Office of Information Technology (OIT)

Privacy Impact Assessment

DFCNet

January 26, 2023

1100 New York Ave NW
Washington, DC 20527

Overview

The U.S. International Development Finance Corporation (DFC) Office of Information Technology (OIT) allows DFC to further its mission by providing the information technology (IT) systems, network connectivity, operating systems, and other IT resources needed for DFC to conduct agency business electronically. This set of interconnected systems, called "DFCNet," serves as the agency's General Support System (GSS) and is comprised of numerous third-party IT solutions. DFCNet connects the entire agency internally and provides the network backbone needed to support distributed access to DFC IT systems. It does not, in and of itself, control what PII is processed by end users (i.e., DFC employees and contractors) who use DFCNet IT solutions (i.e., "components").

This Privacy Impact Assessment (PIA) is being conducted because DFCNet's components collect, maintain, or disseminate information in identifiable form from or about members of the public and contain sensitive PII (SPII) about DFC employees, contractors, and members of the public. Due to the broad nature of DFCNet and the numerous components therein, a separate PIA will be written for each DFCNet component, if required. This PIA provides a general discussion of the privacy risks associated with the use of DFCNet as an infrastructure.

DFCNet's components are broadly categorized as follows:

Audio/Visual Communications: Webex, Zoom for Government
Authentication and Identity Management: Login.gov, Okta, Zscaler
Backup Storage: AvePoint, Microsoft Azure
Compute Capacity/Analytics and Business Intelligence: Mulesoft, Oracle Cloud Infrastructure Enterprise Data Warehouse
Cybersecurity Tools: Microsoft Purview, Splunk Cloud
Emergency Alert Tool: Everbridge
Mobile Device Management: Absolute, Smarsh
Office Productivity Software: Microsoft 365
Secure File Transfer: Box
Web Hosting: Acquia
Workflow Management Solutions: DocuSign, FDonline Intelliworx, ServiceNow, Unison/PRISM

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
☒ Other: *Specify the PII collected*.

☒ 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)

Due to the broad nature of DFCNet's components, the system could collect, process, or store all types of PII. The following table shows DFCNet's components and their primary functions:

Component	Primary Functions
Absolute	Tracks and remotely deletes mobile devices
Acquia	Web hosting service
AvePoint	Backs up Microsoft 365 data (mailboxes, OneDrive, SharePoint, and Teams) into the cloud
Box	Secure file sharing system
DocuSign	Manages electronic signatures on different devices
Everbridge	Emergency response alert system
FDonline Intelliworx	Online form system used to submit annual financial disclosure filings
Login.gov	Single sign-on solution for government websites
Microsoft 365	Suite of office productivity software
Microsoft Azure	Cloud computing platform that provides applications and services via geographically distributed data centers
Microsoft Purview	eDiscovery searches
Mulesoft	Integration software for connecting applications, data, and devices
Okta	Secure user authentication
Oracle Cloud Infrastructure Enterprise Data Warehouse	Provides compute capacity to support IT workload and analytics and business intelligence functions
ServiceNow	Digital workflow solution that manages Service Desk tickets
Smarsh	Captures and archives mobile phone data
Splunk Cloud	Cloud tool to search, monitor, and analyze machine-generated data

Unison/PRISM	Federal acquisition management system
Webex	Enterprise solution for video conferencing, online meetings, screen share, and webinars
Zoom for Government	Communication and collaboration tool for video, meetings, phone, webinar, and chats
Zscaler	Secure virtual tunnel to remotely access DFC resources

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.

1.4 How is the PII collected?

PII is generally collected directly from the source, but PII may be transferred from another Federal Information Security Modernization Act (FISMA) reportable system into DFCNet. DFC has four FISMA reportable systems: 1) DFCNet, 2) Credit Management System (CMS), 3) Insight, and 4) Oracle E-Business Suite (EBS). Internal end users (i.e., DFC employees and contractors) of CMS, Insight, and EBS have the ability to take PII from those systems and transfer them to DFCNet (such as to store in SharePoint or OneDrive).

1.5 How will the PII be checked for accuracy?

DFCNet, in and of itself, does not check PII for accuracy because it does not control what PII is processed by end users. It is the responsibility of each DFCNet user to ensure the accuracy of the PII they will be collecting. PII that is collected directly from an individual is presumed to be accurate but may be verified with other U.S. Government systems, such as the Office of Management and Budget's Electronic Official Personnel Folder (eOPF) system for human resources information.

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?

