FEDERAL DEPOSIT INSURANCE CORPORATION
INSURING AMERICA'S FUTURE

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

for

General Services Administration (GSA)

USAccess Program

Date Approved by Chief Privacy Officer (CPO)/Designee: 12/18/2017

SECTION I – OUTSOURCED INFORMATION SERVICE DESCRIPTION

1. Describe the outsourced service and its purpose.

The U.S. General Services Administration (GSA) established the USAccess program to provide federal agencies with a managed, shared service that simplifies the process of procuring and maintaining Personal Identity Verification (PIV) compliant credentials, while at the same time meeting the compliance requirements of Homeland Security Presidential Directive (HSPD-12).[1] The Federal Deposit Insurance Corporation (FDIC) is partnering with GSA'S USAccess to facilitate the issuance of PIV cards to FDIC personnel throughout the United States. This partnership will better support the FDIC's national geographic footprint and allow the FDIC to utilize GSA shared badging sites (300+) nationwide for PIV card enrollment, issuance, and activation. The 300+ GSA shared badging sites will allow FDIC Field Office staff to readily access a nearby location to obtain a PIV card without impacting their normal operations. As of December 29, 2016, a PIV card is required to enter a FDIC facility and access FDIC's network and applications. A GSA-issued PIV card will be issued for new employees and contractors, as well as when a legacy FDIC PIV card either expires or is no longer working, as FDIC will be decommissioning its current PIV card issuing system and equipment (i.e., MyID[2]) sometime in 2017.

GSA will provide turn-key services to produce compliant PIV credentials. These services include enrollment services, systems infrastructure, Public Key Infrastructure (PKI)[3] certificates and maintenance of identity accounts, card production, and finalization. Identity proofing and adjudication of individuals sponsored by FDIC are the FDIC's responsibility. Only PIV data required by the PIV data model and operations will be retained by GSA.

The FDIC will provide necessary information to GSA to facilitate the issuance of PIV cards by (1) manually entering information via the Assured Identity Sponsorship Portal[4]; (2) bulk import user records; and/or (3) via a web service interface using message encryption over a mutually authenticated HTTPS channel.

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.

[1] HSPD-12 requires a common identification standard for all Federal employees and contractors for both physical and logical access. It is designed to enhance security, reduce identity fraud, and protect the personal privacy of those issued government identification..
[2] MyID is a commercially available identity and card management system to assist the United States Federal Government agencies in meeting the requirements in HSPD-12. It is the FDIC's legacy system for managing PIV cards.
[3] PKI provides authentication, confidentiality, nonrepudiation, and integrity of messages exchanged between parties. PIV card credentials will include four digital certificates to facilitate credential authentication, credential identitification, e-mail signing, and e-mail encryption.
4 The Assured Identity Sponsorship Portal is a User Interface to the GSA USAccess system that enables an agency Sponsor to manually enter application information into the USAccess system.

GSA collects or receives the following PII about current or prospective FDIC employees and contractors (PIV card applicants and cardholders): full name, picture/facial image, Social Security Number (SSN), date of birth, U.S. citizenship status, country of birth (if not a U.S. citizen), employee or contractor identification number, phone number(s), email address (work-related with limited exceptions explained in Question 4), and fingerprints. In addition, PIV card applicants must provide two forms of identification which are scanned into the GSA USAccess system at the time of enrollment. The identification documents must be in original form and contain at least one acceptable primary source document (e.g., U.S. military ID card, passport, driver's license, etc.) and secondary source document (e.g., U.S. Social Security Card issued by the Social Security Administration, original or certified copy of a birth certificate, etc.) or two primary source documents.[5]

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

GSA uses the PII data identified in Question 2 to verify the identity of the applicant during enrollment and activation of PIV cards; to ensure the applicant has not been previously enrolled in the PIV system; to create the applicant's enrollment record (and to manage and maintain this record throughout the PIV card lifecycle); and to verify, authenticate, and revoke PIV cardholder access to Federal resources.

