Office of Information Technology (OIT)

Privacy Impact Assessment

Credit Management System (CMS)

January 25, 2023

1100 New York Ave NW
Washington, DC 20527

Overview

The U.S. International Development Finance Corporation (DFC) Credit Management System (CMS) houses the loan-by-loan data inputs from the former U.S. Agency for International Development (USAID) Development Credit Authority guarantee portfolios and allows for reporting and invoicing output. It is owned by the Office of Development Credit and externally hosted on Amazon Web Services (AWS) US East/West. CMS has limited the amount of personal data that is maintained within CMS to the smallest amount possible and has a role-based user platform. Any personal information is restricted to access by administrator roles and isolated into specific, detailed screens. There are three types of data collected in the system: that of users, that of guaranteed lending institutions, and that of individual loans to qualifying borrowers.

Users: Only identified CMS Administrators maintaining an Office of Development Credit Management ("ODCM") account type (these are limited to DFC/Mission Transaction Unit (MTU) compliance directors) may add or view user data. The data collected includes name, business phone number, business email, and position title. To become a user (which includes guaranteed lenders, DFC staff, USAID staff, or others with a need to access the system), the user must create a username and password. No users are able to see passwords, not even administrators. ODCM users are responsible for maintaining ongoing awareness of information security, vulnerabilities, and threats to support organizational risk management decisions (i.e., "continuous monitoring"), and as such, must be able to find users to deactivate when necessary, verify any duplicate entries, and ensure user policies are followed.

Guaranteed Lending Institutions: Data collected includes business address and primary contact information (name, business email, and business number).

Loans to qualifying borrowers: This is borrower information provided by the lending institution, and includes transaction report ID (generated by CMS), country, currency of loan, beneficiary name (name of borrower as tracked by the lender – often a business name only but can be a person's name), loan start date, loan end date, loan placed under coverage date, loan removed from coverage date, loan amount, loan type (term loan or overdraft), business/sector, city/town of business or bank branch, state/province/region of business or bank branch, additional information (open field for loan purpose explanations or other qualifying information), purpose of loan, interest rate, collateral value, days in arrears of loan, loan balance, loan guarantee percentages, and whether the loan is to a first time borrower or woman-owned business, current number of employees on payroll, total assets of the registered business (if applicable), and current annual revenue of registered business (if applicable). Note that the name provided here by the bank can be the business name only, and in that case there is no PII as there is no information collected about any individual (name, contact, address, etc.), only the business operation of that business. If the bank provides a name associated with the guaranteed loan, there is no additional information collected about the individual – all loan data is to be associated with business operation and does not include any contact information or credit information beyond the data as described above about only the particular guaranteed loan reported by the lender.

Personal data is only used to identify the recipient of a loan. Detailed borrower information is kept by the banks in their separate systems, which are not related to CMS. The banks have complete control to edit and maintain the borrower information in CMS. The information from CMS is used by DFC to track DFC exposure to help summarize or analyze DFC's guarantee portfolio behavior and trends

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
☐ Other: *Specify the PII collected*.

☐ 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
☐ Citizenship or Immigration Status
☐ Retirement Information
☐ Taxpayer Identification Number (TIN)

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

Business contact information of new users requesting access for any user roles (including guaranteed lenders, DFC staff, USAID staff, or others with a need to access the system) is provided by the users themselves directly to CMS admin users based in the DFC's MTU compliance team. Qualifying borrower information is provided by users that represent the guaranteed lenders and certify the data on their behalf. These are employees of the guaranteed lenders.

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

User information is being collected to create user accounts and keep basic contact information. DFC compliance directors and relationship managers work with these users on a regular basis during the monitoring of the guarantee program. Qualifying borrower information is collected to verify basic qualification terms for guaranteed loans as outlined in the legal agreement. In the case of qualifying borrowers, no personally identifiable

information (PII) is collected unless the bank reports an individual name as the business name, but the name is not used for any purpose other than to make sure that no single business entity exceeds the single borrower lending limit as outlined in the DFC guarantee contract. All other qualifying borrower information is intended to be related to business operation only, not any individual.

