FEDERAL DEPOSIT INSURANCE CORPORATION
INSURING AMERICA'S FUTURE

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

for

CACI Failed Bank Data Services

CFBDS

Date Approved by Chief Privacy Officer (CPO)/Designee: 4/7/2015

PTA/PIA TEMPLATE VERSION 1.5 – July 2014

SECTION I – OUTSOURCED INFORMATION SERVICE DESCRIPTION

1. Describe the outsourced service and its purpose. *In your response, use simple, non-technical language to clearly explain what services will be provided under the contract and the FDIC* ***business functions*** *that will be supported.*

When a financial institution fails, the FDIC as Receiver must retain specific records and types from the failed institution (FI) to meet FDIC's fiduciary requirements, resolve legal issues, perform research and provide on-going customer service. The Failed Bank Data Management Services (FBDS) project, led by the Division of Resolutions and Receiverships (DRR) Business Program Management Section (BPMS), provides the services necessary to collect and store electronically stored information (ESI) from FIs so as to ensure the FDIC's compliance with legal and statutory requirements. The FBDS team currently utilizes outsourced information service providers, including CACI-ISS (hereinafter CACI) and CACI's approved subcontractors to securely capture, image, index, and maintain ESI from failed financial institutions.

At the direction of the FDIC, the CACI FBDS capture team travels to the FI data site(s) to capture ESI from FI systems, servers, storage and other computing devices, as required to capture the requisite records. The captured ESI generally includes the following standard data sets: asset/loan, deposit, financials (e.g., General Ledger, Accounts Payable, Wire & Transaction History), email and file shares. These data sets have the potential to contain sensitive financial information and personally identifiable information (PII) about bank customers, borrowers, guarantors, and vendors who performed business with the FI, as well as bank employees, officers, directors, attorneys and other "Persons-of-Interest" (POIs) who are subjects of FDIC/DRR investigations. In addition, FDIC/Receivership or DRR Investigations staff may collect records (e.g., Board minutes, loan records, etc.) belonging to the FI and securely ship them in accord with DRR's secure shipping policy, to a scanning facility operated by an authorized CACI vendor for imaging. The hardcopy records may contain sensitive data and PII pertaining to POIs, as well loan and deposit data with financial information and PII pertaining to bank customers, borrowers and guarantors. All captured data is either securely uploaded to the FBDS solution or loaded to encrypted hard drives and securely transported or shipped to CACI's Operations Facility . where the data is subsequently loaded to the secure FBDS solution.

The FBDS solution provides a standardized method of maintaining, locating and managing data from failed financial institutions including: secure data migration, conversion, cataloging, indexing, storage, archival and retrieval of bank data. CACI's secure off-site data center is scalable and flexible to allow for the timely addition of institution data as FDIC's needs arise. Data in the FBDS solution is accessible through a secure web portal to authorized FDIC users for investigation, litigation, research and customer service support purposes.

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

Data collected from failed financial institutions' paper and electronic records may include any of the following: Loan and Collateral Files, Deposit Files, FI Financials, Email, File Shares, Suspicious Activity Reports (SAR), Reports of Examinations (ROEs), Payroll records, HR records, Board Minutes, and other related FI records as necessary to meet the FDIC statutory requirements. This data has the potential to include any and all of the PII specified in Section 2.5, including but not limited to: full name, date of birth (DOB), social security number (SSN), mother's maiden name, home address, financial information, employment status/history, etc., pertaining to the following categories of individuals:

- Borrowers
- Customers
- Complainants
- Claimants (Depositors or Non-Depositors)
- Guarantors
- Failed Bank Creditors or Vendors and
- Failed Bank Officers/Directors/Employees

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

When an FDIC-insured financial institution fails, the FDIC as Receiver must retain certain failed institution records, which may include any and all of the PII identified above to resolve legal issues, perform research, provide on-going customer service,

and meet FDIC's fiduciary responsibilities. As part of these responsibilities, the FDIC is prohibited under 12 U.S.C § 1821(d) (15)(D) from destroying any records of an insured depository institution for which it has been appointed Receiver. The FDIC as Receiver must retain FI records going back ten (10) years from the date of Receivership and must maintain these records for at least six (6) years. To this end, the FBDS solution provides the services necessary to collect, organize, store and retrieve ESI from failed institutions to ensure FDIC's compliance with legal and statutory requirements.

