Version Number: 01-2015

U.S. Department of Commerce

OFFICE OF THE CHIEF OF INFORMATION SYSTEMS

Privacy Impact Assessment
for the
Accenture Federal Services (AFS) HR ServiceNow

Reviewed by: Kathy Gioffre, Deputy Director and 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

Catrina D. Purvis

Digitally signed by Catrina D. Purvis
DN: cn=Catrina D. Purvis, o=Office of the Secretary, Office of Privacy and Open Government, ou=US Department of Commerce, email=cpurvis@doc.gov, c=US
Date: 2017.06.08 09:33:32 -04'00'

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

Revision History

Revision Number	Summary of Revision	Revision Author	Date	Accepted By
v1.0	Initial Approved PIA	Art Gonzalez	12/21/2016	
v1.1	Updated to incorporate PAR Tracking Module	Art Gonzalez	05/24/2016	

U.S. Department of Commerce Privacy Impact Assessment
Office of the Secretary
AFS HR ServiceNow

Unique Project Identifier: OSES001 – Enterprise Services ServiceNow

Introduction: System Description

Provide a description of the system that addresses the following elements:

(a) a general description of the information in the system

Enterprise Services (ES) ServiceNow is comprised of a DOC Enterprise Services 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 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.

(b) a description of a typical transaction conducted on the system

HR System Incident Report

- User experiences an incident utilizing a separate supported HR system.
- User submits an incident request via the following:
    - Directly inputting incident via self-service AFS HR ServiceNow web page.
    - Telephoning the Contact Center and having the Tier 1 Customer Service Representative enter the incident record. This can occur by direct telephone communication or through voicemail after operating hours that may or may not require a callback for clarification.
- Tier 1 CSR reviews request and responds with solution by phone or email.
- Tier 1 escalates complex requests to Tier 2 for resolution.
- Tier 2 resolves incident and notifies requestor of resolution by phone or email.

HR System Help Request

- User requests assistance with system navigation for supported HR System.
- User submits a Help Request via the following:
    - Directly inputting a request via self-service AFS HR ServiceNow web page.
    - Telephoning the Contact Center and having the Tier 1 Customer Service Representative enter the help request. This can occur by direct telephone communication, or by leaving a voice mail after operating hours that may or may not require a call-back for clarification.
- Tier 1 reviews request and responds with solution by phone or email.
- Tier 1 escalates complex requests to Tier 2 for resolution.

- Tier 2 resolves incident and notifies requestor of resolution by phone or email.
- User request can include inquiry into PAR transaction status

PAR Tracker

The PAR tracker is an automated tool that tracks a PAR transaction, which is processed in Treasury's HR Connect, to completion through the following states:

- Pending Review
- Awaiting Missing Documentation
- Document Intake Complete
- Ready for Processing
- Packet needs Review
- Quality Check
- Waiting for NFC Status
- Ready for OPF
- Pending Closure
- Closed
- Cancelled.

PAR tracking data is downloaded via HR Connect Secure portal, Google Drive and Accellion. The information is uploaded to Service now using the ServiceNow secure portal.

Transactions are entered into the PAR Tracker using three different ways:

- AFS employee (who has been granted the PAR Processor Role or Document Control Role) keys PAR tracking Data received by mail into ServiceNow manually to ServiceNow via secure HTTPS Connection.
- PAR tracking data, in Excel spreadsheets, are sent using FedRAMP secure Google Cloud by NOAA and via Accellion by DOCHROC HR Point of Contact. An AFS team member (who has been granted the Import Role) uploads these spreadsheets, via GFE laptops, into AFS ServiceNow.
- AFS Staff use GFE laptops to connect to HR Connect via Secure HTTPS Connection and download PAR tracking data to a spreadsheet which is then saved on the GFE laptop and manually uploaded into Service Now via secure HTTPS Connection.

The information collected and distributed by the System is used for authorized activities performed by authorized personnel only.

While information will not be shared with other systems in an ongoing fashion, it will have the capability to produce reports on incidents and requests (i.e. minimizing the occurrence of common issues). Reports contain information about employees impacted by Personnel Action Requests. These reports are shared with authorized personnel who have a "need to know" and approved by the DOC system owner. This information is always shared via Accellion (email relay).

All files from NOAA and DOCROC will be received securely via Accellion or secure Google Cloud. All email transactions are done via a secure communication using Transport Layer security (TLS).

