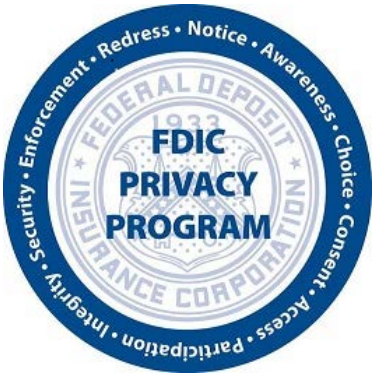
FEDERAL DEPOSIT INSURANCE CORPORATION
INSURING AMERICA'S FUTURE

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

for

Outsourced Legal Support Services (OLSS)

NightOwl Discovery



Date Approved by Chief Privacy Officer (CPO)/Designee: 09/19/2016

SECTION I – OUTSOURCED INFORMATION SERVICE DESCRIPTION

1. Describe the outsourced service and its purpose.

The Federal Deposit Insurance Corporation (FDIC) Legal Division contracts with vendors under a Basic Ordering Agreement (BOA) to provide legal support services and products in order to electronically process, host and store files and data that are part of the Legal Division's investigations, inspections, and litigation activities. These vendors are categorized into the Outsourced Litigation Support Services (OLSS) system and perform a number of tasks on behalf of the Legal Division. This includes enforcement, bankruptcy, corporate, professional liability, and inherited litigation matters. The data collected from internal FDIC data sources as well as open or closed banks pursuant to litigation or investigations will be processed and hosted by contractors and may include any internal FDIC Electronically Stored Information (ESI) or paper records. Potentially relevant data are placed on legal hold and preserved throughout the course of litigation. Specific services are addressed in the Statement of Objectives (SOO) that is included with the vendors' Basic Ordering Agreement for Legal Support Services, and will include:

- Document acquisition, preparation and unitization; scanning, redaction, text extraction or Optical Character Recognition (OCR), ESI processing, image rendering and database creation, as well as creation of production sets to opposing counsel and other entities (e.g, Congress);
- electronic data acquisition and processing;
- pre-trial and trial support (providing resources in support of litigation);
- forensic services performed by certified forensic professionals (such services are also routinely provided by DIT Security staff);
- managed legal review, i.e., providing licensed attorney staff to conduct relevance and privilege reviews of processed data; and
- managed data hosting (provision of review application (web-based), and administrative user access control, etc.)

The contracted vendors primarily support large matters under the supervision of FDIC Legal Division attorneys. FDIC staff gathers and provides the vendors with potentially relevant claims and enforcement case materials. Vendors do not download any ESI directly from FDIC Information Technology (IT) resources. FDIC attorneys also do not scan and upload any documents to vendor web-sites; rather documents are securely shipped to the vendor or transferred using secure file transfer protocol (SFTP). Authorized users can connect to review applications via secure sites. Users are granted access based on role and are only allowed to review and tag documents. They are not allowed to edit or delete documents. Permission to perform any other activities outside of reviewing and tagging must be expressly approved by the Legal Division. Based on circumstances or agreements with opposing counsel or other participants, rights to print or download may be granted for subsets of data upon request.

2. Status of the Outsourced Information Service Provider:

☐ Solicitation/On-Boarding (Pre-Award; or At/Around the Time of Contract Award)
☐ Initial Assessment/Due Diligence (Post-Award)
☒ Ongoing Monitoring of Contract (Post-Award)
☐ Sunset or Disposition of Contract (Post-Award; At or Near Contract Expiration)
☐ Other (*Explain*):

SECTION II – DATA TYPE, SOURCES, AND USE

3. 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. ☐ Not applicable

The FDIC Legal Division obtains professional legal support services and products to electronically process and store files and data. These files contain a significant amount of PII and sensitive data that must be examined, categorized, and appropriately utilized for the purposes of performing tasks associated with investigations, inspections, examinations, and litigation. The work performed involves access to confidential and sensitive information. Confidential information can be found in hard copies and electronic copies of documents as well as in databases.

