Office of Information Technology (OIT)

Privacy Impact Assessment

DFCNet

August 19, 2022

1100 New York Ave NW
Washington, DC 20527

Section 1. Characterization of the Information

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

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

Identify and list all information in identifiable form that is collected and stored in the system. This could include, but is not limited to: name, date of birth, mailing address, telephone number, social security number, email address, zip code, facsimile number, mother's maiden name, medical record number, bank account number, health plan beneficiary number, any other account numbers, certificate/license number, vehicle identifier including license plate, marriage record, civil or criminal history information, device identifiers and serial numbers, uniform resource locators (URLs), education record, Internet Protocol (IP) addresses, biometric identifier, photographic facial image, or any other unique identifying number or characteristic.

The purpose of DFCNet is to provide the U.S. International Development Finance Corporation (DFC) with information technology (IT) systems, network connectivity, operating systems, and other IT resources in support of the agency's mission. DFCNet serves as the agency's IT General Support System (GSS). A GSS is an interconnected set of information resources under the same direct management control that shares common functionality. DFCNet's Information System Owner is the Office of Information Technology (OIT), whose office mission is to advance DFC's ability in driving global development impacts by providing reliable, innovative IT solutions.

DFCNet supports all DFC lines of business and includes but is not limited to on-premise storage (Nutanix and HP Network-attached Storage (NAS)), offsite backups in Microsoft Azure, email (Microsoft Outlook), Microsoft SharePoint, the Microsoft 365 suite of applications (Access, Excel, OneNote, PowerPoint, Project, Publisher, Visio, and Word), StaffCentral (a centralized repository used for collecting information about onboarding and separating employees in SharePoint), Office of Human Resources Management (OHRM) systems, HPE Content Manager (a records management system), and Salesforce.

Examples of offices and systems that use DFCNet to collect PII are:

- Office of Administration (OA) Corporate Security Team – Use to process Personal Identification Verification (PIV) cards (name, photograph, badge number, fingerprint, height, eye color)
- OA Corporate Travel Team – Use for overseas travel and U.S. passport processing (name, photograph, nationality, date of birth, sex, place of birth, signature, flight and lodging details)
- OA Corporate Travel Team – Use to process government purchase/travel charge card applications (name, Social Security number, mailing address, credit card number, signature)
- OHRM Team – Use for hiring and benefits processing (name, Social Security number, employment information, home address, emergency contact, signature, other HR and benefits forms)
- StaffCentral – A SharePoint repository used for collecting information on onboarding and separating employees (name, department, employee type, Entrance on Duty (EOD) date, emergency contact, security records, exit process records)

Due to the nature of DFCNet, users may collect, use, disseminate, or maintain personally identifiable information (PII) in numerous ways using the system. Users may store all types of electronic files in the system, which may include documents, forms, reports, correspondence, briefing papers, committee and meeting minutes, contracts,

grants, leases, permits, audits, manuals, studies, promotional materials, compliance information, and more. As such, there is a potential that large amounts of PII may be included in files contained within the system.

This Privacy Impact Assessment (PIA) discusses DFCNet's role in providing a secure IT platform for DFC staff to perform their duties, but it does not list every way in which users can collect, use, disseminate, or maintain PII within the system. The privacy risks discussed in this PIA are limited because DFCNet is not designed to collect PII but rather to provide the IT infrastructure needed by agency staff to perform their duties. Separate PIAs cover specific applications or user activities within DFCNet that collect, maintain, or disseminate information in identifiable form from or about members of the public or that initiate, consistent with the Paperwork Reduction Act, a new electronic collection of information in identifiable form from 10 or more persons (excluding agencies, instrumentalities, or employees of the federal government).

• If the system creates information (for example, a score, analysis, or report), list the information the system is responsible for creating.

Certain applications within DFCNet, such as Microsoft 365 or Salesforce Insight, allow users to perform analytical functions and create reports that calculate or summarize data based on assigned values or categories.

