Privacy Impact Assessment for

Enterprise Cost Accounting System (ECAS)

November 7, 2022

Contact Point
Katina Cotton
Executive Officer & Chief, Resource Management Office
Office of the Chief Financial Officer

Reviewing Official
Kellie Cosgrove Riley
Chief Privacy Officer

Abstract

The U.S. Office of Personnel Management (OPM) is the central human resources agency for the Federal Government. The Office of the Chief Financial Officer (OCFO) provides critical accounting and financial management services and reporting to achieve OPM's mission objectives. OPM must price reimbursable services to recover the total cost of those services, including direct and indirect costs, for both functional and enabling support areas. To provide additional visibility in tracking and reporting these costs across the agency, OPM OCFO has implemented the Enterprise Cost Accounting System (ECAS). This Privacy Impact Assessment is being conducted because the ECAS program uses masked Social Security numbers and names to link data sets and validate that data imports were successful.

Overview

The Office of Personnel Management (OPM)'s Office of the Chief Financial Officer (OCFO) has implemented the Enterprise Cost Accounting System (ECAS) to comply with regulations, set forth by the Department of Treasury and the Office of Management and Budget (OMB) regarding agency financial reporting. Those regulations require OPM to price reimbursable services to recover the full cost of services. These costs include direct and indirect costs for functional and enabling support areas, spanning different funding sources. ECAS provides OPM with greater granularity, transparency, accuracy, and expediency in determining activity, information technology, and service costs.

ECAS aims to standardize cost management programs and practices across OPM and provide financial and operational metrics to inform management decision-making as part of routine business practices. It traces all costs reported in OPM financial reports to OPM's services in a centralized and standardized format enabling analysts to understand their costs.

Information in ECAS comes from a variety of systems and programs, including the Federal Aviation Agency (FAA) shared-service financial reporting system, Delphi, which serves as OPM's financial management system of record by generating proprietary, fiduciary, and budgetary financial transactions to provisional financial statements; Human Resources IT Transition to Transformation (HR Links), which is the information system supporting the day-to-day operating needs of its human resource operations and management; and the Labor Distribution System (GSA Payroll). Information is also gathered regarding contractors, projects, and costs (billing) in summary form from general ledgers and sub-ledger information.

After manually ingestion into ECAS, costs from programs and offices are mapped to funding sources, time periods, and other requirements, then aggregated and summarized into various reports to be used within OPM in order to make routine management decisions.

There are two primary types of users within ECAS, Administrators and End Users. Administrators have access to the different component software and underlying data. Administrators can view and change all underlying data sources. There are a limited number of Administrators for ECAS (currently six) with access to Personally Identifiable Information (PII) that the Administrators need to link data sets and create reports for End Users. End Users access ECAS via the reporting software only. End Users cannot access or see any of the PII utilized in the model. End Users are only able to view and analyze aggregated, summarized data.

Masked SSNs and employee names are used and stored within ECAS. Masked SSNs are a common identifier used to connect the separate roster and payroll data sets from the Human Resource Links (HRLinks) system. This allows data associated with one person in the HRLinks System to be matched to payroll data and provide a more useful data set. This matching is performed within the Administrators' environment; masked SSNs are used to ensure accuracy, and access is strictly limited to a small number of Administrators. Before use, the SSNs have an encryption masking algorithm

applied by a designated OPM administrator to minimize exposure of the data within the program and prevent true SSNs from being stored or used in the ECAS applications and any corresponding risk. Names are also included in the Extract, Transform, and Load (ETL) process and can be used as part of the reconciliation of total hours to hours used in the cost model.

The number of hours in the model and the number of hours in the labor cost by pay period report may vary. The labor and payroll reports are aggregated within the cost model to create information for end users. No PII is available in the reporting.

The system is hosted in the OPM-managed instance of Microsoft Azure Commercial Cloud (security rated FedRAMP Moderate) and is comprised of Commercial-off-the-Shelf (COTS) software. Access is only allowed through an OPM Virtual Private Network (VPN) using Personal Identity Verification (PIV) card access to authorized users within the agency.

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?

The primary legal basis for collection the information in ECAS is 31 U.S.C., Subtitle II, which defines the budget process and describes the method for establishing and accounting for an agency's Federal budget, and 31 U.S.C., Subtitle III, which describes the Federal financial management requirements and responsibilities to record accounting activities. Data will be used for financial tracking, reporting, and forecasting.

