Template Version Number: 01-2020

U.S. Department of Commerce
International Trade Administration (ITA)

Privacy Impact Assessment
for the
ITA Amazon Web Service Platform (ITA_AWS_PF)

Reviewed by: Chad Root, 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 09/21/2021

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

U.S. Department of Commerce Privacy Impact Assessment
[International Trade Administration/AWS Platform]

Unique Project Identifier: 2571

Introduction: System Description

Provide a description of the system that addresses the following elements:
The response must be written in plain language and be as comprehensive as necessary to describe the system.

(a) *Whether it is a general support system, major application, or other type of system:* General Support System (GSS)

(b) *System location:* The ITA AWS Platform is an Infrastructure as a Service (IaaS) Platform that provides ITA enterprise system infrastructure and architecture via cloud servers hosted and maintained by Amazon Web Services in the AWS US East cloud.

(c) *Whether it is a standalone system or interconnects with other systems (identifying and describing any other systems to which it interconnects):* The ITA AWS IaaS Platform utilizes cloud-based AWS communications components connected to ITA Headquarters (HQ) located in the Herbert C. Hoover Building (HCHB) in Washington, DC.

(d) *The way the system operates to achieve the purpose(s) identified in Section 4:* The AWS system is comprised of two distinct administrative domains: ITA's global network (comprising general users, legacy cloud datacenter infrastructure, System Operations functions (SysOps), and Security Operations (OpSec) personnel), and Active Directory (AD) (providing federated identity functions for ITA cloud services including ITA's Microsoft Office 365 tenant). Internet-facing traffic and processes are segregated within the DMZ Virtual Private Cloud (VPC), while ITA-internal traffic and processes reside within the separate Core VPC. These domains are further subdivided and secured using AWS Security Groups.

(e) *How information in the system is retrieved by the user:* Users access non-privileged information on the AWS platform via internet traffic routed through a Trusted Internet Connection (TIC) connected to the AWS DMZ VPC. Privileged access to ITA AWS resources (including server and security group controls) is available via HTTPS AWS Management Portal, only available to users with credentialed accounts controlled via AWS IAM. There is also a dedicated private point-to-point VPN connection between ITA HQ and AWS for internal traffic.

(f) *How information is transmitted to and from the system:* AWS provides internet connectivity through a local Internet Service Provider (ISP) that is routed through a Trusted Internet Connection (TIC)

(g) *Any information sharing conducted by the system:* The ITA AWS Platform collects PII solely for authentication purposes. Only PII necessary to authenticate the user's identity is collected by the system. ITA AWS shares PII solely within the Department of Commerce for the purposes of identity federation (i.e., a shared Global Address List between DoC agencies)

(h) The specific programmatic authorities (statutes or Executive Orders) for collecting, maintaining, using, and disseminating the information: 15 U.S.C. 1512

(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.
_____ 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):					

__X__ 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		h. Alien Registration		l. Vehicle Identifier	
d. Employee ID	X	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:					

General Personal Data (GPD)					
a. Name	X	h. Date of Birth		o. Financial Information	
b. Maiden Name		i. Place of Birth		p. Medical Information	
c. Alias		j. Home Address		q. Military Service	
d. Gender		k. Telephone Number		r. Criminal Record	
e. Age		l. Email Address		s. Physical Characteristics	
f. Race/Ethnicity		m. Education		t. Mother's Maiden Name	
g. Citizenship		n. Religion			
u. Other general personal data (specify):					

Work-Related Data (WRD)					
a. Occupation	X	e. Work Email Address	X	i. Business Associates	
b. Job Title	X	f. Salary		j. Proprietary or Business Information	
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	
b. IP Address	X	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	
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.

Users sign a Privacy Act statement consenting to and acknowledging the accuracy of their PII as part of their employment. Unused accounts are automatically disabled and/or removed on a schedule.

2.4 Is the information covered by the Paperwork Reduction Act?

	Yes, the information is covered by the Paperwork Reduction Act. Provide the OMB control number and the agency number for the collection.
X	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	
For administrative matters	X	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)	X	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).

The PII collected in Section 2.1 and maintained by ITA Technology, Innovation, and Services (TSI) is used for administrative purposes and to promote information sharing initiatives. The PII is collected from federal employees and contractors that use ITA systems. User ID's, IP addresses, Data and Time of access are collected for user access and cyber security investigative purposes.

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.)

To reduce the risk of account compromise, ITA employs appropriate security controls for the system in accordance with NIST 800-53, as described in Section 8.1 below. Additionally, insider threats are a potential threat to privacy. To combat this, ITA mandates annual refresher Cyber Security Awareness Training (CSAT) to maintain access to their ITA user accounts. ITA user accounts that are not compliant with annual CSAT requirements are disabled. ITA user accounts are also automatically disabled after 45 days of inactivity. Disabled accounts are reviewed monthly and deleted after 45 days of disablement. ITA users also consent to a System Use Notification when accessing ITA 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
DOC bureaus		X	
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.

