U.S. International Development Finance Corporation

Privacy Impact Assessment (PIA)

Office of Information Technology
U.S. International Development Finance Corporation (DFC)
1100 New York Ave, N.W.
Washington, DC 20527

Overview

Date of Submission:	01/22/2021
System Owner:	John Glaser
Department(s):	OIT/Technical Services
Title of the System:	DFCNet (formally, OPICNET)
Is this system or information collection new?	Yes

PIA Approval

I have reviewed the DFCNet Privacy Impact Analysis (PIA) and concur with the information presented below.

MARK REIN Digitally signed by MARK REIN
DN: c=US, o=U.S. Government, ou=Overseas Private Investment Corporation, cn=MARK REIN, 0.9.2342.19200300.100.1.1=71001003107466
Date: 2021.02.10 14:48:09 -05'00'

Senior Agency Official for Privacy (SAOP) Date

Digitally signed by JOHN GLASER
Date: 2021.01.27 13:23:13 -05'00'

DFCNet System Owner Date

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 addresses, biometric identifier, photographic facial image, or any other unique identifying number or characteristic.

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

- DFCNet serves as the Information Technology (IT) General Support System (GSS) that supports all DFC lines of business, including but not limited to, on premise storage (Nutanix), backups in Azure, O365 email, SharePoint, O365 Microsoft Office Suite of applications, Visitor registration, Staff Central

(onboarding and offboarding employees in SharePoint), HR systems, Records management (HPECM), Salesforce, etc.

- DFCNet's primary mission is not to collect personally identifiable privacy information (PII). The purpose of DFCNet is to provide IT systems, network connectivity, operating systems and other IT resources to support DFC's mission.
- DFC systems do not create or analyze PII information. Many DFC systems do capture, record, or store PII information. These DFC systems and departments that collect PII information are:
    - Staff Central _used for onboarding employees and contractors.
    - The Security team - when requesting PIV cards
    - The DMA Travel team – for overseas travel and passports
    - The DMA Acquisition team – for travel and purchase credit cards
    - The HRM team – for hiring and benefits

• 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.

- N/A for DFCNet GSS

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?

- During hiring process, new employee record is added to staff central. DFC net directly receives needed information from staff central.

• 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.

- N/A

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

- DFC systems do not create or analyze PII information. Many DFC systems do capture or store PII information. These DFC systems and departments that collect PII information are:
    - Staff Central _used for onboarding employees and contractors.
    - The Security team - when requesting PIV cards
    - The DMA Travel team – for overseas travel and passports
    - The DMA Acquisition team – for travel and purchase credit cards
    - The HRM team – for hiring and benefits

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.

- PII is used to verify an individual's identity when they onboard and receive an DFC account, when they apply for government benefits, when they receive a PIV card for access to DFC space, when requesting travel or purchase cards, passports, and when mailing them IT equipment.

• 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.

- N/A

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?

- Information is typically collected directly from the individual and shared electronically.

• 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.

The DFC Privacy program provides this control to DFCNet system. For further information please reach out to DFC Privacy Program.

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.

- Employee's show state issued photo ID or passport prior to onboarding and orientation. No other checks for accuracy are executed.

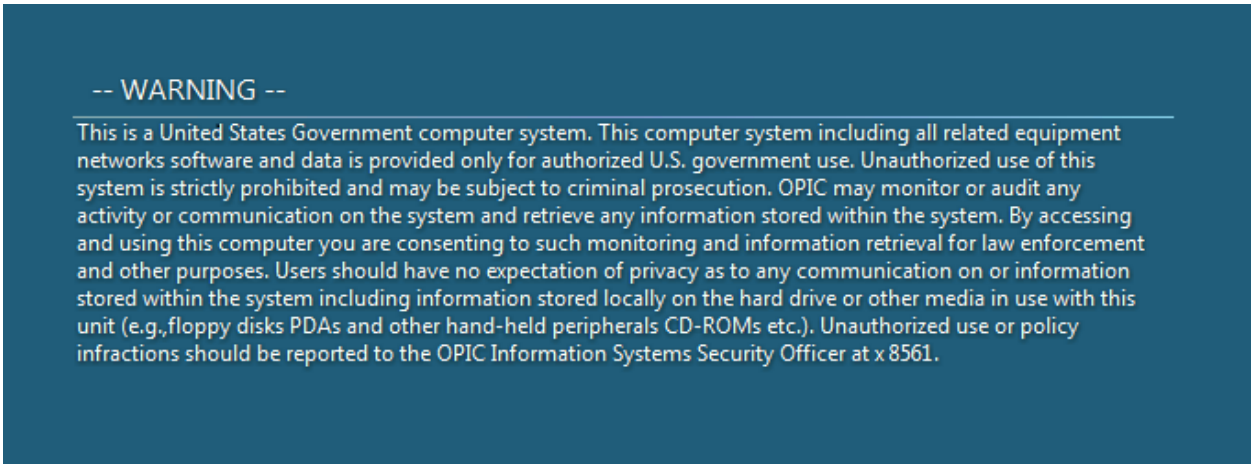
• If the system checks for accuracy by accessing a commercial aggregator of information, describe this process and the levels of accuracy required by the contract.