In addition, other relevant authorities include the Chief Financial Officers Act of 1990, Public Law 101-576; the Federal Financial Management Improvement Act (FFMIA) of 1996, Public Law 104-208; OMB Circular A-123, Management's Responsibility for Enterprise Risk Management and Internal Control; OMB Memorandum M-16-11, Improving Administrative

Functions Through Shared Services (May 2016); and OMB Memorandum M-13-08, Improving Financial Systems Through Shared Services.

The specific legal basis for the collection of Social Security numbers is Executive Order 9397 as amended by Executive Order 13478; Pub. L. 100-202, Pub. L. 100-440, and Pub. L. 101-509.

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

ECAS does not retrieve information by a personal identifier, and therefore, ECAS is not itself a Privacy Act system of records. However, the information contained in ECAS is obtained from other sources that constitute a system of records and is covered by OPM/Internal 5: Pay, Leave, and Travel Records.

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

The ECAS System has an actively maintained System Security Plan (SSP) and associated plans, regularly reviewed in conjunction with the office of the Chief Information Security Officer (CISO).

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

Records are covered by the NARA, General Records Schedule 1.1, items: 001, 010, 012, 013, 020, 040, 070, and 071.

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.

The collection of information by ECAS is not covered by the Paperwork Reduction Act (PRA). No information is obtained directly from individual members of the public.

Section 2.0. Characterization of the Information

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

ECAS collects, uses, disseminates, or maintains various information that it obtains from other systems and programs in both individual-level and aggregate form. Information about individuals in ECAS, which is visible and accessible to only a minimal number of system administrators, includes the following fields: masked Social Security number (SSN); Pay Plan; Pay Plan Paid; Pay Plan Worked; Pay Status; Last Name; First Name; Budget Object Class; Hours and Type of Hours; Pay and Type of Pay; Cost and Type of Cost; OPAC Reference; Labor Code; Fund; Program; Labor Code Organization; Overlay Reference; Project; Agency; Facility; Organization; Cost Organization; User ID; Department ID; Accounting Code; Occupational Series; Office Title; Position Description/Function Statement; Pay Plan; Grade; Step; Location; Description; City; County; State; Grade and Step.

The following limited fields, without associated identifying name and SSN, are available to end users: Pay Plan; Pay Plan Paid; Pay Plan Worked; Budget Object Class; Hours and Type of Hours; Pay and Type of Pay; Cost and Type of Cost; OPAC Reference; Labor Code; Fund; Program; Labor Code Organization; Overlay Reference; Project; Agency; Facility; Organization; Cost Organization; Department ID; Accounting Code; Occ Series; Office Title; Position Description/Function Statement; Pay Plan; Grade; Step; Location; Description; City; County; and State.

In addition, ECAS collects, maintains, or disseminates other information it obtains from other systems and programs in the aggregate.

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

Data collected and used by the ECAS system are provided in flat file static exports from other systems, internal and external to OPM. Information about individuals in identifiable form, as well as aggregate information, is obtained

from Delphi, HRLinks, Labor Distribution System, and OPM operating unit accounting groups. Aggregate information, not identifiable to particular individuals is also obtained from the following systems: Purchase Request Information System for Management (PRISM), Facilities, Security, and Emergency Management (FSEM) Personal Identity Verification (PIV) Card System, Object Business Intelligence Enterprise Edition (OBIEE), Annuity Roll Processing System (ARPS), Document/ Case Control System (DCSS), and Services Online, as well as from internal OPM program offices. These files will be regularly (e.g., quarterly) deposited on an OPM shared drive, where they will be merged and then transmitted via SFTP protocol to the ECAS cloud environment through an OPM VPN. At this point, ECAS will extract, transform, and load (ETL) the data into the system.

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

ECAS does not use information from commercial sources, nor does it use any publicly available data sources.

2.4. Discuss how accuracy of the data is ensured.

The accuracy of the data is dependent upon the assessment and analysis of data maintained in the authoritative source systems from which ECAS obtains the data. The ECAS system ingests data from other systems and accuracy of the ingested data will be ensured through testing of the system's ETL processes to ensure complete and correct loading. The ECAS program will perform recurring data audits and testing whenever the system is modified. Additionally, the database automatically generates log files that capture updates to the data. These log files can be used for auditing purposes if needed.

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

Privacy Risk: There is a risk that PII, and particularly Social Security numbers, will be unnecessarily collected and maintained in ECAS.