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: ITA AWS Platform maintains a connection with ITA ADFS and the Physical Network Platform (PNP). The PNP system is comprised of routers and firewalls that direct ITA traffic to cloud hosted systems. ACLs and access management controls are in place to prevent PII leakage.
	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://connection.commerce.gov/sites/connection.commerce.gov/files/media/files/2014/citr-022_access_and_use.pdf .	
X	Yes, notice is provided by other means.	Specify how: ********** WARNING!....WARNING!....WARNING! **********This is a United States Government computer system, which may be accessed and used only for official Government business by authorized personnel. Unauthorized access or use of this computer system may subject violators to criminal, civil, and/or administrative action. All information on this computer system may be intercepted, recorded, read, copied, and disclosed by and to authorized personnel for official purposes, including criminal investigations. Access or use

		of this computer system by any person whether authorized or unauthorized, constitutes consent to these terms.
	No, notice is not provided.	Specify why not:

7.2 Indicate whether and how individuals have an opportunity to decline to provide PII/BII.

	Yes, individuals have an opportunity to decline to provide PII/BII.	Specify how:
X	No, individuals do not have an opportunity to decline to provide PII/BII.	Specify why not: This is an operational requirement by the Department of Commerce for all employees. Users accept the System Use Notification/Warning Banner whenever they authenticate into ITA IT systems.

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: Users waive control over the uses of their PII upon signing their Privacy Act agreement upon the initiation of their employment. Employees and contractors sign a written Access and Use policy which specifies that data they choose to provide in DOC systems (including ITA) are non-private and could be used for investigation purposes as per CITR-022.
	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: Users are permitted to review and update their PII data (e.g., in the event of a name change) via a service request ticket submitted to the ITA TSI Service Desk
	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: *Only authorized government/contractor personnel are allowed access to PII within the system. Authorizations for users occur annually, at a minimum in accordance with applicable Bureau, Agency, and Federal policies/guidelines. In addition, audit logs are in place and assessed per NIST control AU-03, Content of Audit Records.*
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): _____8/1/2021_____ ☐ 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.
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).*

Active Directory and other PII/BII sources are limited to privileged administrator access only. Non-credentialed users do not have access to these sources.
ITA IT systems employ a multitude of layered security controls to protect PII at rest, during processing, and in transit. These NIST 800-53 controls, at a minimum, are deployed and managed at the enterprise level, including (but not limited to) the following:

- Intrusion Detection / Prevention Systems (IDS/IPS)
- Firewalls
- Mandatory use of HTTPS for ITA public-facing websites
- Use of Trusted Internet Connection (TIC)
- Anti-virus software to protect host/end-user systems
- Encryption of databases
- HSPD-12 compliant PIV cards
- Access Controls

ITA IT systems also follow the NIST standards including special publications 800-53, 800-63, 800-37, etc. Any system within the ITA that contains, transmits, or processes PII has a

current authority to operate (ATO) and goes through continuous monitoring on a yearly basis to ensure controls are implemented and operating as intended. The ITA also deploys a DLP solution for further data protection.

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)*: COMMERCE/DEPT-25 Access Control and Identity Management System http://www.osec.doc.gov/opog/PrivacyAct/SORNs/dept-25.html provides coverage for the PII collected and maintained to facilitate secure on-line communication between Federal employees or contractors and to provide mechanisms for non-repudiation of personal identification and access to electronic systems. Content management sites, that contain PII beyond that covered by COMMERCE/DEPT-25, are governed by a SORN specific to the record types stored within the IT system and must be used in accordance with the purpose(s) enumerated in the SORN.
	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.)*

X	There is an approved record control schedule. Provide the name of the record control schedule: NARA General Records Schedule 5.1
	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: PII collected can be indirectly used to identify individuals or if combined with other data elements may uniquely identify an individual.
X	Quantity of PII	Provide explanation: The collection is for ITA bureau employees; therefore, a serious or substantial number of individuals would be affected if there was loss, theft, or compromise of the data.
X	Data Field Sensitivity	Provide explanation: The PII, alone or in combinations, may be relevant in some other contexts and may, in those contexts, make

		the individual or the Bureau vulnerable to harm.
	Context of Use	Provide explanation:
X	Obligation to Protect Confidentiality	Provide explanation: Covered under the Privacy Act
	Access to and Location of PII	Provide explanation:
X	Other:	Provide explanation: Previously noted connection to ITA ADFS services and network traffic routing through PNP components

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.)

Active Directory and other PII/BII sources are limited to privileged administrator access only. Non-credentialed users do not have access to these sources. Only PII/BII necessary to authenticate the user's identity is collected by the system. As such, PII implicated is generally non-sensitive, such as employee/contractor first name, last name, work email address, username, work phone number, office location, and other basic business contact information as necessary. As such the risk to privacy for this system is low. The primary risks to the system are information misuse or compromised accounts, with mitigations discussed in section 5.2 above.

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.