Office of Information Technology (OIT)

Privacy Impact Assessment

Microsoft 365

November 30, 2022

1100 New York Ave NW
Washington, DC 20527

Overview

The U.S. International Development Finance Corporation (DFC) Office of Information Technology (OIT) has an enterprise agreement with Microsoft to use their Microsoft 365 suite of productivity software. The purpose of Microsoft 365 is to provide the agency with essential office tools and computing functionalities, including word processing, email, spreadsheets, presentations, file sharing, office calendars, event scheduling, audio/visual (A/V) communications, online chatting, and other business and collaborative capabilities. Microsoft 365 is a subscription-based Software as a Service platform that is authorized to operate as a federal Cloud Service Offering by the Federal Risk and Authorization Management Program (FedRAMP). This PIA is being conducted because DFC uses Microsoft 365 to collect, maintain, or disseminate information in identifiable form from or about members of the public. This PIA describes the privacy risks associated with DFC's use of the following Microsoft 365 applications:

- Desktop Applications: Word, Excel, PowerPoint, Excel, Access, Visio, Project, OneNote, Publisher
- File Sharing and Collaboration: SharePoint, OneDrive, Teams
- Email/Office Calendar: Outlook, Bookings

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

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 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
☒ Other: *Specify the PII collected*

☒ 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
☒ Citizenship or Immigration Status
☒ Retirement Information

Due to the nature of Microsoft 365, DFC users could use the platform's applications to collect, use, disseminate, or maintain all types of PII. Electronic files contained in Microsoft 365 applications may include documents, forms, reports, correspondence, photographs, audio and video recordings, project schedules, surveys, briefing papers, committee and meeting minutes, contracts, loan applications, grants, leases, permits, audits, manuals, studies, promotional materials, and compliance information. As such, there is the potential that large amounts of PII could be created or stored through Microsoft 365. The following table shows the Microsoft 365 applications used by DFC and their primary functions.

Applications	Primary Functions
Access	Database management
Bookings	Event scheduling
Excel	Spreadsheets
OneDrive	File hosting
OneNote	Note-taking
Outlook	Email and office calendars
PowerPoint	Presentations
Project	Project management software
Publisher	Desktop publishing
SharePoint	File sharing and collaboration
Teams	Audio/visual communications and text chats
Visio	Diagramming and vector graphics

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

The sources of the PII are DFC stakeholders, including employees, contractors, and members of the public.

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

The PII can be collected, used, disseminated, or maintained for any reason related to DFC's mission and business operations, such as to maintain details on a DFC project, to record loan information, to process human resources documentation, and to communicate with external stakeholders.

1.4 How is the PII collected?

PII is generally collected directly from the source. However, PII that has been collected by DFC through another system may be transferred to Microsoft 365 applications. For example, a member of the public who has applied for a DFC loan by completing a loan application on the DFC Insight (Salesforce.com) data collection system may have their application uploaded to SharePoint and then shared with the program office that is responsible for making a determination on the loan. Similarly, information containing PII may be transferred to Word or Excel to aggregate numerous files into one document for ease of use and viewing.

1.5 How will the PII be checked for accuracy?

PII that is collected directly from the source is presumed to be accurate, but DFC personnel may reach out to submitters to correct any errors as needed. The Office of Human Resources verifies employment information

about new hires with the human resources office from the individual's previous federal agency if they are transferring from a different federal agency. Due to the unstructured nature of Microsoft 365 applications, DFC personnel will need to determine the accuracy of data that they enter into an application based on business knowledge and need, such as whether the information will be used to make a determination on an 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?

DFC uses the suite of Microsoft 365 applications as an information technology (IT) platform for performing routine office functions and conducting agency business. A System of Records Notice (SORN) does not apply to Microsoft 365 as a technology but applies to the individual information collections that use Microsoft 365 to create Privacy Act systems of records. DFC personnel who use Microsoft 365 applications to create systems of records are responsible for ensuring that an appropriate SORN is assigned to their respective Privacy Act systems.

In general, 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. Based on the type of information collected, there may be additional legal authorities that govern the collection of PII.

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 relevant and necessary.

Mitigation: This risk is partially mitigated. All DFC personnel that conduct activities involving PII must follow the DFC privacy compliance process and complete a Privacy Threshold Analysis (PTA) as the first step in the privacy process. The PTA includes questions on why specific types of PII are collected and what the legal authority is to do so. The PTA initiates the communication and collaboration between program officials and the privacy program at the earliest stages of the information life cycle to ensure that any PII collected will be relevant and necessary to the agency's underlying mission and is consistent with the information collection's enabling authority.

Privacy Risk: There is a risk that the PII collected will be inaccurate or incomplete.