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. The System of Records Notice (SORN) that applies to the information collections in DFCNet will vary based on the types of information collected.

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. All DFC personnel that conduct activities involving PII should 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. DFCNet does not, in and of itself, control what PII is processed by end users. Each DFCNet user is responsible for ensuring the accuracy and completeness of the PII they will be collecting in cases where such verification is necessary (such as when PII will be used to make a determination on an individual) and practicable.

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.

OIT's vision is "to become an agile IT enterprise that adapts quickly to new technology and industry standards, enabling secure, innovative, cost efficient support to our DFC customers." Its mission is "to advance DFC's ability in driving global development impacts through providing reliable, innovative IT solutions." To accomplish OIT's business purpose, DFCNet provides the IT solutions that enable the agency to collect PII in support of DFC business, whether it is used to conduct financial transactions, resolve Service Desk tickets, capture loan transactions, process travel requests, etc.

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

Data analysis is initiated in several ways. Splunk Cloud, a security tool managed by the Chief Information Security Officer (CISO) team, receives system logs from key systems in the environment to analyze account and system access and to identify asymmetrical user behavior. The CISO team also responds to Freedom of Information Act requests and supports investigations on employees or systems when needed to investigate potential fraud, waste, or abuse. To locate responsive records, the CISO team runs eDiscovery queries in Microsoft Purview by using key words across communication mechanisms in the DFCNet environment, including Microsoft Outlook, SharePoint, OneDrive, Teams, etc.

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

N/A; DFCNet does not use commercial or publicly available data to collect information on 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. 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.

Retention schedules will vary based on subject matter. Every effort is made during the PIA review process to ensure that PII in DFCNet is maintained under a National Archives and Records Administration (NARA)-approved records retention schedule, which could either be the NARA General Records Schedule (GRS) or a DFC records schedule approved by the Archivist of the United States.

Common records found in DFCNet are listed below:

1. PII created and maintained related to protecting the security of DFCNet is managed in accordance with NARA GRS 3.2: Information System Security Records.
2. User emails are managed under a Capstone approach in accordance with NARA GRS 6.1: Email and Other Electronic Messages Managed under a Capstone Approach.

3.2 For what reason is the PII retained?

Common reasons PII is retained in DFCNet are listed below:

1. NARA GRS 3.2: Information Systems Security Records - These records are created as part of the user identification and authorization process to gain access to systems. Records are used to monitor inappropriate systems access by users. Includes records such as:
    - User profiles
    - Log-in files
    - Password files
    - Audit trail files and extracts
    - System usage files
    - Cost-back files used to assess charges for system use

2. NARA GRS 6.1: Email and Other Electronic Messages Managed under a Capstone Approach - Capstone Officials are senior officials designated by account or position level. Emails and other electronic messages are retained due to the historical significance of Capstone Officials' communications to the agency.

3.3 How long is the PII retained?

Common retention periods for PII retained in DFCNet are listed below.

1. NARA GRS 3.2: Information System Security Records:
    - Systems not requiring special accountability for access (Item 030): Temporary. Destroy when business use ceases.
2. NARA GRS 6.1: Email and Other Electronic Messages Managed under a Capstone Approach:
    - Email and other electronic messages of Capstone officials (Item 010): Permanent. Cut off and transfer in accordance with the agency's NA-1005, *Verification for Implementing GRS 6.1*. This will be between 15 and 30 years, or after declassification review (when applicable), whichever is later.
    - Email and other types of electronic messages of Non-Capstone officials (Item 011): Temporary. Delete when 7 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?

At the end of the retention period, the PII is electronically deleted from DFCNet if it is a temporary record or accessioned to NARA if it is a permanent record.

3.5 Privacy Impact Analysis: Related to Retention of PII

Privacy Risk: There is a 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 records schedule, and privacy reviews are occasionally conducted to see that PII is not retained for a longer period than necessary.

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?

Internal sharing is permitted on a need-to-know basis. DFC employees and contractors should only have access to PII they are authorized to see. The types of PII shared will vary based on a program office's needs and the duties of the employee or contractor. For example, specific members from the CISO team have access to SPII when conducting eDiscovery searches in response to FOIA requests, government investigations, and litigation. They also have access to SPII when the Data Loss Prevention (DLP) tool blocks outgoing unencrypted emails as the CISO team has to decide whether the email should be released or not.

