FEDERAL DEPOSIT INSURANCE CORPORATION
INSURING AMERICA'S FUTURE

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

for

Executive Search Services

Heidrick & Struggles International, Inc.

(RECVR-16-G-0537)

Date Approved by Chief Privacy Officer (CPO)/Designee: 07/18/2017

SECTION I – OUTSOURCED INFORMATION SERVICE DESCRIPTION

1. Describe the outsourced service and its purpose.

The Federal Deposit Insurance Corporation (FDIC), established under the Banking Act of 1933, maintains the stability and public confidence in the nation's financial system by (1) insuring deposits, (2) examining and supervising financial institutions, and (3) managing receiverships. Under the Federal Deposit Insurance Act (FDIA), the primary objectives of the FDIC as receiver are to maximize the value of assets from failed banks, limit losses to the deposit insurance fund, and manage a claims process for the benefit of creditors including uninsured depositors and general unsecured creditors. As such, the FDIC has an important role in liquidating these assets in the most cost-effective manner possible.

The Competitive Equality Banking Act of 1987 authorized the FDIC to establish Bridge Depository Institutions (bridge banks). A bridge bank is a temporary national bank chartered by the Office of the Comptroller of the Currency and organized by the FDIC to take over and maintain banking services for customers of a failed bank. It is designed to "bridge" the gap between the failure of a bank and the time when the FDIC can implement a satisfactory acquisition by a third party. An important tool available to the FDIC for the resolution of large or complex failing banks, a bridge bank provides the time the FDIC needs to take control of a failed bank's business, stabilize the situation, effectively market the bank's franchise, and determine an appropriate resolution where an immediate sale of the deposits and assets of institution is not feasible.

The FDIC's Division of Resolutions and Receiverships (DRR) is tasked with the preparation for the resolution of failing and failed FDIC-insured depository institutions (banks), which includes all governance-related matters for FDIA bridge banks in accordance with the conditions and requirements of the FDIA.

With the signing of the Dodd-Frank Wall Street Reform and Consumer Protection Act (DFA) into law on July 21, 2010, the FDIC is further responsible for resolving failing and failed Systemically Important Financial Institutions (SIFIs), which may include bank holding companies and non-insured depository institutions, as well as certain non-bank financial companies. The DFA provides the FDIC as receiver for a SIFI with powers to form a bridge financial company that are in many respects comparable to the authority to organize a bridge bank under the FDIA. There are, however, important differences between the two statutory regimes and between the business models that would apply to bridge financial companies as compared to bridge banks.

The Banking Act of 1933 also authorized the FDIC to establish a Deposit Insurance National Bank (DINB) to assume the insured deposits of a failed bank. This authority is now codified in the FDIA. Under this authority, the FDIC may organize a DINB as a national bank to assume and pay the insured deposits of the failed bank and perform certain other temporary functions. A DINB is chartered with limited life and is granted limited powers. A DINB provides an additional approach for a failed bank to be liquidated in an orderly fashion, minimizing disruption to local communities and financial markets by allowing depositors to access their accounts and provide time to open accounts at other financial institutions.

To most efficiently meet its objectives, the FDIC is soliciting the services of Heidrick & Struggles International, Inc. (Heidrick) to provide executive search and leadership consulting services in assisting the FDIC with a range of projects and efforts related to governance preparedness for an

FDIA bridge bank or other resolution matter. Heidrick's services are to be sufficient for application to the various sizes and complexities of all FDIC-insured banks and Systemically Important Financial Institutions (SIFIs), and their respective subsidiary entities.

Heidrick will conduct executive searches using their internal candidate database to select possible candidates for a FDIC bridge bank, DINB, bridge financial company, or other resolution matter. Heidrick will then send candidates' information (detailed in question 2) to the FDIC for consideration. Necessary recruitment profiles may include the positions of Chief Executive Officer (CEO), Chief Financial Officer (CFO), other Executive or C-suite Professionals, Trust Company Executives, Product Line or Affiliated Businesses Executives, Board Members Advisory Board Members, Executive or Board-Level Consultants, and various levels of management.

Heidrick will provide strategic advice on a range of issues relating to the governance of an FDIC bridge bank, DINB, bridge financial company or other resolution matter. In addition to providing traditional executive search services, Heidrick, on an as needed basis, will provide leadership consulting, industry analysis, and related reporting on matters affecting the governance of FDIC–insured banks and SIFIs, and their respective subsidiary entities.

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 FDIC DRR Oversight Manager assigns Heidrick executive search requirements to conduct on possible candidates for a potential FDIC bridge bank, DINB, bridge financial company or other resolution matter via the FDIC Secure Email Service. Heidrick then conducts executive searches using Heidrick's customized search system utilizing their internal candidate database. Based on the results, Heidrick will select the appropriate candidates based on the requirements. Heidrick will submit the candidate's full name, email address, telephone number(s), and employment information to the FDIC for consideration. Heidrick may also send candidates' resumes, which could contain other PII, but resumes are not required under the terms of this contract. Dependent upon the FDIC's request, Heidrick will screen and potentially interview possible candidates and present them to the FDIC Oversight Manager for consideration via the FDIC Secure Email Service.

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

Heidrick provides executive search and leadership consulting services in assisting the FDIC with a range of projects and efforts related to governance preparedness for an FDIA bridge bank or other resolution matter. Heidrick may be asked to provide a list of candidates and their resumes, based on a recruiting profile for the FDIC to contact and interview to meet a staffing need. Heidrick will provide strategic advice on a range of issues relating to the governance of an FDIC bridge bank, DINB, bridge financial company or other resolution matter. In addition to providing traditional executive search services, Heidrick, on an as-needed basis, will provide leadership consulting,

industry analysis, and related reporting on matters affecting the governance of FDIC–insured banks and SIFIs, and their respective subsidiary entities.

