Privacy Impact Assessment

Miscellaneous Administrative Systems Group (ADMIN)

- Version: 2.3
- Date: November 2018
- Prepared for: USDA National Finance Center
- Miscellaneous Administrative Systems Group

United States Department of Agriculture

Privacy Impact Assessment for the

Miscellaneous Administrative Systems Group (ADMIN)

November 2018

<u>Contact Points</u>
Debby Tatum, Associate Director
Web Applications Directorate
504-426-7664

<u>Reviewing Official</u>
Ivan Jackson, Associate Director
Information Technology Security Directorate
504-426-7551

USDA National Finance Center
United States Department of Agriculture

Abstract

The National Finance Center (NFC) is a Shared Service Center (SSC) under the OPM Human Resources Line of Business (HRLOB). 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 Miscellaneous Administrative Systems Group (ADMIN), 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 (GESD), which falls under the USDA National Finance Center (NFC), is responsible for development, deployment, maintenance, and testing of the NFC ADMIN major application (MA).

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

Overview

ADMIN is compiled of NFC designed, implemented, managed, and maintained applications performing a variety of administrative functions. All applications within ADMIN are used by NFC to gather statistical information and/or to simplify/automate redundant tasks.

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 NFC ADMIN MA is composed of NFC-managed applications performing a variety of GESD administrative functions using IDMS and DB2 databases on the NFC Mainframe. These applications are used by NFC to aid in debt collection, gather statistical information, and/or to simplify/automate redundant tasks. The following types of information are collected and maintained: batch jobs processing details (SITS);

Name and payment information about accounts receivable (DOTS/DOTSE), informational display system of delinquent debts to Treasury (SOAP); and statistical data about documents processed by NFC (STAT). The data elements include: Name, Date of birth, Address information, Personal identification number (e.g. social security number), and Financial data (check numbers, bank account numbers, and cancelled and returned check information).

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

Customer agencies provide data for use in the system.

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

The purpose of the data in ADMIN is to enable NFC to perform administrative functions to aid in debt collection, to gather statistical data, and to automate redundant tasks.

1.4 How is the information collected?

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

1.5 How will the information be checked for accuracy?

ADMIN 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 ADMIN 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 tile collection, use and safeguarding of data collected on individuals.

1.7 <u>Privacy Impact Analysis</u>: 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 the Federal Information Security Management Act (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 data in ADMIN is used to enable NFC to perform administrative functions to aid in debt collection, to gather statistical data, and to automate redundant tasks.

The purpose and routine uses of the data include recording, processing, and reporting the personnel and payroll data for USDA and other Federal agencies.

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

ADMIN has data validation routines built into the interface that checks 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. Individuals and agencies 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 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 individual, customer, or agency; ADMIN 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.

ADMIN uses role based access and UserID/password to protect access to data. Individuals only have access to their own records. Access to information is provided on a need-to-know basis and follows our "least privilege" policy. Top Secret, DB2 Secure Table and Windows file security are used to manage end user security. ADMIN maintains strong role based security controls. The purpose and routine uses of the data include recording, processing, and reporting the personnel and payroll data for USDA and other Federal agencies.

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 data contained in this system is covered by NFC Schedule NC1-16-78-6, which identifies a retention period of 10 years.

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

Yes. NFC Schedule NC1-16-78-6 has been approved

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, debt, and payment amounts. 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 system/agency security officers handle all 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 requested/determined by personnel/payroll offices who submit the data. NFC will grant authority to use/access ADMIN to individual users at the request of the agencies approved by the user's Agency security officer.

ADMIN exchanges data with the following systems within USDA:

- NFC Administrative Billings and Collections System (ABCO). DOTS exchanges data with the ABCO system via internal NFC Mainframe FTP to establish an accounts receivable when appropriate.
- NFC Payroll Accounting System (PAS) DISB application. DOTS interfaces with Disbursing (DISB) systems to reissue checks.
- NFC Payroll Personnel System (PPS) PAYE application. DOTS interfaces with the Payroll/Personnel (PAYE) system to reissue checks.

4.2 How is the information transmitted or disclosed?

Data is exchanged between ADMIN and other NFC applications via internal NFC Mainframe FTP process.

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.

Data is exchanged between ADMIN and other NFC applications via internal NFC Mainframe FTP process.

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?

ADMIN exchanges data with the following:

- Department of the Treasury, Bureau of the Fiscal Service - Payments, Claims and Enhanced Reconciliation (PACER) system. PII shared consists of Personnel Data: SSN, Name, and Check Number. The ADMIN Document Tracking System (DOTS) receives a daily Cancelled and Returned Checks report from the Treasury PACER system. The file contains all checks issued by NFC which may have been returned to Treasury due to closed accounts, incorrect addresses, etc.
- Department of the Treasury, Bureau of the Fiscal Service – Treasury Offset Program (TOP). PII shared consists of Personnel Data: SSN, Name. The ADMIN Salary Offset Agency Process (SOAP) sends TOP a list of offsets collected from employees who are indebted to the government. TOP sends to SOAP information on debts owed by employees.

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.

NFC follows the USDA/OP-1, Personnel and Payroll System for USDA Employees Customer agency SORN as reference.

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

ADMIN exchanges data with the Department of the Treasury via a secure VPN connection.

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

Only authorized individuals 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?

Most data in ADMIN is obtained from other NFC applications. Any personal data in ADMIN was provided by agencies to these applications. Agencies are responsible for notifying employees of personal information collected.

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

Agencies are responsible for notifying employees of information collected.

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

Agencies are responsible for notifying employees of information collected and obtaining consent.

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

Agencies are responsible for notifying employees of information collected. From a regulatory and management controls perspective, a copy of the redacted PIA is available on USDA's Office of the Chief Information Officer web site.

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 ADMIN 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 would provide this information to individuals.

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 the data. NFC access control procedures, role based security of the application, and agency reporting of individual access and utilization aid agency officials to mitigate the risks of agency individuals with 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 Security Program and Directive 2, Access Management.

8.2 Will Department contractors have access to the system?

Yes, if authorized a valid role.

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

Employees and contractors must complete annual security training and be properly trained on the system.

8.4 Has Assessment & Authorization 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?

ADMIN 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 ADMIN 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?

ADMIN is a group of several administrative systems that NFC uses to perform administrative functions to aid in debt collection, to gather statistical data, and to automate redundant tasks.

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

No. ADMIN is an established mainframe application with no web component. The ADMIN system has undergone a detailed security vulnerability assessment and has been Assessed 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?

ADMIN 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?

Not applicable.

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)?

Not applicable.

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?

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 <u>Privacy Impact Analysis</u>: 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

DEBORAH TATUM Digitally signed by DEBORAH TATUM
Date: 2018.11.07 16:06:10 -06'00'

System Manager/Owner

Debby Tatum, Associate Director
Web Applications Directorate
Government Employees Services Division
USDA National Finance Center

IVAN JACKSON Digitally signed by IVAN JACKSON
Date: 2018.11.13 13:39:34 -06'00'

NFC Privacy Officer / ISSPM / CISO

Ivan R. Jackson, Associate Director
Information Technology Security
Information Technology Services Division
USDA National Finance Center

Agency Approval Signature

ADA CHIAPPE Digitally signed by ADA CHIAPPE
Date: 2018.12.04 12:46:45 -06'00'

Authorizing Official Designated Representative

Cristina Chiappe, Director
Government Employees Services Division
USDA National Finance Center