Privacy Impact Assessment

Administrative Billings and Collections System (ABCO)

- Version: 3.1
- Date: April 2019
- Prepared for: USDA National Finance Center (NFC)
- Administrative Billings and Collections System (ABCO)

United States Department of Agriculture

Privacy Impact Assessment for the

Administrative Billings and Collections System (ABCO)

April 2019

Contact Point
Trudy Sandefer
System Owner/Project Manager
504-426-7663

Reviewing Official
Gail Alonzo-Shorts
Information Systems Security Program Manager
504-228-3867

USDA National Finance Center
United States Department of Agriculture

Abstract

The National Finance Center (NFC) is a Shared Service Center under the OPM Human Resources Line of Business. To carry out its wide-ranging responsibilities, the U.S. Department of Agriculture (USDA), and its employees and managers have access to diverse and complex automated information systems, which include system, file servers, local and wide area networks running various platforms, and telecommunications systems to include communication equipment.

The USDA relies on its information technology systems, including the Administrative Billing and Collections (ABCO) system, to accomplish its mission of providing cost-effective and reliable services to the USDA, other Federal agencies, and the public at large.

The NFC Government Employees Services Division, which falls under USDA, is responsible for development, deployment, maintenance, and testing of the NFC ABCO major application.

This Privacy Impact Assessment is being conducted to fulfill the requirements of Section 208 of Public Law 107-347 (the E-Government Act of 2002).

Overview

The ABCO system is used to provide weekly billings for administrative accounts receivable. ABCO is also the accounts receivable system for the United States Department of Agriculture. ABCO provides a method for billing and collecting debts from Federal employees – current, separated, or retired – and vendors who have outstanding debts with the government. ABCO complies with all the requirements of the Debt Collection Act (USC Title 15, Chapter 41-V) and the information processed provides internal accounting control and reporting to USDA agencies, the Department of the Treasury, and numerous other government agencies.

Section 1.0 Characterization of the Information

The following questions are intended to define the scope of the information requested and/or collected as well as reasons for its collection as part of the program, system, rule, or technology being developed.

1.1 What information is collected, used, disseminated, or maintained in the system?

The Administrative Billing and Collections (ABCO) system provides billings for administrative accounts receivable on a weekly basis. It uses HR data of federal employees who have outstanding debts, including their name, their social security number (SSN) (which is stored as "Debtor ID" in ABCO), their mailing addresses used to send bills to, information about the debt owed (to be collected) such as amount, and other system defined tracking numbers such as Claim Number and Debtor Number (which also includes the individual's SSN).

1.2 What are the sources of the information in the system?

Federal agencies and employees can provide data for use in the system.

1.3 Why is the information being collected, used, disseminated, or maintained?

The purpose of the collected data is to provide weekly billings for administrative accounts receivable.

1.4 How is the information collected?

Information is collected via data entry and front end interfaces from federal agencies and authorized agency users. Agencies submit data via connect direct and secure FTP over a VPN connection. Only authorized agency users with an established "need-to-know" may access their specific agency data.

1.5 How will the information be checked for accuracy?

ABCO application code provides reconciliation routines at the application level. These are maintained on the mainframe and applied to data entered and data transferred there. As personnel actions and payroll documents are processed each pay period, updated data replaces existing data elements on the ABCO database. Extensive error-checking routines are built into applications including edits of data received, record counts and database status checking.

1.6 What specific legal authorities, arrangements, and/or agreements defined the collection of information?

5 U.S.C. Sec. 552a governs the collection, use and safeguarding of data collected on individuals.

The SORN is USDA/OCFO-10

1.7 Privacy Impact Analysis: Given the amount and type of data collected, discuss the privacy risks identified and how they were mitigated.

NFC complies with the National Institute of Standards and Technology (NIST) and the Federal Information Security Management Act (FISMA), to ensure that data is protected from unauthorized access, malicious or inadvertent modification, disclosure, and disruption.

