Template Version Number: 01-2020

U.S. Department of Commerce
Office of the Secretary

Privacy Impact Assessment
for the
Commerce Connection Web Application

Reviewed by: Maria D. Dumas, 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

Jennifer Goode 09/14/2021

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

U.S. Department of Commerce Privacy Impact Assessment Commerce Connection Web Application

Unique Project Identifier: [Number]

Introduction: System Description

Provide a description of the system that addresses the following elements:

Connection.Commerce.gov is the Department of Commerce intranet for DOC employees. This internal portal contains agency information on bureaus within the agency. The web space leverages cloud-based services to provide employees with collaboration information. DOC employees using these collaboration tools are supported through Active Directory authentication and generally do not use the tools to collect information beyond business contact information unless otherwise approved.

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

Commerce Connection is a web application.

(b) System location

Commerce Connection is on the OCIO managed azure cloud environment (FIPS 99 moderate), by way of the Office of The Secretary Cloud Services Platform (OSCSP) General Support System (GSS). As described in the PIA for OSCSP, OSCSP is managed through both cloud and physical components residing within the Herbert Clark Hoover Building (HCHB). Physical system location of each cloud service within OSCSP is generally dependent on each vendor leveraging either Microsoft Azure or Amazon Web Services Infrastructure as a Service (IaaS)/Platform as a Service (PaaS).

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

Commerce Connection is a standalone application hosted on a multi-tenant web solution platform, which has an authority to operate.

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

When users go to Connection.Commerce.gov, they automatically see an internal web interface that connects them to the intranet, allowing them to view options of icons at the top of the screen for them select. Depending on the desired use of resources offered, users are offered a "2.0" experience, where they can send and receive information regarding any events or activities in the participating offices. One of those resources is the HTML/web form for the COVID Vaccine Attestation Survey, for a DOC Federal employee to complete. In order to review, complete, and submit the form or provide any other type of information into the system, the user is required to log in. Commerce Connection cannot be accessed without direct connection to the HCHBnet or via VPN. This web application is available to DOC Federal employees and contractors. Authentication occurs when the user connects with use of their PIV card. Sessions between users and Commerce Connection occurs over Secure Sockets Layer (SSL) to provide another layer of security. DOC Federal employees upload proof of vaccination to the COVID Vaccine Tracker website. The website will limit uploads to valid file formats and perform antivirus scans. Users attest to the upload vaccination proof by displaying the uploaded image back to the user.

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

Depending on the need of the user, information may be retrieved by way of completion of a form included in the application, which a Forms PTA is developed for such forms. DOC OCIO system administrators have access to the data via the aforementioned CSV file, where the data is drawn into a report and sent to the appropriate office within the DOC as a status report via encrypted e-mail.

(f) How information is transmitted to and from the system

DOC users are able to log into Commerce Connection and go to the specified location for the activity or resource desired. At that time, they manually input the information, to which data is collected. Upon submission of the data, the data is ingested into the system via a spreadsheet (CSV file) from a web form (i.e. for the Attestation form). The form is then manually sent via encrypted e-mail to the reviewer of the data. No interconnections are planned.

(g) Any information sharing conducted by the system

No information is being shared outside the accreditation boundary of this system. DOC OCIO system administrators (federal employees) within BIS, MBDA and OS will have access to all of the data collected. Drupal results are downloadable as a CSV, where the information from the the forms is collected. This information is then sent to the appropriate office within the DOC.

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

Legal authority to collect PII and/or BII is contained in the following laws or Executive Orders as it may apply: 5 U.S.C. 301; 44 U.S.C. 3101; E.O. 12107, E.O. 131614, 41 U.S.C. 433(d); 5 U.S.C. 5379; 5 CFR Part 537; DAO 202-957; E.O. 12656; Federal Preparedness Circular (65, July 26, 1999, DAO 210-110, E.O. 12554, Public Law 100-71, dated July 11, 1987 Executive Order 13991

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

Moderate

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.

__X__ 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	X
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): Federal employees must attest to vaccination or may also submit to testing using the COVID Vaccine Attestation Survey on the Connection.Commerce.gov application.					

____ 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.

____ 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 or 01-2017).

____ 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 01-2019 or later).

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	X	h. Alien Registration		l. Vehicle Identifier	
d. Employee ID		i. Credit Card		m. Medical Record	X
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:					

General Personal Data (GPD)					
a. Name	X	h. Date of Birth	X	o. Financial Information	
b. Maiden Name		i. Place of Birth		p. Medical Information	X*
c. Alias		j. Home Address		q. Military Service	
d. Gender	X	k. Telephone Number		r. Criminal Record	
e. Age	X	l. Email Address	X	s. Physical Characteristics	
f. Race/Ethnicity		m. Education		t. Mother's Maiden Name	
g. Citizenship		n. Religion			
u. Other general personal data (specify): The user will be required to login the system using their government email account, username and passcode for authentication. *As required by Executive Order 13991.					

