

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



**Privacy Threshold Analysis
for the
ITA Amazon Web Services Platform
(ITA_AWS_PF)**

U.S. Department of Commerce Privacy Threshold Analysis

[International Trade Administration/ ITA Amazon Web Services Platform]

Unique Project Identifier: 2571

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:*

The E-Government Act of 2002 defines “information system” by reference to the definition section of Title 44 of the United States Code. The following is a summary of the definition: “Information system” means a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information. See: 44 U.S.C. § 3502(8).

- 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 located in the Herbert C. Hoover Building (HCHB) in Washington, DC.
- d) *The purpose that the system is designed to serve:* 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 Federated Services (ADFS) (providing federated identity functions for ITA cloud services including ITA’s Microsoft Office 365 tenant).
- e) *The way the system operates to achieve the purpose:* The AWS East environment is broken down into two Virtual Privacy Clouds (VPCs), one for internal networking and communication (INT), and the other for public-facing internet traffic systems (DMZ).

- f) *A general description of the type of information collected, maintained, used, or disseminated by the system:* The ITA AWS Platform collects PII solely for authentication purposes. Only PII necessary to authenticate the user's identity and emergency contact information is collected by the system.
- g) *Identify individuals who have access to information on the system:* Active Directory and other PII sources are limited to privileged administrator access only, tightly controlled via AWS Identity and Access Management (IAM). Non-credentialed users do not have access to these sources.
- h) *How information in the system is retrieved by the user:* User access non-privilege information on the AWS platform via internet traffic routed through a Trusted Internet Connection (TIC) connected to the AWS DMZ VPC. Privilege access to ITA AWS resources (including server and security group controls) is available via HTTPs AWS Management portal, only available to user with credentialed accounts controlled via AWS Identity Access Management (IAM).
- i) *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).

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.*
- _____ 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	
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. *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):			

☒ 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.

☒ 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."

☒ Yes, the IT system collects, maintains, or disseminates PII about: *(Check all that apply.)*

☒ DOC employees

☒ 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.

☒ 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?

☒ 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.

☐ 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 ITA Amazon Web Service Platform 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 ITA Amazon Web Service Platform and as a consequence of this non-applicability, a PIA for this IT system is not necessary.

<p>Information System Security Officer or System Owner (Acting) Name: Chuck Hicks Office: EntOps Phone: 202-482-4853 Email: chuck.hicks@trade.gov</p> <p>I certify that this PIA is an accurate representation of the security controls in place to protect PII/BII processed on this IT system.</p> <p>Signature: <u>CHARLES HICKS</u> <small>Digitally signed by CHARLES HICKS Date: 2021.06.25 07:54:55 -04'00'</small></p> <p>Date signed: _____</p>	<p>Information Technology Security Officer Name: Joe Ramsey Office: TSI IS Phone: 202-482-2785 Email: joe.ramsey@trade.gov</p> <p>Signature: <u>JOSEPH RAMSEY</u> <small>Digitally signed by JOSEPH RAMSEY Date: 2021.08.04 15:50:20 -04'00'</small></p> <p>Date signed: _____</p>
<p>Privacy Act Officer Name: Chad Root (Acting) Office: TSI IS-Comp Phone: 202-482-1883 Email: chad.root@trade.gov</p> <p>Signature: <u>TIMOTHY ROOT</u> <small>Digitally signed by TIMOTHY ROOT Date: 2021.07.29 17:01:43 -04'00'</small></p> <p>Date signed: <u>7/29/2021</u></p>	<p>Authorizing Official Name: Rona Bunn Office: TSI CIO-DCIO Phone: 202-482-9104 Email: rona.bunn@trade.gov</p> <p>Signature: <u>RONA BUNN</u> <small>Digitally signed by RONA BUNN Date: 2021.08.26 20:49:07 -04'00'</small></p> <p>Date signed: _____</p>
<p>Bureau Chief Privacy Officer Name: Chad Root (Acting) Office: TSI IS-Comp Phone: 202-482-1883 Email: chad.root@trade.gov</p> <p>Signature: <u>TIMOTHY ROOT</u> <small>Digitally signed by TIMOTHY ROOT Date: 2021.07.29 17:02:09 -04'00'</small></p> <p>Date signed: <u>7/29/2021</u></p>	