Federal Trade Commission
Privacy Impact Assessment

Federal Human Resources Navigator

(FHR Navigator)

October 2018

Table of Contents

1 System Overview

1.1 Describe the project/system and its purpose.

Federal Human Resources (FHR) Navigator is a collection of software tools owned by Economic Systems, Inc. (EconSys) and used by the Federal Trade Commission (FTC) to navigate and facilitate human resources functions for all FTC employees. FHR Navigator is hosted remotely at a commercial facility; EconSys provides the FTC with access to the platform and website through its secured servers. The data will be stored on EconSys' secure servers and accessible only to authorized FTC and EconSys staff. The most prominent tool within the FHR suite is the Federal Retirement Benefits (FRB) Web, which employees can use to calculate and better understand their benefits. The system allows for more streamlined retirement planning and personal information management. Another key function of FHR Navigator is the Forms Manager, which includes access to over 150 federal forms. These forms can be completed and filed electronically, reducing waste and increasing efficiency within the FTC Human Capital Management Office (HCMO). In the event that an employee transfers to another federal agency, this system allows for a smooth transition of information.

Information in FHR Navigator is compiled from personnel data collected and maintained in the U.S. Department of Interior's Federal Personnel & Payroll System (FPPS). A bi-weekly file is generated by FPPS that contains employee information such as:

- Social Security Number (SSN) – ensures that the correct employee and salary data are associated with the correct individual
- Demographic information – includes employee name, date of birth, and address. Date of birth is used in retirement calculations and is used to populate forms filed via FHR Navigator.
- Organization and agency – employing office code and agency code are used to ensure that employees are coded with the correct agency accounts.
- Retirement specifics – includes sick leave balances, service computation dates, life insurance, health plan option codes, and retirement system codes, etc.
- Current salary – current salary and effective date are required to populate the salary history.

This file is downloaded by FTC HCMO personnel from FPPS and subsequently uploaded into a secure File Transfer Protocol (FTP) website administered by EconSys. The data is protected during transmission via Secured Sockets Layer (SSL) encryption. EconSys staff receive the file from the FTC and upload the information into the FHR Navigator system. Additional optional data in the system is provided by the individual employee at his/her discretion. Employees may fill out and submit HR forms directly via the FHR Navigator system. FTC data within the FHR Navigator system is stored on EconSys' secure servers and accessible only to authorized staff.

1.2 What specific legal authority allows for the collection, maintenance, or dissemination of information for this project/system?

Information maintained in FHR Navigator is collected, maintained, and disseminated pursuant to the Federal Trade Commission Act, 15 U.S.C. §§ 41 *et seq*.

2 Data Type, Sources, and Use

2.1 Specify in the table below what types of personally identifiable information (PII)[1] may be collected or maintained in the system/project. Check all that apply.

PII Elements: This is not intended to be an exhaustive list. Specify other categories of PII as needed.		
☒ Full Name	☐ Biometric Identifiers (e.g., fingerprint, voiceprint)	☒ User ID
☒ Date of Birth	☐ Audio Recordings	☒ Internet Cookie Containing PII
☒ Home Address	☐ Photographic Identifiers (e.g., image, x-ray, video)	☒ Employment Status, History, or Information
☒ Phone Number(s)	☐ Certificates (e.g., birth, death, marriage, etc.)	☐ Employee Identification Number (EIN)
☐ Place of Birth	☐ Legal Documents, Records, Notes (e.g., divorce decree, criminal records, etc.)	☒ Salary
☒ Age	☐ Vehicle Identifiers (e.g., license plates)	☒ Military Status/Records/ ID Number
☐ Race/ethnicity	☐ Financial Information (e.g., account number, PINs, passwords, credit report, etc.)	☐ IP/MAC Address
☐ Alias	☐ Geolocation Information	☐ Investigation Report or Database
☒ Sex	☐ Passport Number	☐ Driver's License/State ID Number (or foreign country equivalent)
☒ Email Address		☒ Other: Life Insurance Status, Health Insurance Status, TSP Status, Retirement Plan
☒ Work Address		
☒ Taxpayer ID		
☐ Credit Card Number		
☐ Facsimile Number		
☐ Medical Information		
☐ Education Records		
☒ Social Security Number		
☐ Mother's Maiden Name		

When completing benefit forms, the employee may choose to enter the place of marriage and the names of other federal agencies where the employee may have previously worked.

