Template Version Number: 01-2020

U.S. Department of Commerce
Enterprise Services

Privacy Impact Assessment
for the
DOC Talent Acquisition Management System (DOC TA)

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 08/12/2021

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

U.S. Department of Commerce Privacy Impact Assessment
Enterprise Services / DOC Talent Acquisition Management System (DOC TA)

Unique Project Identifier: 2813

Introduction: System Description

The Department of Commerce (DOC) Talent Acquisition (TA) system is a system that provides services across four functional towers of the DOC Enterprise Services (ES) – Human Resources (HR), Acquisition (ACQ), Information Technology (IT) and Financial Management (FM).

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

DOC TA is a major application and does not provide any FISMA-moderate control inheritance to any other DOC system.

(b) System location

Three of the 4 SaaS components – Acendre Recruitment, Intelliworx Onboarding, and Nice InContact use Amazon Web Services (AWS) Infrastructure as a Service (IaaS). AWS uses availability zones spread across multiple redundant data centers. If one zone fails, or has some other interruption, the next availability zone seamlessly picks up. Therefore, data could be processed in any one of the three availability zones at any given snapshot in time.

For ServiceNow, they have two data centers. One is located in Cullpepper VA (HEF) and another in Miami FL (MIA). Both data centers mirror each other, and therefore act as both an active and standby facility.

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

DOC TA is comprised of four SaaS providers and interconnects with the following systems:

USAJobs: This is the entry point for any prospect interested in applying for a federal agency job. DOC TA consumes the applicant's USAJobs profile and uses that data to prepopulate information for the job application. Data is transferred using Security Assertion Markup Language (SAML) version 2.0.

Login.gov: This is the secure account management approach to access DOC TA. Login.gov passes the authenticated user to DOC TA with their user attributes as detailed on the website: developers.login.gov/attributes/. Login.gov corresponds to NIST 800-63-2 levels of assurance.

HRConnect: HRConnect supports position classification and generates information needed on the SF-52 Request for Personnel Action form, which is used by the Federal Hiring Manager.

ES ServiceNow: This is the main portal for DOC employees from which they can access DOC TA. Hiring requests are initiated in ES ServiceNow and through ServiceNow Application Programming Interfaces (APIs) the DOC TA gathers the request reference number, description, and category. This information is mapped to a hiring package in DOC TA.

Incidents initiated in ES ServiceNow are passed to the system through ServiceNow delivered APIs. These incidents are loaded into IBM's ticketing solution for resolution. ServiceNow uses basic authentication or OAuth for access management.

The following to-be systems will also interconnect with DOC TA:
National Oceanic and Atmospheric Administration (NOAA) Identity and Access Management (IAM).

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

DOC TA is used for administering HR programs. The four components work in the following way to achieve that purpose:

Acendre Recruitment is the main applicant tracking system responsible for position classification and management, sourcing, recruitment, assessment, selection, and data analytics. This product is the source for all in-scope DOC vacancy announcements, the DOC Position Description Library (PDL), applicants, applications, ranking of candidates, certificates of eligibility, and key data metrics related to 80 day hiring model.

Intelliworx Onboarding (Federal), system fully integrated with Acendre Recruitment to deliver the new hire in-processing and onboarding requirements. This product is the source for in-scope tentative and final job offers as well as onboarding forms and data for new hires

NICE inContact supports the requirements for the contact center. Interactive Voice Response (IVR) provides omnichannel routing for customer calls. This product is the source for all call recordings that are routed to IBM's contact center. NICE inContact utilizes FIPS 140-2 compliant AES256 encryption. Recordings are encrypted in transit and at rest.

ServiceNow ITSM supports the requirements for the contact center. ServiceNow provides the ticketing solution for customer issues related to the IBM Platform. This system stores data related to a helpdesk ticket and may contain PII related to the person who initiated the helpdesk ticket. Data has a FIPS199 categorization of “moderate impact level” for confidentiality, integrity, and availability.