(c) a citation of the legal authority to collect PII

Includes the following, with all revisions and amendments: 5 U.S.C. 301; 44 U.S.C. 3101; 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 serve as the focal point for the collection and reporting of human resources information within the Department of Commerce (DOC) is delegated to the Office of Human Resources Management (OHRM). This authority is identified by Departmental Organization Order (DOO) -- 20-8 - SECTION 4.

(d) the Federal Information Processing Standard (FIPS) 199 security impact category for the system

The *potential impact* is MODERATE based on (FIPS) 199

Section 1: Status of the Information System

1.1 Indicate whether the information system is a new or existing system.

___ This is a new information system.

_X_ 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	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): PAR Tracking due to Notice of Action Code (NOAC)					

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*		e. File/Case ID		i. Credit Card	
b. Taxpayer ID		f. Driver's License		j. Financial Account	
c. Employer ID		g. Passport		k. Financial Transaction	
d. Employee ID		h. Alien Registration		l. Vehicle Identifier	
m. ServiceNow User ID (Derived from email address); HR Connect Employee Id					
*Explanation for the need to collect, maintain, or disseminate the Social Security number, including truncated form:					

General Personal Data (GPD)					
a. Name	X	g. Date of Birth		m. Religion	
b. Maiden Name		h. Place of Birth		n. Financial Information	
c. Alias		i. Home Address		o. Medical Information	
d. Gender		j. Telephone Number	X	p. Military Service	X
e. Age		k. Email Address	X	q. Physical Characteristics	
f. Race/Ethnicity		l. Education		r. Mother's Maiden Name	
s. Other general personal data (specify):					

Work-Related Data (WRD)					
a. Occupation		d. Telephone Number	X	g. Salary	
b. Job Title	X	e. Email Address	X	h. Work History	
c. Work Address	X	f. Business Associates			
i. Other work-related data (specify): Notice of Action Code (NOAC)& Description, Bureau, Veteran's Identifier, Department and Office**.**					

Distinguishing Features/Biometrics (DFB)					
a. Fingerprints		d. Photographs		g. DNA Profiles	
b. Palm Prints		e. Scars, Marks, Tattoos		h. Retina/Iris Scans	
c. Voice Recording/Signatures		f. Vascular Scan		i. Dental Profile	
j. Other distinguishing features/biometrics (specify): N/A					

System Administration/Audit Data (SAAD)					
a. User ID	X	c. Date/Time of Access	X	e. ID Files Accessed	X
b. IP Address		d. Queries Run	X	f. Contents of Files	
g. Other system administration/audit data (specify):					

Other Information (specify):
Reports generated by system queries on PAR Tracking and requests for assistance for process improvement.

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	X	Email	X		
Other (specify): Voicemail with name and business telephone for call back. Emails that contain PII must provide access to this data using DOC secure Accellion file transfer service.					

Government Sources					
Within the Bureau	X	Other DOC Bureaus	X	Other Federal Agencies	X
State, Local, Tribal		Foreign			
Other (specify): A onetime employee listing was extracted from the NFC system in 2016 to facilitate startup. Additionally, PAR transaction requests are extracted using a worklist query from the HR Connect system via a secure HTTPS connection and saved as a spreadsheet to a GFE laptop. AFS staff then manually connects to ServiceNow via secure HTTPS connection to import the saved file into the PAR Tracker application.					

Non-government Sources					
Public Organizations		Private Sector		Commercial Data Brokers	
Third Party Website or Application					
Other (specify): N/A					

2.3 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.

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	
Other (specify):			

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			
To determine eligibility		For administering human resources programs	X
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	X	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).

When Collected the PII will be used for the purpose of supporting and tracking human resources actions, requests or questions.

The information is used by the following:

- DOC Employee Service Contact Center to respond to customer queries and requests.
- AFS PAR Processers for tracking the processing status of a PAR Action.
- Reporting for DOC Authorized Customers for status and process improvements.

Some of the purposes of the collection of this information is to provide the following data:

- Workflows and process management based on the organization needs
- Knowledge repository for all of HR content
- Managed content display based on the organization's HR lifecycle
- Insight into vendor managed transactions
- Single source of truth
- PAR Tracking Transactions Information

The information used and collected by the information system is to track the lifecycle of a PAR Processing request, and provide processing status reports to customers.

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			
Foreign entities			
Other (specify):			

	The PII/BII in the system will not be shared.

