

PRIVACY IMPACT ASSESSMENT

(Rev. 2/2020) (All Previous Editions Obsolete)

Please submit your responses to your Liaison Privacy Official. *All entries must be Times New Roman, 12pt, and start on the next line*. If you need further assistance, contact your LPO. A listing of the LPOs can be found here: https://usepa.sharepoint.com/:w:/r/sites/oei Community/OISP/Privacy/LPODoc/LPO%20Roster.docx

System Name: Region 7 LAN (R07 Daily Flex Schedule)	System Owner: Randy Downs (R7 ISO)
Preparer: Randy Downs	Office: R7/MSD/R7IT
Date: 1/22/2021	Phone: 913-551-7505
Reason for Submittal: New PIA_X_ Revised PIA Annual Review_ Rescindment	
This system is in the following life cycle stage(s):	
Definition \square Development/Acquisition \square Implementation \square	
Operation & Maintenance ⊠ Rescindment/Decommissioned □	
Note: New and Existing Systems require a PIA annually, when there is a significant modification to the system or where privacy risk has increased to the system. For examples of significant modifications, see OMB Circular A-130 , Appendix 1, Section (c) (1) (a-f).	
The PIA must describe the risk associated with that action. For assistance in applying privacy risk see OMB Circular No. A-123 , Section VII (A) (pgs. 44-45).	

Provide a general description/overview and purpose of the system:

The Region 7 LAN (R07LAN) is a local area data and voice general support system (GSS) which provides connectivity and central control of all data processing, telecommunications, electronic mail and internet functions of Region 7. It was developed in 1998 and has been operational since 1998. R07LAN is comprised of file servers, routers, switches and infrastructure that provide Region 7 personnel voice/data, email, file sharing, development and collaboration services. It supports agency administrative functions, document storage and retrieval, emergency response, scientific calculations and modeling and GIS modeling and graphing. It is also used to maintain regional programs environmental databases and an environmental sample analyses database.

Contained within the R07LAN system is the R7 Daily Flexible Schedule (DFS) system. This information

is collected because the EPA time keeping system of record does not have the capability of tracking credit time in by-the-minute intervals. As such this system was developed to track the time for employees' intra-pay period, and at the end of each pay period the information is transposed to the official time keeping system.

Section 1.0 Authorities and Other Requirements

1.1 What specific legal authorities and/or Executive Order(s) permit and define the collection of information by the system in question?

DFS is a system contained within the R07LAN. Per 5 U.S.C 63 – LEAVE (United States Code, 2006 Edition, Supplement 5, Title 5 - GOVERNMENT ORGANIZATION AND EMPLOYEES, Part III – Employees, Subpart E – Attendance and Leave, Chapter 63 – LEAVE, Sections 6301 to 6391) – DFS system collects Employee Name, Pay Period / Date, Employee Time in/ Time Out, Accrued and earned Credit hours, Employee LAN ID, Employee ID, Employee Request for Credit, Manager Approval for Time/ Credit. This information is the same as information tracked under the People Plus SORN.

1.2 Has a system security plan been completed for the information system(s) supporting the system? Does the system have or will the system be issued an Authorization-to-Operate? When does the ATO expire?

Yes, a system security plan has been completed. The current ATO expires 9/30/2022.

- 1.3 If the information is covered by the Paperwork Reduction Act (PRA), provide the OMB Control number and the agency number for the collection. If there are multiple forms, include a list in an appendix.

 No ICR required.
- 1.4 Will the data be maintained or stored in a Cloud? If so, is the Cloud Service Provider (CSP) FedRamp approved? What type of service (PaaS, IaaS, SaaS, etc.) will the CSP provide?

Section 2.0 Characterization of the Information

No.

The following questions are intended to define the scope of the information requested and/or collected, as well as reasons for its collection.

2.1 Identify the information the system collects, uses, disseminates, or maintains (e.g., data elements, including name, address, DOB, SSN).