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: _____)	☐	☒

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

<table>
<tr><th>Data Source[1]
(List all sources that the Outsourced Provider collects, obtains or receives data from, as part of the services provided under the contract.)</th><th>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.)</th><th>Does Data Include PII?</th></tr>
<tr><td>Digital Data captured from Failed Institution (FI) by CACI FBDS Team</td><td>Digital Data Captured by CACI's FBDS Team – The CACI data capture team travels to failed bank sites[2] and works with the appropriate FDIC/Receivership or Assuming Institution (AI) officials on-site to receive read-only access to the IT systems and servers containing the ESI that is within scope of the data capture. The team typically collects the following:
<table>
<tr><th>Data Source</th><th>Information Pertaining To</th><th>Potential PII Data</th></tr>
<tr><td>Loan and Collateral Files</td><td>FI customers, borrowers, and guarantors</td><td>Names, home addresses, loan numbers, balances, rates, payment and transaction histories, participation, collateral and property information, Social Security Numbers (SSNs), credit ratings, financials and tax filings, credit card data, etc.</td></tr>
<tr><td>Deposit Files</td><td>FI depositors</td><td>Names, addresses, account numbers, statements, balance details, SSNs/Tax Identification Numbers (TINs), deposit transaction histories, images of deposited checks, etc.</td></tr>
<tr><td>FI Financials</td><td>FI customers and vendors whose data is included in General Ledger, Accounts Payable, Wire & ACH Transaction History, vendor invoices, the FI's own investments/account analyses, year-end tax processing information, such as W-8s and 1099s, etc.</td><td>In instances where FI customers and vendors are individuals as opposed to businesses: names, SSNs/TINs, addresses, phone numbers (non-work), account numbers, payment information and year-end</td></tr>
</table></td><td>☒ Yes
☐ No</td></tr>
</table>

[1] 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.

[2] Data are typically captured from FI systems that have not yet been decommissioned by the AI. However, data may also be captured from externally hosted platforms, from AI platforms after the data have been migrated or converted by the AI, or from archival systems or media.

			information such as income, payments, tax withheld, etc.	
	Email and File Shares	Bank employees/executives and former employees/ executives. User and Group folders, excluding music, videos and personal pictures.	Any manner of PII could be found in these collections depending upon how they were utilized by bank employees, etc.	
	Suspicious Activity Reports (SAR), Reports of Examination (ROEs) and other Exempt Records	Subjects of SARs, ROEs, Currency Transaction Reports (CTRs) and other exempt records are acquired in the course of collecting the failed financial institution's records. Often, they are co-mingled in the file shares or hard copy records and may contain sensitive data and PII about individuals.	Full names, SSNs or employee identification numbers (EINS), DOBs, home addresses, home phone numbers, driver's license numbers or passport numbers and details of suspicious transactions or financial activities.	
	Payroll/HR	FI employees	Names, employee identification numbers (EINs), SSNs, home addresses, personal telephone numbers, email addresses and salary. Medical benefits information is typically not captured by the CACI FBDS team	
	Other Digital Data	FI bank officers, directors, attorneys, accountants and other "Persons of Interest" (POIs) who are subjects of FDIC/DRR professional liability claims	All manners of PII as described above.	
	The CACI Capture team, whether using Forensic or forensic-like capture methods, loads the captured data onto encrypted hard drives. Drives are securely shipped (in accord with FDIC/DRR shipping procedures) or hand-carried to the CACI Operations Facility where the data is processed and loaded into the FBDS solution. After loading to the FBDS solution, the evidentiary hard drives are stored in CACI's Forensic Lab Evidence vault and/or securely shipped off-site (e.g., another approved, secure CACI location) and maintained in accord with FDIC records retention and contractual requirements.			
Records Captured from FI by DRR Investigations or Other FDIC/Receivership Staff	As applicable, DRR Investigations or other authorized FDIC/Receivership staff collects loan files, Board Minutes, legal correspondence, and other necessary bank records in hard copy or electronic forms from the failed institution. These records have the potential to include sensitive PII about bank officers, directors, and other POIs, as well as bank customers/borrowers as specified above. In instances where there was a lawsuit against the failed institution, the records may contain legal correspondence and complaint details. DRR Investigations or FDIC/Receivership staff ships the records, with a chain-of-custody form and using DRR's secure shipping procedures, to a scanning facility operated by an authorized CACI subcontractor. Per FBDS shipping procedures, all non-hardcopy portable media shall be encrypted prior			☒ Yes ☐ No

	to shipment using FDIC-approved encryption methods. At the scanning facility, staff scans/images the FI records and securely transmits[3] the images and index data to the CACI Operations Facility for loading into FBDS. The scanning vendor returns hardcopy material to a FDIC-designated location, typically either an FDIC office or FDIC's secure Records Storage Vendor (currently Iron Mountain), via secure mail for retention and disposal in accord with FDIC data retention requirements.	