6.2 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 manually receives information from another IT system(s) that are authorized to process PII. At the beginning of the construction of the information system, there was a one-time import of personnel directory data from NFC for the Contact Center's incident transactions, this practice is no longer applicable. PAR tracking data from the EOD list provided by the bureaus and a query pulled from HR Connect is manually uploaded into AFS HR ServiceNow. Only authorized personnel are able to work with this data. The data that is imported includes employee name, EOD, NOA Code, Bureau, Office, Veterans Identifier (Not yet implemented) and Point of Contact information. The data is used in the PAR Tracker. The bureaus use Accellion or FedRAMP Google Cloud solution to provide AFS Staff with PAR tracking data from EOD lists and PAR transactions to be processed. The PAR Tracker is also built with a capability to generate automated emails to notify specific DOC POC's for the PAR transactions referenced, using ServiceNow and DOC email system using all proper FIPS 140-2 crypto module regulations at various stages of PAR Processing (e.g. missing documentation, action successfully applied at NFC etc.)
	No, this IT system does not connect with or receive information from another IT system(s) authorized to process PII and/or BII.

6.3 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.)*

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 other means.	**Specify how**: Yes, the notice is accessible from a "Privacy Policy" link provided on the AFS HR ServiceNow Portal Home Page: https://commerceenterpriseservices.service-now.com/HR
	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:** Individuals are not given an opportunity to give consent after the initial Human Resources hiring process. The accounts are established at inception via Personnel Directory Information imported from NFC.

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:** Individuals are not given an opportunity to give consent after the initial Human Resources hiring process. The accounts are established at inception via Personnel Directory Information imported from NFC.

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.	**Specify how:**
X	No, individuals do not have an opportunity to review/update PII/BII pertaining to them.	**Specify why not:** Employees cannot actively go in and update their PII/BII in AFS HR ServiceNow. For contact center incidents, an individual can call in and a customer service representative (CSR) can update their information for them. This is not true for PAR transactions.

Section 8: 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: All access is recorded by the system as well as the input/output related to all entries in the system. The data is archived for forensic purposes.
X	The information is secured in accordance with FISMA requirements. Provide date of most recent Assessment and Authorization (A&A): December, 2016 ☐ 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 (POAM).
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 ownership rights over data including PII/BII.
X	Acceptance of liability for exposure of PII/BII is clearly defined in agreements with customers.

8.2 Provide a general description of the technologies used to protect PII/BII on the IT system.

The following FIPS 140-2 cryptographic modules are used to encrypt all data at rest as well as in transit. ServiceNow, Inc. uses self-encrypting hard drives for database servers. The drives are encrypted using a key generated by ServiceNow's SafeNet appliance. The hard drives use a FIPS 140-2 Level 2 validated encryption module (Cert# 1635). Service now uses TLS 1.2, AES with 128 bit encryption (High); ECDH with 256 bit exchange for encrypting data in transit.

For application users, AFS HR ServiceNow uses its own Role Based Access Control (RBAC) model, as well as by implementing two factor authentication using google authenticator. The AFS HR Service Now administrators also have the ability to login to the application servers using their proper credentials to perform functions based on the permitted access. Additional security measures include implementing whitelisting to restrict ServiceNow access over the DOC Network (Silver Springs and the HCHB TIC IP Range).

All AFS staff are issued DOC GFE Laptops running a secure government approved baseline that encrypts all data at rest using a FIPS 140-2 validated cryptographic module.

AFS staff uses HR Connect to pull data from queries using HTTPS secure protocol which uses TLS 1.2, AES with 256 bit encryption (High); DH with 1024 bit exchange which ensures the data is encrypted in transit.

DOC's Accellion Secure file transfer is used to transfer data to authorized DOC POC's and AFS Staff from DOC Bureaus. Accellion uses TLS 1.0, AES with 128 bit encryption (High); ECDH with 256 bit exchange to ensure data is secure in transit. NOAA also leverages the Secure FedRAMP

google cloud to provide data to AFS resources to load into the PAR Tracker.

All transactions are processed with GFE and government email accounts to transmit and receive information. ServiceNow has automated emails configured but there is no sensitive information in the emails, and all transactions use secure email encryption.

Sensitive data contained in reports is encrypted using FIPS 140-2 validated cryptographic modules via Accellion and sent only to authorize users approved by DOC. Authorized users are managed on a DOC Approved Access Control List.

