Privacy Impact Assessment for

Employee Express (EEX)

December 17, 2020

Contact Point

Kim Williamson
Project Manager
CIO/FITBS/HRSITPMO/ES

Reviewing Official

Kellie Cosgrove Riley
Chief Privacy Officer

Abstract

Employee Express (EEX) is a system maintained and hosted at the Office of Personnel Management (OPM) Macon, Georgia facility by OPM Human Resources Solutions Information Technology Program Management Office staff. EEX is owned by the EEX User Board, a consortium of agency participants. EEX is a system that allows Federal employees to view and make changes to their payroll and associated personnel records. This Privacy Impact Assessment is being conducted because EEX collects, maintains, and uses personally identifiable information.

Overview

Employee Express (EEX) is an automated system that Federal employees use to make their personnel and payroll transactions electronically. This is a self-service system that allows government agency employees and annuitants to view and make changes to their payroll and associated personnel records in one convenient location. EEX serves as a front-end system for participating agencies' personnel and payroll systems. EEX is intended to provide Federal employees with direct control over their information and eliminate the need to fill out, submit and process paper forms.

EEX is maintained and hosted by the Office of Personnel Management (OPM) but is owned by the EEX User Board, a consortium of Federal agency participants. EEX receives master file data for each of the participating agencies from designated agency payroll providers who collect information from various agencies and provide it to EEX. EEX then makes individual records available to Federal employees and annuitants for viewing through the EEX web site. Individuals are only able to access or update information concerning themselves. This is done through an Internet capable web browser. Updates from individual participants are then forwarded by EEX on a daily basis to the payroll provider, for processing on behalf of the participating agency. EEX does not modify the master file held by EEX, rather any changes that individuals make to their information are made by the agencies in their systems and then reflected when a new master file is received from the agencies' payroll office through the payroll provider.

Each participating agency continues to serve as the system manager of their information and EEX maintains logs of user activity. All user information provided to EEX is owned by the agency providing the data. EEX provides employees and annuitants with several benefits, including a secure Section 508 compliant site for the visually and hearing impaired; immediate access to a one page, printable and downloadable Earnings and Leave Statement; and the ability to update such information as home address and tax information. In particular, employees and annuitants may update the following information in EEX, depending on what options their respective participating agency has permitted:

- Federal and state taxes
- Direct deposit
- Allotments (Financial, Health Savings, Discretionary)
- Home, Thrift Savings Plan (TSP), and Paycheck mailing address(es)
- Federal Employees Health Benefits (FEHB)
- FEHB Premium Conversion
- TSP and TSP Catch-up Contributions
- Federal Employees Group Life Insurance (FEGLI)
- Disability Indicator
- Combined Federal Campaign (CFC)
- Employee Emergency Contact Information

- Ethnicity and Race Indicator

In addition, individuals are able to view, but not make changes to, their Earnings and Leave/Annuity Statements, Online W-2, 1095c and 1099R.

In addition to submitting an individual's changes to the appropriate agency, EEX also transmits specific personnel transaction data to the OPM eOPF system daily for participating agencies. The eOPF provides a consolidated image and data view that digitally documents the employment actions and history of individuals employed by the Federal government. The eOPF is built on the re-creation of the paper personnel folder in a digitally imaged format as well as the going-forward collection of personnel actions from the agency human resource systems.

Information from EEX is sent to eOPF via secure transfer processes and is used to populate an individual's official personnel record.

EEX implements national standards and approved encryption technologies during the entire web-session, while data is stored (at rest) and during the transmission of master files from participating agencies.

Section 1.0. Authorities and Other Requirements

1.1. What specific legal authorities and/or agreements permit and define the collection of information by the project in question?

EEX is owned by the EEX User Board, a consortium of Federal agency participants. The EEX was established to provide Federal employees with a direct means to view and update certain personnel and payroll data. The information in EEX is collected by the participating agencies pursuant to the general authorities related to hiring and payroll in 5 U.S.C., Part III.

1.2. What Privacy Act System of Records Notice(s) (SORN(s)) apply to the information?

The information in EEX consists of personnel and payroll information from the various participating agencies. Some of the records in EEX are covered by Government-wide SORNs, such as OPM/GOVT 1 General Personnel Records, while others are covered by SORNs specific to each participating agency.

1.3. Has a system security plan been completed for the information system(s) supporting the project?

A System Security Plan was developed for the Authority to Operate and is maintained as part of the Continuous Monitoring Requirements.

