, 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

NICHOLAS CORMIER Digitally signed by NICHOLAS CORMIER
Date: 2025.10.29 09:18:43 -04'00'

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

U.S. Department of Commerce Privacy Impact Assessment
Bureau of Industry and Security (BIS)
Compliance Application and Reporting System (CARS)

Unique Project Identifier: 000552001

Introduction: System Description

Provide a brief description of the information system.

The Bureau of Industry and Security (BIS), Office of Information and Communications Technology and Services (OICTS) is expanding the collection of data submitted to the Compliance Application and Reporting System (CARS) by parties subject to 15 C.F.R. § 791 and its subparts.

BIS's OICTS is responsible for implementing the information and communications technology and services (ICTS) Program for the Department of Commerce. OICTS evaluates ICTS transactions which include, but are not limited to, classes of transactions, and individual investigations on a case-by-case basis. 15 C.F.R. § 791 and its subparts apply to all the information collected, maintained, used, and disseminated by CARS. CARS is a web-based application that allows parties subject to 15 C.F.R. § 791 and its subparts to submit declarations of conformity, specific authorization requests, advisory opinion requests, general authorization notifications, general authorization reports, third party supporting information, independent audit reports, requests for additional information, materials and information responsive to OICTS inquiries and ongoing compliance activities, and general inquiries.

OICTS uses information submitted through CARS to monitor compliance with applicable regulatory requirements. Such information also serves as the basis for evaluating and issuing authorizations, as appropriate, under the governing regulatory framework.

Upon consideration of the details in a party's transaction as detailed in submissions to OICTS, OICTS may determine that the transaction is prohibited, not prohibited, or permit an otherwise prohibited transaction subject to the adoption of measures determined to sufficiently mitigate the risks associated with the ICTS transaction.

Address the following elements:

a) *Whether it is a general support system, major application, or other type of system*

CARS is a minor application.

b) *System location*

CARS is located within the Microsoft Azure Government Cloud East.

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

CARS is a minor application that leverages the security, access, and data services offered by Commerce USXPORTS Exporter Support System (CUESS) and BECCI-2.

CUESS: is an application platform comprised of cloud applications and services, which support BIS in carrying out its mission.

BECCI-2: is a general support system that provides the infrastructure used to support the BIS mission applications and services.

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

CARS is a web-based application accessed via the URL https://cars.bis.gov/. The application provides industry users with the ability to submit declarations of conformity, specific authorization applications, advisory opinion requests, general authorization notifications, general authorization reports, requests for additional information, third party supporting information, independent audit reports, materials and information responsive to OICTS inquiries and ongoing compliance activities, and general inquiries on a rolling or annual basis, pursuant to 15 C.F.R §791 and its subparts.

e) *How information in the system is retrieved by the user*

CARS uses application web-based interfaces to retrieve information in the system. Industry users or members of the public who are subject to 15 C.F.R §791 and its subparts must register an account and receive account approval by OICTS to submit or access information contained in the application. Once logged in, industry users can only access their own submissions.

OICTS personnel, whose official duties require access on a need-to-know basis, are provisioned and assigned to specific user roles. Once logged in, approved OICTS personnel can retrieve information within CARS via applicant/party name; affiliated entity; email address; corporate identifier; submission number; submission type; submission date; or submission status.

f) How information is transmitted to and from the system

Data is transmitted to and from CARS using Hypertext Transfer Protocol Secure (HTTPS) and application interfaces.

g) Any information sharing

Information may be shared on a case-by-case basis within the bureau or with other Federal Government personnel.

h) *The specific programmatic authorities (statutes or Executive Orders) for collecting, maintaining, using, and disseminating the information*

- Executive Order (E.O.) 13873, "Securing the Information and Communications Technology and Services Supply Chain," 84 FR 22689 (May 17, 2019);
- E.O. 14034, "Protecting Americans' Sensitive Data from Foreign Adversaries," 86 FR 31423 (June 9, 2021); and
- 15 C.F.R §791 and its subparts.

i) The Federal Information Processing Standards (FIPS) 199 security impact category for the System

CARS is a Moderate system.