The GSA USAccess system requires an individual to have a unique email address. For FDIC employees and most contractors, this will be an FDIC work email address. However, there are some contractors that require physical access to FDIC buildings but do not require logical access to IT systems (e.g. cafeteria staff, maintenance contractors, cleaning staff, etc.). This subset of contractors will need to provide a personal or company-provided email address.

The FDIC will also upload to GSA USAccess the Employee Identification Number (EIN) or Contractor Identification Number. This unique data element allows for corporate reporting across both MyID and USAccess to ensure proper PIV Card management (e.g., all eligible employees and contractors have a valid PIV card; PIV cards are proactively terminated for department employees/contractors; etc.).

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 (Country of Birth, if not U.S. citizen)	☒	☐
Social Security Number	☒	☐
Employment Status, History or Information	☐	☒

[5] For additional information about the identity proofing requirements and acceptable forms of identification that may be collected from applicants and scanned into the GSA USAccess system, refer to the USAccess Acceptable Forms of Identification Guide available at https://www.fedidcard.gov/viewdoc.aspx?id=109.

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) (Note: USAccess requires a unique email address. This will be a work email address for all employees and most contractors. There are some contractors that require physical access to FDIC buildings but do not require logical access to IT systems. This subset of contractors will need to provide a personal or company provided email address.)	☒	☐
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: U.S. citizenship status, facial image, identification source documents-refer to Q2 for details)	☒	☐

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: GSA USAccess uses SSN as the primary identifier for individuals requesting and receiving a PIV card through its managed service. GSA currently provides this managed services to multiple Federal agencies and SSN is the only unique person identifier across the federal government.

b) Provide the legal authority which permits the collection of SSNs. 5 U.S.C. 301; Executive Order 9397, as amended; and Homeland Security Presidential Directive-12 (HSPD-12), Policy for a Common Identification Standard for Federal Employees and Contractors.

c) Identify whether the SSN is masked or otherwise truncated as part of the outsourced service: SSN is not made accessible through the USAccess user interface or system reports.

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[6]: 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[7] (List all sources that the Outsourced Provider collects, obtains or receives data from, as part of the services provided under the contract.)	**Type of Data Provided by Source & How It is Derived** (Describe the type of PII and non-PII data provided by each source. If PII is included in the data, list the specific PII elements, and explain how the PII is derived.)	**Does Data Include PII?**
FDIC Employees and Contractors (PIV Card Applicants and Cardholders)	The PIV card enrollment and activation process requires FDIC employees and contractors (applicants) to schedule and travel to two appointments at a GSA USAccess shared badging site or dedicated FDIC badging office—the first for enrollment, and the second to activate their PIV cards. Applicants use the GSA Online Scheduling System, a publicly available website located at https://app003.timetrade.com/tc/login.do?url=usaccess, to schedule and manage appointments at FDIC badging offices or other designated USAccess Centers. To schedule an appointment, applicants must select an appointment location and enter their full name, email address, telephone number and sponsoring organization. At the enrollment appointment, FDIC applicants must present two original forms of identification source documents (such as a passport, driver's license, social security card, birth certificate, etc.) that will be scanned into their entrollment record by authorized FDIC Division of Administration (DOA) Security and Emergency Preparedness (SEPS) personnel.[8] In addition, SEPS personnel use a biometric reader and digital camera [Light Credentialing Stations (LCS)[9]] and web interface to take the fingerprints and photographs (facial images) of FDIC applicants. Applicant fingerprints are verified at the time of PIV card activation using the same biometric device. PIV cardholders can also reset their PIV PINs via the Light Credentialing Stations. At the activation appointment, the card holder's identity is verified and the certificates are added to the card. The individual and the Activator use an enrollment reader to activate the card in the system and add the certificates. The card status is set to active and the cardholders creates a PIN for the card. The PIN is stored solely on the card. No additional data is entered.	☒ Yes ☐ No

[6] 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.