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

Information can be retrieved by the users who provided them. In other words, authenticated individual users can retrieve only their information. They are not able to query the application for any other non-public information.

Additionally, information can be accessed by a limited set of privileged roles and administrators of the system by querying the application. Designated administrators within each of the four FedRAMP SaaS partners can retrieve information within the DOC TA system with limitations.

End users are only able to view their own information while staff (and contractors) depending on their roles, may be able to query and view non-public information in the system.

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

Information is transmitted over encrypted channels. Port 443 and Transport Layer Security (TLS) 1.2. There are also transmissions using Security Assertion Markup Language (SAML) 2.0

(g) Any information sharing conducted by the system

DOC TA provides data to the below systems, with further data flow and attribute details provided in the Data Dictionary and Integration Template:

ES ServiceNow: DOC TA passes status updates back to ES ServiceNow related to DOC employee-initiated requests and incidents. These status updates do not contain PII/BII. Team IBM works with DOC to determine the frequency of data transfer to ES ServiceNow.

USAJobs: New and updated DOC job vacancies and announcements are pushed to USAJobs. An API key, provided by USAJobs and unique to DOC TA is sent in the API request header.

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

Specific programmatic authorities include the following, with all revisions and amendments:

Executive Order 9397 of November 22, 1943, as amended by Executive Order 13748 (https://www.gpo.gov/fdsys/granule/CFR-2009-title3-vol1/CFR-2009-title3-vol1-eo13478/content-detail.html).

5 U.S.C., Title 31 U.S.C. 66a, 492, Title 44 U.S.C. 3101, 3309, 5 U.S.C. 301; 44 U.S.C. 3101; Executive Office (E.O.) 12107, E.O. 13164, 41 U.S.C. 433(d); 5 U.S.C. 5379; 5 CFR Part 537; DAO 202-957; E.O. 12656; Federal Preparedness Circular (FPC) 65, July 26, 1999; DAO 210-110; Executive Order 12564; Public Law 100-71, dated July 11, 1987. The authority to deliver, maintain and approve department-wide and bureau-specific automated human resources systems and server as the focal point for the collection and reporting of human resources information within the DOC is delegated to the Office of Human Resources Management (OHRM). This authority is identified by Departmental Organization Order (DOO) -- 20-8 - SECTION 4.

(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 (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*	X	f. Driver's License	X	j. Financial Account	X
b. Taxpayer ID		g. Passport	X	k. Financial Transaction	
c. Employer ID		h. Alien Registration	X	l. Vehicle Identifier	
d. Employee ID		i. Credit Card		m. Medical Record	
e. File/Case ID					
n. Other identifying numbers (specify): Job Position #, Occupational Series, Duty Station					

*Explanation for the business need to collect, maintain, or disseminate the Social Security number, including truncated form:

Solicitation of the SSN is authorized as per Executive Order 9397 of November 22, 1943, as amended by Executive Order 13748 (https://www.gpo.gov/fdsys/granule/CFR-2009-title3-vol1/CFR-2009-title3-vol1-eo13478/content-detail.html). The purpose is to provide the SSN as the means of unique identification to facilitate accurate HR processing and reporting for the Department of Commerce. Social Security numbers are not a defined field that is explicitly maintained or requested by the system but may be collected as part of supporting documentation needed to process an HR request, and maintained as unstructured data.

SSN and all data is transmitted to the Federal Human Resources system of record.

All data in the Intelliworx onboarding application is purged after 90 days per OPM mandate.

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

Work-Related Data (WRD)					
a. Occupation	X	e. Work Email Address	X	i. Business Associates	
b. Job Title	X	f. Salary	X	j. Proprietary or Business Information	
c. Work Address	X	g. Work History	X	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	X	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		e. ID Files Accessed	
b. IP Address		f. Queries Run		f. Contents of Files	X
g. Other system administration/audit data (specify): Timestamps of electronic signatures are captured in Intelliworx including the document upon which signatures were applied and data is not subject to the 90-day purge. Also retained is non-PII data associated with the position the employee filled, for aggregated reporting.					