- Data is not checked for accuracy by a commercial aggregator.

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.

- Per DFC policy, see screen print of warning message that is displayed upon access DFC systems:



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 on DFC systems support DFC business in some form or another. Whether with 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.*

· *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.*

- Data analysis is initiated in several ways. Splunk, a security tool managed by the CISO team receives syslogs from key systems in the environment to analyze account and system access and to identify asymmetrical behavior.
- The DFCNet CISO team also responds to FOIA requests and to perform investigations on employees or systems.
- The DFCNet CISO team also has the ability to run queries using key words in email, SharePoint, OneDrive, etc., within the Office 365 portal

• 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.

Response: Security tools, Office 365 DMV tool

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.

- N/A

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

- N/A

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

- N/A

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

- Whenever during O&M, new information previously not maintained by DFC is brought from an outside source, whether commercial or not, new information is evaluated and assessed. DFC Net system owners ensure to adhere to the DFC Privacy program and change management policy and procedures.

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.

- DFCNet serves as the Information Technology (IT) General Support System (GSS) that supports all DFC lines of business, including but not limited to, on premise storage (Nutanix), backups in Azure, O365 email, SharePoint, O365 Microsoft Office Suite of applications, Visitor registration, Staff Central (onboarding and offboarding employees in SharePoint), HR systems, Records management (HPECM), Salesforce, etc.
- DFCNet's primary mission is not to collect personally identifiable privacy information (PII). The purpose of DFCNet is to provide IT systems, network connectivity, operating systems and other IT resources to support DFC's mission.
- DFC Net system do not create or analyze PII information. DFC systems (Major or Minor applications) residing within the DFC Net System (GSS) do capture, record or store PII 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.

- User email is retained in O365 using the following parameters:
    - Each user with a DFC email mailbox is allocated 50GB for inbox online storage space.
    - Email attachments have a 25MB size limitation, sending & receiving
- Online Archived Email (Archived email has 100GB storage)
- A user's email will be archived if any of the following conditions occur:
    - The user manually marks an email to be archived
    - The email is at least two years old
    - The user's mailbox exceeds the allocated 50GB of online space.

- Excess Email

  If a user's archived mail exceeds the 100GB limit, the email system will automatically delete the oldest emails first until the mailbox is below the 100GB limit. Deleted emails are not recoverable.

- All DFC data files are stored in an on-prem HP NAS storage using the following retention policies:

HP NAS

- Daily is 8 weeks.
- Weekly is 8 weeks (only a couple of shares are setup with weekly backups)
- And backed up to Azure Cloud Storage using the following retention policies:

Azure

- Daily is 8 weeks.
- Weekly is 8 weeks (only a couple of shares are setup with weekly backups)
- Monthly backups are archived for 13 months.
- Yearly backups are archived for 10 Years.

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 DFC Records management program provides this control to DFC Net system. For further information please reach out to DFC Record management program via email.

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.

- The Security team and the Human Resources (HRM) share PII and security background info data when an employee is onboarding. Also, the travel team may coordinate with HRM for passport and travel/purchase card information.

• 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.

- Staff Central, E2 Travel, Fed Talent, Department network file shares

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

- The DFC security and Privacy program provides this control to DFC Net system. For further information please reach out to DFC Security and Privacy Program.