Mitigation: This risk is partially mitigated. PII that is collected directly from the source is presumed to be accurate, but DFC personnel may reach out to submitters to correct any errors as needed, if valid contact information has been provided to the agency. To ensure the completeness of PII, some forms created through Microsoft 365 applications can be structured to make certain fields mandatory before the forms can be submitted to the agency. DFC personnel may also reach out to individuals via Outlook to request that they upload additional documentation to DFC's secure Box.com portal to ensure the completeness of their PII.

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 collected using Microsoft 365 applications can be used for purposes related to DFC's mission and business operations. For example, when communicating with a DFC loan applicant via Outlook, the agency could email the individual to request additional information to assist in determining whether their application satisfies DFC's loan eligibility criteria. In addition, when going through the hiring process, the Office of Human Resources could call a job applicant's references and type their comments into a Word document to provide additional insights to the hiring manager regarding a candidate's prior work experience.

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

Microsoft 365 includes tools that are able to analyze data and produce complex reports. For example, Excel provides the ability to produce charts and graphs of data and to calculate risk formulas that could be used by DFC's Risk Committee Division to determine whether a loan is at risk of default. In addition, Microsoft Project can be used to develop a timeline of a project's tasks and determine if completion is far behind schedule, thus enabling the agency to take steps to protect its interests in case a project fails. Financial and demographic data collected from individuals may be aggregated in order to summarize or analyze financial portfolio behavior and trends or to determine if there is a statistically significant difference between populations from different groups. All analyses will be conducted using aggregated data; at no time will any analysis be conducted on data from a single individual.

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

N/A; Microsoft 365 does not use commercial or publicly available data to collect information about individuals.

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. In accordance with agency privacy policy, the use of PII must be compatible with the purpose for the collection. The purpose is included in a Privacy Act Statement or Privacy Notice provided to the individual and describes the specific uses of the PII and whom within the agency will have access to it. Any uses of PII for an unauthorized purpose is prohibited, and a program office's uses of PII are reviewed by the privacy program during the PIA development process.

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.

DFC records maintained in Microsoft 365 applications are retained and disposed of in accordance with the National Archives and Records Administration (NARA) General Records Schedule (GRS) specific to that record. It is the responsibility of DFC personnel to ensure that their records are being retained in accordance with an approved NARA GRS.

Outlook emails are managed under a Capstone approach in accordance with NARA GRS 6.1: Email Managed under a Capstone Approach.

3.2 For what reason is the PII retained?

PII may be retained for authorized purposes related to DFC business. For example, disclosures made to a third party from a Privacy Act system of records are required to be documented in a disclosure accounting form. A Privacy Act system manager must retain the names and addresses of the third-party individuals to whom the disclosure is made in the DFC Disclosure Accounting Form, which is a Word document that is uploaded to the privacy program's SharePoint website. A system manager may download the document, fill it out with the relevant PII, and save it to their OneDrive account for at least five years after the disclosure is made or the life of the record, whichever is longer. Financial information from individuals is also retained in furtherance of the agency's mission. For example, PII from loan applications may be transferred from Insight to SharePoint and shared with the Office of Development Policy to determine the financial wherewithal of the individual to meet their expected obligations under the terms of DFC financing. In general, DFC personnel retain PII in OneDrive and on SharePoint because files are backed up in the DFC cloud (i.e., Microsoft Azure), and these applications allow DFC personnel to share and collaborate on documents with other DFC personnel as needed.

3.3 How long is the PII retained?

Retention periods vary depending on the user created contents.

The following email retention periods apply to Outlook:

- Email of Capstone Officials (Item 010): Permanent. Cut off in accordance with agency's business needs. Transfer to NARA 15-25 years after cutoff, or after declassification review (when applicable), whichever is later.
- Email of Non-Capstone officials:
    - All others except those in item 012 (Item 011 – This item applies to the majority of email accounts/users): Temporary. Delete after 7 years old, but longer retention is authorized if required for business use.
    - Support and/or administrative positions (Item 012 – Includes non-supervisory positions carrying out routine and/or administrative duties): Temporary. Delete when 3 years old, but longer retention is authorized if required for business use.

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

Procedures for disposal of the PII stored in individual Microsoft 365 applications will vary. It is the responsibility of each program office and the DFC personnel that create or maintain records containing PII to dispose of the records in accordance with the appropriate NARA disposition authority. Approved NARA disposal methods include degaussing or erasing of electronic records and shredding or pulping of paper records.

3.5 Privacy Impact Analysis: Related to Retention of PII

Privacy Risk: There is the risk that PII may be retained for a longer period than necessary.

