Template Version Number: 01-2022

U.S. Department of Commerce
Office of the Secretary (OS)

Privacy Impact Assessment
for
Apptio Technology Business Management (TBM)

Reviewed by: Tiffany Daniel, Bureau Chief Privacy Officer (BCPO)

☑ Concurrence of Senior Agency Official for Privacy/DOC Chief Privacy Officer
☐ Non-concurrence of Senior Agency Official for Privacy/DOC Chief Privacy Officer
☐ Concurrence of the BCPO (This is an existing information system that is eligible for an annual certification)

CHARLES CUTSHALL Digitally signed by CHARLES CUTSHALL
Date: 2024.08.26 10:54:16 -04'00'

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

(Or the BCPO if this is an existing system that is eligible for an annual certification)

U.S. Department of Commerce Privacy Impact Assessment
Office of the Secretary (OS) /Apptio TBM

Unique Project Identifier: 3195

<u>Introduction</u>: System Description

Provide a brief description of the information system.

Apptio is a vendor of information technology (IT) cost management and optimization tools that is owned by the International Business Machines (IBM) Corporation. Apptio Technology Business Management (hereafter Apptio TBM) is a Department of Commerce system comprised of two Apptio products, Apptio One and Cloudability, that help standardize IT cost reporting and optimize cloud deployments.

Apptio One creates a unified model combining financial and operational data to allow technology, finance, and business teams to speak a common language and make data-driven technology decisions.

Cloudability is an industry-leading cloud cost management and optimization tool that enables technology, finance, and business teams to maximize the value of their cloud strategy. Cloudability is built to support the organizational adoption of cloud financial management - the process of bringing financial accountability to the scalable, variable, and distributed nature of the cloud.

Address the following elements:

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

General Support System - While this system meets the NIST criteria for classification as a “Minor Application system”, the Department is classifying it as a General Support System (GSS) due to its nature as Software-as-a-Service, the volume and value of integrated data, and the scope of planned use cases. The Department will revisit this classification over time as use cases come online.
In addition, Apptio TBM is a FISMA reportable system.

(b) System location

Cloud hosted SaaS application - Software as a Service.

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

Stand-alone system

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

Manual and automated data ingestion from cloud service providers and financial sources; Metadata tagging using an industry and Government standard taxonomy; provides the capability for reporting and dashboarding.

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

Users will use PIV credentials to log into the Software-as-a-Service application. Information is accessed through in-application search, charts, and reports all of which can be exported to file, as well.

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

A subset of users will be able to upload data directly into the system via a secure internet connection. The goal is to establish Application Programming Interfaces (APIs) with major financial systems to do automatic ingestion also via similar secure connections.

(g) Any information sharing?

No

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

This information is collected, maintained, and used in support of compliance with Federal Information Technology Acquisition Reform Act (FITARA), Capital Planning and Investment Control (CPIC), the Modernizing Government Technology Act (MGT Act), Executive Order 13800, and the Federal Cloud Smart Strategy.

(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.

___X_ 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):					

____ 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.

____ This is an existing information system that is eligible for an annual certification, in which security and privacy controls are properly implemented, changes do not create new privacy risks and there is a SAOP approved Privacy Impact Assessment.

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	X
b. Taxpayer ID		g. Passport		k. Financial Transaction	X
c. Employer ID		h. Alien Registration		l. Vehicle Identifier	
d. Employee ID		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		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. Marital Status	
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		e. Work Email Address	X	i. Business Associates	
b. Job Title		f. Salary		j. Proprietary or Business Information	X
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): Information about procurements and contracts such as contract number, vendor, rate.					

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	X	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	X	Other Federal Agencies	
State, Local, Tribal		Foreign			
Other (specify): Contract terms and amounts, product sales information and architectural implications, and related contractual and product/service information is collected. This information enables automated data validation and analysis across the Commerce IT portfolio, supports cost-effective cloud migration, and provides leadership with a clear and detailed view of financial data, to enable better decision-making and strategic planning.					

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.

- **Data governance:** Enforce data governance policies that define data standards, quality metrics, and responsibilities.
  - Work with data owners to ensure that data going into Apptio TBM is accurate including monthly data accuracy reviews.
  - Facilitate user training and provide guidelines to the Contracting Officer's Representative to ensure data accuracy.
  - Maintain documentation of the use of data, the allocation rules, and the process to update information within Apptio TBM.
  - Ensure that data is sourced correctly.
  - Leverage machine learning to verify/validate the data alignment.
- Error handling & logging policy:
  - Use error-handling mechanisms to capture and address data entry or processing errors.
  - Maintain comprehensive logs to track changes and identify the source of inaccuracies.

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	X
Other (specify):			

	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	
X Other (specify): Aggregation of technical and financial information pertaining to private companies.			

	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)		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 about a federal employee/contractor, member of the public, foreign national, visitor or other (specify).

The BII collected in the Apptio TBM system is about private companies that sell IT products and services to the Department of Commerce. This information enables automated data validation and analysis across the Commerce IT portfolio, supports cost-effective cloud migration, and provides leadership with a clear and detailed view of financial data, to enable better decision-making and strategic planning.

5.2 Describe any potential threats to privacy, such as insider threat, because 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.)

The security for the Apptio TBM system covers multiple security controls with regards to protecting the confidentiality, integrity, and availability of sponsored information systems and the information processed, stored, and transmitted by those systems. The security areas include access control; awareness and training; audit and accountability; certification, accreditation, and security assessments; configuration management; contingency planning; identification and authentication; incident response; maintenance; media protection; physical and environmental protection; planning; personnel security; risk assessment; systems and services acquisition; system and communications protection; and system and information integrity. The Apptio TBM system team has implemented the required security controls based on the tailoring guidance and the Department's policies and procedures.

