FEDERAL DEPOSIT INSURANCE CORPORATION
INSURING AMERICA'S FUTURE

Privacy Threshold Analysis (PTA) and/or Privacy Impact Assessment (PIA)

for

MicroPact

Enterprise Workforce Solution (eWORKS)

Date Approved by Chief Privacy Officer (CPO)/Designee: 12/18/2017

PTA/PIA TEMPLATE VERSION 1.9 – August 2017

SECTION I – OUTSOURCED INFORMATION SERVICE DESCRIPTION

1. Describe the outsourced service and its purpose.

The Federal Deposit Insurance Corporation (FDIC) Division of Administration (DOA) is responsible for end-to-end processes supporting the selection, on-boarding, and off-boarding of FDIC employees and contractors, who are applying to work at the FDIC. DOA has contracted with MicroPact to automate the background investigation (BI) process for FDIC employees and contractor personnel.

MicroPact is the software and services company that utilizes entillitrak, which is a commercial off-the-shelf (COTS) software solution that is preconfigured to support federal agency's personnel security BI process. The Enterprise Workforce Solution (eWORKS) is the technology solution that has been developed to automate the end-to-end processes supporting the selection, on-boarding, and off-boarding of FDIC employees and contractors. MicroPact is providing integration assistance to further configure the entellitrak software to have the capabilities to automate and support FDIC's specific BI process and deploy the configured solution into a production environment for FDIC use. eWORKS is hosted in a dedicated FedRAMP[1] cloud environment.

eWORKS automates FDIC's BI process, which includes the FDIC preliminary review as well as the formal OPM BI. To do this, the system allows authorized entities such as applicants, employees, contractors, and FDIC's DOA's Security and Emergency Preparedness Section (SEPS) personnel to input data into the eWORKS repository. This data includes: completed forms required of applicants, employees & contractors, the results of credit checks, searches of public records and Federal Bureau of Investigations (FBI) Criminal Indices; Reports of Investigation and correspondence back and forth among subjects of investigation; and correspondence to/from offices such as Legal, Ethics, and SEPS. eWORKS's interfaces with the Office of Personnel Management (OPM) to automatically send and receive BI cases electronically, the FBI to receive criminal reports, authorized commercial vendors to receive credit reports, and reports of public record on the applicant, employee, or contractor. Additionally, eWORKS will provide web-based reporting capability on personnel security functions.

eWORKS includes legacy data from the PERSEREC[2] Documentum repository that includes employee and contractor data and BI documents, which maintain the following information: full name, date of birth (DOB), Social Security Number (SSN), home address, employment, family information, references, and all results of associated investigative activity and adjudicative reports pertaining to each individual subject affiliated with FDIC. Limited medical information (psychiatric evaluation[3]) may be included.

[1] The Federal Risk and Authorization Management Program (FedRAMP) is a government-wide program that provides a standardized approach to security assessment, authorization, and continuous monitoring for cloud products and services. For additional information, refer to the https://www.fedramp.gov /.
[2] The Personnel Security Records (PERSEREC) solution is being used to upload DOA/SEPS scanned case files (active and inactive) into FDIC's Enterprise Secured Document Repository/Documentum. For additional information, refer to the FDIC's PERSEREC Privacy Impact Assessment.
[3] Reference SORN FDIC 30-64-0015 and OPM GOVT-5..

Through multiple phases of development, testing and implementation, eWORKS will ultimately initiate, track, and report on the status/completion of on-boarding and off-boarding activities (background investigations, badging, facility access, transportation, emergency preparedness, and office space). This Privacy Impact Assessment will only cover the background investigation phase of the implementation of eWorks which is considered to be phase 1 and 2 of the implementation process, and will be updated as necessary for future phases. Badging, facility access, transportation, emergency preparedness, and office space on-boarding process will be done in later phases of implementation of eWORKS.

SECTION II – DATA TYPE, SOURCES, AND USE

2. Describe all information/data that will be collected, used, maintained or generated by the Outsourced Provider (Vendor) as part of the services provided under the contract. If no information/data is involved, select Not Applicable.