Accounts on LDAP-enabled hosts enforce approved authorizations for logical access in accordance with the account privileges maintained in the LDAP repository. All accounts on non-LDAP-enabled hosts enforce approved authorizations for logical access in accordance with the account privileges maintained locally for the account. Database accounts are managed local to the database schema, so that a user with access to one schema does not automatically have access to other schemas within the database. This is how users for one application are prohibited from accessing data associated with a separate system, this includes data in transit and at rest.

Section 9: Privacy Act

9.1 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 and number *(list all that apply)*: Department 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, a SORN is not being created.

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: The retention periods of data contained in this system are covered by General Records Schedules #1. Civilian Personnel Records have various retention periods for specific types of data. The retention period for these records is guided by the General Records Schedules (GRS) that are issued by the National Archives and Records Administration (NARA) to provide disposition authorization for records common to several or all agencies of the Federal Government. In accordance with GRS 20, item 3, electronic versions of records scheduled for disposal may be deleted at the expiration of the retention period authorized by the GRS for the equivalent paper copies or when no longer needed, whichever is later. Various items in GRS 1, Civilian Personnel Records, authorize the disposition of the records described in this PIA.

	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	X
Degaussing		Deleting	X
Other (specify): The process starts with overwriting the data and is completed by deleting the information to be compliant with NIST 800-88 regulations.			

Section 11: NIST Special Publication 800-122 PII Confidentiality Impact Levels

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.

	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 levels. *(Check all that apply.)*

X	Identifiability	Provide explanation: Name information, Nature of action, veteran identifier, and work related data (WRD – refer to table 2.1), General Personnel Data (GPD – Refer table 2.1), Identifying numbers (IN – Refer table 2.1) is displayed as part of the process and securely archived with in the information System.
	Quantity of PII	Provide explanation:
X	Data Field Sensitivity	Provide explanation: Fields within the form displayed are Name information, Nature of action, veteran identifier (Not yet implemented), work related data (WRD – refer to table 2.1), General Personnel Data (GPD – Refer table 2.1), Identifying numbers (IN – Refer table 2.1) as part of the process. The information is securely archived within the information system.
	Context of Use	Provide explanation:

X	Obligation to Protect Confidentiality	Provide explanation: Based on the system's FIPS 199 security categorization, the management, operational and technical security controls required for the System (ACI) Tracking Solution at a minimum, include all Moderate baseline security controls documented in NIST SP 800-53, Rev. 4. *New* security measurements for the information system were developed to enhance the FedRAMP moderate baseline security controls and additional FedRAMP guidance and requirements. The FedRAMP moderate baseline security controls extend the NIST SP 800-53, Rev. 4 moderate baseline controls are needed for the assurance of government data in cloud products and services. The security information was added to provide the proper confidentiality to the PAR tracker system of the information system.
	Access to and Location of PII	Provide explanation:
	Other:	Provide explanation:

Section 12: Analysis

12.1 Indicate whether the conduct of this PIA results in any required business process changes.

X	Yes, the conduct of this PIA results in required business process changes. Explanation: All authorized users have been trained in the business process changes.
	No, the conduct of this PIA does not result in any required business process changes.

12.2 Indicate whether the conduct of this PIA results in any required technology changes.

X	Yes, the conduct of this PIA results in required technology changes. Explanation: PAR Tracker enhancement and proper security measures are being added to protect current data. Furthermore, the enhancements ensure the confidentiality of Data is properly secure within the information system boundaries.
	No, the conduct of this PIA does not result in any required technology changes.

Appendix A – Privacy Act Notice Language

Authority to Collect

Includes the following, with all revisions and amendments: 5 U.S.C. 301; 44 U.S.C. 3101; 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.

Purpose

The web-based system contains HR LOB support inquiries from users of Department of Commerce Human Resources Systems. Support staff will utilize the information to resolve inquiries regarding system functionality, issues, or status inquiries. Information collected by this system may also be used for litigation, civil enforcement activities and Criminal law enforcement activities.

Routine Uses

The Department will use this information in order to resolve customer inquiries. Disclosure of this information is permitted under the Privacy Act of 1974 (5 U.S.C. Section 552a) to be shared among Department staff for work related purposes. Disclosure of this information is also subject to all of the published routine uses as identified in the Privacy Act System of Records Notice Commerce Dept-18, Employee Personnel Files Not Covered by Notices of Other Agencies.

Disclosure

Furnishing this information is voluntary; however, failure to provide accurate information may delay or prevent processing of inquiries.