U.S. Department of Commerce
Bureau of Industry and Security (BIS)

Privacy Impact Assessment for
OMB Control No. 0694-0145
Compliance Application and Reporting System (CARS)

Reviewed by:

KEVEN VALENTIN
Digitally signed by KEVEN VALENTIN
Date: 2025.03.13 14:51:56 -04'00'

Keven Valentin/Bureau Chief Privacy Officer

Approved by:

CHARLES CUTSHALL
Digitally signed by CHARLES CUTSHALL
Date: 2025.03.13 15:41:06 -04'00'

Charles Cutshall, Chief Privacy Officer and Director of Open Government
U.S. Department of Commerce

Introduction: Why the information is being collected.

Executive Order (E.O.) 13873, ''Securing the Information and Communications Technology and Services Supply Chain,'' 84 FR 22689 (May 17, 2019) delegated to the U.S. Secretary of Commerce broad authority to prohibit or impose mitigation measures on any information and communications technology and services (ICTS) transaction with a foreign adversary nexus that is subject to United States jurisdiction and poses undue or unacceptable risks to the United States. BIS's Office of Information and Communications Technology and Services (OICTS) is responsible for implementing the Information and Communications Technology and Services (ICTS) Program for the Department of Commerce.

The rule—absent a general or specific authorization otherwise—(1) prohibits Vehicle Connectivity System (VCS) hardware importers from knowingly importing into the United States certain hardware for VCS; (2) prohibits connected vehicle manufacturers from knowingly importing into the United States completed connected vehicles incorporating covered software; and (3) prohibits connected vehicle manufacturers from knowingly selling within the United States completed connected vehicles that incorporate covered software. These prohibitions apply to transactions when such VCS hardware or covered software is designed, developed, manufactured, or supplied by persons owned by, controlled by, or subject to the jurisdiction or direction of the People's Republic of China (PRC) or the Russian Federation (Russia). The rule also (4) prohibits connected vehicle manufacturers who are persons owned by, controlled by, or subject to the jurisdiction or direction of the PRC or Russia from knowingly selling in the United States completed connected vehicles that incorporate VCS hardware or covered software (collectively, "Prohibited Transactions").

The new information collection will primarily take the form of Declarations of Conformity, specific authorizations applications, and advisory opinion requests.

Section 1: What information will be collected.

OICTS will collect the following information related to Declarations of Conformity, specific authorizations applications, and advisory opinion requests via a web-portal housed within the Commerce USXPORTS Exporter Support System (CUESS):

- Company name and address of the VCS hardware importer or connected vehicle manufacturer
- Identifying information (name, title, email address, phone number) for individual points of contact
- VCS hardware transaction information, including the FCC ID (if known), HTSUS code (optional), and how the VCS directly enables the function of the vehicle
- Covered software transaction information, including the system it enables and how the covered software directly enables the function of the vehicle
- Vehicle information, including the vehicle make, model, model year, trim, and VIN series
- Documentation in support of the application
- *For Declarations of Conformity specifically:* certifications and identifying information (name, email address, phone number) for an individual or entity that maintains the documentation and third-party assessments for the certification(s)

- *For specific authorization applications specifically:* significant ownership interests of the company, identifying information of the parties engaged in the otherwise prohibited transactions (company name, corporate identifiers, address, point of contact information, ultimate beneficial ownership, transaction role), the nature of the design, development, manufacture, or supply of the VCS hardware item or covered software item made by an entity owned by, controlled by, or subject to the jurisdiction or direction of the PRC or Russia, an internal controls assessment, security standards used, and other actions and proposals.

Section 2: How the information will be used.

Pursuant to 15 C.F.R §791.305, the collected information will be used by the Department's Office of Information and Communications Technology and Services (OICTS) to operate a compliance program to ensure that connected vehicle manufacturers and VCS hardware importers understand and comply with the regulation. OICTS's compliance team will review Declarations of Conformity, specific authorization applications, and advisory opinion requests on a rolling or annual basis, as they are received.

Connected vehicle manufacturers and VCS hardware importers will submit Declarations of Conformity to OICTS to attest that they are not engaging in Prohibited Transactions. The information collected for Declarations of Conformity will largely take the form of certifications. In a Declaration of Conformity, an entity will certify that their covered software or VCS hardware is not designed, developed, manufactured, or supplied by persons owned by, controlled by, or subject to the jurisdiction or direction of the PRC or Russia and attest that they maintain documents, assessments, or otherwise in support of the certification, and can furnish this documentation to OICTS upon request.

OICTS will use the information collected through specific authorization applications to evaluate whether an otherwise Prohibited Transaction can be mitigated through the issuance of a specific authorization. This information collection requirement is essential as OICTS must assess whether the information is substantial enough to demonstrate if the otherwise Prohibited Transaction does not pose undue and unacceptable risk to U.S. national security.

Finally, information collected through advisory opinion requests will be used to advise submitters on whether a prospective transaction is subject to a prohibition.

Section 3: Whether the information will be shared.

Information or documentary materials collected under this rule, and not otherwise publicly or commercially available, will not be released publicly except to the extent required by law on a need-to-know basis. Based on existing statutes, including the criminal provisions of 18 U.S.C. § 1905, federal employees disclosing confidential or business proprietary information may face civil and criminal penalties for doing so.

Section 4: Notice or opportunities to consent.

15 CFR Part 791 Subpart D requires connected vehicle manufacturers and VCS hardware importers to submit, on an annual basis, Declarations of Conformity in CARS. Further, connected vehicle manufacturers and VCS hardware importers may submit specific authorization applications and advisory opinion requests on an as-needed basis.

Lastly, BIS's Privacy Policy Statement is found at https://www.bis.gov/privacy-policy.

Section 5: How the information is secured.

Users must register an account and receive account approval by BIS/OICTS to access information contained in the application. Users can either be standard users or administrators. Personally Identifiable Information (PII) in CARS can be accessed by BIS/OICTS personnel whose official duties require access on a need-to-know basis and who are authenticated via their PIV credentials. The application is housed on the application platform within the BIS secure BECCI General Support System (High). For BIS access to CARS, users must be provisioned as a user in BECCI and assigned to specific user roles.

Section 6: Whether the information will be maintained in a Privacy Act system of records.

The information collected for CARS is not being maintained in a system of record. Any information retrieved within CARS is by reference to a company identifier or nonpersonal indexing scheme.

Section 7: Waiver from the Requirement to Publish the PIA (Optional)

N/A