• If a requesting system receives information from another system, such as a response to a background check, describe what information is returned to the requesting system.

Certain applications within DFCNet, such as Microsoft 365 or Salesforce Insight, allow users to import data from external sources to enhance the reporting capabilities of their data.

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

• List the individual, entity, or entities providing the specific information identified above. For example, is the information collected directly from the individual as part of an application for a benefit, or is it collected from other sources such as commercial data aggregators?

OIT works with program offices and the Office of Administration to procure contracts with third-party vendors who provide the IT services that comprise DFCNet. DFC staff use the system's IT services to create information in line with the agency's mission or to perform essential activities that allow DFC to operate. In most cases, the information is taken directly from the individual, such as when collecting fingerprint samples to process PIV cards or processing employee time and attendance. In some cases, DFC may collect information about individuals from third-party sources, such as when reaching out to an employee's former agency to verify how much of their first paycheck to contribute to their Thrift Savings Plan retirement account or when conducting a background investigation on an employee who is applying for a security clearance. From a mission perspective, DFC may rely on public websites, such as Google, or commercial databases, such as LexisNexis, to conduct research on topics that affect the agency's decisions to invest in certain regions of the developing world. The use of public websites or commercial databases is generally not conducted on private individuals unless it is something as simple as using a vendor's website to identify a point of contact who could potentially help the agency fulfill a business need.

• Describe why information from sources other than the individual is required. For example, if a program's system is using data from a commercial aggregator of information or data taken from public Web sites, state the fact that this is where the information is coming from and then in question 1.3 indicate why the system is using this source of data.

Information from sources other than the individual is typically required to verify information about an employee or for the employee to obtain a benefit. OHRM may conduct reference checks during the hiring process to determine if a job applicant is truly qualified to take a position with the agency. If the agency decides to move forward in the hiring process, OHRM must reach out to an employee's former agency to determine any leave or benefits information that needs to be carried over. Background investigations also require interviews with third-party references to determine if an employee can be trusted to access classified information. To be approved for a government charge card, the bank providing the charge card typically obtains a credit report from one of the three major credit reporting agencies before extending a line of credit to the employee.

• If the system creates information (for example, a score, analysis, or report), list the system as a source of information.

Certain applications within DFCNet, such as Microsoft 365 or Salesforce Insight, allow users to perform analytical functions and create reports that calculate or summarize data based on assigned values or categories.

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

• Include a statement of why the particular information in identifiable form is collected, maintained, used, or disseminated in the system is necessary to the program's or agency's mission. Merely stating the general purpose of the system without explaining why this particular type of information should be collected and stored is not an adequate response to this question.

DFCNet provides a secure IT platform for DFC staff to perform their duties, which at times requires the processing of PII. As with all U.S. Government computer systems, DFCNet also contains system logs of user actions to ensure that government resources are not being used inappropriately.

• If the system collects, uses, disseminates, or maintains commercial data, include a discussion of why commercial data is relevant and necessary to the system's purpose.

Users of DFCNet may collect, use, disseminate, or maintain commercial data in the course of researching or creating studies on topics salient to DFC's mission, but commercial data is usually not used to collect information on private individuals.

1.4 How is the information collected?

• This question is directed at the means of collection from the sources listed in question 1.2. Information may be collected directly from an individual, received via electronic transmission from another system, or created by the system itself. Specifically, is information collected through technologies or other technology used in the storage or transmission of information in identifiable form?

DFCNet users collect the information electronically through any DFCNet application that captures text files, such as Microsoft Word, Excel, Outlook, etc., and the information is shared electronically through any DFCNet collaborative tool, such as SharePoint, OneDrive, Teams, etc. System logs of user actions are automatically generated on the back end of the system.

• If the information is collected on a form and is subject to the Paperwork Reduction Act, give the form's OMB control number and the agency form number.