7. 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: Personal identifiers, such as the name or Social Security Number of POIs and bank customers/borrowers, may be used by FDIC DRR Investigations, DRR Customer Service, Legal Division, and other authorized FBDS users to search in the FBDS database. In FBDS, data can be searched by any field, including full text, within an institution. Data can be retrieved by personal identifiers or by financial institution name or number if those fields exist in a database. Personal information appears on screen associated with assets from the failed institutions.

☐ Not applicable

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 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:

[3] The data can be securely uploaded directly to FBDS, or loaded to encrypted removable media and securely shipped to the CACI facility for loading to FBDS.

- 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

8. 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
8a. FDIC Outsourced Service Provider (OSP) Staff; OSP Subcontractors; and/or OSP Systems	☒	☐	Authorized CACI FBDS staff and CACI third-party vendors (subcontractors) have access to all ESI contained in the FBDS solution, which includes the PII specified in Section 2.5, to perform data loading and processing, scanning/imaging, application/system administration, and data verification, as well as system maintenance. Access to FBDS data is limited to CACI FBDS staff and CACI approved subcontractors on a "need-to-know" basis, in accord with their contractual requirements and signed Confidentiality Agreements with FDIC. Per the contractual agreement with FDIC, CACI takes full responsibility for the conduct of its subcontractors to ensure the confidentiality, integrity and availability of the sensitive information collected and maintained in the FBDS solution.
8b. FDIC Personnel and/or FDIC Systems/ Applications	☒	☐	Unless otherwise justified, FDIC employees and contractors will be granted access to FBDS data as follows: • **Authorized FDIC /DRR Investigations and Legal Division** staff are granted access to all data (forensic and non-forensic) in the FBDS solution, in support of their investigation into the cause of the institution's failure and pursuit of possible civil and criminal legal actions against Persons-of-Interest. • **Authorized FDIC/DRR Customer Service** representatives are granted access to all non-forensic data (e.g., loan and collateral records with borrower/customer/guarantor names, loan numbers, addresses, SSNs, etc.) to respond to incoming calls from failed institution borrowers/customers or data requests from FDIC stakeholders. • **Other FDIC/DRR sections, such as DRR Accounting/Tax and Post Closing Asset Management (PCAM)** staff are granted access to non-forensic data for certain banks, as requested and justified, to support their Receivership job duties. • **Other FDIC Division/Office staff, such as Division of Risk Management and Supervision (RMS) and Division of Insurance and Research (DIR)** staff, are granted access to limited non-forensic data (e.g., Material Loss Reviews, Suspicious Activity Reports, etc.) for certain banks, as

			requested and justified, to support their examination and insurance research activities, respectively. • **Authorized FDIC/DRR Investigations and Legal Division contractors (e.g., Outside Counsel)** who support FDIC employees in investigating bank failures and pursuing civil and criminal claims on behalf of the Receiver may receive access to forensic and non-forensic data maintained in the FBDS solution, which contains some or all of the PII identified in Section 2.5, on an "as-needed" basis for the purposes specified above. FDIC contractors are granted access only to the banks for which they are supporting. Access control procedures specified below also apply to contractor users. To obtain access, users must have the approval of their Manager/Supervisor and the FBDS Program Manager/Data Owner. Users also must sign the FBDS User Confidentiality Agreement and Security Principles of Behavior, certifying that they will abide by the FBDS Rules of Behavior and FDIC privacy/security requirements for protecting data. Further, all FDIC network users must annually complete the FDIC's Information Security and Privacy Awareness training, which includes the Corporation's General Rules of Behavior. Additionally, the FBDS solution's security settings limit a user's access to specific financial institutions and databases. All access granted is determined on a "need-to-know" basis, as defined by the Privacy Act of 1974. Guidelines established in the Corporation's Access Control policies and procedures are also followed. Controls are documented in the system documentation. CACI FBDS IT support staff manages information system accounts, including establishment, activation, modification, review, disablement, and removal. Access for users who have not accessed FBDS in the number of days specified by FBDS policy is suspended. The first quarterly review of users will be conducted in the second quarter of 2015. The review, in conjunction with FDIC program management staff, will identify users who no longer need access to FBDS.
8c. Individual Members of the Public (e.g., bidders, investors, borrowers, customers, etc.)	☐	☒	Not applicable.
8d. Other Non-FDIC Entities / Parties and/or Non-FDIC Systems/ Applications	☒	☐	Forensic subpoenas and discovery orders may result in the requirement for non-FDIC entities or parties, such as Opposing Counsel, to have access to FBDS to search and review forensic and non-forensic data for litigation purposes. This data may include any and all of the PII specified in Section 2.5. Prior to granting access, FDIC Legal must review and authorize all such requests, after which