The information collected consists of data elements necessary to conduct the FDIC preliminary review as well as the formal OPM BI. These data identify the individual; to ensure the integrity and accuracy of the investigative process; and to track completion of security-related processes that ultimately leads to a hiring decision, contractor affiliation or a decision regarding access to classified National Security Information. See question 4 below for PII elements that may be included in this information.

☐ Not applicable

3. Describe the intended purpose and use of the above information/data. If no information/data is involved, select Not Applicable.

The purpose and intended use of the collected data is to: A) ensure the accuracy and integrity of the FDIC preliminary review, investigation and adjudication process; B) create a record in eWORKS, in order to track the OPM security investigation and determination process of potential FDIC employees and contractors; and, C) ensure the proper reinvestigation cycle is maintained for FDIC employees and contractors. The subject files within eWORKS greatly facilitate the comprehensive and timely suitability determinations rendered by SEPS.

☐ Not applicable

4. What types of personally identifiable information (PII) are (or may be) included in the information specified above? *(This is not intended to be an all-inclusive list. Specify other categories of PII, as needed.)*:

PII Element	Yes	No
Full Name	☒	☐
Date of Birth	☒	☐
Place of Birth	☒	☐
Social Security Number	☒	☐
Employment Status, History or Information	☒	☐

Mother's Maiden Name	☒	☐
Certificates (e.g., birth, death, naturalization, marriage, etc.)	☒	☐
Medical Information (Medical Records Numbers, Medical Notes, or X-rays)	☒	☐
Home Address	☒	☐
Phone Number(s) (non-work)	☒	☐
Email Address (non-work)	☒	☐
Employee Identification Number (EIN)	☒	☐
Financial Information (e.g., checking account #/PINs/passwords, credit report, etc.)	☒	☐
Driver's License/State Identification Number	☒	☐
Vehicle Identifiers (e.g., license plates)	☒	☐
Legal Documents, Records, or Notes (e.g., divorce decree, criminal records, etc.)	☒	☐
Education Records	☒	☐
Criminal Information	☒	☐
Military Status and/or Records	☒	☐
Investigation Report or Database	☒	☐
Biometric Identifiers (e.g., fingerprint, voiceprint)	☒	☐
Photographic Identifiers (e.g., image, x-ray, video)	☐	☒
Other (Specify: _____)	☐	☒

5. If Social Security Number (SSN) is checked in question 4, please answer the following:

a) Explain the business purpose requiring the collection of SSNs: eWORKS interfaces with OPM, the FBI, credit bureaus, and public records collection entities which require a SSN to ensure proper identification as well as to send and retrieve data.

b) Provide the legal authority which permits the collection of SSNs: Depending on the purpose of the investigation, the Executive Orders, as amended 9397, 10450, 10577, 10865, 12333, 12968, 13467, 13488, 13549, and 13764; 5 U.S.C. 1103, 1302, 1303, 1304, 3301, 7301, 9101, and 11001; 22 U.S.C. 272b, 290a, and 2519; 31 U.S.C. 1537; 42 U.S.C. 1874(b)(3), 2165, 2201, and 20132; 50 U.S.C. 3341; Public Law 108–136; 5 CFR parts 2, 5, 731, 732, 736, and 1400; and Homeland Security Presidential Directive 12 (HSPD 12) 1537; 42 U.S.C. 1874(b)(3), 2165, 2201, and 20132; 050 U.S.C. 3341; Public Law 108–136; 5 CFR parts 2, 5, 731, 732, 736, and 1400; and Homeland Security Presidential Directive 12 (HSPD 12).

c) Identify whether the SSN is masked or otherwise truncated as part of the outsourced service: SSNs are masked from certain user roles in eWORKS. As necessary, SSNs are displayed in full as DOA/SEPS requires that the SSN is in plain text when displayed in eWORKS.