DFCNet is not subject to the Paperwork Reduction Act because it does not collect PII from members of the public. Users of applications within the system are responsible for ensuring that their information collections have been reviewed by the agency clearance officer for specific requirements under the Paperwork Reduction Act.

1.5 How will the information be checked for accuracy?

• Explain whether information in the system is checked against any other source of information (within or outside your organization) before the information is used to make decisions about an individual. If not, explain whether your organization has any other rules or procedures in place to reduce the instances in which inaccurate data is stored in the system.

It is the responsibility of each DFCNet user to ensure the accuracy of the information they are collecting. Information that is provided by an individual is presumed to be accurate because it is collected directly from the source. In addition, certain forms within SharePoint contain fields that are pre-populated using verified information from StaffCentral.

• If the system checks for accuracy by accessing a commercial aggregator of information, describe this process and the levels of accuracy required by the contract.

Users may use commercial aggregators, such as Google, to ensure the accuracy of the information they are collecting. Checks for accuracy will be conducted in accordance with the specific needs of the activity.

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

• List the full legal authority for operating the system, specifically the authority to collect the information listed in question 1.1. Provide the authorities in a manner understandable to any potential reader, i.e., do not simply provide a legal citation; use statute names or regulations in addition to citations.

DFCNet's legal authority to operate 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.

Program offices that collect or store PII in DFCNet are required to provide legal authorities specific to their collections.

Section 2. Uses of the Information

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

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

• Identify and list each use (both internal and external to DFC) of the information collected or maintained.

All documentation and data files stored in DFCNet support DFC business in one form or another, whether they be financial deals, service desk support incidents, customer relationship management, transaction history, acquisitions, etc.

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

• Many systems sift through large amounts of information in response to a user inquiry or programmed functions. Systems may help identify areas that were previously not obvious and need additional research by agents, analysts, or other employees. Some systems perform complex analytical tasks resulting in, among other types of data, matching, relational analysis, scoring, reporting, or pattern analysis. Describe any type of analysis the system conducts and the data that is created from the analysis.

Data analysis is initiated in several ways. Splunk, 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, or unusual, user behavior. The CISO team also responds to Freedom of Information Act requests and performs investigations on employees or systems when needed to investigate potential fraud, waste, or abuse. Further, the CISO Team can run queries using key words in Outlook, SharePoint, OneDrive, etc.

• If the system creates or makes available new or previously unutilized information about an individual, explain what will be done with the newly derived information. Will it be placed in the individual's existing record? Will a new record be created? Will any action be taken against or for the individual identified because of the newly derived data? If a new record is created, will the newly created information be accessible to Government employees who make determinations about the individual? If so, explain fully under which circumstances and by whom that information will be used.

• This question may be related to questions 1.1 and 1.2 which, among other things, are intended to capture information created by the system.

DFCNet does not make available new or previously unutilized information about an individual, but system log audits do occur. The CISO Team can perform investigations on individuals who use the system in line with the agency's Information System Rules of Behavior and the System Consent to Use Notification Banner, which states, "DFC may monitor or audit any activity or communication on the system and retrieve any information stored within the system." Based on the individual circumstances of the investigation, evidence of misuse may be placed in the individual's existing record or used in other disciplinary procedures.

2.3 If the system uses commercial or publicly available data, explain why and how it is used. This response should explain the following:

• If commercial data or publicly available data (open source) is directly or indirectly used, provide information on those uses in this section.

Users may use commercial data or publicly available data to verify information about individuals, but they should not be used as a primary source of information.

• If a program, system, or individual analyst uses commercial data or publicly available data, provide information on it here.

Users may use commercial data or publicly available data to verify information about individuals, but they should not be used as a primary source of information.

• *If commercial data or publicly available data is used to verify information already maintained by DFC, provide information on it here.*

Users may use commercial data or publicly available data to verify information about individuals, but they should not be used as a primary source of information.

• *If new information previously not maintained by DFC is brought from an outside source, whether commercial or not, provide information on it here.*

Users may use commercial data or publicly available data to verify information about individuals, but they should not be used as a primary source of information.