Mitigation: This risk is mitigated through establishing effective policies to avoid the unnecessary collection of PII. The system developers have carefully evaluated the collection and use of masked SSNs and the program and alternatives were deemed insufficient to meet the business needs of the system and ensure accuracy of the end user reports. The risk associated with the retention of PII, including masked SSNs, is mitigated partly by restricting access to that information within ECAS to only a small number of system administrators. No PII is disseminated or available for reporting. PII is only used to join and connect labor data.

Section 3.0. Uses of the Information

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

The information in ECAS is used for tracing operating unit financial transactions, as well as identifying employees' geographical locations, duty stations, labor hours, labor categories, and labor costs. End users will have access to this data to analyze the dashboard reports. No analysis is performed at an individual level. Analysis is performed only after the data has been joined to aggregate two separate data sets by an ECAS Administrator. The system uses the information to standardize cost management programs & practices across the agency and provide financial and operational metrics to inform management decision-making as part of routine business practices. It traces all costs reported in the agency's financial reports to OPM's external services in a centralized way and in a format to allow all analysts to understand their costs.

Masked SSNs are used to connect the payroll and roster data imported from HRLinks, as it is the only unique identifier common between the two reports. At this time, HRLinks cannot generate a single report containing the information required for use by ECAS.

Individuals' names are used in validation of successful importing following the ETL process. This information is not used to analyze anything related to

an individuals' financial impact on the agency. Individual fields are not disseminated from the ECAS program and are maintained and available only for system administrators to appropriately link data and validate that data imports were successful.

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.

Financial and aggregated personnel data is analyzed using COTS software for patterns related to OPM expenses, labor hours, and financial interactions between OPM Programs/Offices. OPM cost accounting professionals will use these results to report to OPM leadership for budgeting and fiscal year planning.

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

A limited number of representatives from most OPM programs and offices will have access to aggregated financial reports for their area or function. Other OPM users, in limited circumstances and based on a documented need, will be granted access to create and edit cost models; however, these users will not be able to affect raw data directly. No user, other than a limited number of system administrators, will have access to or responsibility for the PII that is maintained in ECAS. User roles and responsibilities will be documented and maintained by the ECAS project team.

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

Privacy Risk: There is a risk that unauthorized users will access the PII contained in ECAS or that an authorized user will access the PII for a purpose inconsistent with the business purpose for which it is being collected and maintained.

Mitigation: This risk is mitigated through Role Based Access Controls (RBAC) comprised of user provisioning, permissions management, and access controls. User access is also mapped to organizational duties performed to ensure that users only process data specific to their authorized functions. A fundamental element of these controls is segregating specific key roles and duties. In addition, ECAS generates audit logs that are available to be reviewed whenever anomalous events are registered.

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.

ECAS is not accessible by individual members of the public and, therefore, does not provide direct notice of its collection of information to individuals. Moreover, the use of an individual's information in ECAS is solely to assist in accurately aggregating information for cost accounting reporting and not to make individual-level decisions. ECAS compiles information from several sources that may collect information directly from individuals and provide appropriate notice regarding the collection and use of their information at the time of collection. Notice regarding ECAS and the information it collects, uses, and disseminates is provided through the publication of this Privacy Impact Assessment.

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

Individuals do not have the opportunity to consent to the collection and use of their information in ECAS.

4.3. Privacy Impact Analysis: Related to Notice

Privacy Risk: There is a risk that individuals are not aware that ECAS collects and uses their information.

Mitigation: This risk is mitigated through the publication of this PIA. Moreover, the system makes no decisions about individuals and so they are not directly affected by the business operations of the system.

Section 5.0. Data Retention by the Project

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

The information in ECAS is subject to General Records Schedule 1.1, items: 001, 010, 012, 013, 020, 040, 070, and 071. Currently, ECAS contains information only dating back to FY2016. ECAS records will be retained for 7 years after the close of the relevant fiscal year.

5.2. Privacy Impact Analysis: Related to Retention

Privacy Risk: There is a risk of retaining information longer than is necessary to meet the business needs of the ECAS program.

Mitigation: This risk will be mitigated by adhering to the relevant records schedule and disposing of the records when there is no longer a business need to keep them.

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.

Information is not shared outside of OPM as part of normal ECAS operations. Potential exceptions may exist if aggregated, un-editable reports are provided as part of audit requests from other Federal agencies, when legally authorized. Under no circumstances is PII shared from ECAS outside of OPM.

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

Information is not shared outside of OPM as part of normal ECAS operations. Potential exceptions may exist if aggregated, un-editable reports are provided as part of audit requests from other Federal agencies, when legally authorized. Such reports are not individual records covered by the SORN referenced in Section 1.2. Under no circumstances is PII shared from ECAS outside of OPM.