1.4 How is the PII collected?

User information is collected in an email request, though the information matches any basic email signature (name, email address, business phone number). Qualifying borrower information is collected directly in the system through Office of Management and Budget (OMB) form DFC-013 ICR REFERENCE NUMBER: 202207-3015-008, which is completed by guaranteed lender users. The systems of record for all qualifying borrower information are the central systems of the guaranteed lenders themselves. The intent of DFC-013, and indeed CMS itself, is to collect a facsimile of broad loan information and semi-annual exposure information, which is all certified and updated by qualifying lenders themselves. Credit decisions are made by lenders using their own system of record, and the results of their lending decisions under a DFC guarantee are then reported into the system to help DFC track loan qualification under the guarantee terms and monitor use of the guarantee generally. The data itself is maintained by the lenders, and if issues are found during loan reviews or claim reviews of loan documentation, CMS would then be updated to reflect the corrected information delivered and verified by the lenders themselves.

1.5 How will the PII be checked for accuracy?

User contact information: This is self-reported by the users. If contact information does not work, and we receive email kickback, DFC compliance directors or relationship managers will follow up directly for more accurate information. But users must contact DFC staff to request access to the system, so contact information is easily verifiable directly with the requesting user.

Qualifying borrowers: The guaranteed institutions are solely responsible for reporting accurate information to CMS about their loans under guarantee coverage. By submitting, they certify accuracy. Verification of reported data is done manually by the lender themselves or when checked by DFC compliance directors during an in-person file audit (during which reporting data is compared to loan files on-site at the guaranteed lender's offices) or when an actual claim payment request is submitted, during which time compliance directors verify qualifying information and outstanding balances before approving payments. Note that verification is done outside of CMS, though reported balances and basic terms are checked against what was reported to DFC.

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 loan information in CMS originates from and is maintained by the lending institutions. The guaranteed institutions are solely responsible for reporting accurate information to CMS about their loans under guarantee coverage. This information is used by DFC to track exposure to help summarize or analyze DFC's guarantee portfolio behavior and trends; the information is not used by the agency to make credit decisions about any borrowers under the guarantee. CMS does not constitute Privacy Act records in a system of records because the information is maintained by the lending institutions, not by the agency, and as such, a SORN is not applicable. The legal authority that enables DFC to collect information in support of its mission is the Better Utilization of

Investments Leading to Development Act (BUILD) Act of 2018, which establishes the DFC to facilitate the participation of private sector capital and skills in the economic development of countries with low- or lower-middle-income economies and countries transitioning from nonmarket to market economies in order to complement U.S. assistance and foreign policy objectives.

1.7 Privacy Impact Analysis: Related to Characterization of the PII

Privacy Risk: There is a risk that inappropriate or unnecessary PII is collected.

Mitigation: Users: Only basic business contact information is collected, the same as would appear on a business card or in an email signature.

Qualifying borrowers: Often, there is no personal information about a business owner or individual borrower included (only the business name). All guaranteed loan information is used to verify basic qualification of loans per the terms of the guarantee contract.

Privacy Risk: There is a risk that PII is inaccurate or incomplete.

Mitigation: All PII is self-reported by users that certify to its accuracy. DFC does not make approval decisions or provide any support, budgetary or otherwise, using any PII through CMS. It is the duty of the qualifying lenders and associated users to ensure any data provided is accurate and complete. If it is not, or if it is found to be inaccurate during an on-site file review or claim analysis (outside of CMS), DFC will ask the guaranteed party to correct the information.

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.

User information only includes basic contact information, which is used to help verify reporting collected by DFC and contact users should there be any questions or issues. The data also helps us institute user monitoring as part of the continuous monitoring requirements.

Qualifying borrower information is collected to assist in basic qualification reviews per the DFC guarantee contracts and to identify general lending trends, impacts, and concentration risks across the DFC portfolio, such as how many loans go to women-owned businesses or in certain regions, for example.