Section 3. Retention of Information

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

3.1 What information is retained?

• *Identify and list all information collected from question 1.1 that is retained by the system.*

The information that is retained must be necessary and relevant to fulfill a business need. This information varies based on the needs of the program office that is collecting the information.

3.2 How long is information retained?

• *In some cases DFC may choose to retain files in active status and archive them after a certain period of time. State active file retention periods as well as archived records, in number of years, as well as the General Records Schedule. The DFC records officer should be consulted early in the development process to ensure that appropriate retention and destruction schedules are implemented.*

Retention periods for records stored in DFCNet vary depending on the types of records being collected. It is the responsibility of each DFCNet user to ensure that their records are being retained in accordance with an approved National Archives and Records Administration (NARA) records retention schedule.

Emails: User emails are managed under a Capstone approach in accordance with NARA General Records Schedule (GRS) 6.1. The following email retention periods apply:

- 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.

Backups: All DFC data files are stored in on-premise Nutanix and HP NAS systems and offsite in Azure cloud storage. Files are backup up daily and weekly (only a couple of shares are set up with weekly backups) and retained for eight weeks. In addition, files stored in Azure are backed up monthly, which are archived for 13 months, and yearly, which are archived for 10 years. These retention periods are in line with NARA GRS 3.2, Item 30 - System Access Records, which states that records that are used to monitor inappropriate systems access by users are temporary and should be destroyed when business use ceases.

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

• An approved records schedule must be obtained for any IT system that allows the retrieval of a record via a personal identifier. The DFC records officer will assist in providing a proposed schedule. The schedule must be formally offered to NARA for official approval. Once NARA approves the proposed schedule, the DFC records officer will notify the system owner.

The retention schedules mentioned in question 3.2 above have been approved by the DFC Records Officer and NARA.

Section 4. Internal Sharing and Disclosure

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

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

• The term "internal" means program offices, contractor-supported IT systems, and any other organization or IT system within DFC. This question is directed at the sharing of information internally within DFC.

Users share information internally with staff in their program offices on a need-to-know basis.

• Identify and list the names of any program offices, contractor-supported IT systems, and any other organization or IT system within DFC with which information is shared.

The internal organizations with which the information is shared vary based on the purpose for the collection and the needs of the agency, such as whether a collection is part of an inter-office project that requires collaboration between departments.

• State the purpose for the internal sharing. If you have specific authority to share the information, provide a citation to the authority.

Each program office that collects PII does so for a specific business purpose. Internal sharing is permitted on a need-to-know basis. For information that is collected as part of a system of records, there is a requirement to

provide a Privacy Act Statement at the point of collection, which includes the specific authority to collect the information and with whom the information will be shared.

• For each interface with a system outside your program office, state what specific information is shared with the specific program office, contractor-supported IT system, and any other organization or IT system within DFC.

Each DFC department has its own department file share with access rights limited to only those department members. Within SharePoint, each department has a SharePoint site where they can grant access to individuals on a need-to-know basis. Different departments often collaborate on a task or project, and these documents can be shared in SharePoint or other collaboration tools with members of other departments. Information can also be shared internally using the agency's external Box.com account.

4.2 How is the information transmitted or disclosed?

• Describe how the information is transmitted to each program office, contractor-supported IT system, and other organization or IT system listed in question 4.1.

Information is transmitted electronically via DFC email, network file share access, SharePoint, OneDrive, or Teams. Paper printouts can also be shared internally. The only method for sharing data using an external method is through the agency's Box.com account.

• For example, is the information transmitted electronically, by paper, or by some other means? Is the information shared in bulk, on a case-by-case basis, or does the sharing partner have direct access to the information?

Information is typically shared electronically on a case-by-case basis.

• If specific measures have been taken to meet the requirements of OMB Memoranda M- 06-15 and M-06-16, note them here.