2.2 What types of information other than PII will be collected, disseminated, or maintained by the project/system? Provide a general description below and be sure to include all data elements.

Other information collected and maintained includes the type of retirement plan selected by the employee and includes the employee's leave balances.

[1] Per OMB Circular A-130, personally identifiable information (PII) means information that can be used to distinguish or trace an individual's identity, either alone or when combined with other information that is linked or linkable to a specific individual.

2.3 What is the purpose for collection of the information listed above?

FHR Navigator provides helpful tools for employees to better understand and plan for their retirement and financial future. The PII collected is necessary for account validation and to provide accurate calculations and figures based on the employee's specific information.

2.4 What are the sources of the information in the system/project? How is the information collected?

Source of Data	*Type of Data Provided & How It Is Collected*
Federal Personnel & Payroll System (FPPS)	All position, personnel, payroll, and leave information for each FTC employee is collected and maintained in the U.S. Department of Interior's FPPS. Personnel data elements required by FHR Navigator are downloaded by FTC HCMO personnel, and then uploaded into a secure portal for FHR Navigator personnel to retrieve and upload into the system. This process occurs on a bi-weekly basis.
FTC Employees	The employee may input data into FHR in order to view different variations of their retirement income. Additionally, electronic versions of HR forms are available within the FHR Navigator system, allowing employees to fill out and file them directly within the system.
FTC HCMO Staff	HCMO staff access the system to view data and assist employees as needed. If there are inaccuracies in the data, that data must first be corrected within FPPS before it can be altered in FHR Navigator. HCMO staff coordinate with Department of Interior staff to address the correction. Then, following the biweekly download/upload process described above, data would automatically be corrected in FHR Navigator.

3 Data Access and Sharing

3.1 In the table below, specify the systems/applications and groups (both FTC and non-FTC) that will have access to or share data in the system/project.

Data Will Be Accessed By and/or Provided To:	*How and Why the Data Will Be Accessed/Shared*
HCMO Administrators and Specialists	HR Administrators and Specialists will use the data received from FPPS to update and log retirement benefit information in FHR Navigator. This will be conducted on a bi-weekly basis at the end of each pay period, depending on the salary and retirement planning schedule of each employee.
FTC Employees	Employees will only have access to their own personal information, which they access through a unique username, password, and numeric code text message sent to their personal cell phone. They may use this information to maintain their personal records and update information as

Data Will Be Accessed By and/or Provided To:	*How and Why the Data Will Be Accessed/Shared*
	necessary. Access for employees who separate from the FTC will be available for 60 days after separation. Then their profile will be converted to inactive and access will no longer be available. The data for that separated employee will be stored in FHR Navigator for two years after separation, then be destroyed, as per FTC's records management schedule. For employees who transfer from the FTC to another government agency, the data within FHR Navigator will be transferred to their new agency within two weeks of their exit from the Commission. They will no longer be able to access FHR Navigator via their FTC profile after the data is transferred to their new agency.
Economic Systems (EconSys) Inc.	EconSys will be providing the platform and website through their secure servers. The data will be stored on EconSys' secure servers and accessible only to authorized staff. If problems arise with use of the system, certain members of the EconSys help desk staff may be required to access FTC employees' data to resolve issues. When an employee leaves the FTC (whether through retirement or transfer to another place of employment), the FTC notifies EconSys; EconSys then updates the information in the FHR Navigator system to reflect the change. Data in the FHR Navigator system is backed up every 24 hours to keep it as current as possible.

3.2 Do contractors and/or third party service providers have access to data in the project/system? If yes, explain what privacy requirements are in place to ensure that data is properly protected.

Yes, EconSys employees have access to the FHR Navigator application and are required to sign a non-disclosure agreement with the FTC. EconSys employees ensure that privacy responsibilities and procedures are included in the security awareness training, which is identical to the Department of Homeland Security (DHS) IT Security Awareness and Privacy training. Role based training is provided to individuals with responsibility for handling PII and privacy requirements.

3.3 If you answered "yes" to 3.2, describe the privacy incident response plan maintained by the contractor's organization or third party service provider.

EconSys maintains an incident response plan that addresses requirements and guidance set forth by the Federal Information Security Modernization Act (FISMA) and includes FedRAMP specific control parameters. It also encompasses minimum security requirements as set forth by the Federal Information Processing Standard (FIPS) 800-53, Revision 4. As part of EconSys' annual assessment, the company reviews its incident response plan and conducts incident response training for its staff. As stated in its incident response plan, EconSys will report incidents detected within FHR Navigator to all affected customer agencies based on the categorization of the incident. For example, all incidents related to unauthorized access or PII

will be reported to US-CERT within one hour of awareness via telephone and followed up with an email; subsequently, it will notify the affected agency regarding the nature and scope of the incident.

