Office of Information Technology (OIT)

Privacy Impact Assessment

ScanWriter by Personable

September 22, 2023

1100 New York Ave NW
Washington, DC 20527

Overview

The U.S. International Development Finance Corporation (DFC) Office of Inspector General (OIG) is seeking to procure software to assist the OIG's investigators and analysts in analyzing financial records in support of investigations. Such software is widely used by federal law enforcement agencies, including OIGs. After conducting extensive research and consulting with other federal users of such software, we have determined that the best software application for our needs is ScanWriter by Personable. ScanWriter automates the process of taking transaction information from bank records and other financial records and putting them in one or more spreadsheets for analysis. The records are typically obtained through a subpoena issued under the OIG's authority under the Inspector General Act of 1978, as amended (IG Act), or through a federal grand jury subpoena issued by the U.S. Department of Justice. The records can be for a business or an individual. The OIG envisions having the software reside in such a way that only select members of the OIG can access the software and the data contained in it. The software will need to be able to access the Internet to get updates and other information from the vendor, but otherwise can and should be isolated from other DFC systems. After the financial analysis is complete, the information will be purged from the system. This Privacy Impact Assessment (PIA) is being conducted because the system uses and processes – but does not collect, maintain, or disseminate – information in identifiable form about members of the public as well as sensitive personally identifiable information (PII) about members of the public, DFC employees, and/or contractors.

Section 1. Characterization of the Personally Identifiable Information (PII)

The following questions are intended to define the scope of the PII 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 PII is collected, used, disseminated, or maintained by the system? Indicate all that apply.

☒ Name
☒ Social Security Number (SSN)
☐ Date of Birth
☐ Place of Birth
☐ Driver's License
☐ Race/Ethnicity
☐ Passport Number
☒ Personal Bank Account Number
☒ Business Bank Account Number
☐ Gender
☐ Religion
☐ Security Clearance
☐ Personal Phone Number
☐ Business Phone Number
☐ Personal Email Address
☐ Business Email Address
☒ Personal Mailing Address
☒ Business Mailing Address
☐ Spouse Information
☐ ID Number
☒ Financial Information
☐ Group Affiliation
☐ Medical Information
☐ Mother's Maiden Name
☐ Marital Status
☐ Disability Information
☐ Biometrics
☐ Fax Number
☐ Health Plan Number
☐ Civil or Criminal History
☐ Alien Registration Number
☐ Photograph
☒ Credit Card Number
☐ Child or Dependent Information
☐ Other Names Used
☐ Law Enforcement
☐ Employment Information
☐ Truncated SSN
☐ Education Information
☐ Military Status/Service
☐ Legal Status
☐ Emergency Contact

☐ Internet Protocol (IP) Address
☐ Account Password
☐ Other: *Specify the PII collected*.

☐ Citizenship or Immigration Status
☐ Retirement Information

☒ Taxpayer Identification Number (TIN)

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

The PII will come from records (e.g., monthly statements, transaction records) obtained from banks and other financial institutions through federal subpoenas. This information is obtained through third parties (banks and other financial institutions) to avoid alerting the subject(s) of an investigation of the existence and nature of the investigation, and because it allows the OIG to obtain records that can be authenticated for use in court.

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

The PII will be used to assist with OIG investigations. Analysis of financial records is a standard part of some (but not all) OIG investigations.

1.4 How is the PII collected?

The PII will be obtained through federal subpoenas (it will not be collected or maintained). Banks and other financial institutions usually produce the information electronically through secure online portals or encrypted email.

1.5 How will the PII be checked for accuracy?

The PII is obtained from reliable third parties with a business interest in maintaining accurate information. It is not checked for accuracy other than to ensure it is for the correct business or individual.

1.6 If the information is retrieved by a personal identifier, what System of Records Notice (SORN) applies to the information. If a SORN is not required, what specific legal authorities, arrangements, and agreements define the collection of PII?

The information will be received in files or batches and will be processed and analyzed as such. Once entered into ScanWriter, the information will not be retrieved by a personal identifier but will be accessed by file name, which would most likely refer to a case name or number and/or bank name. The OIG is authorized to obtain the PII under the IG Act, specifically 5 U.S.C. § 406(a)(4).