Mitigation: This risk is partially mitigated. PII must be retained in accordance with a NARA-approved GRS. A system's records retention procedures are discussed with the privacy program during development of the PIA and at least once every three years thereafter to ensure that PII is retained for only the relevant and necessary period.

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 collected from members of the public is shared internally on a case-by-case basis. PII will only be shared with other DFC personnel who have a need to know to perform their official duties. For example, in a typical transaction, the Service Desk would forward contact information from an IT support ticket to a member of the technical support team to follow up with and help resolve the submitter's technical issue. Conversely, it would not be appropriate to forward this contact information to someone from the Equal Employment Opportunity Office who does not have a need to know to perform their duties.

4.2 How is the PII transmitted or disclosed internally?

The PII can be transmitted internally in several ways. Paper copies of the information can be printed and shared in person or by postal mail. For example, a Word document could be printed and mailed from DFC headquarters in Washington, D.C., to a DFC field office in a different state. The PII can also be shared internally via email (i.e., Outlook) or through a file sharing application (i.e., OneDrive, SharePoint, or Teams). PII is shared on a case-by-case basis with access restricted to persons on a need-to-know basis.

4.3 Privacy Impact Analysis: Related to Internal Sharing and Disclosure

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

Mitigation: This risk is partially mitigated. Access controls in Microsoft 365 collaboration applications enable the agency to share PII internally in accordance with the principle of least privilege. The most common methods of sharing information internally are through SharePoint, OneDrive, and Teams. Each of these applications contains access rights to restrict sharing to those who are authorized to view the PII. Files can be shared with the entire agency, within program offices, or with specific individuals who have a need to know. PII from members of the public will never be shared with the entire agency.

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?

DFC personnel do not share PII with external organizations unless expressly permitted by the subject individual or as allowed by the legal authorities, arrangements, or agreements that define the collection of PII. For example, PII stored in ServiceNow may be exported to an Excel spreadsheet and shared with external contractors who are performing maintenance on the system. External third parties who are given access to Privacy Act-protected information must be covered by a routine use in the SORN or receive consent from the subject individual to do so.

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

To the extent that PII is maintained on an individual in a Privacy Act system of records, the PII will only be shared outside the agency with written consent from the subject individual or pursuant to a published routine use in the associated SORN. The purpose for the disclosure must be compatible with the purpose for the collection as required by the Privacy Act.

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.

See question 5.2.

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

For information that is transmitted electronically, sensitive PII is only shared using DFC's secure Box.com solution or via encrypted email in Outlook. External recipients must sign up for a Box account to access a DFC file shared through the agency's Box.com portal. This provides an additional layer of security so that hyperlinks shared through Box are only accessed by the intended recipient and no one else. PII may also be printed and shared externally by postal mail if requested or when necessary.

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: This risk is partially mitigated. DFC has implemented a Data Loss Prevention (DLP) solution that inspects outbound network communications, such as emails and their attachments. DLP detects and prevents the transmission of unencrypted sensitive data, including but not limited to Social Security numbers, passport numbers, credit card numbers, bank account numbers, and driver's license numbers, from leaving the DFC network. When sharing information via Box, the DFC Box account owner has access to view audit logs that identify

each registered Box account user who has accessed a file. In addition, all DFC personnel must sign the annual DFC Privacy Rules of Behavior attesting that they will handle PII appropriately and are subject to disciplinary and criminal penalties for disclosing Privacy Act-protected information to unauthorized persons.

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?

For DFC's general use of the Microsoft 365 platform, notice is provided to individuals through this PIA. For information collected from members of the public as part of a Privacy Act system of records, notice is provided to individuals in a project-specific PIA, through the SORN(s) associated with the collection, and in a Privacy Act Statement, which is typically placed at the point of collection. For PII not collected as part of a system of records, a Privacy Notice should be provided to the individual to solicit their informed consent before they provide their personal information to the agency.

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 using Microsoft 365 to interact with DFC, there is certain PII that an individual cannot decline to provide. For example, when emailing the agency, individuals must share their email account name and email address with DFC's email application, Outlook. When using Microsoft Bookings, an event scheduling tool, individuals can see each other's meeting dates/times of availability in order to book an appointment with each other during an unscheduled time slot. When joining a Teams meeting, individuals must share their name (or alias) and email address, or, if connecting by phone, phone number, in the Teams participants panel. For other Microsoft 365 applications listed in Section 1.1, individuals have the opportunity and right to decline to provide their PII. However, declining to provide certain PII on a DFC form or application may cause the agency to be unable to process their information or to follow up with the individual for any needed reason.

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

See question 6.2.

6.4 Privacy Impact Analysis: Related to Notice

Privacy Risk: There is a risk that individuals will not be given an opportunity to consent to the uses of their information.