Work-Related Data (WRD)					
a. Occupation		e. Work Email Address	X	i. Business Associates	
b. Job Title		f. Salary		j. Proprietary or Business Information	
c. Work Address		g. Work History		k. Procurement/contracting records	
d. Work Telephone Number		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	
b. IP Address		f. Queries Run		f. Contents of Files	
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		Other Federal Agencies	
State, Local, Tribal		Foreign			
Other (specify):					

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

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

The Commerce Connection web application consists of tools, in which the employee adding the information attests that the information is correct. Employees have to use VPN or authenticate using e-mail address. Two-factor authentication is required.

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. The Commerce Connection COVID Vaccine Attestation Survey is used for collecting medical information and resolution of HR-related requirements to validate DOC Federal Employees vaccination status. Commerce Connection (and OMB control numbers) are specific to the form being used to collect source information at the original point of collection.

	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	X
For administrative matters		To promote information sharing initiatives	
For litigation		For criminal law enforcement activities	
For civil enforcement activities		For intelligence activities	

To improve Federal services online		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).

Commerce Connection offers various resources to DOC employees and contractors, such as use of the staff directory, participating in contests, training or other events. With use of the staff directory, DOC employees and contractors may have names, e-mail addresses and phone numbers listed. The application also captures sensitive PII regarding DOC employees, as needed by the Office of Personnel Management (OPM) and Presidential Directive to collect the status of COVID-19 vaccination.
The information is pulled from the form into a CSV file, when a report is run by system administrators. The system administrators then send the report about DOC employees' vaccination status via an encrypted e- mail to the appropriate office within the DOC.

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.)

There are multiple potential threats to privacy, including insider threat. The system requires training for system users and management of information in accordance with retention schedules as well as the gamut of SP 800-53 controls required of a federal system. Additionally, the annual cybersecurity awareness training helps to mitigate the insider threat.

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			
Federal agencies			
State, local, tribal gov't agencies			
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?

	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.
X	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.

	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.

6.4 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			
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://www.commerce.gov/about/policies/privacy	
X	Yes, notice is provided by other means.	Specify how: Please see Attachment A.
	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: Pending any change of future Federal mandates, Federal employees will have the option not to provide their COVID-19 Vaccination Status.
	No, individuals do not have an opportunity to decline to provide PII/BII.	Specify why not:

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: Pending any change of future Federal mandates, Federal employees will have the option not to provide their COVID-19 Vaccination Status.
	No, individuals do not have an opportunity to consent to particular uses of their PII/BII.	Specify why not:

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: Pending any change of future Federal mandates, Federal employees will have the option not to provide their vaccination status through the Attestation Form, as applicable. Employees can control and verify their information being submitted.
	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.)*

X	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.
X	Access to the PII/BII is being monitored, tracked, or recorded. Explanation: This sub-service inherits auditing system security controls.
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): 05/05/2021 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).
X	A security assessment report has been reviewed for the information system and it has been determined that there are no additional privacy risks.
	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).*

All data is encrypted in transit, and at rest per NIST 800-53 System Security Controls, RMF NIST 37 Rev 2 and FedRAMP guidelines.

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)*: - OPM/GOVT-1 General Personnel Records - COMMERCE/DEPT-18 – Employee Personnel Files Not Covered By Other Agencies - OPM/GOVT – 10, Employee Medical File System of Records
X	Yes, a SORN has been submitted to the Department for approval on April, 27, 2021. COMMERCE/ DEPT-31, Public Health Emergency Records of Employees, Visitors, and Other Individuals at Department Locations
	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.)*

X	There is an approved record control schedule. Provide the name of the record control schedule: Office of the Secretary Records: nc1-040-79-01_sf115.
	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:
X	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	
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: DOC email and username are used as a unique identifier.
X	Quantity of PII	Provide explanation: The quantity of PII to be handled by the system causes for a moderate impact category.
X	Data Field Sensitivity	Provide explanation: DOC employees are limited to the amount of data to be entered into the Commerce Connection Vaccine Attestation form
X	Context of Use	Provide explanation: The context is limited to HR personnel only for capturing federal employee vaccination status.
X	Obligation to Protect Confidentiality	Provide explanation: The Federal Information Security Management Act of 2002 (FISMA) and the Privacy Act of 1974 obligate government agencies to protect sensitive data.
X	Access to and Location of PII	Provide explanation: Access is limited to DOC system administrators.

	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.)

