FEDERAL DEPOSIT INSURANCE CORPORATION
INSURING AMERICA'S FUTURE

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

for

## Independent Third-Party Security Assessment Services

## Blue Canopy Group

## CORFD-17-G-0373


**Date Approved by Chief Privacy Officer (CPO)/Designee: 10/2/2018**

**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)'s Division of Resolutions and Receiverships (DRR) promotes confidence in the nation's financial system by efficiently paying insured depositors, effectively managing failed financial institutions (FIs), and providing superior customer service to all. To execute its mission, DRR seeks assistance from contracted services, often referred to as "DRR service providers." DRR service providers manage data generated by the DRR service provider, data the FDIC provides to the DRR service provider, and data a third party (in the performance of services with the FDIC) provides to the DRR service provider.

To manage information security risks for DRR IT systems and contracted services to include staff augmentation, DRR's Information Security Unit (ISU) implements information security policies and procedures. To manage IT security and privacy risks that pertain to FDIC's data (inclusive of data residing on DRR service providers' IT systems), DRR created the Vendor Risk Management (VRM) program. DRR's ISU performs risk assessments, due diligence reviews, technical control testing, and ongoing security monitoring, which is essential to identify and assess IT security and privacy risks associated with DRR service providers.

To maintain the confidentiality, integrity, and availability of FDIC data that may be stored, processed, or transmitted within the service providers' IT systems or for which they have access, BC (contracted as a DRR service provider) performs independent third-party assessment services to determine the extent in which security and privacy controls are appropriately implemented and operating as intended. BC uses its technical expertise to conduct security and privacy assessments on security controls employed within or inherited by third-party service providers' IT systems, along with identifying and documenting system weaknesses or deficiencies in the controls and identifying vulnerabilities.

## 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.**

To determine the extent to which security and privacy controls are appropriately implemented and operating as intended, BC provides independent third-party security assessment services for DRR on-site at the FDIC, located in Arlington, VA. During a third-party assessment, the third party sends BC data in the form of security documentation. This security documentation may include full names and titles of the third party's Senior Management or IT Security professionals within their organization. BC sends and receives FDIC vendor information via Virtual Data Room (VDR), which is used to upload and download data pertaining to the assessment. Data is not sent via FDIC's Secure Email. BC only uses FDIC's Secure Email for communication purposes to and from the FDIC. BC does not utilize sub-contractors for assistance on this contract. BC uses FDIC government furnished equipment (GFE) for communication purposes to third-party vendors and the FDIC. BC will use their company-provided laptops, which are employed with full disk encryption, to perform their assessments to include but not limited to application security assessments, physical and logical penetration tests, etc. of a third party vendor's system or network.

To conduct security and privacy assessments for third parties, BC gathers and reviews third-party security documentation and, based on its analysis of the received information, reports on discovered findings. BC provides deliverables to the FDIC that consist of project plans, status meetings, minutes and reports, security assessment plan (SAP), security assessment report (SAR), working papers, disaster recovery plans, IT security plans, risk assessments, service auditors report, standard information gathering questionnaire, security test and evaluation report, vulnerability assessments and penetrating testing reports. Upon the FDIC's discretion, and, using standards contained within National Institute of Standards and Technology (NIST) Special Publications (SPs) including 800-53, 800-171, etc., BC performs site inspections at the third party's facility with controls to be specified within the respective task order.

BC must provide two primary deliverables to the FDIC: the SAP and the SAR. The SAP is an essential document to be delivered with every task order document. It consists of the scope of the assessment, a proposed timeline, and objectives for the security control assessment, a detailed roadmap of the approach to be taken to conduct the assessment, and assessment procedures. The SAR report includes necessary information that determines the effectiveness of the security controls, which were deployed within the information system or inherited by the information system based on findings discovered by the contractor. The SAR includes an executive summary, which contains a brief system description that summarizes identified high, moderate, and low risk findings, along with recommendations, a detailed system description with FIPS 199 security categorization, and recommendations that address each risk identified throughout the assessment. The SAR also includes a section with assessment objectives, scope, methodology, tools, and a prioritized list of identified vulnerabilities and impacted hosts with recommended remediation plans.