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.

__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.

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	
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*: N/A					

General Personal Data (GPD)					
a. Name	X	h. Date of Birth	X	o. Financial Information*	X
b. Maiden Name		i. Place of Birth		p. Medical Information	
c. Alias		j. Home Address	X	q. Military Service	
d. Gender		k. Telephone Number	X	r. Criminal Record	
e. Age		l. Email Address	X	s. Marital Status	
f. Race/Ethnicity		m. Education		t. Mother's Maiden Name	
g. Citizenship	X	n. Religion			
u. Other general personal data (specify): ** Examples of Financial Information collected by CARS include significant ownership interest of companies and other regulated persons, or ultimate beneficial ownership.*					

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

Distinguishing Features/Biometrics (DFB)					
a. Fingerprints		f. Scars, Marks, Tattoos		k. Signatures	
b. Palm Prints		g. Hair Color		l. Vascular Scans	
c. Voice/Audio Recording		h. Eye Color		m. DNA Sample or Profile	

d. Video Recording		i. Height		n. Retina/Iris Scans	
e. Photographs		j. Weight		o. Dental Profile	
p. 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	f. Queries Run		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		Hard Copy: Mail/Fax		Online	X
Telephone		Email			
Other (specify):					

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

Non-government Sources					
Public Organizations		Private Sector		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.

CARS is secured using appropriate administrative, physical and technical safeguards against loss or unauthorized access, destruction, usage, modification, or disclosure. These safeguards adhere to security controls mandated by the Federal Information Security Modernization Act of 2014 (FISMA) and various other regulatory control frameworks including the National Institute of Standards and Technology (NIST) special publication 800 series. These security controls include but are not limited to the use of mandatory HTTPS for public facing websites, access controls based on role-based permissions, anti-virus solutions, enterprise auditing/monitoring, encryption of data at rest, and various physical controls at BIS facilities that house Information Technology systems.

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. 0694-0145
	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 no 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	X
For civil enforcement activities	X	For intelligence activities	
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).

CARS collects information about industry or regulated persons who are subject to 15 C.F.R §791 and its subparts. CARS provides users with the online convenience of submitting declarations of conformity, specific authorization applications, advisory opinion requests, general authorization notifications, general authorization reports, requests for additional information, third party supporting information, independent audit reports, materials and information responsive to OICTS inquiries and ongoing compliance activities, and general inquiries. The following provides an overview of the information collected and its use.

In a declaration of conformity, a party will certify (1) the extent of certain ICTS conditions and any required obligations created by 15 C.F.R. § 791 and its subparts, (2) they will maintain records, including documents, assessments, or otherwise, in support of the certification for a minimum of 10 years, and (3) they are able to provide the maintained records to OICTS upon request.

Parties to regulated ICTS transactions may submit a specific authorization application to demonstrate that the risk associated with the prohibited transaction in which they propose to engage is not undue or unacceptable. OICTS will use the information collected through the application process to evaluate whether the undue or unacceptable risk to U.S. national security of an otherwise prohibited ICTS transaction can be mitigated through the issuance of specific authorization, subject to the adoption of mitigation measures associated with the ICTS as determined by OICTS.

Parties can submit advisory opinion requests to solicit OICTS' guidance on whether prospective ICTS transactions is subject to a prohibition or requirement under 15 C.F.R. § 791 and its subparts. OICTS will use the information collected through advisory opinion requests to advise requesters on whether a prospective transaction is subject to a prohibition or other requirements.

Under certain regulations, some parties subject to such regulation may be required to submit general authorization notifications to avail themselves of general authorizations issued by OICTS for otherwise prohibited transactions. OICTS will issue general authorizations for regulated ICTS transactions where certain factors reduce the U.S. national security risk to an acceptable level. The information collected for general authorization notifications will generally take the form of certifications.

