U.S. Department of Commerce
Office of the Secretary

Privacy Threshold Analysis
for the
Accenture Federal Services (AFS) HR ServiceNow

Revision History

Revision Number	Summary of Revision	Revision Author	Date	Accepted By
v1.0	Initial Approved PTA	Art Gonzalez	11/29/2016	
v1.1	Updated to incorporate PAR Tracking Module	Art Gonzalez	05/23/2016	

U.S. Department of Commerce Privacy Threshold Analysis

Office of the Secretary

Unique Project Identifier: [Number]

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).

The DOC has developed this Privacy Threshold Analysis (PTA) to present existing and planned information for ensuring protecting Moderate System in accordance with applicable laws.

The purpose of this PTA is to provide an overview of the security/privacy requirements of the Moderate System as well as to delineate the responsibilities and expected behavior of all individuals who access the system. The PTA shall be viewed as documentation of the structured process of planning adequate, cost-effective security/privacy protection for a system.

Description of the information system and its purpose
Enterprise Services (ES) ServiceNow is comprised of a DOC Enterprise Services Human Resources (HR) Landing Web Page, HR Incident and User Support Ticketing system, and a Personnel Action Request (PAR) Tracking tool that tracks PAR status changes using limited employee data. (ES) ServiceNow is managed and maintained by Accenture Federal Services to provide enabling technologies for the DOC Support Services Initiative - Human Resources (SSI-HR) BPA. The system uses the FedRAMP Moderate ServiceNow Service Automation Government Cloud Suite that uses Continental United States (CONUS)-based dedicated infrastructure (facilities, servers, databases, and networking devices) to process, store, and transmit government information.

Access to the information in the AFS HR ServiceNow system is restricted via multifactor authentication. Only authorized AFS HR ServiceNow Staff or government personnel with a business need can access the information in the system. AFS resources connect to the AFS HR ServiceNow information via DOC issued GFE laptops via an encrypted VPN connection to a DOC network.

The data collected is encrypted using FIPS 140-2 validated module while the data is at rest (cert#2264). Safe guards are in place to ensure all AFS HR ServiceNow information is encrypted using FIPS-140-2 validated cryptographic module while in transit.

DOC plans multiple phases to implement the HR Line of Business (LOB) services via incremental deliveries.

Initial Phase – ATO Granted December 2016

Enterprise Services ServiceNow obtained an Authorization to Operate (ATO) in December 2016 to provide an HR Landing Web Page and an HR Incident and User Support Ticketing tool. HR Customer Support services included the ability for DOC employees and contractors to:

- Report Issues and Ask Questions
- Access HR Rules and Regulations
- Communicate with HR Service Center staff

Employee data collected in this phase includes employee identification and contact data such as name, phone number, and email address where employee can be reached. On some occasions, users might substitute their business phone number with personal phone number. This information is required to enable AFS HR ServiceNow Agency Designees to document and track support requests. AFS is the Agency Designee that will track and document all the information for this particular system.

Phase 2 –PAR Tracking – ATO in process

In phase two, Enterprise Services ServiceNow is providing mission enabling tools including a PAR Tracking capability. The system will track 'PAR Processing' for the Department of Commerce Human Resources Operations Center (DOCHROC) and National Oceanic and Atmosphere Administration (NOAA).

Employee data collected includes employee identification and contact data such as name, email address, Notice of Action Code (NOAC), NOAC description, Veterans Identifier, and a phone number.

Authorized AFS HR Personnel access the PAR Tracking tool to:

- Import PAR tracking data from Treasury's HR Connect,
- Import PAR tracking data from an Entry on Duty (EOD) list provided by the bureaus,
- Track a PAR transaction to completion, and
- Identify PAR tracking anomalies (e.g., missing documentation) for system to send an automated notification to authorized bureau POC(s). No PII is contained in the automated notification.

Questionnaire:

1. What is the status of this information system?

__ This is a new information system. *Continue to answer questions and complete certification.*

__X__ 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	X	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	X	f. Commercial Sources		i. Alteration in Character of Data	
j. Other changes that create new privacy risks (specify): AR Tracking due to Notice of Action Code (NOAC)					

____ This is an existing information system in which changes do not create new privacy risks. *Skip questions and complete certification.*

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.

__X__ 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 about: *(Check all that apply.)*

____ Companies
____ Other business entities

__X__ No, this IT system does not collect any BII.

4. Personally Identifiable Information

4a. Does the IT system collect, maintain, or disseminate personally identifiable information (PII)?

As per OMB 07-16, Footnote 1: "The term 'personally identifiable information' refers to information which can be used to distinguish or trace an individual's identity, such as their name, social security number, biometric records, etc... alone, or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, mother's maiden name, etc..."

__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
_____ 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 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.

4c. 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, and/or 4c are "Yes," a Privacy Impact Assessment (PIA) must be completed for the IT system. This PTA and the 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 AFS HR ServiceNow Solution 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 AFS HR ServiceNow Solution and as a consequence of this non-applicability, a PIA for this IT system is not necessary.

Name of Information System Security Officer (ISSO) or System Owner (SO) Arthur Gonzalez

Signature of ISSO or SO: ARTHUR GONZALEZ Digitally signed by ARTHUR GONZALEZ DN: c=US, o=U.S. Government, ou=Department of Commerce, ou=Office of the Secretary, cn=ARTHUR GONZALEZ, 0.9.2342.19200300.100.1.1=13001000091193 Date: 2017.05.31 13:49:31 -04'00' Date: 5/31/2017

Name of Information Technology Security Officer (ITSO): Jun Kim

Signature of ITSO: Digitally signed by JUN KIM DN: c=US, o=U.S. Government, ou=Department of Commerce, ou=Office of the Secretary, cn=JUN KIM, 0.9.2342.19200300.100.1.1=13001001483988 Date: 2017.05.31 15:41:41 -04'00' Date: 5/31/2017

Name of Authorizing Official (AO): Renee Macklin

Signature of AO: Date: 5/31/2017

Name of Bureau Chief Privacy Officer (BCPO): Kathy Gioffre

Signature of BCPO: KATHLEEN GIOFFRE Digitally signed by KATHLEEN GIOFFRE DN: c=US, o=U.S. Government, ou=Department of Commerce, ou=Office of the Secretary, cn=KATHLEEN GIOFFRE, 0.9.2342.19200300.100.1.1=13001000075444 Date: 2017.06.06 21:28:39 -04'00' Date: 6/6/2017