NFC also works diligently to secure Personally Identifiable Information (PII) by requiring adequate training of employees and contractors that have access to the data. NFC provides the degree of protection (administrative, technical, and physical safeguards) for the data collected as prescribed by the Privacy Act of 1974, 5 U.S.C. Section 552a. NFC ensures all data included in data file transmissions are provided, received, and stored in a secure manner. NFC protects, labels, and handles the data in accordance with 5 U.S.C. Section 552, Privacy act of 1974, as amended and applicable to agency regulations. All employees and contractors adhere to security requirements for handling and storing of Federal data as directed by the Electronic Government Act Title III, also known as FISMA.

Section 2.0 Uses of the Information

The following questions are intended to delineate clearly the use of information and the accuracy of the data being used.

2.1 Describe all the uses of information.

The purpose and routine uses of the data is to provide weekly billings for administrative accounts receivable.

2.2 What types of tools are used to analyze data and what type of data may be produced?

ABCO has data validation routines built into the interface that check for required fields, data types, and data ranges. Additionally, the business logic layer processes data before it is committed to the database, checking the data against business logic for accuracy and consistency. Authorized agency users may run predefined and custom reports against the data and have the ability to access data elements depending on access privileges requested by authorized agency security personnel.

2.3 If the system uses commercial or publicly available data please explain why and how it is used.

All information is provided by the agency and does not use commercial or publicly available data.

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

ABCO uses mainframe CA Top Secret System (TSS) userid and password for authentication and authorizations are based upon IDMS security access codes granted through role base access to protect data. Only authorized agency users have access to these records. Access to information is provided on a need-to-know basis and follows our "least privilege" policy. Top Secret and IDMS are used to manage end user security. The purpose and routine uses of the data is to provide weekly billings for administrative accounts receivable.

Section 3.0 Retention

The following questions are intended to outline how long information will be retained after the initial collection.

3.1 How long is information retained?

The retention periods of data contained in this system are covered by NARA General Records Schedule GRS-1-1 (Financial Management and Reporting Records). ABCO data on the mainframe is retained indefinitely.

3.2 Has the retention period been approved by the component records officer and the National Archives and Records Administration (NARA)?

Yes. This system complies with the guidance contained in the NARA General Records Schedule GRS-1-1 (Financial Management and Reporting Records).

3.3 Privacy Impact Analysis: Please discuss the risks associated with the length of time data is retained and how those risks are mitigated.

The purpose of retaining the information is to provide historical data to respond to any issues including but not limited to payroll and benefit corrections. Risks are mitigated via controls identified in para 2.4 above.

Section 4.0 Internal Sharing and Disclosure

The following questions are intended to define the scope of sharing within the United States Department of Agriculture.

4.1 With which internal organization(s) is the information shared, what information is shared and for what purpose?

Authorized agency users of approximately 35 USDA agencies have access to this data. The agency security officers handle all security access requests for any information pertaining to user accounts/access based on supervisory requests. Access is based on the principle of least

privilege, which refers to granting the minimum required system resources to a user that enables them to perform their duties/access their data. Access is determined by agencies functional managers and submitted by the agency security officers. NFC will grant authority to use/access ABCO to authorized users at the request of the agencies security officer.

ABCO exchanges data with the following within USDA:

- NFC Enterprise Infrastructure and Platforms
- NFC Payroll/Personnel System Major Application
- NFC Payroll Accounting System Major Application
- NFC WebApps Major Application
- NFC Miscellaneous Administrative Systems Group Major Application
- NFC Insight Major Application
- USDA OCFO/FMS - Financial Management Modernization Initiative
- USDA OCFO/FMS - Reporting of IPAC Transactions for Agriculture

4.2 How is the information transmitted or disclosed?

Information is collected via data entry and front end interfaces from authorized agency users. Agencies submit data via connect direct and secure FTP over a VPN connection. Only authorized agency users with an established "need-to-know" may access the specific agency data.

4.3 Privacy Impact Analysis: Considering the extent of internal information sharing, discuss the privacy risks associated with the sharing and how they were mitigated.

The agency security officer handles requests for information pertaining to user accounts. Access control is based on the principle of least privilege, which refers to granting the minimum required system resources to a user that enables them to perform their duties. Access is determined by the agency and based upon the application need, and level to access the data. Authorized agency users only have access to their specific agency data. There is no risk of other agency data being accessed by an unauthorized user.

Section 5.0 External Sharing and Disclosure

The following questions are intended to define the content, scope, and authority for information sharing external to USDA which includes Federal, state and local government, and the private sector.