6a. Please provide an estimate of the number of records maintained by the vendor for this contract that contain PII:

Estimated Number of Records Containing PII				
0 ☐	1-500 ☐	501-1,000 ☐	1,001 – 2,500 ☐	2,501 – 5,000 ☐
5,001 – 7,500 ☐	7,501 – 10,000 ☐	10,001 – 50,000 ☐	50,001 – 100,000 ☒	over 100,000 ☐

6b. If "0" was answered for 6a, please explain[4]: N/A

7. What are the sources of data (both PII *and* non-PII) for the outsourced service/project? How is the data derived?

Data Source[5] (List all sources that the Outsourced Provider collects, obtains or receives data from, as part of the services provided under the contract.)	**Type of Data Provided by Source & How It is Derived** (Describe the type of PII and non-PII data provided by each source. If PII is included in the data, list the specific PII elements, and explain how the PII is derived.)	**Does Data Include PII?**
PERSEREC Documentum Repository	Legacy data and documents will be extracted from the PERSEREC repository and transmitted to eWORKS using SSH encryption protocols. PERSEREC data and documents may contain the following information: full name, date of birth (DOB), Social Security Number (SSN), home address, employments, family, references, and all results of associated investigative activity and adjudicative reports pertaining to each individual subject affiliated with FDIC.	☒ Yes ☐ No
Employee/contractor/potential candidate applicants through efile	Applicant will enter data via the following digital forms: • FDIC 2120/16: Applicant Certification Statement • OPM 306: Declaration for Federal Employment • FDIC 1600/18: Tax Check Waiver • FDIC 1600/04: Background Investigation Questionnaire for Contractor Personnel & Subcontractors • FDIC 1600/07: Background Investigation Questionnaire for Contractors • • FDIC 1600/25: Additional Background Security Questions for Contractor Personnel Necessary to initiate the pre-clear and suitability to determination process via an entellitrak module called "eFile" – the applicant is sent a secure email invitation with a link to an eFile interface to enter their information. The email also contains a username and temporary password that must be changed on the initial login to the eFile interface.	☒ Yes ☐ No
OPM e-QIP	Applicant will enter PII elements listing in Question 4 into (electronic forms above) necessary to perform a full investigation for a Public Trust or Security clearance into the e-Qip system.	☒ Yes ☐ No
OPM e-Delivery	Background Investigation results of the applicant are returned by OPM and input automatically into eWORKS.	☒ Yes ☐ No
OPM Central Verification System	SEPS Personnel will check that prior FDIC files are retrieved and a credit report is obtained and loaded into the file for the applicant, employee, or contractor by SEPS personnel. SEPS personnel will also load a report capturing public record information is loaded, as well as a report that checks the FBI's Criminal Indices	☒ Yes ☐ No
Equifax	eWORKS will utilize the Equifax Credit Bureau Report and SEPS personnel will manually import the report into the applicant,	☒ Yes ☐ No

[4] If the vendor has not received work to date for this contract and "0" is checked in 6a, please explain approximately how many records may be maintained by the vendor if they are awarded work under this contract in the future. Additionally, the Division responsible for this vendor must update this PIA to reflect the accurate number of records containing PII that the vendor maintains if this changes in the future.

[5] Examples of potential data sources include, but are not limited to: internal (FDIC) or external (non-FDIC) systems, websites, individual members of the public (e.g., customers, borrowers, etc.), FDIC employees, FDIC contractors, credit bureaus, commercial entities, public records, government agencies, etc.