There are multiple potential threats to privacy, to include insider threat. However, the system requires training for system users and management of information in accordance with retention schedules as well as the gamut of SP 800-53 controls required of a federal system. Administrators are also required to attend the annual cyber security awareness training, which helps to mitigate this threat.

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.

Please check the box below that coincides with your vaccination status.

Vaccination Status: As required by the White House and the Office of Management and Budget (OMB), please select the below statement that best describes your current vaccination status. *

- ○ **I am fully vaccinated — Employees are considered "fully vaccinated" two weeks after completing the second dose of a two-dose COVID-19 vaccine (e.g., Pfizer or Moderna) or two weeks after receiving a single dose of a one-dose vaccine (e.g., Johnson & Johnson/Janssen).**
- ○ **I am not yet fully vaccinated — I received my first dose of Moderna or Pfizer, and my second appointment is scheduled, or I received my final dose less than two weeks ago.**
- ○ **I have not been vaccinated.**
- ○ **I decline to respond.**

Employees who choose not to complete the form will be assumed to be not fully vaccinated for purposes of application of the safety protocols. If you are not vaccinated due to medical or religious reasons, please check either "I have not been vaccinated" or "I decline to respond." Note that if you have already received one dose of a vaccine, but are not yet fully vaccinated, or if you received your final dose less than two weeks ago, then you will be treated as not fully vaccinated until you are at least two weeks past your final dose and resubmit your vaccination information.

Supervisor Information

First Name *

Last Name *

E-mail *

I understand that a knowing and willful false statement on this form can be punished by fine or imprisonment or both (18 U.S.C. 1001). Checking "I decline to respond" does not constitute a false statement. I understand that making a false statement on this form could result in additional administrative action including an adverse personnel action up to and including removal from my position.

Certification of Vaccination for Federal Employees

Privacy Act Statement
Authority: We are authorized to collect the information requested on this form pursuant to Executive Order 13991, Protecting the Federal Workforce and Requiring Mask-Wearing (Jan. 20, 2021), Executive Order 12196, Occupational Safety and Health Program for Federal Employees (Feb. 26, 1980), and 5 U.S.C. chapters 11, and 79.
Purpose: This information is being collected and maintained to promote the safety of Federal buildings and the Federal workforce consistent with the above-referenced authorities, the COVID-19 Workplace Safety: Agency Model Safety Principles established by the Safer Federal Workforce Task Force, and guidance from Centers for Disease Control and Prevention and the Occupational Safety and Health Administration.
Routine Uses: While the information requested on this form is intended to be used primarily for internal purposes, in certain circumstances it may be necessary to disclose this information externally, for example to disclose information to: a Federal, State, or local agency to the extent necessary to comply with laws governing reporting of communicable disease or other laws concerning health and safety in the work environment; to adjudicative bodies (e.g., the Merit System Protection Board), arbitrators, and hearing examiners to the extent necessary to carry out their authorized duties regarding Federal employment; to contractors, grantees, or volunteers as necessary to perform their duties for the Federal Government; to other agencies, courts, and persons as necessary and relevant in the course of litigation, and as necessary and in accordance with requirements for law enforcement; or to a person authorized to act on your behalf. A complete list of the routine uses can be found in the system of records notice associated with this collection of information, OPM/GOVT-10, Employee Medical File System of Records, 75 Fed. Reg. 35099 (June 21, 2010), amended 80 Fed. Reg. 74815 (Nov. 30, 2015).
Consequence of Failure to Provide Information: Providing this information is voluntary. However, if you fail to provide this information, you will be treated as not fully vaccinated for purposes of implementing safety measures, including with respect to mask wearing, physical distancing, testing, travel, and quarantine.

Attestation *

- ☐ **I attest that the information provided in this form is accurate and true to the best of my knowledge.**

Submit

Please check the box below that coincides with your vaccination status.

Vaccination Status: As required by the White House and the Office of Management and Budget (OMB), please select the below statement that best describes your current vaccination status. *

- (●) **I am fully vaccinated — Employees are considered "fully vaccinated" two weeks after completing the second dose of a two-dose COVID-19 vaccine (e.g., Pfizer or Moderna) or two weeks after receiving a single dose of a one-dose vaccine (e.g., Johnson & Johnson/Janssen).**
- ( ) **I am not yet fully vaccinated — I received my first dose of Moderna or Pfizer, and my second appointment is scheduled, or I received my final dose less than two weeks ago.**
- ( ) **I have not been vaccinated.**
- ( ) **I decline to respond.**

Employees who choose not to complete the form will be assumed to be not fully vaccinated for purposes of application of the safety protocols. If you are not vaccinated due to medical or religious reasons, please check either "I have not been vaccinated" or "I decline to respond." Note that if you have already received one dose of a vaccine, but are not yet fully vaccinated, or if you received your final dose less than two weeks ago, then you will be treated as not fully vaccinated until you are at least two weeks past your final dose and resubmit your vaccination information.