If parties availed themselves of general authorizations issued by OICTS for otherwise prohibited transactions, discovered a change in circumstance affecting their eligibility to qualify for the general authorization, and determined that the general authorization was used outside the conditions therein, those parties are required to submit to BIS reports identifying any prohibited transactions, the number of regulated items or services implicated, and the party's proposed remedial measures. OICTS will use this information to evaluate whether a violation of the rule may have occurred and inform what actions BIS may take as a result, if any.

Parties subject to 15 C.F.R. § 791 and its subparts may provide responses to OICTS' requests for additional information pertaining to any submission or declaration provided to OICTS. OICTS will use this information to clarify parties' submitted responses and inform OICTS' review of parties' prospective and regulated ICTS transactions.

Third parties affiliated with regulated ICTS transactions can submit materials or information as third party supporting information to support regulated parties' submissions. Third party affiliated parties include, but is not limited to, law firms and their representatives; accountants; consultants; financial firms; independent auditors; and persons involved in the supply chain of parties subject to 15 C.F.R. § 791 and its subparts. OICTS will use the information collected through third party supporting information to supplement its review of regulated entities' submissions regarding prospective or regulated ICTS transactions.

Parties subject to 15 C.F.R. § 791 and its subparts may be required to provide materials or information responsive to OICTS inquiries or ongoing compliance activities. OICTS will use the materials or information collected to evaluate parties' continued compliance with 15 C.F.R. § 791 and its subparts.

Finally, parties may submit general inquiries or engage with OICTS through the regular course of business regarding 15 C.F.R. § 791 and its subparts. OICTS will use the information collected through general inquiries to provide interpretive guidance and through such engagement to inform the administration of 15 C.F.R. § 791 and its subparts.

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.)

Potential threats to inappropriate disclosure of PII/BII, due to insider threats or adversarial attack to the systems, can lead to loss of confidentiality, accessibility, and integrity of information. To address these risks, BIS protects PII with reasonable security safeguards against loss or unauthorized access, destruction, usage, modification, or disclosure. These safeguards adhere to security controls mandated by the Federal Information Security Modernization Act of 2014 (FISMA) and various other regulatory control frameworks including the National Institute of Standards and Technology (NIST) special publication 800 series. These security controls include but are not limited to the use of mandatory HTTPS for public facing websites, access controls, anti-virus solutions, enterprise auditing/monitoring, encryption of data at rest, audit logs, and various physical controls at BIS facilities that house Information Technology systems.

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	X	X
DOC bureaus	X		
Federal agencies	X		
State, local, tribal gov't agencies	X		
Public			
Private sector			
Foreign governments			
Foreign entities			
Other (specify):			

	The PII/BII in the system will not be shared.

6.2 Does the DOC bureau/operating unit place a limitation on re-dissemination of PII/BII shared with external agencies/entities?

X	Yes, the external agency/entity is required to verify with the DOC bureau/operating unit before re-dissemination of PII/BII.
	No, the external agency/entity is not required to verify with the DOC bureau/operating unit before re-dissemination of PII/BII.
	No, the bureau/operating unit does not share PII/BII with external agencies/entities.

6.3 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: Again, CARS is a minor application that leverages the security, access, and data services offered by Commerce USXPORTS Exporter Support System (CUESS) and BECCI-2. Security safeguards for BECCI-2, and CUESS meet the NIST SP 800-53 (Rev. 5) requirements set forth in their respective System Security and Privacy Plan (SSPP), BIS Cybersecurity baseline policy, and other higher directives. BECCI-2 and CUESS are monitored to identify near real-time risks and vulnerabilities. Additional security controls include, but are not limited to, the use of mandatory HTTPS for public facing websites, access controls, anti-virus solutions, enterprise auditing/monitoring, encryption of data at rest and in transit, boundary protections (such as NEXTGEN firewalls; web application firewalls; endpoint security; and network segments) and various physical controls at BIS facilities that house Information Technology systems.
	No, this IT system does not connect with or receive information from another IT system(s) authorized to process PII and/or BII.

6.4 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		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://cars.bis.gov/privacy.	
X	Yes, notice is provided by other means.	Specify how: Through this PIA
	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: Providing information is voluntary and individuals or entities may decline to provide information.
	No, individuals do not have an opportunity to decline to provide PII/BII.	