4.2 How is the PII transmitted or disclosed internally?

PII is transmitted or disclosed internally through Microsoft Outlook, SharePoint, OneDrive, Teams, or file shares in DFCNet. PII may also be disclosed through individual DFCNet components. For example, the Ethics Office has access to the PII contained in Office of Government Ethics (OGE) Form 450, *Confidential Financial Disclosure Form*, which is electronically submitted by certain DFC employees annually through the FDonline Intelliworx component.

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 are employed across all DFCNet components. In addition, OIT conducts periodic scans of DFCNet repositories, and if PII is detected that should not be widely disseminated, the access to the PII will be closed off.

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?

As a general matter, non-sensitive PII from DFC personnel, which is typically found on a business card or email signature block, may be shared externally without restriction, but SPII requires stricter handling requirements. SPII shared externally must be compatible with the purpose for the collection. For example, information about a DFC employee's assets and income, liabilities, outside positions, and gifts and travel reimbursements from OGE Form 450, *Confidential Financial Disclosure Form*, is required to be shared with OGE as required by the Ethics in Government Act of 1978. This information is collected from employees and furnished to OGE to determine DFC's compliance with applicable federal conflict of interest laws and regulations.

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

Program offices may share PII with external organizations with written consent from the subject individual or in accordance with a routine use in the SORN, pursuant to a Memorandum of Understanding/Agreement, or to the extent required by law. The purpose for the disclosure must be compatible with the purpose for the collection as required by the Privacy Act and in alignment with the Fair Information Practice Principles.

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?

DFC personnel are only permitted to electronically share SPII with individuals outside the DFC network via encrypted email in Microsoft Outlook or by uploading the files to DFC's secure Box solution and inviting the external recipients to access the files as a collaborator. These methods of sharing are formally defined in the DFC memorandum titled *Transmitting Sensitive Data Outside the DFC Network* and are in place to prevent unsecure methods of transmission.

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 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, and driver's license numbers, from leaving the DFC network. DFC personnel must also sign the DFC Privacy Rules of Behavior, which include disciplinary measures for knowingly, willfully, or negligently 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?

DFCNet provides notice to DFC personnel before they log into the DFC network. The Privacy Notice is displayed below:

----------WARNING----------

> You are accessing a U.S. Government information system. By using this information system, you understand and consent to the following when you access this U.S. agency's information system which includes (1) this computer (2) this computer network, (3) all computers connected to this network, and (4) all devices and storage media attached to this network or to a computer on this network: This information system is provided for U.S. Government-authorized use only. Unauthorized or improper use of this system may result in disciplinary action, as well as civil and criminal penalties. The Government, acting directly or through its contractors, routinely monitors communications occurring on this information system. You have no reasonable expectation of privacy regarding any communications or data transiting, or stored on, or traveling to or from this information system. At any time, the government may for any lawful government purpose monitor, intercept, search, and seize any communication or data transiting, stored, or traveling to or from this information system, and any communications or data transiting, stored on, or traveling to or from this information system may be disclosed or used for

any lawful government purpose. Unauthorized use should be reported to the DFC CISO at ciso@dfc.gov.

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

No, individuals must consent to all terms of the DFCNet Privacy Notice before logging into the DFC network. While DFCNet does not inherently request PII from end users, it captures all end user actions to ensure that individuals are using the system lawfully.

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

Generally, no (see Section 6.2). However, it is up to each individual not to enter unnecessary PII into DFCNet if they do not want their information to be monitored.

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. DFCNet captures all end user actions to ensure that individuals are using the system lawfully. However, if DFC personnel do not consent to the uses of their information, they simply do not have to enter any information into DFCNet that they do not want to have monitored.

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?

DFCNet contains PII from internal sources (DFC employees and contractors) and external sources (members of the public). If an internal source wants to gain access to their own DFCNet system access logs, they can do so by reaching out to OIT and requesting access to their information.

To make a Privacy Act request for records in a system of records, 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?

Since system access logs are automatically captured by DFCNet, they are not able to be changed.

To make a Privacy Act amendment request on records in a system of records, 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 DFCNet. 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.

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. 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 can request access or correction of their information. For information not maintained in a system of records, individuals can reach out to the DFC official who took in their information to request access or correction of their information.

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 DFCNet 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. 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 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 and Authorization (A&A) has been completed for DFCNet by the CISO team. An authorization to operate (ATO) letter was signed by DFC and re-authorized 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 risk is partially mitigated. DFCNet is protected by best-in-class endpoint security, cutting edge artificial intelligence, Zero Trust solutions, multi-factor authentication, and DLP to identify threats to the DFC network and prevent data breaches from occurring.