[7] 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] Depending on their location, certain FDIC contractors (e.g., Field Office contractors) may enroll and activate their PIV card at other Federal Agencies' Shared Service badging centers, in which case those Federal Agencies will obtain/access the aforementioned data, in accordance with their respective USAccess Interagency Agreements, for the purpose of enrolling applicants and activating their PIV cards.)

[9] The Light Credentialing Stations (LCS) contain all the software and hardware peripherals (i.e., laptop computer, digital camera, fingerprint reader, scanner, etc.) needed to enroll applicants and activate credentials; they enable USAccess Credentials to be activated, and post issuance activities to be performed from an Internet Web portal.

FDIC Corporate Human Resources Information System (CHRIS HR) via Person Master Data (PMD)	For the initial data upload[10] to the GSA USAccess Identity Management System (IDMS[11]), FDIC/DIT Enterprise Information Management (EIM)[12] will extract all required data elements in the GSA USAccess specified format from Person Master Data (PMD). PMD will send the files via encrypted email to FDIC's Chief Physical Security Officer who, in turn, will upload these files to the USAccess Identity Management System using the Security Officer Portal[13]. This process, as described above, is a manual process requiring human intervention. By Q3 2017, the FDIC plans to implement an automated system interface between PMD and USAccess that queries PMD and sends the required data elements via HTTPS to the USAccess AgencyService secured web service. The web service (GSA SIP) specification is provided by GSA. The web service conforms to the OASIS WS-Security standard[14] and requires the use of message encryption over a mutually authenticated HTTPS channel.	☒ 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)?

FDIC will initially upload bulk user data through a secure portal to GSA using a VPN connection. Long-term, this data will be maintained by an automated interface through an encrypted mutually authenticated HTTPS channel.

FDIC Administrators that have been trained on the USAccess system can search, edit and delete employee and contractor records in the system according to the role they have been assigned. The USAccess system relies on Social Security Number or Last Name and Date of Birth as unique identifiers for searching records in the system.

In compliance with FIPS PUB 201-2, GSA requires the use of personal identifiers to verify FDIC personnel for enrollment in the PIV program, and again for activation of each PIV card (e.g. driver's license, passport, etc.); this information is stored in USAccess.

The applicable System of Records Notices (SORNs) for this outsourced service are noted in Question 9.

[10] FDIC data can be entered into the GSA Identity Management System (IDMS) in one of three ways: (1) manually keyed in by an FDIC Administrator directly to the IDMS via web interface over HTTPS, (2) bulk upload through the Security Officer Interface/Portal, or (3) via a web service interface using message encryption over a mutually authenticated HTTPS channel. The initial upload of FDIC data, which includes the PII specified in Section 2, will occur using the Security Officer Portal using the process described in Question7.

[11] USAccess Identity Management System (IDMS) is the system used by GSA to manage and maintain PIV Card applicant data throughout the PIV Card lifecycle, including issuance and activation of cards, as well as verification, authentication, and revocation of a PIV Cardholder's access to Federal resources.

[12] FDIC/DIT Enterprise Information Management (EIM) maintains Person Master Data (PMD) as a source of FDIC employee and contractor reporting data generated via FDIC's Corporate Human Resources Information System (CHRIS HR).

[13] The Security Officer Portal is a User Interface to the GSA USAccess managed service that provides the Security Officer role the ability to bulk upload application information into the USAccess system.

[14] A Web Service Security Standard issued by the Organization for the Advancement of Structured Information Standards (OASIS) in 2004, recognized by the Open Web Application Security Project (OWASP).

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

The applicable SORNs for this outsourced service are: FDIC 30–64–0035, Identity, Credential and Access Management Records (*80 FR 67023*) and GSA-GOVT-7, Federal Personal Identity Verification Identity Management System (PIV IDMS) (*73 FR 22378*).