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: Those subject to 5 C.F.R. § 791 and its subparts can choose to enter and submit the information to OICTS.
	No, individuals do not have an opportunity to consent to particular uses of their PII/BII.	

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: All FOIA and Privacy Act procedures are handled by the BIS Office of the Chief Financial Officer and Director of Administration (OCFO/DOA). All requests for CARS data unrelated to a pending criminal investigation or case will be forwarded to the Office of the Chief Counsel for Industry and Security (OCC-IS) for consultation. System data will be made available to BIS OCC-IS as needed.
	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.
	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: Audit logging into the security information and event management (SIEM) tool allows security operations analysts to monitor and track to PII/BII data management activities.
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): CARS is a minor application under CUESS whose most recent A&A was on 2/18/2025
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.
	Contracts with customers establish DOC 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).*

BIS protects PII with reasonable security safeguards against loss or unauthorized access, destruction, usage, modification, or disclosure. These safeguards adhere to security controls mandated by the Federal Information Security Modernization Act of 2014 (FISMA) and various other regulatory control frameworks including the National Institute of Standards and Technology (NIST) special publication 800 series. These security controls include but are not limited to the use of mandatory HTTPS for public facing websites, access controls, anti-virus solutions, enterprise auditing/monitoring, encryption of data at rest and in transit, boundary protections (such as NEXTGEN firewalls; web application firewalls; endpoint security; and network segments) and various physical controls at BIS facilities that house Information Technology systems.

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)*: BIS-1, Individuals Identified in Export Transactions and Other Matters Subject to BIS Jurisdiction. Note: BIS is currently implementing IT systems modernization. This SORN will be updated once modernization of this system is completed.
	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.
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: Records control schedule for OICTS is currently in the disposition determination phase.
	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	X
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, 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 level. *(Check all that apply.)*

X	Identifiability	Provide explanation: Information generated from the CARS application may either directly or indirectly identify an individual.
X	Quantity of PII	Provide explanation: Information generated from the CARS application may include moderate to large quantities of PII including an individual's name; date of birth; home address; and telephone number.
	Data Field Sensitivity	Provide explanation:
X	Context of Use	Provide explanation: Pursuant to 15 C.F.R §791 and its subparts, the collected information will be used by OICTS to operate a compliance program to ensure that parties to regulated ICTS transactions understand and comply with the regulation. OICTS' compliance team will review declarations of conformity, specific authorization applications, advisory opinion requests, general authorization notifications, general authorization reports, requests for additional information, third party supporting information, independent audit reports, materials and information responsive to OICTS inquiries and ongoing compliance activities, and general inquiries on a rolling or annual basis, as they are received.
	Obligation to Protect Confidentiality	Provide explanation:
X	Access to and Location of PII	Provide explanation: Access is restricted by a role-based and least privilege principles. Access by BIS authorized users to the CARS system requires PIV authentication. External non-BIS personnel are required to log-in solely with appropriate assigned credentials.
	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 privacy risk associated with sharing data within the CARS platform is that the data may be disclosed to individuals who do not require access and heightens the threat of the information being misused. Controls to mitigate these risks include Access restrictions to authorized officials; Only authorized use of information shared; Limits on uses and additional sharing; Maintaining retention periods or return of information shared, data destruction as well as utilizing Secure File Transfer Protocols for transmission of information. Information or documentary materials collected under this rule, and not otherwise publicly or commercially available, will not be released publicly. ICTS transactions related PII or business identifiable information (BII) is located on a network and IT system controlled by BIS. In addition to those disclosures generally permitted under the Privacy Act of 1974 (5 U.S.C. Section 552a(b), access to the information is limited to those with a need-to-know in accordance with the Department's published system of record notice (SORN) - Commerce/BIS-1, Individuals Identified in Export Transactions and Other Matters Subject to BIS Jurisdiction , December 8, 20215, 80 FR 7626; and the routine uses outlined therein.

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.