Data is automatically extracted and collected from various sources that store ESI in hardcopy or electronic format for secure transmission and/or shipment to the contracted legal service providers. Material is collected, scanned and redacted. The media is encrypted and delivered to the vendors. Examples of various sources from which data may be retrieved by Legal, DIT Security, or others and shared with the vendors include the following:

- Enterprise Vault (EV): email communications (represents most of the data)
- FDIC desktops, laptops, server shares, and SharePoint sites
- Failed Bank Data Services (FBDS): imaged data related to failed financial institutions; such data may be accessed and retrieved by FDIC Division of Resolutions and Receiverships (DRR – Investigations and Customer Service personnel), Legal Staff, and retained Counsel firms and experts
- Examination data: Regional Automated Document Delivery System (RADD), ViSION, Examiner emails, work-papers, Report of Examinations (hard copies)
- Consumer complaint information (e.g., Kansas City call center data)

OLSS is expected to include the following services, which may involve accessing or utilizing PII:

1) Document acquisition, preparation, unitization: Includes organizing documents; identification of document boundaries (e.g., inserting slip sheets); numbering documents; creating box or file level indices; capturing document images (e.g., single-page Tiff format or PDF format); copying documents; preparing documents for production; documenting procedures; and performing quality control.
2) Database creation: Includes Optical Character Recognition (OCR) documents; document coding/data entry; creating databases (e.g., Summation) or database load files (e.g., eDII); documenting procedures; and performing quality control.
3) Electronic data acquisition, processing: Includes extracting and converting data files, including email files and other files in their native formats; automated and manual analysis of files to identify relevant or priority material; analyzing and reporting file type and other data metrics; assisting in the production of electronic data; documenting procedures; and performing quality control.
4) Pre-trial and trial support, including courtroom services: Includes providing administering, operating and maintaining equipment and other resources in support of litigation; exhibit preparation; courtroom presentation and audio/visual services; and performing quality control.
5) Forensic services: Includes forensic data collection performed by certified forensics professionals as needed at sites throughout the United States; data analysis and reporting; documenting procedures; and performing quality control.
6) Managed legal review: Includes acquisition and processing of electronic data for the purpose of batching/loading the data into a review application; domestic review of documents by licensed attorneys for relevance and identification of legal privileges; redaction; creation of privilege logs; production of electronic and imaged data; documenting procedures; and performing quality control.

7) Managed data hosting: Includes secure hosting of data for access by FDIC (or others as designated by FDIC); administration and support of web-based database/legal review applications (e.g., Summation; Relativity); documenting procedures; and performing quality control.

OLSS may on occasion contain information imported or scanned into the system previously received from State Regulators or Federal agencies involved in certain legal matters. These entities may include the Federal Trade Commission (FTC), Securities and Exchange Commission (SEC), U.S. Department of Justice (DOJ), U.S. Attorneys' Office, and Federal or local Law Enforcement.

OLSS may also contain information imported or scanned into the system received from parties involved in legal matters, such as assuming institutions, Servicers, Bank and Law Firm retained vendors, FDIC outside counsel, and other individuals or entities pertinent to the respective legal matter or resolution of the matter.

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

The FDIC Legal Division uses these professional legal support services and products to electronically process and store files and data for the purposes of performing tasks associated with investigations, inspections, examinations, and litigation. Assistance is required from outside vendors to respond to information requests from many sources, including, Congressional and third-party subpoenas, as well as audits and to provide assistance to the Legal Division attorneys and other professional staff members to acquire, organize, analyze and present evidence in conducting a lawsuit or investigation.

5. 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: _All manner of PII may be included in OLSS.___)	☒	☐

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 ☐	10,000 – 50,000 ☐	50,000 – 100,000 ☐	over 100,000 ☐

6b. If "0" was answered for 6a, please explain[1]: Outsourced Services Provider, NightOwl, has not received any work yet from FDIC. Currently, they are maintaining no PII. However, when they get matters to review, the amount of PII they maintain may in all likelihood exceed 100,000.

7. What are the sources[2] 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?**
Enterprise Vault	Email communications. All PII data elements may be included; which are derived by data which is extracted and collected from email communications that store ESI in hardcopy or electronic format. Material is collected, scanned and redacted as appropriate, then copied onto secure DVD or thumb drives or sent via secure FTP. The media is encrypted and delivered to the vendors.	☒ Yes ☐ No
FDIC desktops, Laptops, server shares, SharePoint sites	ESI-Native files, text and images. All PII data elements may be included; which are derived by data which is extracted and collected from FDIC desktops, laptops, server shares and SharePoint sites that store ESI in hardcopy or electronic format. Material is collected, scanned and redacted as appropriate, then copied onto secure DVD or thumb drives or sent via secure FTP. The media is encrypted and delivered to the vendors.	☒ 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.

