FEDERAL DEPOSIT INSURANCE CORPORATION
INSURING AMERICA'S FUTURE

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

for

FDIC On-line Store

E Group

Date Approved by Chief Privacy Officer (CPO)/Designee: 8/11/2016

PTA/PIA TEMPLATE VERSION 1.6 – March 2016

SECTION I – OUTSOURCED INFORMATION SERVICE DESCRIPTION

1. Describe the outsourced service and its purpose.

This service supports the FDIC's Rewards and Recognition (R&R) Program administered by the Division of Administration (DOA) Human Resources Branch (HRB) to provide formal recognition of employee achievements and time in service. The R&R Program guidelines are described in full within FDIC Circular 2420.1, FDIC Rewards and Recognition Program.

The contractor, E Group, provides support and assistance in the administration of the FDIC R&R Program, including the development of an on-line website for FDIC's Non-Monetary Awards Program (referred to as FDIC On-line Store). The service provides authorized Division and Office personnel the ability to procure items on behalf of their respective Division or Office using the FDIC Procurement Card for the purpose of delivering Recognition of Service awards as well as other FDIC approved items, such as:

- Retirement Medallions
- Award (plaques) and Lapel pins
- Federal Service Anniversary Mementos
- Non-Monetary Awards
- FDIC logo & Special Order Items

Pre-authorized users will log into the On Line Store from the FDIC Intranet site to access the application by use of their User ID and Password. Initially, the vendor (E Group) will generate unique passwords that will be assigned to each authorized user, which is provided in an encrypted email to the respective user. When users sign in for the first time, they will need to change their passwords to a password of their choice.

Orders are submitted from the OM to E Group via secured email. The information for the FDIC Online store will be held on a database located at E-Group's subcontractor, CoreXpand. Orders and order information for the awards program will be securely stored within the vendor's encrypted electronic job jacket.

Orders may include former employees or retirees. In these instances, the vendor sends the retirement medallion and the service anniversary items to the home address (provided through Secure email). If the award recipient does not attend the ceremony or pick up their award plaque or board resolution after the ceremony, the plaque is either sent to their office or home mailing address.

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 majority of purchases will be for FDIC's recognition of employees. Goods and/or services are procured by the contract Oversight Manager by issuing a Call Order via email, following the specifications for each type of order, to include the following information:

- Contract Number
- Call Order Number
- Contractor's Name
- Description of the Goods/Services Ordered
- Call Order Estimated Amount
- Place of Delivery
- Delivery Schedule
- Completion Date

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

The information listed under 3, above is necessary for the contractor, E-Group, to ensure the timely processing, tracking and fulfillment of orders procured by FDIC employees.

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.)*: Please see the chart below.

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: _	☐	☒

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]: Not applicable.

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

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?**
FDIC Online Store	Order date, dollars spent, product name, quantity, price, Employee name, business email, ship to address (business), phone, FDIC procurement credit card number (only last 4 of credit card number are stored)	☒ Yes ☐ No
Email to Vendor (Call Order)	Recipient Name, home address, email address, years of service, employment status, and type of award	☒ 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/Reports can be retrieved by the E-Group custom representative that has been assigned to FDIC when FDIC requests reports on account activity. Reports can be run to retrieve data by User Name, Date Range, Item purchased etc. Only the E-Group customer representative is able to run the queries for FDIC.
☐ Not applicable

[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.

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	☒	☐	*A limited number of authorized individuals at E Group will have access to names of employees, years of service, and home addresses in order to provide them with service awards. This information will be provided to E Group from the OM via secured email that will be protected by the E Group via an encrypted electronic jacket.*
9b. FDIC Personnel and/or FDIC Systems/ Applications	☒	☐	*Names, item (s) ordered, shipping address can be provided to Online Store OM for tracking purposes only. The information will be provided via a secure email.* *A limited number of DOA HR staff have access to data in order to track orders, manage fulfillment, and manage inventories.*
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	☐	☒	*Not applicable. There are no other entities or system/applications that have access.*
9e. Federal, State, and/or Local Agencies	☐	☒	*Not applicable. Federal, state and local agencies do not have access.*
9f. Other	☐	☒	*Not applicable.*

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: The other documents are not needed/do not apply for this requirement.		

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.):*** This information will be needed to place and order from the FDIC Online store. Information is obtained from FDIC sources. Individuals are not provided the opportunity to "opt out".
☐ 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. *[Provide the name of the Outsourced Service Provider and check all applicable box(es).] E Group and subcontractor CoreXpand*

☒ If it has gone through the Methodology, has it been approved? E Group and subcontractor CoreXpand have 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? ☒ PENDING ☐ NO ☐ YES
☒ The FDIC conducts background investigations (BIs) on personnel and other applicable personnel prior to their beginning work on the contract.
☐ The [Outsourced Information Service Provider name] is subject to periodic compliance reviews by FDIC.
☐ 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.***

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 FDIC employees. As such, the FDIC and its vendors rely on the individuals who are placing the orders 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, an [authorized user or administrator] of the [System/Project Name] checks the data for completeness by reviewing the information, verifying whether or not certain documents or data is missing, and as feasible, updating this data when required.
☐ Other (*Please explain.*)

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 OnlineStore 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 a POC 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.

The information for the FDIC Online store will be held on a database located at E-Group's subcontractor, CoreXpand. The information for the awards program will be securely stored with the electronic job jacket.

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 information will be retained throughout the existence of the contract. Control of the information / data will comply with the contract in that it belongs to the FDIC. The vendor will provide the data to FDIC in the format best suitable to the FDIC.