1.4. Does a records retention schedule approved by the National Archives and Records Administration (NARA) exist?

The records in EEX are subject to General Record Schedule 2.4; however, within EEX system they are transitory records subject to General Records Schedule 5.2. The transaction history within EEX is subject to GRS 3.1, Item 20.

1.5. 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.

EEX is a self-service system that allows government agency employees and annuitants to view and make changes to their payroll and associated personnel records in one convenient location. If information is gathered by forms subject to the PRA, it is gathered by the participating agencies from the individual employees and annuitants and any PRA requirements are addressed at that point of collection.

Section 2.0. Characterization of the Information

2.1. Identify the information the project collects, uses, disseminates, or maintains.

Participating agencies provide personnel and payroll information to EEX so that their employees can access it and make changes. The exact information provided by each of the participating agencies will vary depending on what transactions they want their employees to be able to conduct within EEX

For every employee that uses EEX, the master file contains full name, social security number, and in some instance home addresses. In addition, the master file contains specific information, set forth below, related to the transactions the agencies have elected to make available in EEX.

- Financial transaction information: direct deposit, health savings, and financial allotments, bank routing code, account number, account type, deduction amount;

- FEHB information: FEHB enrollment code, date of birth, premium conversion information, relationship type, marital status, gender, dependent/spouse information (name, SSN, address, date of birth, phone number, email address);

- Thrift Savings Plan/Roth information: dollar amount, percentage amount, future effective date;

- CFC information: charity code, deduction amount, annual charity amount, work phone, work email, work address, agency bureau, home email;

- Federal and state tax information: marital status, number of exemptions, additional deduction amount;

- Address transaction-related information: paycheck/home mailing address (street, city, state, zip code, county);

- Disability indicator: disability categories and associated impairments;

- Ethnicity and race: ethnicity and race category;
- Emergency contact information: home phone number, email address;
- Federal Employees Group Life Insurance: Basic, Option A, Option B, Option C.

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

data from each of the participating payroll providers containing information provided by participating agencies that elect to utilize EEX. EEX then makes individual records available to employees and annuitants for viewing through EEX. The payroll providers transmit personnel and payroll data securely to EEX according to their bi- weekly payroll schedules.

Information is also collected directly from employees and annuitants who initiate access via a front-end web interface. Employees and annuitants make changes to their payroll and personnel information using EEX. Changes made by employee and annuitants are recorded and sent to the payroll providers on a daily basis.

EEX does not modify the master file, thus any requested changes are reflected in the next pay cycle when EEX receives a new master file from the agency’s payroll office through the respective payroll provider.

2.3. Does the project use information from commercial sources or publicly available data? If so, explain why and how this information is used.

EEX does not use information from commercial sources or publicly available data.

2.4. Discuss how accuracy of the data is ensured.

To ensure transaction data submitted to and from the agency is accurate, the payroll provider and EEX support staff verify the data upon receipt based on the unique key provided by the agency and record counts generated prior to transmission and upon receipt. Employee and annuitant data submitted to EEX is verified for accuracy using manual and automated processes. Record counts are used for validation. Specific data collected from the employee or annuitant is checked for accuracy via system generated confirmations that require user acceptance and automated data validations of zip codes and financial routing codes.

2.5. Privacy Impact Analysis: Related to Characterization of the Information

Privacy Risk: There is a risk that the information that is input by individual users will not be accurate or that the information will not be accurately transmitted to the appropriate payroll provider and participating agency.

Mitigation: This risk is mitigated because the system employs user verification prompts which require the employees and annuitants to confirm the accuracy of their information before a transaction is finalized. In addition, EEX implements logging and reporting of all transactions to check for anomalies and verify capture. Failure notifications are sent to system administrators for corrective action, when necessary.

Privacy Risk: There is a risk that more information than is necessary will be maintained in EEX.

Mitigation: This risk cannot be completely mitigated by EEX as it is the responsibility of each agency to determine which transactions its employees will be able to conduct in the system and what information the agency provides to enable those transactions.

Section 3.0. Uses of the Information

3.1. Describe how and why the project uses the information.

EEX uses the information provided by the payroll providers and participating agencies to allow individual users to update that information. This includes a variety of discretionary personnel and payroll transactions (e.g., changes to

Financial Allotments, Health Benefits, Thrift Savings Plan, Direct Deposit, Federal and State Taxes, and Home Address). EEX is intended to provide employees with direct control over their information and eliminate the need to fill out, submit, and process paper forms.