• 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 department has their own department file share with access rights limited to only those department members. Within SharePoint, each department has a SharePoint site where they can share information that is available for the entire agency.
- Different departments often collaborate on a task or project and these documents can be shared in SharePoint and specific access can be assigned to members of different departments.
- We also have BOX, where we can share data with external entities using a variety of restrictions.

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.

- Electronically

• 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?

- Electronically and on a case-by-case basis. Data files can be shared electronically via email, network file share access, SharePoint, OneDrive, Teams, etc. Paper printouts can also be shared. The only method for sharing data with external entities is using BOX. DFC staff can share data files via Box for collaboration, send a link to either upload or download a document. DFC also has the ability to place an expiration period of the shared link, so the data will be inaccessible after a specified period of time.

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

- Data files can be shared electronically via email, network file share access, SharePoint, OneDrive, Teams, etc. Paper printouts can also be shared.

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.

- DFC Net GSS does not share any information with external organizations. HRM hosted within the DFCnet GSS receives and shares information with OPM. OPIC/DFC used USAID as the Inspector General for auditing purposes.

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

- DFC Net GSS does not share any information with external organizations.

- HRM hosted within the DFCnet GSS receives and shares information with OPM. OPIC/DFC used USAID as the Inspector General for auditing purposes.
    - Office of Personnel Management
    - Office of the Inspector General
    - United States Agency for International Development

• 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.

- N/A

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

- N/A

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?

- N/A for DFCNet GSS
  DFC is in process of developing a governance policy for the use of BOX for document sharing with external entities.

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.

- N/A for DFCNet GSS

• 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.

- N/A for DFCNet GSS

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?

- N/A for DFCNet GSS
  Typically, data is shared electronically on a case-by case basis. Those individuals who are granted permissions have direct access.

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

- N/A for DFCNet GSS
  Electronically via BOX, or on occasion, an encrypted flash drive may be used.

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

- N/A for DFCNet GSS
  All DFC laptops have Bitlocker installed, approved flash drives are Kingston DataTraveler FIPs 140-2 level 3 encryption, Intune enforces iOS/iPadOS device-level encryption on DFC GFE mobile phones.

• 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.

- N/A for DFCNet GSS
  DFC plan to implement Cloud Lock, which monitors traffic flowing to/from Box. DFC had the same security measures configured for Dropbox. The tool can scan and identify files for PII, but no automated process is in place to block or quarantine PII data.

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.

- All Employees receive a security and ethics briefing during orientation that covers privacy disclosures.

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

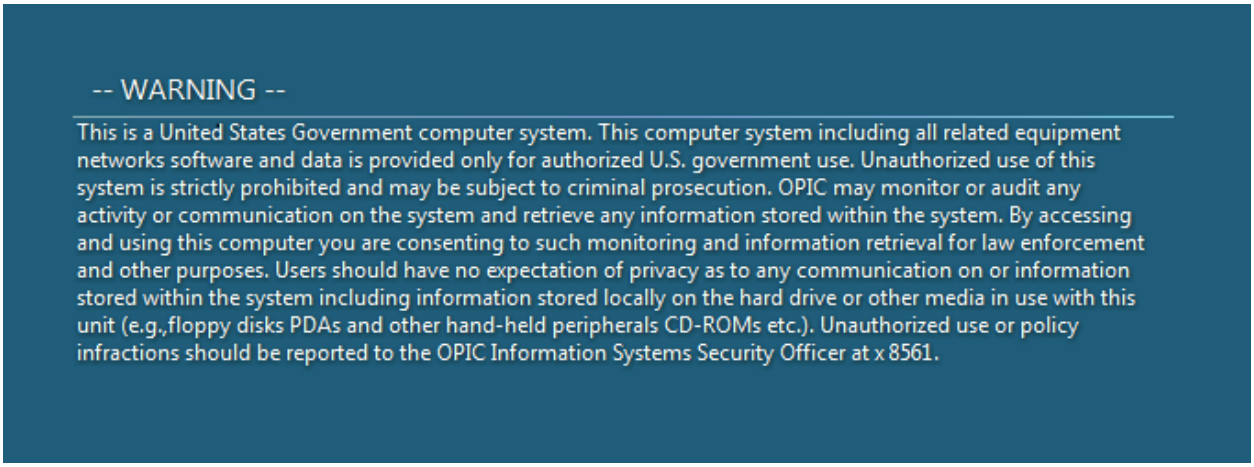
- N/A

• 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.

