FEDERAL DEPOSIT INSURANCE CORPORATION
INSURING AMERICA'S FUTURE

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

for

Legal Hold Support

LHS

Date Approved by Chief Privacy Officer (CPO)/Designee: 09/27/2017

SECTION I – OUTSOURCED INFORMATION SERVICE DESCRIPTION

1. Describe the outsourced service and its purpose.

The FDIC has contracted with AITHERAS, LLC ("vendor" or "outsourced service provider")[1] to build and maintain the Legal Hold Support (LHS) system, a configurable commercial off-the-shelf (COTS) product. LHS is a new legal hold management solution that will automate many of the steps in the legal hold process[2] and provide a single authoritative platform for more effective managing, monitoring and reporting of legal holds for attorneys and non-attorneys alike.

This system will preserve relevant litigation and legal hold tracking information and will provide:

- Real-time access to legal holds for all supervisors/managers so they can monitor and manage legal holds under their supervision.
- Promote greater cross-divisional collaboration on legal hold processes and procedures, particularly among Division of Administration (DOA) Records and Information Management Unit (RIMU) and Human Resources Branch (HR), Information Security and Privacy Staff (ISPS), and the Legal Division.
- Enable the Legal Division to generate a report showing that the FDIC took "reasonable steps" when implementing the legal hold for that particular matter to share with courts and counter-parties.
- Significantly reduce the risk of inadvertent destruction of information.

There are two sides of the tool, including the:

- **Legal Hold Center** where the logged-in users can initiate a hold, and view all of their holds; the ones that they initiated, as well as the ones they have been worked on by other users; and
- **Custodian Portal** which provides a listing of all the logged-in user's active notifications, along with the user's current acknowledgement status (response) for each of those holds.

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.

LHS will maintain tracking information related to litigation and legal hold matters,[3] including: Matter Number, Matter Name, Institution Name, Institution Cert, Financial Institution Number (FIN), Oversight Attorney (Employee ID, Name and Work Email Address), Delegated Authority (Employee ID, Name and Work Email Address), Paralegal (Name, Work Email Address) and Section

[1] The vendor hosts applications and databases using Amazon Web Services (AWS) secure cloud services platform. Services are designed as single-instance/multi-tenant applications, delivered via Software-as-a-Service model. Applications are designed to meet commonly-accepted industry practices for ensuring protection and security of customer's data and restrict access to customer data based on user credentials and role.

[2] The legal hold management process refers to the process which FDIC uses to preserve all forms of relevant information when litigation is in existence, or is reasonably anticipated following the issuance of a legal hold notice; including the steps taken to collect and preserve related data and information, and subsequent reporting on the same.

[3] All matters that are currently (at the time of the migration) open with Legal Hold will be migrated into the outsourced service from Advanced Legal Information System (ALIS).

Name. In addition, LHS will maintain FDIC employee profile information for the document custodians involved in the legal hold, including their Names, Identification Numbers (Employee IDs and Contractor IDs), Network IDs (NTIDs), Divisions/Departments, and FDIC Email Addresses.

When holds are created, the individual creating the actual hold to be issued may include additional information as identified in Q4 below. This could include employment status, home address, and a variety of legal terminology that could include sensitive information.

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

The purpose of the above information is to record, track, and report on the FDIC's legal holds.

4. What types of personally identifiable information (PII) are (or may be) included in the information specified above?

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: Work email address, NTID	☒	☐

*Note: Employee Identification Number (EIN) will be masked before being migrated to LHS.

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: N/A
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: N/A

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?**
Advanced Legal Information System (ALIS)	All matters that are currently (at the time of the migration) open with Legal Hold within ALIS will be securely migrated into LHS. Data elements to be migrated include: Matter Number, Matter Name, Institution Name, Institution Cert, Institution FIN, Oversight Attorney(Employee ID, Name and Work Email Address), Delegated Authority(Employee ID, Name and Work Email Address), Paralegal (Name, Work Email Address) and Section Name.	☒ Yes ☐ No
Personal Master Dimension (PMD)	PMD securely provides employee profile information to LHS via a nightly automated feed. Data elements include: Name, Employee ID/Contractor ID, NTID, Status, Division, Section/Unit ID, Section/Unit Name, Contact Type, FDIC Email Address, and Date Last Changed.	☒ Yes ☐ No
Manual entry by individual creating the hold	For employment litigation matters: When holds are created, the individual creating the actual hold to be issued may report additional information as identified in Q4. This information is self-reported by the complainant and included in LHS (via manually typing it in) by the oversight attorney or paralegal assigned to the hold. This could include employment status, home address, or similar information, and a variety of legal terminology that could include sensitive information. For all other legal holds: When holds are created, some information is manually entered by the assigned attorney or paralegal. This information generally references the subpoena or other court documents. These other holds do not generally contain PII.	☒ 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.

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)?

Data can be retrieved using a personal identifier, but this is not how information is routinely retrieved. Data will be most commonly retrieved through searching and reporting by the matter name and the name of the FDIC employees assigned to or involved in the matter (Oversight Attorney, Paralegal Employee, Document Custodian).

