Office of Information Technology (OIT)

Privacy Impact Assessment

Insight

August 5, 2022

1100 New York Ave NW
Washington, DC 20527

Section 1. Characterization of the Information

The following questions are intended to define the scope of the information requested and collected as well as the reasons for its collection as part of the program, IT system, or technology being developed.

1.1 What information is collected, used, disseminated, or maintained in the system?

- The system creates an Impact Quotient score used to help determine the approval of a project request.
- The system collects the information below from customers:
    - Name
    - Personal Address (if provided by customer)
    - Citizenship
    - Date of Birth
    - Place of Birth (if provided by customer)
    - Social Security Number (if provided by customer)
    - Driver's License Number (if provided by customer)
    - Passport Number (if provided by customer)

1.2 What are the sources of the information in the system?

- DFC Customers enter this information into application Personal Information Form (PIF). In rare cases, DFC Employees or Contractors working as origination or monitoring officers may collect this information from the customer and enter it into a PIF if a client is unable to complete the form.
- All personal information noted comes from the customer.
- The system is the source for the Impacts Quotient.

1.3 Why is the information being collected, used, disseminated, or maintained?

- The information is captured to perform background and credit checks required for each transaction under DFC's Know Your Customer (KYC) /Character Risk Due Diligence policies.
- The system does not collect, use, or disseminate commercial data.

1.4 How is the information collected?

- The information is typically collected via the Personal Information Form (PIF). Sometimes other methods of communication are used by the customer (telephone call, document sent via courier).
- OMB No. 3015-0010; DFC Form 006 Personal Identification Form

1.5 How will the information be checked for accuracy?

- The system does not check information from any other source.
  In order to help ensure accuracy, the cover page of the PIF (which submitters are obliged to read and check a box saying that they have read it) states that there are potential criminal penalties for not providing truthful/accurate information on the Form 129/Form 006.
- The system does not check for accuracy by accessing a commercial aggregator of information.

1.6 What specific legal authorities, arrangements, and agreements defined the collection of information?

- The Better Utilization of Investments Leading to Development Act of 2018 (the "BUILD Act"), section 1422 (b)(4) requires that DFC protect the financial interests of the United States (which includes performing background checks on key customer personnel using their submitted PII).

Section 2. Uses of the Information

The following questions are intended to clearly delineate the use of information and the accuracy of the data being used.

2.1 Describe how the information in the system will be used in support of the program's business purpose.

- The information is used solely to perform Character Risk Due Diligence/Know Your Customer due diligence.

2.2 What types of tools are used to analyze data and what type of data may be produced?

- Not Applicable

2.3 If the system uses commercial or publicly available data, explain why and how it is used.

- Insight does not pull in commercial or publicly available data.

Section 3. Retention of Information

The following questions are intended to outline how long information will be retained after the initial collection.

3.1 What information is retained?

- Name
- Personal Address (if provided by customer)
- Citizenship
- Date of Birth
- Place of Birth (if provided by customer)
- Social Security Number (if provided by customer)
- Driver's License Number (if provided by customer)
- Passport Number (if provided by customer)

3.2 How long is information retained?

- Official document files requiring record retention are interfaced and subsequently stored in Content Manager (CM), DFC's official records management system. CM enforces record retention and destruction on these files according to the defined records retention policy.

3.3 Has the retention schedule been approved by the DFC records officer and the National Archives and Records Administration (NARA)? If so, please indicate the name of the records retention schedule.

- DFC policy dictates that project related data be stored for at least seven years after the end of the project.

Section 4. Internal Sharing and Disclosure

The following questions are intended to define the scope of information sharing within DFC.

4.1 With which internal organizations is information shared? What information is shared, and for what purpose?

- The relevant "line department" (SMEF, SFI, IFD, PMD/FMD) officers and the project attorney(s) (Legal) working on a particular transaction review the data. The line department officers share the identifying information contained in each Form 129/006 submission with the Information Center for the purpose of conducting background/credit checks. This is done as part of the Character Risk Due Diligence/Know Your Customer process.

4.2 How is the information transmitted or disclosed?

- All parties use Insight to view customer information. The line department officers and the project attorneys view information from Form 129/006 submissions in Insight. The line officers can see the names of the parties, but they cannot see the related SPII. The line officers send the CRDD Requests to the Information Center through Insight, and only Information Center personnel can see the SPII necessary to run the required background and/or credit checks.
- All information is viewed on a case-by-case basis.
- Access to PII is controlled by role assignment to only those users with a need-to-know. In addition, key PII fields are encrypted in back-end storage.

Section 5. External Sharing and Disclosure

The following questions are intended to define the content, scope, and authority for information sharing external to DFC, which includes Federal, State, and local governments, and the private sector.