Physical, technical, and administrative safeguards have been implemented to ensure that agency data is shared securely. All DFCNet data is stored behind locked doors that require physical keycard access. Information may only be taken off DFCNet using a secure transmission method. DFC requires that all USB flash drives be encrypted with Bitlocker or another Federal Information Processing Standards (FIPS) 140-3 certified cryptographic module before being granting write access. Users may also transfer data off DFCNet using the agency's secure Box.com account or via an encrypted email attachment. Employees and contractors must take annual privacy awareness training and security training, which instruct users on the need to protect agency data and provide best practices for handling sensitive data.

Section 5. External Sharing and Disclosure

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

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

• The term "external" means other departments, agencies, and organizations that are not part of DFC. This could be other departments, law enforcement and intelligence agencies, the private sector, and State and local entities.

This question is directed at sharing information with other agencies, as well as with private entity and State or local governments.

Program offices that retrieve records by personal identifier must abide by the routine uses in their SORN, which list the external entities with whom the information can be shared and for what reason.

- *Identify and list the names of any Federal, State, or local government agency or private sector organization with which information is shared.*

The list of Federal, State, or local government agencies or private sector organizations with whom the information can be shared varies depending on the SORN used.

- *If a system of records notice (SORN) has been published for the system, summarize the most relevant routine uses. For example, if the system provides full access to another agency for their use of the information, include it in the summary. An example of a less relevant routine use listed in the SORN that does not need to be included in this summary would be that the system does not regularly handle requests from Congressional members.*

The most relevant routine uses vary depending on the SORN used.

- *For each interface with a system outside DFC, state what specific information is shared with each specific partner.*

Program offices that retrieve records by personal identifier are responsible for knowing what specific information is shared with which partners if there is an interface with a system outside DFC.

- *Where you have a specific authority to share the information, provide a citation to the authority and statute name.*

Program offices that retrieve records by personal identifier are responsible for having a specific authority to share the information externally.

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

- *What legal mechanisms, authoritative agreements, documentation, or policies are in place detailing the extent of the sharing and the duties of each party?*

Program offices that share information outside the agency are responsible for doing so only if the sharing is compatible with the original purpose for the collection and if legal mechanisms, authoritative agreements, documentation, or polices are in place detailing the extent of the sharing and the duties of each party.

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

- *Indicate the name of the SORN and briefly describe the routine use from the applicable SORN.*

Program offices are responsible for only sharing information outside the agency pursuant to a routine use in the SORN.

• If a memorandum of understanding (MOU) or other formal agreement is not in place, is the sharing covered by a routine use in the SORN and does it comply with the routine uses? If not, explain the steps being taken to address this omission.

Program offices should have a memorandum of understanding or other formal agreement in place for sharing information with external entities. At a minimum, the program office should provide a disclosure letter to the recipient that contains conditions on whether additional sharing of the information is permitted.

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

• Is the information shared in bulk, on a case-by-case basis, or does the organization have direct access to the information?

Any information shared outside the agency is typically done on a case-by-case basis and must be sent securely through the agency's Box.com account, via an encrypted email attachment, or, on occasion, using a FIPS 140-3 certified USB flash drive. The organizations with whom the information is shared usually have direct access to the information.

• Describe how the information is transmitted to entities external to DFC and whether it is transmitted electronically, by paper, or by some other means.

Information is transmitted to entities external to DFC through the agency's Box.com account, via an encrypted email attachment, or, on occasion, using a FIPS 140-3 certified USB flash drive.

• If specific measures have been taken to meet the requirements of OMB Memoranda M- 06-15 and M-06-16, note them here.

Physical, technical, and administrative safeguards have been implemented to ensure that agency data is shared securely. All DFCNet data is stored behind locked doors that require physical keycard access. Information may only be taken off DFCNet using a secure transmission method. DFC requires that all USB flash drives be encrypted with Bitlocker or another FIPS 140-3 certified cryptographic module before being granted write access. Users may also transfer data off DFCNet using the agency's secure Box.com account or via an encrypted email attachment. Employees and contractors must take annual privacy awareness training and security training, which instruct users on the need to protect agency data and provide best practices for handling sensitive data.