Mitigation: This risk is partially mitigated. Members of the public are in complete control of any PII that they submit to the agency through a Microsoft 365 application (mostly through Outlook). The vast majority of PII that is collected from the public is done through systems outside of Microsoft 365. For example, loan applications, surveys, and other project data are submitted to DFC through the agency's Insight data collection portal.

Onboarding forms for new hires are submitted through the New Employee Onboarding website, which is hosted by the Department of the Interior. PII may be transferred from these other systems to a Microsoft 365 application, and any use of the information must be compatible with the purpose for the collection.

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?

In general, individuals who interact with DFC though a Microsoft 365 application already have access to their own information since they are the ones submitting the information. For information that is processed as part of a Privacy Act system of records, individuals should follow the process below to request access to their records:

To make a Privacy Act request, a requester may submit a written request to the Director of Human Resources Management, either by mail or delivery, to U.S. International Development Finance Corporation, 1100 New York Ave NW, Washington, DC 20527 or electronic mail to privacy@dfc.gov. The envelope or subject line should read "Privacy Act Request" to ensure proper routing. Individuals requesting access must comply with DFC's Privacy Act regulations regarding what information to include in the request and provide the proper verification of identity (22 CFR Part 707). To protect PII in transit, individuals should encrypt any sensitive PII sent to the agency over email or request to submit it to through DFC's secure Box.com portal. Alternatively, a requester may address the request to the system manager that is provided in the SORN. For information not maintained in a Privacy Act system of records, the individual may reach out to the person they submitted the information to in order to request access to their information.

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

To make a Privacy Act amendment request, a requester may submit a written request to the Director of Human Resources Management, either by mail or delivery, to U.S. International Development Finance Corporation, 1100 New York Ave NW, Washington, DC 20527 or electronic mail to privacy@dfc.gov. The envelope or subject line should read "Privacy Act Request" to ensure proper routing. Individuals requesting amendment must comply with DFC's Privacy Act regulations regarding what information to include in the amendment request and provide the proper verification of identity (22 CFR Part 707). To protect PII in transit, individuals should encrypt any sensitive PII sent to the agency over email or request to submit it to through DFC's secure Box.com portal. Alternatively, a requester may address the request to the system manager that is provided in the SORN. For information not maintained in a Privacy Act system of records, the individual may reach out to the person they submitted the information to in order to correct inaccurate or erroneous information.

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

This PIA provides notice to individuals on how to correct information that is processed by the agency through a Microsoft 365 application. Additional notice is provided by DFC's Privacy Act regulations and in the PIAs, SORNs, and Privacy Act Statements/Privacy Notices that govern DFC's collections of PII from members of the public.

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

N/A; formal redress is provided through the Privacy Act request process.

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: This risk is partially mitigated. Individuals who interact with the agency through Outlook or Teams are directly responsible for any information that they send to the agency. If an individual has mistakenly submitted incorrect information, they may reach out to the DFC official who was responsible for intake to request that the information be corrected. For any information that DFC collects about individuals that is maintained in a Privacy Act system of records, the agency has published its Privacy Act Regulations on the DFC website that detail how individuals should request access to or request amendment of their records.

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?

DFC contractors have access to the agency's Microsoft 365 applications to perform their duties. During the official solicitation process, the Office of Administration includes the applicable Federal Acquisition Regulation privacy clauses and other privacy provisions into contracts, as appropriate, that outline roles, responsibilities, training, incident reporting, and other privacy requirements for contractors who have access to PII. PII is only shared with contractors on a need-to-know basis based on the duties of the contractor and the needs of the agency.

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 sensitive PII.

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

Assessment and Authorization (A&A) was conducted for Microsoft 365 by an independent assessor as part of the FedRAMP authorization process. A FedRAMP Authorization to Operate (ATO) was first authorized for Microsoft 365 on November 20, 2014, and re-authorized by the Pension Benefit Guaranty Corporation on October 25, 2022. DFC has leveraged the FedRAMP A&A package and also performed A&A on a limited number of controls to ensure that Microsoft 365 is secure to operate in the DFC 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. Microsoft 365 is a FedRAMP-approved cloud service that has undergone a rigorous security assessment by an independent third-party assessor and is authorized to operate at a Moderate impact level, meaning it is approved to handle documents containing PII and Controlled Unclassified Information. All PII stored on Microsoft 365 applications are protected by DFC firewalls from outside access. DFC has employed numerous information security tools to identify threats to the DFC network and to prevent data leaks from

occurring. Notably, DFC has deployed DLP to detect and block the unencrypted transmission of sensitive PII outside the DFC network.