Template Version Number: 01-2020

U.S. Department of Commerce
Office of the Secretary

Privacy Threshold Analysis
for the
Commerce Connection Web Application

Template Version Number: 01-2020

U.S. Department of Commerce Privacy Threshold Analysis
Office of the Secretary
Commerce Connection Web Application

Unique Project Identifier:

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:*

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 199 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 purpose that the system is designed to serve

Commerce Connection is a web application designed as a multi-faceted tool for DOC Federal employees and contractors, for accessing relevant information for the various offices within DOC, linking people, training, and personnel resources.

e) The way the system operates to achieve the purpose

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.

f) A general description of the type of information collected, maintained, used, or disseminated by the system

The types of Personally Identifiable Information (PII) include name, email address, supervisor's name and email address, age, date of birth, medical information, COVID vaccination card, etc. All users will be authenticated before access is granted. The PII is Transport Layer Security (TLS) encrypted and data at rest encryption is compliant with FIPS 140-2.

g) Identify individuals who have access to information on the system

DOC Federal employees and contractors within BIS, MBDA and OS will have access to information shared on the application. However, only DOC employees and contractors assigned as system administrators have access to any data collected by the user. Drupal results are downloadable as a CSV, where the information from a form is collected. This information is then sent to the appropriate office within the DOC.

h) 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.

i) 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 sent manually via encrypted e-mail to the reviewer of the data. No interconnections are planned.

Questionnaire:

1. Status of the Information System

1a. What is the status of this information system?

_____ This is a new information system. *Continue to answer questions and complete certification.*

__X___ 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	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. *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 or 01-2017). *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 01-2019 or later). *Skip questions and complete certification.*

1b. Has an IT Compliance in Acquisitions Checklist been completed with the appropriate signatures?

____ Yes. This is a new information system.

____ Yes. This is an existing information system for which an amended contract is needed.

____ No. The IT Compliance in Acquisitions Checklist is not required for the acquisition of equipment for specialized Research and Development or scientific purposes that are not a National Security System.

__X__ No. This is not a new information system.

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):			

___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.)."

____ Yes, the IT system collects, maintains, or disseminates BII.

_X___ 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.)*

__X_ DOC employees
__X_ Contractors working on behalf of DOC
____ Other Federal Government personnel
____ 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?

____ 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.
Provide the legal authority which permits the collection of SSNs, including truncated form.

__X__ 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.

__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, 4c, and/or 4d are "Yes," a Privacy Impact Assessment (PIA) must be completed for the IT system. This PTA and the SAOP 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 Commerce Connection web application 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 Commerce Connection web application and as a consequence of this non-applicability, a PIA for this IT system is not necessary.

Information System Security Officer or System Owner Name: Prab Bajwa Office: OCIO/SDD Phone: 202-748-4252 Email: pbajwa@doc.gov Signature: Prabhjot Bajwa Digitally signed by Prabhjot Bajwa Date: 2021.08.24 16:10:10 -04'00' Date signed:	**Information Technology Security Officer** Name: Jerome Nash Office: OCIO/SSD Phone: 202-482-5929 Email: Jnash@doc.gov Signature: JEROME NASH Digitally signed by JEROME NASH Date: 2021.08.23 14:21:19 -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 Signature: TAHIRA MURPHY Digitally signed by TAHIRA MURPHY Date: 2021.09.15 08:13:42 -04'00' Date signed:	**Authorizing Official** Name: Lawrence W. Anderson Office: OCIO/OS Phone: 202-482-4444 Email: Landerson@doc.gov Signature: LAWRENCE ANDERSON Digitally signed by LAWRENCE ANDERSON Date: 2021.08.24 18:28:55 -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 Signature: MARIA STANTON-DUMAS Digitally signed by MARIA STANTON-DUMAS Date: 2021.09.15 11:58:01 -04'00' Date signed:	