EEX transmits the information entered by employees and annuitants to the payroll providers so that participating agencies can update their payroll and personnel records. The participating agency then provides an updated record to EEX that the user can access after the transaction is processed. The user transactions are maintained in EEX for display purposes to facilitate user verification and quality control. Application and security logs are also maintained.

3.2. Does the project use technology to conduct electronic searches, queries, or analyses in an electronic database to discover or locate a predictive pattern or an anomaly? If so, state how OPM plans to use such results.

EEX does not use technology to conduct electronic searches, queries or analyses of the information it collects and stores.

3.3. Are there other programs or offices with assigned roles and responsibilities within the system?

Only the OPM EEX project team, support staff, and network administrators have access to EEX within OPM. EEX does share information with OPM’s Electronic Personnel Folder (eOPF) system and OPM’s Federal Employees Health Benefits Systems (FEHB) Data Hub, but those programs do not have direct access to EEX.

3.4. Privacy Impact Analysis: Related to the Uses of Information

Privacy Risk: There is a risk that an unauthorized user may access the information or that authorized administrative users of EEX may access EEX information for non-authorized purposes, such as performing searches on themselves, friends, relatives, or neighbors.

Mitigation: OPM provides all personnel (users, developers, system admins, and help desk personnel) with initial and annual IT Security and Privacy Awareness training to educate them concerning the proper handling of personally identifiable information and the protection of information systems. EEX users also receive agency specific training for EEX and complete agency specific System Rules of Behavior. EEX access controls prevent employees and annuitants from accessing any other EEX user's information. In addition, access to "production" data is limited to EEX database administrators and enforced through system access controls. All access to EEX is logged to include session details such as logon/logoff, actions taken, date and time, and other events required to investigate misuse or unauthorized access to information.

Section 4.0. Notice

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

Federal employees and annuitants who log into EEX are provided notice concerning EEX and the information it collects through the website's Privacy Policy and through a series of frequently asked questions About Employee Express. In addition, when participating agencies provide instructions to their employees concerning the use of EEX, they are provided with information concerning the system and their ability to conduct transactions. This PIA also provides notice to individuals regarding EEX.

4.2. What opportunities are available for individuals to consent to uses, decline to provide information, or opt out of the project?

Employees and annuitants who do not wish to make use of EEX can instead submit equivalent changes on paper forms to their agencies. Those employees and annuitants who do make use of EEX are consenting to their information being provided to their respective agency in order to update their information.

4.3. Privacy Impact Analysis: Related to Notice

Privacy Risk: There is a risk that individuals were not provided notice prior to the collection of their information and are unaware that their agency provides their information to EEX.

Mitigation: This risk is mitigated by providing information to employees and annuitants when they log in to EEX. In addition, participating agencies provided information to their employees and annuitants concerning EEX and how it is used.

Section 5.0. Data Retention by the Project

5.1. Explain how long and for what reason the information is retained.

Within EEX, the information provided by the payroll providers is overwritten on a daily basis as updated information is transferred to the system because these are transitory records that are deleted when no longer needed for business use. The information is retained at each agency in accordance with GRS 2.4, referenced in Section 1.4. Transaction history is subject to GRS 3.1 and available to be viewed by employees and annuitants who use the system for five years.

5.2. Privacy Impact Analysis: Related to Retention

Privacy Risk: There is a risk that information in EEX will be retained for longer than is necessary for its intended purpose.

Mitigation: This risk is mitigated by identifying appropriate NARA retention schedules for the information in the system and adhering to the established timeframes.

Section 6.0. Information Sharing

6.1. Is information shared outside of OPM as part of the normal agency operations? If so, identify the organization(s) and how the information is accessed and how it is to be used.

EEX receives master files from each of the participating payroll providers that elect to use EEX. EEX provides information submitted by employees and annuitants to the participating agency through the payroll provider. OPM does not otherwise provide the information in EEX to any other third party in the normal course of business.

6.2. Describe how the external sharing noted in 6.1 is compatible with the SORN noted in 1.2.

The participating agencies that provide information to EEX are responsible for ensuring that their applicable SORNs permit that disclosure. EEX itself serves as a technical interface for the participating agency employees and annuitants and does not own the information or share it with any third party.