• Any sharing conducted per a routine use in the applicable SORN should be transmitted in a secure manner. Additionally, if information is shared under an MOU, memorandum of agreement (MOA), or similar formal agreement, describe whether and how the agreement requires secured transmission and storage of shared data.

Program offices should have a memorandum of understanding or other formal agreement in place for sharing information with external entities. At a minimum, the program office should provide a disclosure letter to the recipient that contains conditions on whether additional sharing of the information is permitted.

Section 6. Notice

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

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

• This question is directed at the notice provided before collection of the information. This refers to whether the person is aware that his or her information is going to be collected. A notice may include a posted privacy policy, a Privacy Act statement on forms, or a SORN published in the Federal Register. If notice was provided in the Federal Register, provide the citation.

DFCNet provides notice before the individual logs in to the DFC network. All users must accept the System Consent to Use Notification Banner before accessing DFC systems. A user will not be granted access to DFCNet, or DFC systems, if they do not accept the terms of the notice. In addition, all users must complete annual privacy awareness training and security training and electronically agree to the DFC Information Systems Rules of Behavior, which inform users that there is not expectation to privacy while using the system. Any user or program office that collects PII as part of a system of records must also provide a Privacy Act Statement at the point of collection informing individuals of the authority for the collection, the purpose of the collection, routine uses for external sharing, and whether the providing the information is mandatory or voluntary.

• If notice was not provided, explain why. If it was provided, attach a copy of the current notice.

N/A; DFCNet provides notice before the individual logs in to the DFC network, and a Privacy Act Statement is required at the point of collection for any information that will go into a system of records.

• Describe how the notice provided for the collection of information is adequate to inform those affected by the system that their information has been collected and is being used appropriately. Provide information on any notice provided on forms or on Web sites associated with the collection.

DFCNet provides a System Consent to Use Notification Banner before logging in to the DFC network that states, "DFC may monitor or audit any activity or communication on the system and retrieve any information stored within the system." In addition, a Privacy Act Statement is required at the point of collection for any information that will go into a system of records.

• The issue of notice, particularly notice found in a SORN, involves the advice of counsel. Consult your assigned counsel on issues concerning the sufficiency of notice to the public on an information collection.

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

• This question is directed at whether the person from or about whom information is collected can decline to provide the information and if so, whether a penalty or denial of service is attached.

To access DFCNet, an individual must consent to all the terms of the System Consent to Use Notification Banner before logging in to the DFC network. If the individual declines to accept the terms of the notice, then the individual will not be allowed access to the DFC network.

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

• This question is directed at whether an individual may provide consent for specific uses or the consent is given to cover all uses (current or potential) of his or her information. If specific consent is required, how would the individual consent to each use?

To access DFCNet, an individual must consent to all the terms of the System Consent to Use Notification Banner before logging in to the DFC network. There is not an option for the individual to consent to particular uses of the information.

Section 7. Access, Redress, and Correction

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

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

• Cite any procedures or regulations your program has in place that allow access to information. These procedures, at a minimum, should include the agency's FOIA/Privacy Act practices, but may also include additional access provisions. For example, if your program has a customer satisfaction unit, that information, along with phone and email contact information, should be listed in this section in addition to the agency's procedures.

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 a proper verification of identity (22 CFR Part 707). Alternatively, a requester may address the request to the system manager that is provided in the SORN.

• If the system is exempt from the access provisions of the Privacy Act, please explain the basis for the exemption or cite the source where this explanation may be found, for example, a Final Rule published in the Code of Federal Regulations (CFR).

While DFCNet is considered a privacy-sensitive system, it is not a Privacy Act system because it does not collect PII from which records are retrieved by personal identifier. Rather, the tools within the system allow users to collect information that may go into a Privacy Act system. DFCNet simply provides the IT platform for DFC staff to use to perform their duties.