The Region 7 Daily Flexible Schedule (DFS) with Credit Tracking contained with the R07LAN collects the following: Employee Name, Pay Period / Date, Employee Time in/ Time Out, Accrued and earned Credit hours, Employee LAN ID, Employee ID, Employee Request for Credit, Manager Approval for Time/ Credit. This information is the same as information tracked under the People Plus SORN.

2.2 What are the sources of the information and how is the information collected for the system?

Only two sources for information are created in the DFS system. Employee general information is added when they are given access to the system. Employee time and requests for credit time are entered by the employee. Employee approval for time and credit are entered by managers. The information is entered by the employee, or the employee's manager.

2.3 Does the system use information from commercial sources or publicly available data? If so, explain why and how this information is used. No

2.4 Discuss how accuracy of the data is ensured.

The information in the DFS system is validated against the information in People Plus the official timekeeping system of record. Discrepancies are corrected in the corresponding system, managers are the determining official.

2.5 Privacy Impact Analysis: Related to Characterization of the Information

Discuss the privacy risks identified for the specific data elements and for each risk explain how it was mitigated. Specific risks may be inherent in the sources or methods of collection, or the quality or quantity of information included.

Privacy Risk:

Potential exposure of employee name, LAN ID, and employee ID if accidental or unauthorized access is gained to DFS system or data exposed to unauthorized user with corresponding time and attendance records.

Mitigation:

Access to information is controlled. See Section 3 for details.

Section 3.0 Access and Data Retention by the System

The following questions are intended to outline the access controls for the system and how long the system retains the information after the initial collection.

3.1 Do the systems have access control levels within the system to prevent authorized users from accessing information they don't have a need to

know? If so, what control levels have been put in place? If no controls are in place why have they been omitted?

Mandatory access controls are in place so that authorized users only have access to their specific information in the DFS system. Timekeepers only have access to user information of users they are specifically assigned by an admin. This assignment changes when a user changes division/branch to which a different timekeeper would be assigned.

Manager/Supervisors would have a read-only view of users under their supervision. A DFS Group administrator controls user and timekeeper access. A system administrator maintains the DFS system.

3.2 In what policy/procedure are the access controls identified in 3.1, documented?

A "DFS User guide.pdf" outlines the roles and procedures for the DFS system. It is available on the R07LAN

3.3 Are there other components with assigned roles and responsibilities within the system?

Participants(users), Timekeeper, Supervisor, Group Administrator, System Administrator

3.4 Who (internal and external parties) will have access to the data/information in the system? If contractors, are the appropriate Federal Acquisition Regulation (FAR) clauses included in the contract?

In the DFS application, mandatory access controls have been implemented so participants/users have access to their own data, managers/supervisors have access to the data for people under their direct control but are not allowed to alter it. Timekeepers have access to the people under their direct control and can enter time for participants. Group administrators enter participant info and assign participants to a timekeeper. System administrators maintain the system as a whole, can see all data, and is a contractor. Yes, there is a clause in the contract.

3.5 Explain how long and for what reasons the information is retained. Does the system have an EPA Records Control Schedule? If so, provide the schedule number.

Timekeeping information is retained indefinitely and archived by DFS system. This system is covered under records schedule 1006 b, administrative management. Schedule 1006 b specifies that record can be closed when discontinued, superseded, or canceled, or when no longer needed for current agency business. It is "Disposable" and can be destroyed 6 years after closure.

3.6 Privacy Impact Analysis: Related to Retention

Discuss the risks associated with the length of time data is retained. How were those risks mitigated? The schedule should align the stated purpose and mission of the system.

Privacy Risk:

The longer the DFS timekeeping records are retained, more records would be accessible in the event of unauthorized exposure.

Mitigation:

Access controls in place to limit who has access to data (See Sections 3.1, 3.4), User cannot access information after the end of the pay period.