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

The CMS system has a series of summary and specific reports for each guarantee and for portfolio data. It is used to track DFC contingent liability exposure at the credit agreement level and portfolio level as well as guarantee terms and qualifying borrower business data to summarize and analyze disbursement and claim trends across the

portfolio. Guarantee-level summary reports are also used to verify contract term qualification during semi-annual reporting. User reports are produced by the System Owner during continuous monitoring exercises.

Summary reports are produced by CMS and can be downloaded to .csv and .xls files. Summary analyses are generally done in Microsoft Excel on DFC computers. More robust portfolio-level visualization and analysis maybe done in Power BI or Tableau by DFC analysts in-house. That summary information, which does not contain PII, may be presented by DFC officers when discussing disbursement or guarantee portfolio trends, but will not include any loan-specific data or any user data.

Some trend data produced for Excel download in CMS may be used by relationship managers or other MTU or DFC officers to prioritize partner training or interventions (based on a lack of disbursements or increase in claims submitted), or by credit policy to observe risk trends across portfolios. Again, these analyses do not include individual loan-specific data nor any names of businesses or borrowers.

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

N/A; CMS only uses information input by DFC staff or by users.

2.4 Privacy Impact Analysis: Related to Uses of the PII

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

Mitigation: The system is role-based, meaning the system limits users that are granted access to specific types of information. Downloadability of any information is restricted to certain roles as well, with roles outlined in CMS user guidance documentation. The system runs all required security scans and other required security controls effectively to secure system access and protection. Any actual official loan file information shared with DFC by guaranteed lenders about an individual loan is outside of CMS. All information in CMS is collected directly from individuals certifying on behalf of the contract partner, and all user information is collected directly from users through access requests. All information collected in CMS is outlined in legal contracts, so signatories understand what data DFC will request before agreeing to guarantee coverage.

If a guaranteed lender uses an individual name as the name of a qualifying business (qualifying borrower), only the business information included in form DFC-013 is associated, but no contact information, personal records, business identification numbers or records, or other higher-risk information are collected in the system.

CMS states “Please do not disseminate, distribute or copy information from this system without DFC's prior written consent” on each page, and the login screen states, “You are accessing an official UNCLASSIFIED U.S. Government System. This United States Development Finance Corporation (DFC) computer system is provided only for official U.S. Government business. Information system usage may be monitored, recorded, and subject to audit. Unauthorized use of the information system is prohibited and subject to criminal and civil penalties. Use of the information system indicates consent to monitoring and recording.”

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.

User account information is maintained under the National Archives and Records Administration (NARA) General Records Schedule 3.2 - Information Systems Security Records, Item 030 - System access records.

Qualifying loan information is maintained by the guaranteed lender, but DFC uses the information for business purposes. However, CMS does not retain qualifying loan information as currently listed in NARA-approved records retention schedules. DFC will keep the data for business purposes and until further notice, and DFC will work to incorporate CMS data into a revised retention schedule, to be approved through NARA.

3.2 For what reason is the PII retained?

User account information is retained in order to authenticate users to access CMS.

Qualifying loan information is retained for business use for historic data analytics purposes and claim recovery accounting support.

3.3 How long is the PII retained?

Inactive user accounts are deactivated and archived in the system after 90-days of non-use. The records are temporary and deleted when business use ceases, which is set at 365 days after deactivation.

Qualifying loan information is historically archived when program authorization changes and the data is no longer relevant for business use.

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

Inactive user accounts are automatically deleted from the system at the end of the retention period.

Qualifying loan information is archived from the user interface of CMS when there is no longer a business use but held within the SQL database.

3.5 Privacy Impact Analysis: Related to Retention of PII

Privacy Risk: There is a risk that PII is retained longer than required for business use.

Mitigation: Data in CMS is archived or deleted when no longer required for business use. DFC is working to incorporate a NARA-approved records retention schedule to the qualifying loan information, which is currently archived when program authorization changes and the data is no longer relevant for business use. Inactive user accounts are archived in the system after 90 days of non-use and then automatically deleted 365 days after deactivation.