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

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 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 outsourced service provider (OSP) will generally not have access to the PII that is being migrated to or stored in LHS for routine tasks. OSP personnel are strictly tasked with maintaining the system. In this capacity, there are three roles assigned to the OSP: • System Administrators – Perform system administration and therefore may have access to PII data. • Engineering – Have administrative privileges for deployment purposes which does not involve/require direct access to PII, but could access data through self-escalate privileges. • Customer Support Services – Have no direct access to PII data, but they could have access to PII through screen sharing with users during trouble shooting.
10b. FDIC Personnel and/or FDIC Systems/ Applications	☒	☐	There are two sides of the tool: The **Legal Hold Center** is where logged-in users can initiate a hold and view all of their holds (any holds that they have initiated as well as any they have been included on by other users). The roles within the Legal Hold Center that will have access to PII include: • Oversight Attorney: FDIC attorney in charge of the matter; • Delegated Authority: FDIC approving official – typically the supervisor of the attorney issuing the hold; and • Paralegal: FDIC personnel working directly with the attorney in crafting the language of the hold, and responsible for following up with communications pertaining to the hold. The **Custodian Portal** provides a listing of all the logged-in user's active notifications, along with their current acknowledgement status (response) for each of those holds. A custodian is the person who is responsible to keep records. Custodians will only have access to their own PII in the Custodian Portal.
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	☒	☐	FDIC does not directly share data within LHS with non-FDIC parties, but a requesting party may subpoena the FDIC to provide specific data, which could include data present in LHS and maintained outside of the system. Generally, this data

			request would include information such as: when the legal hold was issued, who it was sent to, the date/time it was sent, and a general summary of the hold itself. This is commonly done when there is a protective order in place, and the counter-parties, courts, and administrative tribunals will only receive a summary of this information to demonstrate that a legal hold was, in fact, issued and done so appropriately
10e. Federal, State, and/or Local Agencies	☒	☐	FDIC does not directly share data within LHS (i.e. reports) with other agencies, but a requesting party may subpoena the FDIC to provide specific data, which could include data present in LHS and maintained outside of the system. Generally, this data request would include information such as: when the legal hold was issued, who it was sent to, the date/time it was sent, and a general summary of the hold itself. This is commonly done when there is a protective order in place and the counter-parties, courts, and administrative tribunals will only receive a summary of this information to demonstrate that a legal hold was, in fact, issued and done so appropriately.
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: AITHERAS, LLC is an outsourced service provider.

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.):*** Individuals do not have the opportunity to opt out of providing their data to LHS, as information is not collected directly from individuals and the information is required to process legal holds.

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

☒ The vendor 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 AITHERAS, LLC personnel and other applicable personnel prior to their beginning work on the contract.

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

☒ As necessary, Legal Hold Support checks the data for completeness by reviewing the information, verifying whether or not certain documents or data are 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 Legal Hold Support 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 Technology Officer (CTO) 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 OSP will host all customer data in data centers provided by secure web-hosting service providers. Physical access to computing facilities is strictly controlled to restrict access only to authorized personnel, including visitor sign-in and supervision, use of proximity-based access cards and biometric and scanners (or similar approved security authentication methods), and monitored internal visual surveillance mechanisms. Environmental controls will be in place to minimize the effect of malfunction or physical disaster to any data facilities, including access to dedicated and redundant power supplies, HVAC, backup power, temperature and humidity monitoring, smoke and water detection monitoring, and central fire suppression systems. Application and server infrastructure will be continually monitored to guard against any unplanned network or server outages, and OSP service level agreements with hosting providers require rapid response to any security incident or identified error condition. All customer information being transmitted to and from the OSP's applications and a customer's web browser (data-in-transit) is encrypted. All customer information being retained on storage area networks (data-at-rest) will be encrypted.

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 retained by the OSP will accommodate varying retention schedules (i.e. time, event or ad-hoc) based on the types of legal matters (e.g. criminal, employment, supervision, and etc.). The OSP retains data for three years following final payment under the contract, or for any longer period required by statute or another clause in the contract. It will make the data available to the FDIC for audit, examination and reproduction, at reasonable times during the retention period. It will also provide the FDIC with working space at its facilities to conduct the audit and examination.

Upon termination/conclusion of the contract, the OSP will maintain the data for three years following any final settlement that it must maintain. It will make available to the FDIC, records relating to appeals under the "Disputes" clause of the contract, or to claims or litigation arising under or from the contract, until the appeals, claims, or litigation are resolved.

The OSP will use best efforts to propose for the transition of data, documentation, configurations, cloud environments, licenses (if any), source code repositories, DevOps processes, and services for a follow-on service provider or the FDIC to continue identical services. It will propose a cost effective approach to support the transition, provide the ability for FDIC to export the legal hold data for future use in a FDIC approved format as determined at the end of the contract period and provide list of non-proprietary formats available to FDIC to export data.