5.1 With which external organization(s) is the information shared, what information is shared, and for what purpose?

Approximately 160 Federal agencies payroll by the NFC have access to their specific agency information. Information collected by ABCO is owned by each agency. Each agency determines the use and sharing of their information. NFC maintains and secures the information on behalf of our customers. Access is determined by agencies functional managers and submitted to agency security officers. NFC will grant authority to use/access ABCO to authorized users at the request of the agencies security officer.

ABCO provides data to the following:

- Department of Treasury – Treasury Offset Program
- Department of Treasury – Intra Governmental Payment and Collection System
- Iron Mountain - Digital Records Center for Images System

5.2 Is the sharing of personally identifiable information outside the Department compatible with the original collection? If so, is it covered by an appropriate routine use in a SORN? If so, please describe. If not, please describe under what legal mechanism the program or system is allowed to share the personally identifiable information outside of USDA.

Please see Section 5.1 above. NFC follows the USDA/OCFO-10, Financial Systems SORN as reference.

5.3 How is the information shared outside the Department and what security measures safeguard its transmission?

Information is collected from authorized agency users. Agencies submit data and file transfers via connect direct and secure FTP over a VPN connection. Only authorized agency users with an established "need-to-know" may access their specific agency data. ABCO exchanges data with Treasury systems TOP and IPAC via VPN. Iron Mountain contractors at a local facility in Harahan, LA, convert Payroll reports from ABCO into PDF files, encrypt the files, and transmit them to Iron Mountain in Boyers, PA.

5.4 Privacy Impact Analysis: Given the external sharing, explain the privacy risks identified and describe how they were mitigated.

Only authorized agency users can access information under the "need-to-know" policies. The proper controls are in place to protect the data and prevent unauthorized access.

Section 6.0 Notice

The following questions are directed at notice to the individual of the scope of information collected, the right to consent to uses of said information, and the right to decline to provide information.

6.1 Was notice provided to the individual prior to collection of information?

No. The ABCO system uses personal data provided by agencies to generate reports or notices. These are used by each agency to notify the individual of the status of debts owed. Only authorized agency users have access to ABCO data.

6.2 Do individuals have the opportunity and/or right to decline to provide information?

Not applicable.

6.3 Do individuals have the right to consent to particular uses of the information? If so, how does the individual exercise the right?

Not applicable.

6.4 Privacy Impact Analysis: Describe how notice is provided to individuals, and how the risks associated with individuals being unaware of the collection are mitigated.

Not applicable.

Section 7.0 Access, Redress and Correction

The following questions are directed at an individual's ability to ensure the accuracy of the information collected about them.

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

Individuals do not have access to ABCO data. Only authorized agency users have access to data in the system.

7.2 What are the procedures for correcting inaccurate or erroneous information?

Information in the system must be corrected by authorized users from the individual agency or at the request of the agency.

7.3 How are individuals notified of the procedures for correcting their information?

Each agency using the system is responsible for the accuracy of the data and would provide this information to individuals. The system generates reports and notices that are used by each agency for notification purposes.

7.4 If no formal redress is provided, what alternatives are available to the individual?

Please refer to Section 7.3.

7.5 Privacy Impact Analysis: Please discuss the privacy risks associated with the redress available to individuals and how those risks are mitigated.

It is the responsibility of the agency to ensure that personnel with access to correct data on individuals have the proper clearances, position sensitivity designations, and appropriate system access to file data. NFC access control procedures, role based security of the application, and agency reporting of authorized user access and utilization aid agency officials to mitigate the risks of improper access.

Section 8.0 Technical Access and Security

The following questions are intended to describe technical safeguards and security measures.

8.1 What procedures are in place to determine which users may access the system and are they documented?

The agencies determine user access. NFC follows Directive 58, Information Systems Security Program Revision 3, and Directive 2, Access Management.

8.2 Will Department contractors have access to the system?

Yes, if authorized by agency functional manager and submitted by the agency security officer.

8.3 Describe what privacy training is provided to users either generally or specifically relevant to the program or system?

Authorized agency users and contractors must complete annual security awareness and rules of behavior training and be properly trained on the system.

8.4 Has Assessment & Accreditation been completed for the system or systems supporting the program?

Yes.