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?

System access records containing user information are shared with the DFC Chief Information Security Officer (CISO) team as part of continuous monitoring. Qualifying borrower information from CMS is not shared with other offices or systems.

4.2 How is the PII transmitted or disclosed internally?

User information is shared via electronic spreadsheet with the DFC CISO team as part of continuous monitoring. Qualifying borrower summary information may be downloaded by DFC staff users or users from the reporting guaranteed lender.

4.3 Privacy Impact Analysis: Related to Internal Sharing and Disclosure

Privacy Risk: There is a risk that information will be shared internally with individuals who do not have a need to know.

Mitigation: CMS data in the system is viewable according to user roles. Only DFC monitoring staff may access user information. Information for DFC reporting purposes is provided by specific request to other DFC staff, and any DFC internal users are provided appropriate user roles according to their needs.

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?

Only USAID as an external organization sees any of the qualifying borrower information described above, and this is restricted to USAID-sponsored guarantees (see Transaction Note of any USAID-sponsored DFC guarantee). No external organizations see any user information.

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

Yes. USAID sponsors some guarantees by providing budget or technical assistance to establish and support the project. They do this for their own development impact outcomes, and so seeing disbursement trends and sectors verifies the impacts intended by their budget outlay.

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.

The BUILD Act requires DFC to work alongside USAID in establishing pipeline and executing projects for shared interagency outcomes. USAID sponsors transactions by providing budget, pipeline, technical assistance, or other support, and in so doing outlay budget for DFC loans and guarantees. CMS hosts data for these shares guarantees, and USAID, for its own project and budget-use monitoring purposes, insists on access to guarantee portfolio data as part of our shared project execution. There is also an Interagency Agreement that outlines agency expectations, and the guarantee contract section on Information and Publicity requires the guaranteed lender to acknowledge that DFC may share information regarding this Agreement within the U.S. Government.

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

USAID users that have access to a sponsored guarantee can view summary reports of qualifying borrowers. Each user is specified a role and granted access to specific guarantees in their sponsored portfolio, and all new users (including all roles) are required to certify completion of a privacy and system security training when logging into the system for the first time and again annually. The training includes handling of PII, encryption, rules of behavior for system access and data management, common Internet threats, and how to report possible issues to DFC.

5.5 Privacy Impact Analysis: Related to External Sharing and Disclosure

Privacy Risk: There is a risk that PII may be shared externally with individuals who do not have a need to know.

Mitigation: USAID access to CMS data is role-based and derived from expectations of USAID sponsorship and shared responsibilities as established in the DFC 2023 Field Manual and Interagency Agreements.

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?

Users requesting a username send their contact information directly to DFC. Any information regarding qualifying loans is done by guaranteed lenders, who submit the information directly to DFC. It is the responsibility of the guaranteed lenders to alert, in loan documentation, their borrowers about collection of any associated loan information.

When collecting information, DFC provides a Privacy Notice to users, which is placed in email communication intended to collect information as well as within the CMS system itself. The Privacy Notice reads as follows:

> The U.S. International Development Finance Corporation (DFC), in its implementation of authorities outlined in 22 U.S.C. § 9601, the "Better Utilization of Investments Leading to

Development Act of 2018" and the Foreign Assistance Act of 1961, as amended, collects certain data to ensure reporting compliance and qualification of certain investments and liabilities as outlined in financing and guarantee contracts. Guarantee reporting data entered into CMS is required specifically as defined in DFC's finance and insurance contracts. This data is used to ensure qualification of transactions under contractual requirement, DFC liability reporting as required by law and regulation, and for general business analytics.

For Users of the Credit Management System (CMS), PII collection is limited to business contact information (name, business email address, and business phone number) that is used by DFC staff to create User Accounts and contact Users if correction or clarification is needed on their reporting data. User Account information is required for DFC to verify permissions for all users, internal and external, to obtain access to the system. Providing contact data is voluntary, though lending institutions are still responsible for submission of required guarantee reporting, and without contact information, the ability to fulfill contract obligations is limited. User contact information is not shared outside of DFC except to the extent required by law or as necessary to represent the agency in litigation.