	employee, or contractor file.	
TLOxp/Lexus Nexus	eWORKs will utilize TLOxp and Lexus Nexus, and will manually import a report of information obtained from searches of public records. The contents of this report are based upon associations established through names and addresses.	☒ Yes ☐ No
Fieldprint	Fieldprint handles the fingerprinting process from collection through transmission to the FBI, ensuring that information is collected in a secure, timely, and convenient manner for employees, applicants, and contractors. The FBI, in turn, processes the digital fingerprints through their Criminal Justice Information Services Division (CJIS) and returns the results to Fieldprint. Fieldprint maintains the results in a secure, FDIC-specific section of their website for review and retrieval by pre-approved SEPS personnel. Authorized SEPS personnel access the Fieldprint portal, retrieve the FBI record, and manually upload to eWORKS.	☒ Yes ☐ No
Employee, applicant & contractor interaction with SEPS	Questions or concerns that develop during any phase of the vetting process are addressed with the individual through secure email communication or a formal issuance of a Letter of Interrogatory (LOI) that must be responded to by the individual if the vetting process is to continue. All communications are manually uploaded and incorporated into the eWORKS file.	☒ Yes ☐ No (when necessary)

8. How will FDIC and/or the Outsourced Service Provider retrieve data or records as part of the outsourced service or project? Can data be retrieved using a personal identifier (e.g., name, address, SSN, EIN, or other unique identifier)?

Yes, personal identifier may be used to retrieve information. The data in eWORKS can be retrieved using name or full SSN.

9. In the Federal Register, under which Privacy Act Systems of Record Notice (SORN) does this system operate? Provide number and name.

FDIC-30--64—0015 / Personnel Records, (*80 FR 67001) (October 30, 2015)*

This completes the PTA.

- Do not complete the rest of the form, if the service provider is not processing or maintaining sensitive PII. This is the case, if you checked:
    - NOT APPLICABLE for question 3 and NO for all items in question 4; OR
    - Only Full Name in question 4.

- Continue completing the remainder of the form, i.e., Sections III thru VI in their entirety (questions 10 through 18), if the service provider is processing or maintaining sensitive PII. This is the case, if you checked:
    - YES for Social Security Number (SSN) in question 4; OR
    - YES for SSN or for Full Name in addition to one or more boxes in question 4.

- If you have questions or are unsure about whether or not you should complete the remainder of this form, please contact your Division ISM or the Privacy Program Office (privacy@fdic.gov).

SECTION III – DATA ACCESS AND SHARING

10. In the table below, specify the systems/applications and parties (FDIC and non-FDIC) that will access or receive PII data as part of the outsourced service/project. ***(Check "No" or "Yes" for each category. For each category checked "Yes," specify who will have access to, be provided with, or maintain the PII, what PII elements will be accessed/shared/maintained by them, how the access or sharing will occur, and the purpose and use of this PII.)***

PII Will Be Accessed By and/or Provided To:	Yes	No	If Yes, Explain How and Why the PII Will Be Accessed/Shared
10a. FDIC Outsourced Service Provider (OSP) Staff; OSP Sub-contractors; and/or OSP Systems	☒	☐	The vendor will perform a one-time data migration from PERSEREC to eWORKS and will have access to the data during that time. Following the data migration, the vendor will not have access to the data, which is encrypted. Access to eWORKS is role-based and no one from the OSP will have a role in eWORKS.
10b. FDIC Personnel and/or FDIC Systems/ Applications	☒	☐	Authorized DOA/SEPS applicant processing staffs are users of eWORKS. eWORKS uses a role-based access control system to restrict user access to the minimum necessary to perform specified duties critical to ensuring FDIC is in compliance with 5 CRF 5, 731, 736 and related Executive Orders. The SEPS Federal Personnel Security Specialists oversee, perform a quality review, and sign off on all personnel security case work performed by the contractor staff. Preparing case files for review by the Federal Specialists entails performing a series of records checks, all of which require inclusion of PII in order to ensure the accuracy of the results obtained. Moreover, these checks cannot even be initiated without use of PII (to include the SSN). After receipt of all checks, plus the required forms and authorizations completed by the individual subjects, the contractor staff prepares the case for Federal staff review and signature by summarizing and making recommendations predicated upon national suitability and security standards. Questions, issues, and inconsistencies are first addressed through Letters of Interrogatory that are also signed out to the subject by the Federal Specialists. Oversight Managers (OMs) and Administrative Officers (AOs): Will have limited access to eWORKS. OMs and AOs have the ability to initiate a Background Investigation and check on where it is in the process through a status report contained within eWORKS. They will not have access to full SSN or any details of the case. Ethics/Legal: When a case file contains information regarding such issues as bankruptcy or a felony arrest/conviction, the case file is to be referred to Ethics or Legal as appropriate. In particular, CFR 732 forbids FDIC from hiring or contracting with an individual guilty of defalcation or who has a felony conviction. In all such referrals, only extracts from the eWORKS files will be provided to Ethics or Legal. These case extracts are normally delivered directly to the respective office and, in turn, hand carried back to SEPS. It is possible for the extract to be delivered to the respective office employing