5.1 With which external organizations is information shared? What information is shared, and for what purpose?

- No information is shared with any external organization for that organization's use. The Information Center staff may enter certain pieces of information into their Exiger DDIQ system to which DFC subscribes in order to perform background checks necessary for customer background checks (KYC).
- The SORN for this system lists due diligence background checks as a routine use of the information.

- The SORN citation is:
  DFC-02 Salesforce Customer Relationship Management System (Insight) 85 FR 43210
  As published in:
  Federal Register / Vol. 85, No. 137 / Thursday, July 16, 2020

5.2 Is the sharing of information outside the agency compatible with the original collection?

- Yes. The sole purpose of this information collection is to enable the performance of background checks as documented in the SORN referenced in section 5.1 above.

5.2.1 If so, is it covered by an appropriate routine use in a SORN? If not, please describe under what legal mechanism the IT system is allowed to share the information in identifiable form or personally identifiable information outside of DFC.

- The sole purpose of this information collection is to enable the performance of background checks as documented in the SORN referenced in section 5.1 above.

5.3 How is the information shared outside the agency and what security measures safeguard its transmission?

- DFC enters Personal and Organizational information in Exiger DDIQ system for due diligence background checks on a case-by-case basis.
  - DFC Information Center staff manually enter information directly into the DDIQ system via a secured HTTPS connection to DDIQ. DDIQ also requires users to log into the application using a user name / password.
- PII is safeguarded via access control to DDIQ and a secure HTTPS connection to the DDIQ system.
- All sharing occurs under the standard uses documented in the SORN referenced in section 5.1 above.

Section 6. Notice

The following questions are directed at providing notice to the individual of the scope of information collected, the right to consent to uses of the information, and the right to decline to provide information.

6.1 Was notice provided to the individual before collection of the information?

- See section 5.1 above for a citation of DFC's Insight SORN
- Notice is provided to the customer.
- The PIF contains notification of DFC policy detailing how DFC intends to use the information. This notification is provided prior to the submitter clicking the "Submit" button on the form. The party always has the option not to submit the form.

6.2 Do individuals have the opportunity and right to decline to provide information? If so, is a penalty or denial of service attached?

- Any individual or corporate entity may decline to complete a PIF providing PII. Depending upon how critical that party's role is in the transaction, that may affect DFC's ability to perform a background check (KYC) on that induvial, which may impact DFC's decision to underwrite the transaction.

6.3 Do individuals have the right to consent to particular uses of the information? If so, how does the individual exercise the right?

- This information has only one use, which is to conduct due diligence background checks (KYC) as stated in the notification presented to the user submitting the PIF. Individuals may decline to provide PII via the PIF as noted in section 6.2 above.

Section 7. Access, Redress, and Correction

The following questions are directed at an individual's ability to ensure the accuracy of the information collected about him or her.

7.1 What are the procedures that allow individuals to gain access to their information?

- Any party that submits a PIF may log into their Forms account at any time and view a PDF version of their submission. If they have difficulty accessing the account or the PDF of the submission, DFC technical or program office personnel can assist them with accessing the information.
- Insight is not exempt from the Privacy Act.
- Not Applicable.

7.2 What are the procedures for correcting inaccurate or erroneous information?

- Any customer may correct inaccurate or erroneous information by working with their assigned program / loan officer. Typically, the PIF is reopened, allowing the customer to update their information.

7.3 How are individuals notified of the procedures for correcting their information?

- On the submission page of the PIF in the Forms system, it explains that DFC personnel will review the submitted information and are able to open the form back up for editing by the submitter if necessary.

7.4 If no formal redress is provided, what alternatives are available to the individual?

- N/A – Redress is documented in section 7.3 above.

Section 8. Technical Access and Security

The following questions are intended to describe technical safeguards and security measures.

8.1 What procedures are in place to determine which users may access the system, and are they documented?

- Individuals requesting access have to submit the appropriate MyForms request, including the particular system role request. This access request is reviewed and approved by their Supervisor, the Application Owner, the Information Owner and the System Owner before access is granted for that role in Insight.
- Currently, no access is granted to users from other agencies.
- There are presently approximately 15 role profiles in Insight. One profile provides read-only access to all project records. The remaining profiles are for specific functional roles. Each role allows access to information specific to the that role.

8.2 Will DFC contractors have access to the system?

- Yes, contractors have access to the system. They are reviewed on a Quarterly basis by the System Owner. All contractors must be approved by the DFC Security Office prior to access to DFC physical and technical assets. In addition, contractors follow the same access request process as other users to gain access to Insight, as documented in section 8.1 above.

8.3 Describe what privacy training is provided to users either generally or specifically relevant to the program or system?

- All DFC staff and contractors are required to complete initial Privacy training upon onboarding to DFC in order to gain access to DFC's systems. In addition, DFC requires all staff and contractors to complete annual refresher training in order to maintain access to DFC systems. These courses include training on the handling of PII.

8.4 Has A&A been completed for the system?

- The Insight ATO was granted on Feb 5th, 2020.