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

BC is responsible for analyzing all available security and privacy documentation from third parties to identify the system boundary of all IT components owned by the third party, subcontractors, and hosted services used to store, process or transmit FDIC information. BC generates assessments such as Penetration Test Reports, Vulnerability Assessments, Perform Physical Site inspections, etc. to determine whether security and privacy controls are implemented to ensure FDIC's data is protected while safeguarding the confidentiality, integrity, availability and privacy of FDIC data.

**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: _____) | ☒ | ☐ |

***Please Note:** While, BC does not store or process PII, they may have the ability to read any kind of PII that is stored or processed by another contractor working for DRR; (e.g., vulnerabilities being successfully exploited through a penetration test, hence, having the ability to view PII as a result of the exploit).

**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:** (*Please explain*.)

BC does not store or process PII, but may have the ability to read any kind of PII that is stored or processed by another contractor working for DRR; e.g., (In the case of a contractor providing a service for DRR for the purpose of marketing assets, BC could see loan information which could possibly contain the SSN's of borrowers given that BC successfully exploit as a result of a penetration test).

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

N/A

**c) Identify whether the SSN is masked or otherwise truncated as part of the outsourced service:** (*Please explain*.)

If vulnerabilities are successfully exploited through a penetration test, BC may have the ability to view PII as a result of the exploit; hence, the potential of SSN's being exposed.

**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]:**

[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

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**[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?** |
|---|---|---|
| Virtual Data Room (VDR) | BC uses the FDIC's VDR for the transmittal of documentation such as project plans, status meetings, minutes and reports, security assessment plan (SAP), security assessment report (SAR), working papers, disaster recovery plans, IT security plans, risk assessments, service auditors report, acceptance of risk documentation, application security assessment, site visit assessment reports, standard information gathering questionnaire, security test and evaluation report, vulnerability assessments, penetrating testing reports, etc. BC may receive one element of PII that contain full names on the security documentation such as the names of security professionals employed with the company BC is assessing. The Virtual Data Room is not hosted by BC. | ☒ Yes ☐ No |

**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 Outsourced Service Provider will retrieve records using the file names in SharePoint. There are no unique identifiers.

**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 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.


**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.**

| 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** | ☒ | ☐ | The OSP will use Virtual Data Room to store PII that is the names of IT professionals that create their own security documentation which is protected with access control and least privilege. There is no purpose for this PII, it is ancillary to the security assessment document. |
| **10b. FDIC Personnel and/or FDIC Systems/ Applications** | ☒ | ☐ | FDIC DRR employees will have access to assessment documents that could have the name of a DRR contractor who Blue Canopy is working with. There is no purpose for accessing that PII element, it could just be included in the documentation. Access is provided through the VDR and the document will be shared on FDIC's SharePoint server. |
| **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** | ☒ | ☐ | *Any type of PII listed in question 4 could be accessed through a successful penetration test. The PII is not processed or maintained by the OSP and there is no purpose or use of this PII.* |
| **10e. Federal, State, and/or Local Agencies** | ☐ | ☒ | |
| **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 is an Outsourced Information Service Provider and therefore is not subject to MOUs or ISAs**

## 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.):*** There is no use of their information.

☐ 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.):***

**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.**

☒ Blue Canopy 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 Blue Canopy personnel and other applicable personnel prior to their beginning work on the contract.

☒ The Blue Canopy 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?**

☒ 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 conjunction with inputting 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.**

☒ Within FDIC, the Blue Canopy 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 Team Lead Harun Karaman 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.**

Blue Canopy is not storing or maintaining PII identified above.

**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 outsourced service provider maintains all records by the FDIC, and will continue to maintain all records related to the FDIC translation packages until completion or termination of the contract or until the Contracting Officer makes the request in writing per contract stipulation.