- During onboarding, at employee orientation, privacy data is discussed.

• 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.

- Per DFC policy, see screen print of warning message that is displayed upon access DFC systems. All users must accept this policy statement before accessing DFC systems.



- A user cannot be granted access to DFCNet, or DFC systems if they do not accept the terms of agreement for the agency and complete the following required training sessions:
    - DFC Rules of Behavior,
    - DFC Cyber Security Awareness
    - DFC Privacy training
- All training sessions are required before a user is granted access to DFCNet. Training sessions are required on an annual basis.
- DFC staff is provided with a H drive personal network share drive and a OneDrive to store person documents. Department network file shares and SharePoint sites are also provided for shared data files and for collaboration. If data appears to have changed, a file or folder restoration can be requested from a daily, weekly or monthly backup.

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.

- A user cannot be granted access to DFCNet, or DFC systems until they accept the terms of agreement for the agency and complete the following mandatory training sessions:
    - DFC Rules of Behavior,

    - DFC Cyber Security Awareness
    - DFC Privacy training
- All training sessions are required before a user is granted access to DFCNet. Training sessions are required on an annual basis.

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?

- All data stored on DFC systems is owned by DFC is an is considered government property. A privacy officer may be able to provide additional information in terms of consent.

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.

- An employee cannot be granted access to DFCNet, or DFC systems until they accept the terms of agreement for the agency and complete the following mandatory training sessions:
    - DFC Rules of Behavior,
    - DFC Cyber Security Awareness
    - DFC Privacy training

• 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).

- There are no exceptions, all users must complete required mandatory trainings.

• 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.

- The DFC security and Privacy program provides this control to DFCNet system. For further information regarding FOIA, please reach out to DFC Security and Privacy Program via email

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.

- Staff Central is DFC's is a source of authority for account information. And if an error is discovered in relation to a any information. HR representative will correct the information in Staff Central. DFC Net POC

will update the correct information in Active Directory and in HR systems. This is achieved via service desk tickets.

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.

- Agency wide changes are communicated via the SharePoint Notice System, or by sending notices to DFC All distribution group. If there is a change that impacts one employee, a appropriate party will notify the employee directly.

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.

- If data appears to have changed, a file or folder restoration can be requested from a daily, weekly or monthly backup.

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 validates the employees required background, security clearance or security reciprocity, the HRM team adds the employee to Staff Central with an onboarding date. Once the employee onboards and participates in orientation then they must complete the following mandatory training sessions before being granted access to DFC systems.
    - DFC Rules of Behavior,
    - DFC Cyber Security Awareness
    - DFC Privacy training
- For administrators, they must complete a Privileged User training session and complete a MyForms Admin Request form to obtain proper approvals before being granted elevated access.

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

- DFC does not grant access to users from external agencies

• 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.

- A user cannot be granted access to DFCNet, or DFC systems until they accept the terms of agreement for the agency and complete the following mandatory training sessions:
    - DFC Rules of Behavior,
    - DFC Cyber Security Awareness
    - DFC Privacy training
- All training sessions are required before a user is granted access to DFCNet. Training sessions are required on an annual basis.
- DFC does not allow access to employees from other agencies. Only DFC employees with a DFC account can be granted access to DFCNet.
- DFC has two types of users, 1. regular users with read/write access to their own personal and department data and 2. Administrators. Administrators can have a variety of permissions depending on their role. DFC does implement a least privilege access model. The CISO team does have "read only" access to many of our infrastructure systems, i.e., O365 and Azure.

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 our IT support team is comprised of contractors. Contractors accounts are reviewed on an annual basis or as needed. Administrator accounts are reviewed every two months. We do monitor account inactivity and an admin 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.

- All employees must accept the terms of agreement for the agency and complete the following mandatory training sessions:
    - DFC Rules of Behavior,
    - DFC Cyber Security Awareness
    - DFC Privacy training
- All training sessions are required before a user is granted access to DFCNet. Training sessions are required on an annual basis.

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.

DFC Net ATO: 06/18/2019