Failed Bank Data Services (FBDS)	Imaged and native ESI related to failed financial institutions; such data may be accessed and retrieved by FDIC DRR, Legal staff, outside counsel, OIG, and opposing counsel. All PII data elements may be included; which are derived from data which is extracted and collected from failed financial institutions that store ESI in hardcopy or electronic format. Material is collected, scanned and redacted as appropriate, then copied onto secure DVD or thumb drives or sent via secure FTP. The media is encrypted and delivered to the vendors.	☒ Yes ☐ No
Regional Automated Document Distribution and Imaging (RADD)	Examination data: All PII data elements may be included; which are extracted and collected from examiner emails, workpapers and Reports of Examination (RoE) that store ESI in hardcopy or electronic format. Material is collected, scanned and redacted as appropriate, then copied onto secure DVD or thumb drives or sent via secure FTP. The media is encrypted and delivered to the vendors.	☒ Yes ☐ No
Virtual Supervisory Information on the Net (ViSION)	Examination data: All PII data elements may be included; which are extracted and collected from email communications that store ESI in hardcopy or electronic format. Material is collected, scanned and redacted as appropriate, then copied onto secure DVD or thumb drives or sent via secure FTP. The media is encrypted and delivered to the vendors.	☒ Yes ☐ No
Consumer Complaint Information	FDIC call center data. All PII data elements may be included; which are extracted and collected from consumer complaint information that store ESI in hardcopy or electronic format. Material is collected, scanned and redacted as appropriate, then copied onto secure DVD or thumb drives or sent via secure FTP. The media is encrypted and delivered to the vendors.	☒ Yes ☐ No
State Regulators	Joint exams and correspondence with state regulators. All PII data elements may be included; which are derived from data which is extracted and collected from financial institutions that store ESI in hardcopy or electronic format.	☒ Yes ☐ No
Federal Agencies	Federal Trade Commission, Security and Exchange Commission, U.S. Department of Justice, U.S. Attorneys Office, Federal and local law enforcement. All PII data elements may be included, should they be received from State Regulators or Federal Regulators and imported or scanned into the system.	☒ Yes ☐ No

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

☐ No (Explain how data will be retrieved: _____) \
☒ Yes (Explain how data will be retrieved, and list the personal or unique identifiers: _Data is retrieved on a routine basis about employees or members of the public using a personal identifier such as the individual's full name , account number or borrower number)
☐ Not applicable

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 5; OR
  - Only Full Name in question 5.

- Continue completing the remainder of the form, i.e., Sections III thru VI in their entirety (questions 8 thru 16), 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 5; OR
  - YES for SSN or for Full Name in addition to one or more boxes in question 5.

- 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

9. In the table below, specify the systems/applications and parties (FDIC and non-FDIC) that the Outsourced Service Provider will share or provide PII data to as part of the outsourced service. ***(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
9a. FDIC Outsourced Service Provider (OSP) Staff; OSP Subcontractors; and/or OSP Systems	☒	☐	NightOwl Staff have access to PII within OLSS as specified in Question 5 to perform the work that is stated in the BOA. PII can be found in hard copies and electronic copies of documents as well as in databases. As a result, access to data and secure contractor facilities are restricted to and those contractor employees who have been authorized to have access to the data and facilities. The contractor must meet all security requirements detailed in the BOA for Legal Support Services. The contractor's system administrator will have access. The purpose for the system administrator to have access to this information is for maintenance purposes only; this includes adding users to the system, performing system upgrades, and troubleshooting users' system problems. In these situations, the data itself is not reviewed by the system administrator.
9b. FDIC Personnel and/or FDIC Systems/ Applications	☒	☐	Authorized internal FDIC users include Legal Division attorneys and paralegals, RMS examiners or investigators and DRR investigators supporting Legal investigations or litigation. The purpose of Legal Division attorneys, paralegals and FDIC Outside Counsel having access to the information is to review records for potential relevance to an investigation or matter in litigation, or to respond to discovery or subpoena and other document requests. The following categories and number of FDIC employees will have access to the PII data: • Legal Division Attorneys and Paralegals: 50 • RMS Examiners and investigators: less than 25 (to assist with case preparation and serve as witnesses) • DRR Investigators: approx. 25 (to assist with case preparation and serve as witnesses) Access to the data is limited by role. Authorized FDIC users and FDIC's retained counsel may have the ability to print and possibly download working copies.

9c. Individual Members of the Public (e.g., bidders, investors, borrowers, customers, etc.)	☐	☒	*Not applicable. Individual members of the public do not have access.*
9d. Other Non-FDIC Entities/ Parties and/or Non-FDIC Systems/Applications	☒	☐	Other non-FDIC entities that may access OLSS include Outside Counsel, Contractor personnel, FDIC expert witnesses, and Opposing Counsel. Opposing Counsel may have a very limited/controlled access to subsets of data within the OLSS databases. They have the ability to view and tag items; however, they would not be able to print or download data from OLSS. For example, the Opposing Counsel can log into the system to view and tag relevant documents. Once completed, a representative from FDIC counsel would review the potentially relevant tagged data to determine confidentiality, non-relevance, and privileged documents for exclusion. ESI containing PII may be produced to external parties, including Opposing Counsel or the courts. In such cases, certain PII would be redacted prior to production, and/or would be produced subject to a court-entered protective order. FDIC's retained counsel may have the ability to print and possibly download working copies.
9e. Federal, State, and/or Local Agencies	☒	☐	On occasion, material may be shared with other federal or state agencies including, but not limited to, the Department of Justice (DOJ), the Office of the Comptroller of the Currency (OCC), the Federal Bureau of Investigations (FBI), FDIC Office of Inspector General (OIG), and other law enforcement agencies or bank regulatory agencies. Consumer complaint information may be shared with agencies such as the Federal Trade Commission (FTC) or the Consumer Financial Protection Bureau (CFPB).
9f. Other	☐	☒	*Not applicable. No other entities have access to, or provide data.*