8.5 What auditing measures and technical safeguards are in place to prevent misuse of data?

ABCO provides auditing at the application, database and network/operating system levels.

8.6 Privacy Impact Analysis: Given the sensitivity and scope of the information collected, as well as any information sharing conducted on the system, what privacy risks were identified and how do the security controls mitigate them?

A Risk Assessment was performed on ABCO, and security controls have been documented in the System Security Plan. These controls are tested annually under the continuous monitoring and SSAE-18 programs.

Section 9.0 Technology

The following questions are directed at critically analyzing the selection process for any technologies utilized by the system, including system hardware and other technology.

9.1 What type of project is the program or system?

The ABCO system provides billings for administrative accounts receivable on a weekly basis. Most administrative billings are on a one-time basis with some accounts being liquidated by partial payments. ABCO complies with all requirements of the Debt Collection Act and provides internal accounting control and reporting to agencies, the Department of the Treasury, etc.

9.2 Does the project employ technology which may raise privacy concerns? If so please discuss their implementation.

No. ABCO is an established mainframe application with no web component. The ABCO system has undergone a detailed security vulnerability assessment and has been certified and authorized.

Section 10.0 Third Party Websites/Applications

The following questions are directed at critically analyzing the privacy impact of using third party websites and/or applications.

10.1 Has the System Owner (SO) and/or Information Systems Security Program Manager (ISSPM) reviewed Office of Management and Budget (OMB) memorandums M-10-22 "Guidance for Online Use of Web Measurement and Customization Technology" and M-10-23 "Guidance for Agency Use of Third-Party Websites and Applications"?

Yes.

10.2 What is the specific purpose of the agency's use of 3rd party websites and/or applications?

ABCO does not utilize 3rd party websites.

10.3 What personally identifiable information (PII) will become available through the agency's use of 3rd party websites and/or applications.

Not applicable.

10.4 How will the PII that becomes available through the agency's use of 3rd party websites and/or applications be used?

Not applicable.

10.5 How will the PII that becomes available through the agency's use of 3rd party websites and/or applications be maintained and secured?

Not applicable.

10.6 Is the PII that becomes available through the agency's use of 3rd party websites and/or applications purged periodically?

No.

If so, is it done automatically?

Not applicable.

If so, is it done on a recurring basis?

Not applicable.

10.7 Who will have access to PII that becomes available through the agency's use of 3rd party websites and/or applications?

Not applicable.

10.8 With whom will the PII that becomes available through the agency's use of 3rd party websites and/or applications be shared - either internally or externally?

Not applicable.

10.9 Will the activities involving the PII that becomes available through the agency's use of 3rd party websites and/or applications require either the creation or modification of a system of records notice (SORN)?

No.

10.10 Does the system use web measurement and customization technology?

No.

If so, is the system and procedures reviewed annually to demonstrate compliance to OMB M-10-23?

Not applicable.

10.11 Does the system allow users to either decline to opt-in or decide to opt-out of all uses of web measurement and customization technology?

Not applicable.

If so, does the agency provide the public with alternatives for acquiring comparable information and services?

Not applicable.

10.12 Privacy Impact Analysis: Given the amount and type of PII that becomes available through the agency's use of 3rd party websites and/or applications, discuss the privacy risks identified and how they were mitigated.

Not applicable.

Agency Responsible Officials

CHERIE LANDRY

Digitally signed by CHERIE LANDRY
Date: 2019.05.24 10:02:10 -05'00'

System Manager/Owner
Trudy Sandefer, Associate Director
Mainframe Applications Directorate
Government Employees Services Division
USDA National Finance Center

GAIL ALONZO SHORTS

Digitally signed by GAIL ALONZO SHORTS
Date: 2019.05.28 22:29:18 -05'00'

NFC Privacy Officer/ISSPM/CISO
Gail Alonzo-Shorts, Branch Chief
Access Management Branch
Information Technology Services Division
USDA National Finance Center

Agency Approval Signature

ANITA ADKINS

Digitally signed by ANITA ADKINS
Date: 2019.07.26 17:26:34 -05'00'

Authorizing Official Designated Representative
Anita Adkins, Acting Director
Government Employees Services Division
USDA National Finance Center