Information entered into CMS is exempt from disclosure under the Freedom of Information Act, 5 U.S.C. § 552 and under the Trade Secrets Act, 18 U.S.C. § 1905. CMS may contain information that is private and proprietary and is intended solely for the use of the individual or entity to whom they are addressed. Please do not disseminate, distribute, or copy information from the system without DFC's prior written consent.

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

By becoming a CMS user, there is some PII that an individual cannot decline to provide. For example, when emailing the user request, individuals must share their email account name and email address to do so, and that is their primary contact business email associated with their username. Users who do not provide any business contact details can therefore not be granted a username.

For qualifying borrowers, it is the responsibility of the guaranteed lenders to alert, in loan documentation, their borrowers about collection of any associated loan information. If a lender is unable to provide certain information, DFC works directly with the lender to establish what can fairly be collected and reported. Since the data on qualifying borrowers is business loan information, and not an individual borrower's personal information, this is only occasionally an issue with the borrower name (per specific international data regulations), in which case DFC is flexible to accommodate the guaranteed lender's specific needs.

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

For users, the information provided is only used for continuous monitoring purposes, and users would not have the ability to opt out of that particular use as it is a basic CMS account security check.

For qualifying borrowers, it is the responsibility of the guaranteed lenders to alert, in loan documentation, their borrowers about collection and use of any associated loan information and offer such an opt out. DFC does not

have a direct opt out for reporting of loans under coverage as DFC does not have any direct contact with any qualifying borrowers (intentionally). DFC uses information collected for portfolio/trend analytics and basic qualification verification.

6.4 Privacy Impact Analysis: Related to Notice

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

Mitigation: DFC provides notice to the public in this PIA and in the Privacy Notice that is placed in email communication intended to collect information as well as within the CMS system itself. User data is only used for required account security purposes, to which users cannot be given the ability to opt out. Guaranteed lenders must alert their borrowers to general use of data submitted to the bank, as DFC intentionally does not have direct contact with any individual borrowers.

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?

Users already have access to their own information since they are the ones submitting the information. Guaranteed lenders reporting any information on qualifying loans can see that information they have previously reported at any time.

Note that the guaranteed institutions are solely responsible for reporting accurate information to CMS about their loans under guarantee coverage. This information is used by DFC to track exposure to help summarize or analyze DFC's guarantee portfolio behavior and trends; the information is not used by the agency to make credit decisions about any borrowers under the guarantee. Therefore, CMS does not constitute Privacy Act records in a system of records because the information is maintained by the lending institutions, not by the agency.

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

If any user needs to change contact information, or if guaranteed lenders need to adjust reported qualifying loan information in form DFC-013, they can request that change directly to MTU monitoring staff over email or may email cms@dfc.gov.

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

DFC monitoring staff regularly trains partners and outlines process expectations in guarantee contracts. In addition, this PIA provides notice to individuals on how to correct this information.

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

N/A; formal redress is available to individuals as described in Section 7.2 of this PIA.

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

Privacy Risk: There is a risk that individuals will not be able to access or correct any information maintained on them by DFC.

Mitigation: All data is sent directly to DFC by users. CMS only holds user business contact information, and if that changes, they may contact DFC to change it directly. Guaranteed lenders can access their reported information at any time.

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. Security controls as discussed in the CMS System Security Plan, and the Relational Database Service instance does not have a public IP address and must be accessed on a private subnet.

(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?

DFC's contracted CMS system developers have access to the system. Contracts are reviewed periodically by the Contracting Officer's Representative and Contracting Officer, at minimum during modifications, addition of new key personnel, and the annual contract option.

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

Employees 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 sensitive PII. New CMS users must certify completion of a brief security training before accessing the system for the first time.

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

Assessment and Authorization (A&A) is scheduled for completion in fiscal year 2023.

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 is mitigated through a series of technical and administrative controls and user training.