Section 4.0 Information Sharing

The following questions are intended to describe the scope of the system information sharing external to the Agency. External sharing encompasses sharing with other federal, state and local government, and third-party private sector entities.

- 4.1 Is information shared outside of EPA as part of the normal agency operations? If so, identify the organization(s), how the information is accessed and how it is to be used, and any agreements that apply.

 No
- 4.2 Describe how the external sharing is compatible with the original purposes of the collection. $_{\mbox{\scriptsize N/A}}$
- 4.3 How does the system review and approve information sharing agreements, MOUs, new uses of the information, new access to the system by organizations within EPA and outside?

 N/A
- 4.4 Does the agreement place limitations on re-dissemination? $\rm N\!/\!A$
- 4.5 Privacy Impact Analysis: Related to Information Sharing

Discuss the privacy risks associated with the sharing of information outside of the agency. How were those risks mitigated?

Privacy Risk:

None. There is no information sharing.

Mitigation:

N/A

Section 5.0 Auditing and Accountability

The following questions are intended to describe technical and policy-based safeguards and security

5.1 How does the system ensure that the information is used as stated in Section 6.1?

Within DFS, data validation ensures that the user is entering valid time increments with a corresponding work code. Timekeepers have access to the people under their direct control and compare this data against EPA's official timekeeping system (People Plus) for discrepancies in hours and time codes used. This is carried out for each pay period.

5.2 Describe what privacy training is provided to users either generally or specifically relevant to the system/collection.

General privacy training is given to all users on an annual basis via FedTalent's mandatory Information Security and Privacy Awareness Training (ISPAT) training.

5.3 Privacy Impact Analysis: Related to Auditing and Accountability

Privacy Risk:

There is a low risk of DFS system data loss or corruption when information is audited

Mitigation:

The DFS system is an Oracle database and utilizes RMAN (Recovery Manager) as a backup and recovery manager. It provides automated backup, restore, and recovery capabilities addressing high availability and disaster recover concerns. There is a full database backup that takes place which includes all objects within the DFS database. A second backup is an incremental backup for files that are for updates to the database. There is Flashback backup which allows for a recovery to certain date and time based on setting to the automated backup settings.

Section 6.0 Uses of the Information

The following questions require a clear description of the system's use of information.

6.1 Describe how and why the system uses the information.

Only two sources for information are created in DFS system. Employee general information is added when they are given access to the system. Employee time and requests for credit time are entered by the employee. Employee approval for time and credit are entered by managers.

This information is collected because the EPA time keeping system of record does not have the capability of tracking credit time at the single minute increment required by R7. As such the DFS system was developed to track the time for employees' intra-pay period, and at the end of each pay period the information is transposed to the official time keeping system.

6.2 How is the system designed to retrieve information by the user? Will it be retrieved by personal identifier? Yes_X_ No___. If yes, what

identifier(s) will be used. (A personal identifier is a name, social security number or other identifying symbol assigned to an individual, i.e. any identifier unique to an individual. Or any identifier that can be linked or is linkable to an individual.)

LAN ID is the identifier in which the DFS system links timekeeping data to an individual. A user's EPA LAN ID is a unique field in Active Directory comprised of a user's first name initial and up to seven letters of a user's last name. Common names such as "MSMITH" have a numerical value added to ensure that ID uniquely identifies a user, example "MSMITH12".

6.3 What type of evaluation has been conducted on the probable or potential effect of the privacy of individuals whose information is maintained in the system of records?

The privacy data is limited to name, LAN ID, or employee ID. Technical controls are in place to limit employee access to their own data, timekeepers to their assigned group of employees through their EPA LAN ID. They must authenticate to EPA LAN and then the DFS application's login ID must match that of the LAN ID for access to the application.

6.4 Privacy Impact Analysis: Related to the Uses of Information

Describe any types of controls that may be in place to ensure that information is handled in accordance with the uses described above.