10. 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: NDAs, ISAs, or other applicable agreements are not entered into because protective orders and confidentiality agreements bind the parties in matters before Federal and state courts.

SECTION IV – NOTICE AND CONSENT

11. 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.):*** Information contained in OLSS is not collected directly from the individual. The data is derived from internal FDIC sources and FDIC insured banks. Individuals would have the opportunity to "opt out" or provide consent if they were parties to the litigation at issue. Generally, however, the data belongs to the receivership, trustee, or other corporate entity subject to the litigation, and such data providers; therefore, individuals do not have an opportunity to "opt-out" of providing their data and/or consent.

☐ 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.):***

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

12. 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

13. Please assert what administrative procedures and technical safeguards are in place to protect sensitive PII data in the Outsourced Information Service Provider's care.

☒ NightOwl 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 Outsourced Litigation Support Services personnel and other applicable personnel prior to their beginning work on the contract.

☒ NightOwl 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.***

Guidelines for accessing data in OLSS are in keeping with current FDIC information security policies and practices. The following policies are applicable:

- FDIC 1360.1, *Automated Information Systems (AIS) Security Program*
- FDIC 1360.8, *Information Security Categorization*
- FDIC 1360.9, *Protecting Sensitive Information*
- FDIC 1360.12, *Reporting Computer Security Incidents*
- FDIC 1360.15, *Access Control for Information Technology Resources*
- OMB Circular A-130, *Management of Federal Information Resources*

The Contract Oversight Manager (OM) is responsible for ensuring that sufficient safeguards and controls are in place to avoid the unauthorized or unintended release of personal data by the vendors. The Program Manager (PM) maintains overall responsibility for OLSS and is accountable for establishing the criteria, procedures, controls, and responsibilities to prevent a compromise of the integrity of the data being collected. All OLSS contractors must abide by the terms and provisions specified under Section 9 of the BOA pertaining to the security of information technology (IT) systems and FDIC information.

14. 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. FDIC provides outside vendors with encrypted collections of data migrated out of the FBDS central repository for managed review.

☒ The vendor/contractor works with FDIC to verify the integrity of the data in conjunction with, and inputting it into the system or using it to support the project. Data normalization and "clean-up" is often necessary. On the uncommon occasion of processing by outside vendors, the data is run through both an inclusion and exclusion list to remove system and other non-essential files.

☒ As necessary, an authorized user of the OLSS Project 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. Quality control is part of every project.

☒ Other (*Please explain.*)
The data itself is scrubbed to eliminate NIST identified system files and to produce clean subsets. SQL Database reports may be generated and compared against inventory reports from systems in which co-existing data was retrieved such as:

- Enterprise Vault (EV): email communications (represents most of the data)
- Failed Bank Data Services (FBDS): imaged data related to failed financial institutions, such data may be accessed and retrieved by FDIC DRR personnel (Investigation and Customer Service) and Legal Staff
- Examination data: Regional Automated Document Delivery System (RADD), ViSION, Examiner emails, work-papers, Report of Examinations (hard copies)
- Consumer complaint information (e.g., Kansas City call center data)

15. 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, the Outsourced Litigation Support Services 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 Project Manager/Key Personnel 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

16. Where will the Outsourced Service Provider store or maintain the PII data identified in question 5? Describe both electronic and physical storage repositories, as applicable.

NightOwl manages the data transferred to them in accordance with their contract with FDIC. Once the data is reviewed, the product is transferred back to the FDIC either via secure FTP or via removable encrypted media (the FDIC preference is secure FTP). Once the data is received by FDIC, then the Outsourced Service Provider destroys any copies of the media and verifies to the FDIC in writing that the media has been destroyed. Verification is often done via e-mail.

17. 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 until the end of the affected litigation or e-Discovery production. Once the production is completed, the Outsourced Service Provider destroys or returns any copies of the data and verifies to FDIC in writing that they have destroyed or returned all related copies as specified in 9.1.(c) of the Basic Ordering Agreement.