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 the Outsourced Service Provider will share or provide PII data to as part of the outsourced service.

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	☒	☐	OSP System: FDIC data, including the PII specified in Question 5, will be uploaded and maintained in the GSA USAccess Identity Management System (IDMS). The initial upload of FDIC data will occur using the Security Officer Portal using the process described in Question 7. In addition, the automated system interface between PMD and USAccess queries PMD and sends the required data elements via HTTPS to the USAccess AgencyService secured web service[15]. The web service conforms to the OASIS WS-Security standard and requires the use of message encryption over a mutually authenticated HTTPS channel. OSP Staff, Contractors and Subcontractors: Authorized GSA staff, contractors, and subcontractors will have access to GSA IDMS and the PII contained within for database administration and PIV credential troubleshooting. In addition, as noted in Section II, in cases where certain FDIC personnel (e.g., FDIC Field Office contractors) enroll and activate their PIV cards at non-FDIC, GSA shared service badging centers, authorized security/badging personnel at these locations may have access to applicant PII for purposes of enrolling applicants and activating their PIV cards.
10b. FDIC Personnel and/or FDIC Systems/ Applications	☒	☐	Authorized FDIC Division of Administration (DOA) Security and Emergency Preparedness (SEPS) staff, contractors, and subcontractors in the roles below (See Table 9b.1) will have access to the PII specified in Question 5 for purposes of data entry and maintenance, verification of identity, distribution of PIV credentials, and reporting. FDIC SEPS personnel will use the Light Credentialing Stations (LCS)[16] and web interface to enroll/sponsor, print and activate PIV cards. Light Credentialing Stations can also be used to reset PIV PINs. Note that USAccess contains a number of standard reports. FDIC will rely on these reports to track and manage the process of credentialing applicants. The FDIC will not receive any

[15] Agencies can use any of three methods for creating, updating, and querying sponsorship and adjudication data in the USAccess IDMS: (1) manually entering information via the Assured Identity Sponsorship Portal ; (2) bulk import user records; and/or (3) via a web service interface (the USaccess AgencyService secured web service) using message encryption over a mutually authenticated HTTPS channel.

[16] The Light Credentialing Stations (LCS) contain all the software and hardware peripherals (i.e., lap top computer, digital camera, fingerprint reader, scanner, etc.) needed to enroll applicants and activate credentials; they enable USAccess Credentials to be activated, and post issuance activities to be performed from an Internet Web portal.

<table>
<tr><td></td><td></td><td></td><td>invoices containing PII data.

FDIC's Physical Access Control system (CCure) will require the Federal Agency Smart Credential Number (FASC-N) number from the PIV card to be entered in order to provide physical access to FDIC facilities. Currently, this is a manual data entry but may be automated in the future via a software solution.

Table 10b.1<table><tr><th>Role Name</th><th>How many users of this role?</th><th>Brief Description of Role</th></tr><tr><td>Sponsor</td><td>10</td><td>Sponsors FDIC employee/contractor to receive badge</td></tr><tr><td>Adjudicator</td><td>5</td><td>Verifies background investigation for FDIC employee/contractor that needs to be badged</td></tr><tr><td>Security Officer</td><td>5</td><td>Batch imports sponsorship records, reviews identity documents flagged by Registar, and collects & destroys credential at termination of employment</td></tr><tr><td>Registrar</td><td>30</td><td>Registers FDIC employee/contractor in USAccess system to be badged</td></tr><tr><td>Role Administrator</td><td>5</td><td>Can assign roles in USAccess to properly trained users</td></tr></table></td></tr>
<tr><td>10c. Individual Members of the Public (e.g., bidders, investors, borrowers, customers, etc.)</td><td>☐</td><td>☒</td><td></td></tr>
<tr><td>10d. Other Non-FDIC Entities/ Parties and/or Non-FDIC Systems/Applications</td><td>☒</td><td>☐</td><td>GSA sends the individual's name, facial image and Agency Name to Oberthur Systems[17] for the physical production of the PIV Card. The long term plan is to print all PIV cards locally at FDIC facilities (HQ and Field Offices).</td></tr>
<tr><td>10e. Federal, State, and/or Local Agencies</td><td>☒</td><td>☐</td><td>GSA is the outsourced service provider. See Question 9a above.