4 Notice and Consent

4.1 How are individuals provided with notice prior to the collection of their PII? If notice is not provided, explain why.

A preliminary HCMO email will be sent out to new FTC employees about the collection of their PII for use within FHR Navigator. Additionally, users are provided with a Privacy Act notice on the FHR Navigator login page.

☒ Notice is provided via (*check all that apply*):
- ☒ Privacy Act Statement (☒ Written ☐ Oral)
- ☐ FTC Website Privacy Policy
- ☐ Privacy Notice (e.g., on Social Media platforms)
- ☐ Login banner
- ☒ Other (*explain*): Employees receive an email from the HCMO administrator informing employees about the collection of their information for the FHR Navigator system.

4.2 Do individuals have the opportunity to decline to provide information or to consent to particular uses of their information (other than required or authorized uses)?

FTC employee data is automatically uploaded to FHR Navigator for the purpose of calculating and maintaining their retirement plan. Therefore, they do not have the opportunity to decline to provide their information. Because the system is vital in properly administering retirement benefits and updating HR Forms, all employees will have their information transferred from FPPS into the new FHR Navigator system via the process identified in Section 2.4. However, employees are not obligated to log into FHR Navigator and provide additional information about themselves or actively use the system.

4.3 Are there procedures in place to allow individuals access to their personally identifiable information? Explain.

Individuals are able to access their own personally identifiable information through the FHR Navigator website by using their login name and password. There is a two factor authentication process in which employees will receive a new code text messaged to their phone every time they attempt to log in to the system.

4.4 Are there procedures in place to allow individuals the ability to correct inaccurate or erroneous information? What is the process for receiving and responding to complaints, concerns, or questions from individuals? Explain.

Data received from FPPS and subsequently uploaded to FHR Navigator cannot be changed by anyone other than HCMO staff and HR Administrators/Specialists. Incorrect data will first need to be changed in FPPS; once this has been completed, the updated information will be downloaded/uploaded via the process identified in Section 2.4, thus correcting the data in FHR Navigator. If employees notice that information regarding their retirement plans or other benefits is incorrect, they must contact HCMO and request the change or update. It is the policy of HCMO to respond to the request within two business days.

Employees do have the ability to add or modify limited information within the system such as information from their Thrift Savings Plan account. When completing forms directly via FHR Navigator, individuals have the opportunity to verify the accuracy of their information before submitting the form. Additionally, if individuals choose not to submit the forms via FHR Navigator, they have the option of filling them out manually, verifying the information is accurate, and submitting them in hardcopy form to HCMO.

5 Data Accuracy and Security

5.1 Are there procedures in place to ensure that the information maintained is accurate, complete, and up-to-date?

The information is transferred from FPPS into FHR Navigator via the process described in Section 2.4. If an employee notices the information maintained about them in FHR Navigator is inaccurate, the employee must notify HCMO in order to correct the discrepancy. See 4.4.

5.2 Are there administrative procedures and technical safeguards in place to protect the data in the system/project? What controls are in place to ensure proper use of the data? Please specify.

HCMO staff are responsible for assigning roles and access rights for FTC users. Authorized EconSys staff have access to the system for maintenance and troubleshooting purposes. The FHR Navigator interface gives administrative users access to PII only on a role and need-to-know basis. Individuals in roles where the information is necessary for the completion of tasks will be given access to said information at the discretion of the system administrators and data managers. All data in FHR Navigator is encrypted and stored in a secure EconSys server; the data is restricted to authorized users in a locked facility.

FTC employees will have access to training modules within the FHR Navigator system that they can use to further their understanding of securing and protecting data in addition to the FTC's required annual privacy and security training. Privacy notices are also displayed whenever an employee logs into the system to warn against misuse or unauthorized access to data.

5.3 Has the system/project undergone the appropriate security risk assessment and received authority to operate?

Yes, FHR Navigator is a FedRAMP cloud system that has undergone a security risk assessment. FHR Navigator has a Provisional Authority to Operate (PATO) issues by the FedRAMP Joint Authorization Board (JAB). The system is reassessed on an annual basis by an approved third party according to FedRAMP guidelines. In addition, FHR Navigator has a current authorization to operate (ATO) issued by the FTC.