1.7 Privacy Impact Analysis: Related to Characterization of the PII

Privacy Risk: There is a risk that more PII will be collected than is necessary and relevant.

Mitigation: This risk is partially mitigated. OIG investigators are trained to obtain information that is necessary and relevant to investigations. Further, OIG subpoenas are reviewed by OIG attorneys to ensure they are legally justified and limited in scope.

Section 2. Uses of the PII

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

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

The PII will be used to support OIG investigations. Analysis of financial records is a standard part of some (but not all) OIG investigations.

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

In addition to the software itself, the main tool that will be used to analyze the data is Excel spreadsheets. The data produced will include spreadsheets, charts, and system-generated reports.

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

The vendor creates templates for data conversion based on the format of various banks and other financial institutions statements. Otherwise, the system does not use commercial or publicly available data.

2.4 Privacy Impact Analysis: Related to Uses of the PII

Privacy Risk: There is a risk that PII will be used inappropriately.

Mitigation: This risk is partially mitigated. All DFC personnel are required to take annual privacy awareness training and sign the DFC Privacy Rules of Behavior to attest that they will handle PII appropriately.

Section 3. Retention of PII

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

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

PII will not be retained in the ScanWriter system. PII processed in ScanWriter will either be transferred to an OIG investigative case file (for which there is a National Archives and Records Administration (NARA)-approved retention schedule) or deleted/destroyed.

3.2 For what reason is the PII retained?

PII will not be retained in the system.

3.3 How long is the PII retained?

PII will not be retained in the system.

3.4 How is the PII disposed of at the end of the retention period?

PII will not be retained in the system. PII processed by ScanWriter will be disposed of using NARA-approved methods to ensure secure deletion or destruction of PII in a manner that prevents loss, theft, misuse, or unauthorized access. This includes electronically deleting any PII from ScanWriter after the financial analysis is complete.

3.5 Privacy Impact Analysis: Related to Retention of PII

Privacy Risk: There is a risk that PII could remain in the system.

Mitigation: This risk is partially mitigated. OIG personnel with access to the system will be trained and reminded to purge all information, including PII, from the system after analysis is complete.

Section 4. Internal Sharing and Disclosure

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

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

PII will not be shared outside the OIG.

4.2 How is the PII transmitted or disclosed internally?

PII will not be shared outside the OIG.

4.3 Privacy Impact Analysis: Related to Internal Sharing and Disclosure

Privacy Risk: There is a risk that PII could be viewed by DFC employees outside the OIG.

Mitigation: This risk is partially mitigated. Only OIG employees with a need to know will have access to the system and the data produced by it.

Section 5. External Sharing and Disclosure

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

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

PII processed by the system may be shared with federal prosecutors and other federal law enforcement agencies in support of criminal investigations and prosecutions. The OIG is authorized to share such PII under various provisions of the IG Act, including 5 U.S.C. § 404(d).

5.2 Is the sharing of PII outside the agency compatible with the original purpose for the collection?

Yes, the reason for sharing PII is the same as the reason for obtaining it – to investigate suspected violations of federal law involving DFC.

5.3 Is the external sharing 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 outside of DFC.

Under § 404(d) of the IG Act, the OIG is *required* to report to the Department of Justice if the OIG has reasonable grounds to believe there has been a violation of federal criminal law.

5.4 How is the PII shared outside the agency and what security measures safeguard its transmission?

PII will be shared outside the agency using DFC Office of Information Technology (OIT)-approved file sharing technology (e.g., Box).

5.5 Privacy Impact Analysis: Related to External Sharing and Disclosure

Privacy Risk: There is a risk that PII could be accessed by unintended recipients.

Mitigation: This risk is partially mitigated. The PII will only be transmitted through DFC OIT-approved technology and will only be made available to users outside the OIG with a need to know.

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 PII?