Training is available for system users; rules of behavior is required for users.

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		X
DOC bureaus	X		X
Federal agencies			
State, local, tribal gov't agencies			
Public			
Private sector			
Foreign governments			

Recipient	How Information will be Shared		
	Case-by-Case	Bulk Transfer	Direct Access
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?

X	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.
	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	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.)*

	Yes, notice is provided pursuant to a system of records notice published in the Federal Register and discussed in Section 9.	
	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:	
X	Yes, notice is provided by other means.	This PIA serves as notice.
	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.	
X	No, individuals do not have an opportunity to decline to provide PII/BII.	Specify why not: PII/BII is not collected from individuals

7.3 Indicate whether and how individuals have an opportunity to consent to uses of their PII/BII.

	Yes, individuals have an opportunity to consent to particular uses of their PII/BII.	
X	No, individuals do not have an opportunity to consent to particular uses of their PII/BII.	Specify why not: PII/BII is not collected from individuals

7.4 Indicate whether and how individuals have an opportunity to review/update PII/BII pertaining to them.

	Yes, individuals have an opportunity to review/update PII/BII pertaining to them.	
X	No, individuals do not have an opportunity to review/update PII/BII pertaining to them.	Specify why not: PII/BII is not collected from individuals

Section 8: Administrative and Technological Controls

8.1 Indicate the administrative and technological controls for the system. *(Check all that apply.)*

	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: System audit logs monitor, track, and record each time the system and the information therein, including PII/BII, are accessed; by whom; when; and additional details described in section 2.1.
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): ________ ☒ 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). No open POAMS
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.
X	Contracts with customers establish DOC ownership rights over data including PII/BII.
X	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).*

Data security is achieved through the combination of security controls offered by the Apptio Government Cloud network infrastructure, database management systems and resource management. To ensure the consistent implementation of security controls across the various layers of infrastructure and services, Apptio has implemented an organization-wide security program consistent with commercial (e.g., ISO 27001, SSAE16, PCI) and U.S. Government (e.g., FIPS 200 and NIST 800-53 Rev. 5., FedRAMP moderate) requirements and practices including but not limited to the following:

ACCESS CONTROL
- Single Sign-On for centralized and consistent user provisioning
- Assignment of access and separation of functions based on job responsibilities.
- User profiles, permission sets and respective roles define their level of accessibility.
- Limiting the number of concurrent sessions allowed per user.
- Implementing automated system notification and deactivation of user accounts due to inactivity

IDENTIFICATION AND AUTHENTICATION
- Strong authentication mechanism for system users and processes via the Department's Identity, Credential, and Access Management (ICAM) solution

AUDIT AND ACCOUNTABILITY
- Logging and auditing of system logs
- Login history: a one-year history of all log-in attempts to Apptio TBM, including username, Internet Protocol address, success/failure, and time and date is available upon demand.
- Audit trail logs: a one-year history of setup changes made by the system administrator is also available upon demand and can be used to troubleshoot and audit administrative activities.
- Record Modification Fields Tracking: All objects include fields to store the name of the user who created the record and who last modified the record. This provides some basic auditing information.
- Field History Tracking

DATA SECURITY
- All encryption methods used within the Apptio TBM system are FIPS 140-2, Security Requirements for Cryptographic Modules compliant, and all systems have, as appropriate, at a minimum 128-bit Transport Layer Security (TLS) v1.2 or better encryptions. The following using FIPS 140-2 approved algorithms are currently in place:
    - Virtual Private Network – Advanced Encryption Standard (AES)-256; TLS v1.2 or better, Secure Hashing Algorithm (SHA)-256 with Rivest-Shamir-Adleman (RSA) encryption.
    - Government Telecommunications Network - AES-256; TLS v1.2 or better, SHA-256 with RSA encryption.
    - Web Certificates – SHA-256 with RSA Encryption; TLS v1.2 or better
    - Backups/Disk Encryption – AES-256;

<u>Section 9</u>: Privacy Act

9.1 Is the PII/BII searchable by a personal identifier (e.g, name or Social Security number)?

____ Yes, the PII/BII is searchable by a personal identifier.

__X__ 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."

	Yes, this system is covered by an existing system of records notice (SORN). Provide the SORN name, number, and link. *(list all that apply)*:
	Yes, a SORN has been submitted to the Department for approval on (date).
X	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: **National Archives and Records Administration General Records Schedule 3**
	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 with the schedule. Provide explanation:

10.2 Indicate the disposal method of the PII/BII. *(Check all that apply.)*

Disposal			
Shredding		Overwriting	X
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.)*

X	Low – the loss of confidentiality, integrity, or availability could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals.
	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: Only the names of Department employees and contractors are identified in the records.
X	Quantity of PII	Provide explanation: Only the names of Department employees and contractors are identified in the records.
	Data Field Sensitivity	Provide explanation:
	Context of Use	Provide explanation:
	Obligation to Protect Confidentiality	Provide explanation:
X	Access to and Location of PII	Provide explanation: Data is encrypted at rest and in transit and access is secured via the Department's ICAM solution.
	Other:	Provide explanation:

Section 12: Analysis

12.1 Identify and evaluate any potential threats to privacy that exist considering the information collected or the sources from which the information is collected. Also, describe the choices that the bureau/operating unit made regarding 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 no potential threats to personal privacy existing based on the information collected or sources. Threats related to the collection of BII concerning company information and transactions with the Government are mitigated by both the system security controls put in place and that the information collected is generally publicly available via SAM.gov, company websites, and other similar sources. The minimum amount of information necessary to support analysis and decision-making will be collected to further protect companies engaged in business with the Department.

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.