Privacy Risk:

There is a low risk of inappropriate use of DFS timekeeping data other than for system's intended purpose.

Mitigation:

EPA Rules of Behavior apply to all users, timekeepers, admins and other employees must be acknowledged prior to having access to any government systems and then again annually as part of mandatory ISPAT training. Specifically, a user must not "bypass or attempt to bypass system controls or access data for any reason other than official duties." See EPA Information Security-National Rules of Behavior, Directive No. CIO 2150-S-21.1

*If no SORN is required, STOP HERE.

The NPP will determine if a SORN is required. If so, additional sections will be required.

Section 7.0 Notice

The following questions seek information about the system's notice to the individual about the information collected, the right to consent to uses of information, and the right to decline to provide information.

7.1 How does the system provide individuals notice prior to the collection of information? If notice is not provided, explain why not.

The privacy notice pops up at the beginning of the application and requires that the user click "OK" to acknowledge or "X" to close out message before proceeding to the application.

Privacy Act Statement × ****** ****** PRIVACY ACT STATEMENT Chapter 63 of Title 5, United States Code, authorizes the collection of information. The primary use of this information is by management to approve and record credit hours earned, and credit hours used in association with the Region 7 flexible work schedule. Additional disclosures of the information may be made to a Federal, State, or Local law enforcement agency when the EPA becomes aware of a violation or possible violation of civil or criminal law; To a Federal agency when conducting an investigation for employment or security reasons, or the General Services Administration in connection with its responsibilities for records management.

Furnishing the requested information is voluntary, but failure to do so

may delay or prevent action on the application.

Any individual who wants to know whether this system of records contains a record about him or her, should make a written request to the Attn: Agency Privacy Officer, MC 2831T, 1200 Pennsylvania Ave., NW., Washington, D.C. 20460, privacy@epa.gov.

7.2 What opportunities are available for individuals to consent to uses, decline to provide information, or opt out of the collection or sharing of their information?

Furnishing the requested information is voluntary, but failure to do so may delay or prevent action on the application.

7.3 **Privacy Impact Analysis:** Related to Notice

Discuss how the notice provided corresponds to the purpose of the project and the stated uses. Discuss how the notice given for the initial collection is consistent with the stated use(s) of the information. Describe how the project has mitigated the risks associated with potentially insufficient notice and opportunity to decline or consent.

Privacy Risk:

User doesn't read the notice.

Mitigation:

Notice pops up every time the application is opened. User's receive yearly security training that covers accessing systems and protecting data.

Section 8.0 Redress

The following questions seek information about processes in place for individuals to seek redress which may include access to records about themselves, ensuring the accuracy of the information collected about them, and/or filing complaints.

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

They can access their current information when they open the application.

Individuals seeking access to information in this system of records about themselves are required to provide adequate identification (e.g., driver's license, military identification card, employee badge or identification card). Additional identity verification procedures may be required, as warranted. Requests must meet the requirements of EPA regulations that implement the Privacy Act of 1974, at 40 CFR part 16.

8.2 What procedures are in place to allow the subject individual to correct inaccurate or erroneous information?

They can correct inaccurate information during the current pay period, or for past events, have their timekeeper correct the inaccurate information.

Requests for correction or amendment must identify the record to be changed and the corrective action sought. Complete EPA Privacy Act procedures are described in EPA's Privacy Act regulations at 40 CFR part 16.

8.3 Privacy Impact Analysis: Related to Redress

Discuss what, if any, redress program the project provides beyond the access and correction afforded under the Privacy Act and FOIA.

Privacy Risk:

Integrity of individual DFS data could potentially be at risk if user enters inaccurate time into the system. A user only has access to edit their individual data for the current time period.

Mitigation:

Redress claims in the DFS system accessible by the individual user alone are limited to their current pay period. All time submissions must be reviewed by a timekeeper to be accepted to limit inaccuracy. A user cannot change past pay period information without a timekeeper's assistance.