Template Version Number: 01-2020

U.S. Department of Commerce
Office of the Secretary

Privacy Threshold Analysis
for the
DOC Talent Acquisition Management System (DOC TA)

U.S. Department of Commerce Privacy Threshold Analysis

Office of the Secretary/ DOC Talent Acquisition Management System (DOC TA)

Unique Project Identifier: 2813

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).

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 purpose that the system is designed to serve

The system is designed to consolidate and streamline human resource services.

e) The way the system operates to achieve the purpose

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.

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

The system collects Personally Identifiable Information (PII) primarily used for identification and authentication of individuals. It also collects Information Technology (IT) management and Human Resource (HR) management information. The information collected is disseminated on a need-to-know basis only.

g) Identify individuals who have access to information on the system
Designated administrators within each of the four FedRAMP SaaS partners supporting the system have access to data required to discharge program responsibilities (consistent with least permission and least functionality) with restrictions, limitations, and monitoring of those access and use of the information.

Further, candidates using the DOC TA system have access to their own record but do not have access to any other user's data, nor do they have access to any administrative functions or data associated with those administrative roles.

h) 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.

i) 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

Questionnaire:

1. Status of the Information System

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

__X__ 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):					

____ 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?

__X__ 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.

____ 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.

__X__ ·Yes. *(Check all that apply.)*

Activities			
Audio recordings	X	. 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.

_X___No, this IT system does not collect any BII.

4. Personally Identifiable Information (PII)

4a. Does the IT system collect, maintain, or disseminate PII?

As per OMB 17-12: "The term PII refers to information that can be used to distinguish or trace an individual's identity either alone or when combined with other information that is linked or linkable to a specific individual."

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

__X__DOC employees
__X__Contractors working on behalf of DOC
____ Other Federal Government personnel
__X__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?

__X__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. 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.

Provide the legal authority which permits the collection of SSNs, 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).

____ No, the IT system does not collect, maintain, or disseminate SSNs, including truncated form.

4c. Does the IT system collect, maintain, or disseminate PII other than user ID?

_X___Yes, the IT system collects, maintains, or disseminates PII other than user ID.

____ No, the user ID is the only PII collected, maintained, or disseminated by the IT system.

4d. Will the purpose for which the PII is collected, stored, used, processed, disclosed, or disseminated (context of use) cause the assignment of a higher PII confidentiality impact level?

Examples of context of use include, but are not limited to, law enforcement investigations, administration of benefits, contagious disease treatments, etc.

____ Yes, the context of use will cause the assignment of a higher PII confidentiality impact level.

__X__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 DOC TA 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 DOC TA and as a consequence of this non-applicability, a PIA for this IT system is not necessary.

Points of Contact and Signatures

Information System Security Officer or System Owner Name: Gary Haney Office: US Department of Commerce Phone: 202-482-1691 Email: ghaney@doc.gov Signature: GARY HANEY Digitally signed by GARY HANEY Date: 2021.05.27 10:18:35 -04'00' Date signed: 05-27-2021	**Information Technology Security Officer** Name: Jerome Nash Office: US Department of Commerce Phone: 202-482-5929 Email: Jnash@doc.gov Signature: JEROME NASH Digitally signed by JEROME NASH Date: 2021.06.09 17:43:34 -04'00' Date signed: 06/09/2021
Privacy Act Officer Name: Tahira Murphy Office: Office of Privacy and Open Government Phone: 202-482-8075 Email: tmurphy2@doc.gov Signature: TAHIRA MURPHY Digitally signed by TAHIRA MURPHY Date: 2021.08.09 11:26:09 -04'00' Date signed:	**Authorizing Official** Name: Lawrence W. Anderson Office: US Department of Commerce Phone: 202-482-4444 Email: Landerson@doc.gov Signature: LAWRENCE ANDERSON Digitally signed by LAWRENCE ANDERSON Date: 2021.07.29 08:34:58 -04'00' Date signed:
Bureau Chief Privacy Officer Name: Maria D. Dumas Office: Office of Privacy and Open Government Phone: 202-482-5153 Email: mDumas@doc.gov on behalf of: Signature: TAHIRA MURPHY Digitally signed by TAHIRA MURPHY Date: 2021.08.09 13:26:25 -04'00' Date signed:	