Other Information (specify)	SSN and results of a background check or other combinations of PII justify the impact level.

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	X	Other Federal Agencies	X
State, Local, Tribal	X	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.

There are detective controls that try to validate input e.g. date of birth of the current year. There are also corrective controls where a user gets a chance to review information entered to ensure they are accurate prior to submission. Implementation of the NIST 800-53 Rev 4 controls for a FedRAMP Moderate system (e.g., access controls, encryption, border protection, security monitoring, security awareness training). All modules are located within the Amazon Web Services (AWS) GovCloud Infrastructure as a Service (IaaS).

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. IBM Talent Platform is used for intelligent selection and resolution of HR-related issues with information previously collected through source systems. Information collections (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.

<u>Section 3</u>: System Supported Activities

3.1 Indicate IT system supported activities which raise privacy risks/concerns. *(Check all that apply.)*

Activities			
Audio recordings	X	Building entry readers	
Video surveillance		Electronic purchase transactions	
Other (specify): Building candidate profiles			

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	X
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).

The system captures data and signatures for the purpose of completing the hiring process of DOC Federal employees. The system also captures information about contractors and members of the public seeking to apply to open DOC positions and the system captures information about contractors working on behalf of DOC. Further, the system captures information to support employee or customer satisfaction criteria related to the application and hiring process.

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			X
Federal agencies		X	
State, local, tribal gov't agencies		X	
Public			
Private sector			
Foreign governments			
Foreign entities			
Other (specify): Federal Human Resource Systems			X

	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	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: Parts of the system connect to HR Connect and USAJobs. The connection uses APIs where data is encrypted in transit and at rest.
	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 *	X	Government Employees	X
Contractors	X		
Other (specify): Users have access to their own PII			

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	
	Yes, notice is provided by other means.	Specify how:
	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: A candidate can make use of the service without providing PII but it is not possible to opt-out if the candidate is interested in applying for a position. PII is required for the application process.

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

	Yes, individuals have an opportunity to consent to particular uses of their PII/BII.	Specify how:
X	No, individuals do not have an opportunity to consent to particular uses of their PII/BII.	Specify why not: Within the Intelliworx Onboarding module, individuals are not able to opt out of providing PII or consenting to only a particular use. The PII collected and used is required by the HR system. Declining to provide PII effectively declines employment.

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: During the application process (before being selected) and during Federal onboarding, candidates can update their information.
	No, individuals do not have an opportunity to review/update PII/BII pertaining to them.	Specify why not:

<u>Section 8</u>: 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: Intelliworx logs all access by all users into the app during the 90 day period before being purged
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).
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).*

All data is encrypted in transit, and at rest per 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 • OPM/GOVT-5 Recruiting, Examining, and Placement Records • OPM/GOVT-6 Personnel Research and Test Validation Records • OPM/GOVT-7 Applicant Race, Sex, National Origin and Disability Status Records • COMMERCE/DEPT-18 – Employee Personnel Files Not Covered By Notices of Other Agencies
	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: GRS 02-1 Employee Acquisition Records
	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	SSN is used as a unique identifier.
X	Quantity of PII	The quantity of PII to be handled by the system causes for a moderate impact category.
X	Data Field Sensitivity	SSN and the results of a background check or other combinations of PII justifies the Moderate Impact Level, per NIST 800-60.
	Context of Use	Provide explanation:
X	Obligation to Protect Confidentiality	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	There are numerous fields of sensitive informationPII is stored in Acendre, Intelliworx, NICE inContact, and ServiceNow FedRAMP SaaS providers to support recruiting / hiring.
	Other:	Provide explanation:

<u>Section 12</u>: 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.