6.3. Does the project place limitations on re-dissemination?

EEX directs agencies via signed ISAs and MOUs to delete the transaction files that they receive from OPM thorough EEX within 90 days. There are no other limitations on re- dissemination of the information imposed by EEX because the master file information in EEX is owned and governed by each participating agency.

6.4. Describe how the project maintains a record of any disclosures outside of OPM.

The participating agencies that provide information to EEX are responsible for ensuring that their applicable SORNs permit any disclosures they make and are responsible for recording those disclosures. EEX itself serves as a technical interface for the participating agency employees and annuitants and does not own the information or share it with any third party.

6.5. Privacy Impact Analysis: Related to Information Sharing

Privacy Risk: There is a risk that information in EEX will be shared externally for a purpose inconsistent with the original purpose for which it was collected.

Mitigation: This risk is mitigated through ISAs and MOUs that outline the purpose of EEX and appropriate actions concerning the data. These agreements require both OPM and the participating agencies to adhere to Privacy Act requirements in any information use or disclosure. This risk cannot be completely mitigated by OPM, however, because the participating agencies retain ownership and control of their master file information.

Section 7.0. Redress

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

EEX is intended to provide employees and annuitants with direct access to their information. Employees and annuitants are initially provided a temporary password to access their information in EEX. During their initial access they are instructed on establishing a username and password and/or registering their PIV.

In addition to direct access to EEX, employees and annuitants can request access to their information by following the procedures set out in the applicable SORN or in their agency's Privacy Act regulation.

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

Employees and annuitants who have received an EEX temporary password or who have established a username and password or registered their PIV card in EEX have direct access to their information to make certain corrections or provide updates. To the extent there is information in EEX that the employee or annuitant cannot correct, for example, because it is not the type of transaction their agency has opted to address in EEX, or if there is information that the employee or annuitant corrected in EEX but a corresponding correction was not made in the agency's master file and returned to EEX, the employee or annuitant must contact their agency directly. This can be accomplished according to the procedures set out in the applicable SORN and/or in the agency's Privacy Act regulation, or as otherwise instructed by the individual agency.

7.3. How does the project notify individuals about the procedures for correcting their information?

Participating agencies provide information regarding EEX directly to their employees concerning how to use EEX and what transactions they can access and correct. In addition, individuals are provided notice of procedures through the applicable SORN, Privacy Act regulation, and this PIA. Employees and annuitants can also contact the EEX customer service helpdesk for information and instruction concerning how to correct their information.

7.4. Privacy Impact Analysis: Related to Redress

Privacy Risk: There is a risk that employees and annuitants will not understand how to access and correct their records in EEX.

Mitigation: This risk is mitigated by the participating agencies, who provide direct information and instructions to their employees, and by OPM, which maintains a customer service helpdesk and also provides information on the EEX website in the form of frequently asked questions and other documentation. Moreover, the paper-based processes that EEX automates are still in use and available to those who choose not to, or are unable to, utilize EEX to submit corrections to their agency.

Section 8.0. Auditing and Accountability

8.1. How does the project ensure that the information is used in accordance with stated practices in the PIA?

All ISAs and MOUs related to EEX are reviewed annually to ensure that that they are accurate and being implemented appropriately. EEX also undergoes an annual Statement on Standards for Attestation Engagement (SSAE18) audit conducted by a third party.

8.2. Describe what privacy training is provided to users either generally or specifically relevant to the project.

All OPM employees receive annual IT Security & Privacy Awareness Training which covers the proper handling of PII. In addition, the EEX User Board requires that all participating agencies provide specific training regarding EEX for their employees.

8.3. What procedures are in place to determine which users may access the information and how does the project determine who has access?

EEX can be accessed through the Internet (www.employeeexpress.gov). Each participating agency provides information to their employees concerning how to access EEX. Each participating agency chooses which EEX system options are visible and available on the EEX external website accessed by users from their own agency.

8.4. How does the project review and approve information sharing agreements, MOUs, new uses of the information, new access to the system by organizations within OPM and outside?

All ISAs and MOUs are reviewed annually. Annual reviews consist of examining the technical and security aspects of the data connections, securing of information exchanged and status of system accreditations. Participating agencies are responsible for providing their employees and annuitants with access and determining which transactions will be available and what information to provide in the master file.

Responsible Officials

Kim Williamson

Project Manager

CIO/FITBS/HRSITPMO/ESOH

Approval Signature

Signed Copy on file with Chief Privacy Officer

Kellie Cosgrove Riley
Chief Privacy Officer