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.)*: *Note: The only PII involved in this contract that Heidrick provides to the FDIC is the candidate's name, email address, telephone number, and employment information (position titles, company names, etc.) Heidrick may provide resumes of candidates, which may contain any other PII elements, but this is not a requirement for the purposes of this contract.*

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:

SSNs are not requested by the FDIC for the purposes of this contract, but could be included in a resume submitted by Heidrick to the FDIC. Any SSNs that may be included in a resume submitted to the FDIC should be masked or deleted prior to storage in an FDIC system.

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

The collection of SSNs is not required for the scope of work being conducted. Sections 9, 11, and 13 of the Federal Deposit Insurance Act (12 U.S.C. 1819, 1821, and 1823) and

applicable State laws provide the legal authority governing the liquidation of assets and wind-up of the affairs of failed financial institutions.

c) Identify whether the SSN is masked or otherwise truncated within the system:
Any SSNs contained in the documents provided to Heidrick may or may not be masked or truncated. As noted earlier, any collection of SSNs would be incidental.

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[1]: To date, Heidrick has not been awarded any task orders under this agreement.

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

Data Source[2] (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?**
FDIC DRR Oversight Manager	The FDIC DRR Oversight Manager assigns Heidrick executive search requirements to conduct on possible candidates for a potential FDIC bridge bank, DINB, bridge financial company or other resolution matter via the FDIC Secure Email Service. The requirements provided by the Oversight Manager do not contain any PII. Heidrick then conducts executive searches using Heidrick's customized search system. Based on the results of the search and the requirements, Heidrick will select the appropriate candidates to present to the FDIC via the FDIC Secure Email Service.	☐ Yes ☒ No
Heidrick's existing internal candidate database	Heidrick, as part of the service that it offers to its customers, has existing data from prospective applicants. The types of PII that could be stored or processed are listed in question 4.	☒ Yes ☐ No

[1] 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.

[2] 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.

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)?

The FDIC does not retrieve data with a personal identifier. Emails containing candidate information and/or resumes are deleted after no longer required, and if stored on SharePoint, are stored using the bank name or task order.

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

N/A

This completes the PTA.

Do <u>not</u> complete the rest of the form, if the service provider is <u>not</u> 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 Subcontractors; and/or OSP Systems	☒	☐	Authorized Heidrick staff that perform executive searches on behalf of the FDIC have access to the PII listed above in Question 4 on "need to know" basis of potential candidates to fill the executive positions of a bridge bank organized by the FDIC. In addition, authorized Heidrick personnel generate leadership consulting, industry analysis, and related reporting on matters affecting the governance of FDIC–insured banks and SIFIs, and their respective subsidiary entities. Reports that are generated by Heidrick do not contain PII but may be considered sensitive. Heidrick personnel that are working under the engagement have been cleared by the FDIC.
10b. FDIC Personnel and/or FDIC Systems/ Applications	☒	☐	Heidrick shares their completed executive search results, reports related to leadership consulting and industry analysis services, and resumes of potential candidates back to the FDIC DRR Oversight Manager via the FDIC Secure Email Service. FDIC/DRR staff has access to the final executive search results, report and the resumes of the potential candidates in order to fulfill requirements regarding preparations for the resolution of failing and failed FDIC-insured depository institutions.
10c. Individual Members of the Public (e.g., bidders, investors, borrowers, customers, etc.)	☐	☒	Not Applicable
10d. Other Non-FDIC Entities/ Parties and/or Non-FDIC Systems/Applications	☐	☒	Not Applicable
10e. Federal, State, and/or Local Agencies	☐	☒	Not Applicable
10f. Other	☐	☒	Not Applicable

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:

Heidrick & Struggles is an outsourced service provider and therefore is not subject to MOUs or ISAs. Heidrick does not share any data for the purposes of this contract outside of the FDIC.

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 why individuals are not able to opt out (either for specific data elements or specific uses of their data.):***

☒ Yes. Individuals have the opportunity to decline to provide their personal data or to consent to particular uses of their information. ***(Explain how individuals may decline or consent to the use of their information.):***

Any prospect or candidate can decline, in verbal or written form, to provide information needed in the customary verification process or to provide personal information for our use. Candidates who decline to have their information provided to the FDIC will not be considered for recruiting needs.

☐ Not applicable. Information is not collected directly from individuals.

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

Note: Heidrick does maintain a public-facing website to collect candidates' information, with a privacy policy posted. However, the PII in the Heidrick internal candidate database is collected prior to the task order being assigned, and as such, is the property of Heidrick. It is not considered as being collected as part of this outsourced service.

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).]***

☒ Heidrick & Struggles 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 Heidrick & Struggles personnel and other applicable personnel prior to their beginning work on the contract.

☒ Heidrick & Struggles 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 [before, in conjunction with, and/or after] inputting it into the system or using it to support the project.

☒ As necessary, an authorized Heidrick & Struggles staff 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, Heidrick & Struggles' 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 its Chief Information Security Officer 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.

The primary data storage for Heidrick's search engine is at Salesforce, which is replicated to Heidrick's collocated database servers in Sungard Datacenter in Wooddale, Illinois. Availability and backup of data at Salesforce is handled by constant replication of Heidrick's data between Salesforce primary and secondary datacenters in Irving, Texas and Chandler, Arizona. Executive search and leadership consulting reports are also stored on Heidrick's collocated servers at the Sungard Datacenter.

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 normal retention period of FDIC data is indicated to be 3 years. Heidrick must dispose of or return FDIC data “as FDIC directs” “Upon completion or termination of the contract, or at any time the Contracting Officer requests it in writing”, there is no contractual requirement regarding duplication of data.