5.4 Is PII used in the course of system testing, training, or research? If so, what steps are taken to minimize and protect PII during this process?

☒ Not Applicable

Only fictitious or dummy data is used for system testing or training. No real or live PII is used.

6 Data Retention and Disposal

6.1 Specify the period of time that data is retained in the system/project. What are the specific procedures for disposing of the data at the end of the retention period?

All data will be retained in the system until the employee separates from the agency. Access for employees who separate from the FTC will be available for 60 days after separation. Then their profile will be converted to inactive status and access will no longer be available to the individual. Data for former FTC employees are stored in FHR Navigator for two years after separation before being destroyed per FTC's records management schedule. If an employee leaves the Commission to work for another government agency, his/her data transferred to their new agency account within the FHR Navigator system. They will no longer be able to access FHR Navigator via their FTC profile after the data is transferred to the new agency.

7 Website Privacy Evaluation

7.1 Does the project/system employ the use of a website? If so, describe any tracking technology used by the website and whether the technology is persistent or temporary (e.g., session cookie, persistent cookie, web beacon). Describe the purpose of using such tracking technology.

The system utilizes session (temporary) cookies in order to maintain and manage user information during user progression through the registration process and online application. There is no use of persistent (permanent) cookies. Sessions are timed out after 60 minutes of inactivity.

8 Privacy Risks and Evaluation

8.1 Considering the type of information collected and sources of collection, what privacy risks were identified and how were these risks mitigated?

Sources of Collection	*Mitigation Strategy*
Employee information is maintained after separation	Access for employees who leave the FTC will be available for 60 days after separation. Then their profile will be converted to inactive and access will no longer be available. Data for former employees will be stored in FHR Navigator for two years after separation, then be destroyed per FTC's records management schedule. For individuals who leave employment with the FTC to move to another government agency, their data is transferred to their new organization within the FHR Navigator system. These individuals will no longer be able to access FHR Navigator via their FTC profile after the data has been transferred to the new agency.
Additional risk in allowing employees to submit sensitive information via electronic forms on FHR Navigator	While is some additional risk involved when employees complete and submit forms electronically via FHR Navigator, all data in the system is encrypted and stored in a secure server. If employees feel uncomfortable providing this data via FHR Navigator, they may opt into completing the forms on paper and submit them manually to HCMO in order to protect their information.
HCMO employees have access to employee personal information	Having employee personal information accessible by other FTC employees (HCMO users) may put the data at risk of unauthorized disclosure. However, there are access controls in place to reduce this risk. Only HCMO Administrators will be able to see all levels of the data. HR Specialists can see and edit all data pertaining to individual benefits. HR Assistants can only input data into the system. Non-HCMO employees are only able to see their own data, and may only access data following the two-factor authentication procedure. They are also only able to input their own information for their personal records that only HR Administrators have access to.
EconSys staff have access to data	Although EconSys stores the data, the FTC is still considered the owner of the information. EconSys has security measures in place to ensure that only those with access are able to see and update information. See 5.3.
Any device with an internet connection may access the system	Any device with an internet connection can access this system in order to optimize convenience and functionality. EconSys encrypts all data that is uploaded and protects its servers behind two firewalls.

8.2 Does the project/system employ the use of automated privacy controls or enhanced capabilities designed to support privacy? Explain.

The system employees a two-factor authentication process each time an employee logs on. The first time they log in, employees will have to input their last name, Social Security Number, and Date of Birth. They will then be prompted to create a username and password; they must also provide a mobile phone number and agree to receive text messages from the service.

Every subsequent time that they log in, employees will be able to use their username and password along with a unique text message code sent to their mobile phone.

8.3 Has a Privacy Act System of Records Notice (SORN) been published in the Federal Register for this system/project? If so, list the applicable SORN(s).

FHR Navigator is covered under the Privacy Act System of Record Notice (SORN) FTC-II-1 – General Personnel Records-FTC as well as FTC-VII-3 – Computer Systems User Identification and Access Records-FTC.

8.4 How does the project/system ensure that the information is collected, used, stored, or disseminated in accordance with stated practices in this PIA?

HCMO system administrators are responsible for maintaining up-to-date and accurate information and ensuring proper use by HCMO staff. The FTC and EconSys have non-disclosure agreements in place to ensure confidentiality of FTC data. EconSys is responsible for adhering to FTC's data privacy and security contract requirements.