			internal email encryption (Azure Information Protection [AIP]). Little or no PII is typically involved in this process. However, when attempting to resolve issues associated with defalcation, the Legal Department will require PII to support their inquiries.
10c. Individual Members of the Public (e.g., bidders, investors, borrowers, customers, etc.)	☐	☒	
10d. Other Non-FDIC Entities/ Parties and/or Non-FDIC Systems/Applications	☒	☐	eWORKS will pull a report from the Equifax data system and utilize the report via SEPS personnel manually import upon satisfying matching criteria.
10e. Federal, State, and/or Local Agencies	☐	☒	Once the preliminary files have been completed, the applicant, employee, or contractor that is the subject of the requirement is automatically initiated into OPM's eQIP system. Once the individual has completed the eQIP process, a copy of the eQIP submission is captured and uploaded into eWORKS by SEPS personnel. OPM will conduct their investigation and adjudication process and all materials associated with the investigation and adjudication will be incorporated into the eWORKS file manually by SEPS personnel for the applicant, employee, or contractor
10f. Other	☐	☒	

11. If data will be provided to, shared with, or maintained by non-FDIC entities (such as government agencies, contractors, or Outsourced Information Service Providers), have any of the following agreements been issued?

Data Protection and/or Sharing Agreements	Yes	No
FDIC Confidentiality Agreement (Corporation)	☒	☐
FDIC Confidentiality Agreement (Individual)	☒	☐
Non-Disclosure Agreement (NDA)	☒	☐
Memoranda of Understanding (MOU)	☒	☐
Information Sharing Agreements (ISA)	☒	☐
Authentication Risk Assessment	☐	☒
Other Applicable Agreement(s) (*Specify*: _____)	☐	☒

If you answered NO to any item above, please provide additional information if available: Blue Canopy will conduct a Technical Security Assessment(TSA) which are against the NIST 800-53 Controls (same as those measured in a risk assessment)

SECTION IV – NOTICE AND CONSENT

12. Do individuals have the opportunity to decline to provide information or to consent to particular uses of their information (other than required or authorized uses)?

☒ No. Individuals do not have the opportunity to "opt out" of providing their data and/or consenting to particular uses of their information. Explain: Individuals cannot "opt out" of providing their personal information or consent to only particular uses. All PII collected is necessary to complete BIs as a condition of employment with the FDIC.

☐ Yes. Individuals have the opportunity to decline to provide their personal data or to consent to particular uses of their information. Explain:

13. If PII is being collected via a public-facing website and/or application as part of this outsourced service, has the Outsourced Information Service Provider posted any of the following types of privacy policies or Privacy Act notices?

☐ No
☐ Yes *(If yes, check applicable box(es) below.)*
- ☐ Link to FDIC Privacy Policy
- ☐ FDIC Privacy Act Statement
- ☐ Contractor Privacy Policy or Statement
- ☐ No Privacy Policy has been posted

☒ Not applicable

SECTION V – DATA SECURITY AND ACCURACY

14. Please assert what administrative procedures and technical safeguards are in place to protect sensitive PII data in the Outsourced Information Service Provider's care. *[Provide the name of the Outsourced Service Provider and check all applicable box(es).]*

☒ MicroPact has gone through the security review required by the FDIC's Outsourced Information Service Provider Assessment Methodology to determine and/or verify their having appropriate physical, technical, and administrative security measures to safeguard FDIC-provided PII and other sensitive data. If it has gone through the Methodology, has it been approved? ☐ NO ☒ YES

☒ The FDIC conducts background investigations (BIs) on key MicroPact personnel and other applicable personnel prior to their beginning work on the contract.