FDIC contractors may enroll and activate their PIV card at other Federal Agencies' Shared Service badging centers, in which case those Federal Agencies will be able to access FDIC data for the purpose of enrolling applicants and activating their PIV card. The data can only be accessed while the FDIC employee is in their presence. Any federal agency that uses the USAccess system has an Interagency Agreement Amendment (IAA) on file. GSA and any contractors using USAccess must protect sensitive data.</td></tr>
<tr><td>10f. Other</td><td>☐</td><td>☒</td><td></td></tr>
</table>

[17] Oberthur Systems provides card-based solutions, software and applications, including smart cards. Oberthur is the company GSA uses to produce the PIV Cards.

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*: Interagency sharing agreement)	☒	☐
If you answered NO to any item above, please provide additional information if available: The outsourced service provider is a government agency.		

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.

Federal identification badge (PIV smartcard) is mandated by Presidential Directive HSPD-12 and OMB Memorandum M-16-04, *Cybersecurity Strategy and Implementation Plan (CSIP) for the Federal Civilian Government*. FDIC's Legal Division determined that M-16-04 applies to the FDIC. In the near term, a PIV card will be mandatory to enter a FDIC facility and access FDIC's network and applications. A GSA-issued PIV card will be required as FDIC will be decommissioning its current PIV card issuing system and equipment (i.e., MyID).

☐ 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 (www.fedidcard.gov)
- ☐ 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.

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

☒ GSA 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.)

All GSA and FDIC Role Holders (users) with access to the data sent to, and received from, the USAccess infrastructure must be U.S. Citizens with a valid and current suitability Background Investigation.

The security of the information being transmitted on all interconnections shall be protected through the use of FIPS 140-2 validated encryption mechanisms. Individual users will not have access to the data except through system security software inherent to the USAccess infrastructure. All access to USAccess and USAccess system data is controlled by strong authentication methods

Refer to Question 15 for an explanation of additional technical safeguards in place to protect PII data in GSA's care.

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 and in conjunction with inputting it into the system or using it to support the project. The USAccess bulk upload process has a validation check for data integrity prior to upload and also generates upload success/error reports on completion of the upload process.

☒ As necessary, FDIC DOA administrators of CHRIS HR 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 collected from individuals is verified for accuracy and reviewed by key personnel (Approved USAccess Role Holders) at several stages: during the sponsorship process, during the enrollment process, and during the adjudication process.

The following technical controls also ensure the completeness of the data:

- Consistency and reasonableness checks;
- Validation during data entry and processing; and
- Use of required fields to prevent critical data from being omitted.

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 DOA 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 Harry Freer, Information System Security Organization, GSA, 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 requirements outlined in the Memorandum of Agreement (MOA) which requires GSA to notify FDIC of any security breaches, incidents, or operational issues that may affect performance or security, as well as manage security incident assessments and responses.

☐ 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.

GSA hosts its Security Operations Center, primary production environment, all non-production environments (Development, Test, Staging, Training), and configuration management applications in its Orlando, FL facility.

The failover site for disaster recovery is in Alpharetta, GA.

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.

USAccess does full backups of its Identity Management System (IDMS), Card Management System (CMS), and Biometric system (BIODB) production databases weekly and incremental backups daily. All customer data is included in the backup and retained indefinitely on the SAN. Additional SANs are added as required.

Tapes are kept onsite at the Orlando Data Center for three (3) weeks and offsite for 3 years.

This backup policy is only modified at the conclusion of the contract. At the end of the contract, the retention time for a "final" backup of data is seven (7) years (as per the contract).