Date of last vaccine dose received *

Year | Month | Day

Supervisor Information

First Name *

Last Name *

E-mail *

I understand that a knowing and willful false statement on this form can be punished by fine or imprisonment or both (18 U.S.C. 1001). Checking "I decline to respond" does not constitute a false statement. I understand that making a false statement on this form could result in additional administrative action including an adverse personnel action up to and including removal from my position.

Certification of Vaccination for Federal Employees

Privacy Act Statement

Authority: We are authorized to collect the information requested on this form pursuant to Executive Order 13991, Protecting the Federal Workforce and Requiring Mask-Wearing (Jan. 20, 2021), Executive Order 12196, Occupational Safety and Health Program for Federal Employees (Feb. 26, 1980), and 5 U.S.C. chapters 11, and 79.

Purpose: This information is being collected and maintained to promote the safety of Federal buildings and the Federal workforce consistent with the above-referenced authorities, the COVID-19 Workplace Safety: Agency Model Safety Principles established by the Safer Federal Workforce Task Force, and guidance from Centers for Disease Control and Prevention and the Occupational Safety and Health Administration.

Routine Uses: While the information requested on this form is intended to be used primarily for internal purposes, in certain circumstances it may be necessary to disclose this information externally, for example to disclose information to: a Federal, State, or local agency to the extent necessary to comply with laws governing reporting of communicable disease or other laws concerning health and safety in the work environment; to adjudicative bodies (e.g., the Merit System Protection Board), arbitrators, and hearing examiners to the extent necessary to carry out their authorized duties regarding Federal employment; to contractors, grantees, or volunteers as necessary to perform their duties for the Federal Government; to other agencies, courts, and persons as necessary and relevant in the course of litigation, and as necessary and in accordance with requirements for law enforcement; or to a person authorized to act on your behalf. A complete list of the routine uses can be found in the system of records notice associated with this collection of information, OPM/GOVT-10, Employee Medical File System of Records, 75 Fed. Reg. 35099 (June 21, 2010), amended 80 Fed. Reg. 74815 (Nov. 30, 2015).

Consequence of Failure to Provide Information: Providing this information is voluntary. However, if you fail to provide this information, you will be treated as not fully vaccinated for purposes of implementing safety measures, including with respect to mask wearing, physical distancing, testing, travel, and quarantine.

Attestation *

- ☐ **I attest that the information provided in this form is accurate and true to the best of my knowledge.**

Submit

Points of Contact and Signatures

Information System Security Officer or System Owner Name: Prabhjot Bajwa Office: US Department of Commerce Phone: 202-748-4252 Email: PBajwa@doc.gov I certify that this PIA is an accurate representation of the security controls in place to protect PII/BII processed on this IT system. Signature: Prabhjot Bajwa Digitally signed by Prabhjot Bajwa Date: 2021.08.24 16:09:02 -04'00' Date signed:	**Information Technology Security Officer** Name: Jerome Nash Office: US Department of Commerce Phone: 202-482-5929 Email: Jnash@doc.gov I certify that this PIA is an accurate representation of the security controls in place to protect PII/BII processed on this IT system. Signature: JEROME NASH Digitally signed by JEROME NASH Date: 2021.08.23 14:09:58 -04'00' Date signed:
Privacy Act Officer Name: Tahira Murphy Office: Office of Privacy and Open Government Phone: 202-482-8075 Email: Tmurphy2@doc.gov I certify that the appropriate authorities and SORNs (if applicable) are cited in this PIA. Signature: TAHIRA MURPHY Digitally signed by TAHIRA MURPHY Date: 2021.09.15 09:51:16 -04'00' Date signed:	**Authorizing Official** Name: Lawrence W. Anderson Office: US Department of Commerce Phone: 202-482-4444 Email: Landerson@doc.gov I certify that this PIA is an accurate representation of the security controls in place to protect PII/BII processed on this IT system. Signature: LAWRENCE ANDERSON Digitally signed by LAWRENCE ANDERSON Date: 2021.08.24 18:27:40 -04'00' Date signed:
Bureau Chief Privacy Officer Name: Maria D. Dumas Office: Office of Privacy and Open Government Phone: 202-482-5153 Email: mDumas@doc.gov I certify that the PII/BII processed in this IT system is necessary and this PIA ensures compliance with DOC policy to protect privacy. Signature: MARIA STANTON-DUMAS Digitally signed by MARIA STANTON-DUMAS Date: 2021.09.15 11:53:51 -04'00' Date signed:	

This page is for internal routing purposes and documentation of approvals. Upon final approval, this page must be removed prior to the publication of the PIA.