☒ MicroPact is subject to periodic compliance reviews by FDIC. Per the contract, scheduled and unannounced inspections and assessments of the Outsource Service Provider's facilities, personnel, hardware, software and its security and privacy practices by either the FDIC information technology staff, the FDIC Inspector General, or the U.S. General Accountability Office (GAO). These inspections may be conducted either by phone, electronically or in-person, on both a pre-award basis and throughout the term of the contract or task order, to ensure and verify compliance with FDIC IT security and privacy requirements.

☐ Other (Explain any other administrative and/or technical safeguards in place to protect PII data in the Outsourced Information Service Provider's care.) ***Attach the Contract Clause Verification Checklist to the back of this form.***

15. What are the procedure(s) for ensuring that the information maintained is accurate, complete and up-to-date? *[Check all applicable box(es) and insert the appropriate response and System/Project name.]*

☒ Data is collected directly from individuals and/or from the failed financial institutions. As such, the FDIC and its vendors rely on the individuals and/or financial institutions to provide accurate data.

☒ The vendor/contractor works with FDIC to verify the integrity of the data eWORKS in putting it into the system or using it to support the project.

☐ As necessary, an [authorized user or administrator] of the [System/Project Name] checks the data for completeness by reviewing the information, verifying whether or not certain documents or data is missing, and as feasible, updating this data when required.

☐ Other (*Please explain*.)

16. In terms of assuring proper use of the data, please assert whether the following statements are true for the Outsourced Information Service Provider. (*Check all applicable box(es) and insert the name of the Outsourced Information Service Provider and title of the firm's senior management official.*)

☒ Within FDIC, MicroPact's Program Manager/Data Owner, Technical Monitors, Oversight Manager, and Information Security Manager (ISM) are collectively responsible for assuring proper use of the data. In addition, it is every FDIC user's responsibility to abide by FDIC data protection rules which are outlined in the FDIC's Information Security and Privacy Awareness training course which all employees take annually and certify that they will abide by the corporation's Rules of Behavior for data protection.

☒ Additionally, the Outsourced Information Service Provider is responsible for assuring proper use of the data. Policies and procedures have been established to delineate this responsibility, and the vendor has designated the Information Security Manager to have overall accountability for ensuring the proper handling of data by vendor personnel who have access to the data. All vendor personnel with access to the data are responsible for protecting privacy and abiding by the terms of their FDIC Confidentiality and Non-Disclosure Agreements, as well as the vendor's corporate policies for data protection. Access to certain data may be limited, depending on the nature and type of data. (Refer to Section III of this Privacy Impact Assessment for more information on data access criteria.)

☒ The Outsourced Provider must comply with the Incident Response and Incident Monitoring contractual requirement.

☐ None of the above. *(Explain why no FDIC staff or Outsourced Information Service Provider personnel have been designated responsibility for assuring proper use of the data.)*

SECTION VI – DATA RETENTION AND DISPOSAL

17. Where will the Outsourced Service Provider store or maintain the PII data identified in question 4? Describe both electronic and physical storage repositories, as applicable.

Data is stored within the database server and is encrypted using FIPS 140-2 validated AES 256-bit encryption on Intel multi-core processors. The servers are located at:

Primary Data Center:
Equinix – DC3
44470 Chilum Place
Ashburn, VA 20147

Alternate Data Center:
Level3
180 Peachtree Street
Atlanta, GA 30303

18. Specify the period of time that data is retained by the Outsourced Service Provider and the specific procedures for disposing of or returning the data at the end of the retention period or contract, whichever is first.

The data is retained for 5 years after employment ends. Procedures for disposition of the data at the end of the retention period are established in accordance with FDIC Records Retention and Destruction Policy. Additionally, the contract specifies that MicroPact cannot retain or reproduce any data collected in eWORKS.