It depends on the circumstances. If a federal grand jury subpoena is used to obtain an individual's financial records, the individual generally will not be notified, consistent with the Right to Financial Privacy Act (RFPA), 12 U.S.C. § 3413(i). If an OIG subpoena is used to obtain an individual's financial records, the individual generally will be notified, consistent with the RFPA, unless an exception under the RFPA applies (e.g., 12 U.S.C. § 3413(g)).

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

Under the RFPA, an individual may have an opportunity to contest an OIG subpoena. See 12 U.S.C. § 3410.

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

No.

6.4 Privacy Impact Analysis: Related to Notice

Privacy Risk: There is a risk that notice has not been given to individuals on the use of PII.

Mitigation: This risk is partially mitigated. Privacy risk is accounted for in the RFPA and its protections, and this PIA provides notice to individuals on how their PII might be used.

Section 7. Access, Redress, and Correction

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

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

Information processed by the system will be used only for OIG investigations, as authorized under the IG Act. As stated above, the information will not be collected, maintained, or disseminated. If criminal charges are brought against an individual, then the individual will have rights under the Constitution and the Federal Rules of Criminal Procedure to obtain and challenge evidence obtained by the OIG.

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

N/A – see question 7.1.

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

N/A – see question 7.1.

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

N/A – see question 7.1.

7.5 Privacy Impact Analysis: Related to Access, Redress, and Correction

Privacy Risk: There is a risk that inaccurate information about an individual could be obtained and analyzed.

Mitigation: This risk is partially mitigated. The information is obtained from reliable third parties with a business interest in maintaining accurate information (i.e., banks and other financial institutions). Further, the Constitution and federal law provide individuals with certain rights in criminal cases.

Section 8. Technical Access and Security

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

8.1 How will the PII be secured?

(1) Physical Controls. Indicate all that apply.

☒ Security Guards
☐ Key Guards
☒ Locked File Cabinets
☒ Secured Facility
☐ Closed Circuit Television
☐ Cipher Locks
☒ Identification Badges
☐ Safes
☒ Combination Locks
☒ Locked Offices
☐ Other. *Describe*

(2) Technical Controls. Indicate all that apply.

☒ Password
☒ Firewall
☒ Encryption
☒ User Identification
☒ Biometrics
☒ Intrusion Detection System (IDS)
☒ Virtual Private Network (VPN)
☒ Public Key Infrastructure (PKI) Certificates
☒ Personal Identity Verification (PIV) Card
☐ Other. *Describe*

(3) Administrative Controls. Indicate all that apply.

☒ Periodic Security Audits
☒ Backups Secured Off-site
☒ Rules of Behavior
☒ Role-Based Training
☒ Regular Monitoring of Users' Security Practices
☒ Methods to Ensure Only Authorized Personnel Have Access to PII
☒ Encryption of Backups Containing Sensitive Data

☒ Mandatory Security, Privacy, and Records Management Training
☐ Other. *Describe*

8.2 Will DFC contractors have access to the system? If so, how frequently are contracts reviewed and by whom?

We do not envision contractors having access to the system.

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

Employees and contractors must take annual privacy awareness training and information security awareness training, which instruct users on the need to protect agency data and provide best practices for handling PII.

8.4 Has Assessment and Authorization (A&A) been completed for the system?

Assessment & Authorization (A&A) has not been completed for ScanWriter at this time. Should DFC decide to purchase ScanWriter, it will need to be put through the A&A process in accordance with DFC policy and standards. ScanWriter is an on-premises solution and only receives updates to its software when communicating with the Personable server. No data is transferred from the OIG's local system to the cloud. As such, this software does not require authorization from the Federal Risk and Authorization Management Program (FedRAMP) to operate in a U.S. Government environment.

8.5 Privacy Impact Analysis: Related to Technical Access and Security

Privacy Risk: There is a risk that PII will not be properly secured.

Mitigation: This risk is partially mitigated. Because the ScanWriter software will operate within DFC's information technology environment, it will be protected by best-in-class endpoint security, cutting edge artificial intelligence, zero trust solutions, multi-factor authentication, and the use of data loss prevention software to identify threats to the DFC network and prevent data breaches from occurring.