• If the system is not a Privacy Act system, please explain what procedures and regulations are in place that covers an individual gaining access to his or her information.

Requests for access to a user's own DFCNet system logs may be made by contacting the Information System Owner or the Privacy Data Officer.

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

• Describe the procedures and provide contact information for the appropriate person to whom such issues should be addressed. If the correction procedures are the same as those given in question 7.1, state as much.

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 access must comply with DFC's Privacy Act regulations regarding what information to include in the amendment request and provide proper verification of identity (22 CFR Part 707). Alternatively, a requester may address the request to the system manager that is provided in the SORN.

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

• How is an individual made aware of the procedures for correcting his or her information? This may be through notice at collection or other similar means. This question is meant to address the risk that even if procedures exist to correct information, if an individual is not made fully aware of the existence of those procedures, then the benefits of the procedures are significantly weakened.

This PIA provides notice to individuals on how to correct their information. Additional notice is provided by DFC's Privacy Act regulations and the published SORNs covering the various types of records that are processed through DFCNet.

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

• Redress is the process by which an individual gains access to his or her records and seeks corrections or amendments to those records. Redress may be provided through the Privacy Act and Freedom of Information Act (FOIA), and also by other processes specific to a program, system, or group of systems.

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

Section 8. Technical Access and Security

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

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

• Describe the process by which an individual receives access to the system.

After the Security Team clears an individual to start working, the OHRM Team adds the employee to StaffCentral with an EOD date. Once the employee attends new employee orientation, they must complete mandatory training courses in FedTalent, DFC's learning and management system, to receive access to the system. New employees are assigned the DFC New Employee Orientation (NEO) Onboarding Program in their FedTalent account. The DFC NEO Program has eight courses that must be completed in the employee's first week. Four courses must be completed within the individual's first two days of employment at DFC: 1) DFC Privacy Training – NEO, 2) DFC Rules of Behavior – NEO, 3) Insider Threat Awareness, and 4) Cybersecurity – NEO. The last four courses must be completed by the end of the employee's first week at DFC: 5) Records & Management (RIM) Overview, 6) No Fear

Act – NEO, 7) The Plain Writing Act, and 8) The U.S. Constitution. If a user does not complete their training within their allotted time, then their access privileges will be revoked until the training is completed.

• Identify users from other agencies who may have access to the system and under what roles these individuals have access to the system.

N/A; users from other agencies do not have access to DFCNet unless they are on detail from another agency.

• Describe the different roles in general terms that have been created to provide access to the system. For example, certain users may have "read-only" access while others may be permitted to make certain amendments or changes to the information.

DFCNet has two types of users: 1) regular users with read/write access to their personal and department data, and 2) Administrators. Administrators may have a variety of permissions depending on their role. DFC implements a "principle of least privilege" model in which a user account only has access to the information necessary to execute the user's official responsibilities.

8.2 Will DFC contractors have access to the system?

• If so, how frequently are contracts reviewed and by whom? Describe the necessity of the access provided to contractors to the system and whether clearance is required.

A large percentage of DFC's IT Support Team is comprised of contractors. Contractor accounts are reviewed on an annual basis or as needed. DFCNet administrator accounts are reviewed every two months. The IT Support Team monitors account inactivity, and a DFCNet Administrator account with 14 days of inactivity is disabled.

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

• DFC offers privacy and security training. Each program or system may offer training specific to the program or system that touches on information handling procedures and sensitivity of information. Please describe how individuals who have access to PII are trained to handle it appropriately.

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

8.4 Has A&A been completed for the system?

• If so, provide the date the Authority to Operate (ATO) was granted. Please note that all systems containing PII are categorized at a minimum level of "moderate" under Federal Information Processing Standards Publication 199.

Assessment and Authorization was completed for DFCNet. An Authorization to Operate was granted by DFC on June 18, 2019.