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

Information is not shared outside of OPM as part of normal ECAS operations. Potential exceptions may exist if aggregated, uneditable reports are provided as part of audit requests from other Federal agencies, when legally authorized. Under no circumstances is PII shared from ECAS outside of OPM. Re-dissemination of aggregated reports will only be permitted for reporting cost accounting financials within OPM, as applicable and approved by OPM procedures.

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

The project, program, or system does not maintain an accounting of disclosures since personal information is not disseminated. The system will only provide financial and operational metrics and aggregated, un-editable reports to inform management as part of routine business.

6.5. Privacy Impact Analysis: Related to Information Sharing

Privacy Risk: There is a risk that information about individuals may be shared outside of OPM contrary to the business purpose of ECAS.

Mitigation: This risk is mitigated by restricting access to PII to a limited number of system administrators. The risk is further mitigated because ECAS is not configured to connect, receive, or share PII with any other internal or external programs or systems.

Section 7.0. Redress

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

Individuals do not directly access ECAS or the information contained therein. ECAS does not use any information to make decisions about individuals, and the PII it contains is not observable within ECAS' management reports. The limited number of system administrators with access to PII use it only to aggregate information for end user reports properly. To the extent individuals wish to access the records covered by the SORN identified in Section 1.2, they may do so by contacting OPM's Chief Financial Officer, 1900 E Street, N.W., Washington, DC 20415-1200 and providing the following information: full name, date of birth, SSN, and employment identification number. Individuals requesting access must also comply with OPM's Privacy Act regulations regarding verification of identity and access to records at 5 C.F.R. part 297.

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

Individuals cannot request that information in ECAS be corrected or amended. ECAS is not the source system for any of the information about individuals that is used, and ECAS does not use any information to make decisions about individuals; therefore, any corrections for inaccurate or erroneous must be made in the originating system. To the extent individuals wish to request an amendment to records covered by the SORN identified in Section 1.2, they may do so by contacting OPM's Chief Financial Officer, 1900 E Street, N.W., Washington, DC 20415-1200, and providing the following information: full name, date of birth, SSN, and employment identification number. Individuals requesting access must also comply with OPM's Privacy Act regulations regarding verification of identity and access to records at 5 C.F.R. part 297.

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

Individuals cannot request access to or amendment of their information in ECAS. Notice concerning procedures to access and amend records in ECAS that are covered by the SORN referenced in Section 1.2 are provided through publication of that SORN and through publication of this PIA.

7.4. Privacy Impact Analysis: Related to Redress

Privacy Risk: There is a risk that individuals may not be able to access information about them that is contained in ECAS nor be afforded adequate opportunity to correct that information.

Mitigation: This risk is not mitigated within ECAS. The system does not use personally identifiable information in a manner that affects individual interests. It is mitigated, however, by providing individuals with appropriate information about accessing and correcting information of the type contained in ECAS through the publication of the SORN referenced in Section 1.2 and through publication of this PIA.

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?

The ECAS system will be administered by a limited privileged group of individuals with appropriate training in maintaining information privacy and security. Additionally, all users will need to access ECAS via OPM's VPN, through which they will have agreed to abide by OPM information privacy rules and regulations.

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

All employees and contractors with access to ECAS must complete annual Security and Privacy Awareness training. In addition, all users of ECAS are

provided with user guides and role-specific training, including information regarding appropriate access and use of the information in the system.

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

Access to ECAS is allowed only through an OPM VPN by authorized users with a PIV card. End users' access with be defined to provide only access to aggregate information necessary for reporting purposes. Only a limited number of individuals responsible for administering the system will be able to access information about individuals in identifiable form. Administrative users and access are determined by the business needs and requirements within CFO. The elements are limited by what can be studied in accordance with the regulations set forth by Department of Treasury and OMB.

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?

Currently, there is no current or planned information sharing arrangements for ECAS. If there are future information sharing arrangements, OPM security staff works with the requesting organization to enter into an ISA and MOU. These are reviewed by relevant OPM stakeholders and signed by both parties. The ISAs and MOUs are updated every three years or when there are changes to the system.

Responsible Officials

Douglas Glenn
Chief Financial Officer
Office of the Chief Financial Officer

Approval Signature

Signed Copy on file with the Chief Privacy Officer

Kellie Cosgrove Riley
Chief Privacy Officer