			authorized Opposing Counsel are provided direct, read-only access to segmented, sub-folder information within FBDS Relativity, a web-based, e-discovery review platform that is a component of the FBDS solution. Opposing Counsel is granted access to a subset of data on the Relativity platform, based upon need to know and approval by FDIC Program Management.
8e. Federal, State, and/or Local Agencies	☒	☐	Congressional inquiries, subpoenas, discovery orders, and other legal/investigatory matters may result in the need to provide subsets of FBDS data to federal government agencies, such as the Security Exchange Commission (SEC), Office of Inspector General (OIG), the Federal Bureau of Investigations (FBI), Department of Justice (DOJ), Department of Treasury, and other requesting government agencies. All access requests received from government agencies must be approved by an authorized FDIC manager/supervisor, as well as by FDIC Legal if the requests involve subpoenas or exempt information (e.g., Reports of Examination, Currency Transaction Reports, Suspicious Activity Reports). Once access is approved by FDIC, government officials do not receive direct access to the FBDS solution via Relativity. Rather, CACI FBDS staff loads the requested data, which may include any and all of the PII specified in Section 2.5, to FIPS 140-2 validated encrypted hard drives and securely sends them to the requesting agency official(s).
8f. Other	☐	☒	*Not Applicable*

9. 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: The CACI FBDS solution is a web-based platform hosted and maintained by the outsourced service provider. The associated ISA/MOU for the transition from the prior provider is temporary and only applicable during the transition of data and services from the prior outsourced service provider to the new provider.

SECTION IV – NOTICE AND CONSENT

10. 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.):*** All information on individuals has been obtained from failed financial institutions and is needed for the resolution and termination of the institutions. Therefore, opting out is not an option.

☐ 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.

11. 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

12. 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).]*

☒ CACI-ISS will go 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 ☒ PENDING

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

☒ CACI-ISS 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 may be conducted 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.***

The CACI FBDS solution is protected by multi-factor authentication and encryption. In addition, the data is encrypted in transport via FIPS 140-2 validated encryption solutions. Removable media is encrypted with FIPS 140-2 validated encryption solutions as well. CACI's data centers are protected with approved physical safeguards as prescribed in the System Security Plan.

13. 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 failed financial institutions. As such, the FDIC and its vendors rely on the financial institutions to provide accurate data.

☐ The vendor/contractor works with FDIC to verify the integrity of the data [in conjunction with] inputting it into the system or using it to support the project.

☐ As necessary, an [authorized user or administrator] of the [FBDS] 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*.)

Data is collected from the failed institutions "as is," in accord with the FBDS contract and statement of work. The following methods are used to ensure the integrity and completeness of captured data:

1. Data capture certification is performed at the institution site and is completed before the data capture equipment leaves the site. Additionally, source data extracts are verified against copied data and data back-up logs at the institution site, and against restored data in the CACI Data Center.

2. Data hosting certification is performed at the CACI Data Center and is completed once all the data has been loaded into FBDS, verified by CACI's independent test team, and undergone user acceptance testing by FDIC.

14. 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 CACI-ISS 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 Susan Sparrow, CACI Program Manager, to have overall accountability for ensuring the proper handling of data by vendor personnel who have access to the data. All vendor personnel with access to the data are responsible for protecting privacy and abiding by the terms of their FDIC Confidentiality and Non-Disclosure Agreements, as well as the vendor's corporate policies for data protection. Access to certain data may be limited, depending on the nature and type of data. (Refer to Section III of this Privacy Impact Assessment for more information on data access criteria.)

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

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

SECTION VI – DATA RETENTION AND DISPOSAL

15. 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.

The data will be loaded to and maintained in the secure CACI FBDS solution, which is protected by multi-factor authentication and FIPS 140-2 validated encryption. The system is hosted at a primary site and the disaster recovery site is a hot backup of the primary site. All data is replicated continuously throughout the day. The evidentiary hard drives (original and forensic copies) are stored in CACI's Forensic Lab Evidence vault in CACI's secure data center(s). The removable media (e.g., hard drive, CD) are encrypted via FIPS 140-2 validated encryption solutions as well. CACI's data centers are protected with approved physical safeguards as prescribed in the System Security Plan.

16. 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.

Data is retired and destroyed in accordance with National Archives and Records Administration (NARA) guidance and FDIC Records Retention and Disposition Schedules. The FBDS solution must retain record for at least six (6) years or longer should there be a litigation hold. CACI will destroy data with FDIC's approval utilizing approved methods at the time of the destruction. Data will typically be sanitized and/or wiped using approved methods for online storage and hard copies will be disposed using approved methods as well.