



Privacy Impact Assessment (PIA)

Paycheck7

Version: 2.4

USDA FOREST SERVICE

Prepared for: Human Capital Management

Prepared By:



*19886 Ashburn Road
Ashburn, Virginia 20147*

Date: March 2008

DOCUMENT INFORMATION

Owner Details	
Name	Laree Edgecombe
Contact Number	703-605-0820
E-mail Address	ledgecombe@fs.fed.us

Document Revision and History			
Revision	Date	Author	Comments
2.0	1/4/2008	Xacta	Updated based on new USDA FS templates
2.1	1/11/2008	GN	Addressed comments and reviewed for accuracy
2.2		Xacta	2nd Review
2.3	3/10/2008	GN	2nd FS Review
2.4	3/11/2008	Xacta	Updated based on FS comments

Distribution List			
Name	Title	Agency/Office	Contact Information
Douglas Nash	FS Information Systems Security Program Manager	USDA FS IRM Information Security Arlington, VA	703-605-4892
Mike Grube	FS Information Security Staff	USDA FS IRM Information Security Asheville, NC	828 257-4335
Irene Savanyo	FS Information Security Staff	USDA FS IRM Information Security Taos, NM	505 758-6330
Laree Edgecombe	HCM Asst Dir, HR Technology	USDA FS HCM, WO Arlington, VA	703 605-0820
Janet Ford	HCM Branch Chief, Pay, Staffing and Classification	USDA FS HCM WO Arlington, VA	703 605-0828
Ginger Nethery	HCM Program Manager, Paycheck	USDA FS HCM WO Arlington, VA	703 605-0850
Deborah Rigden	HCM FS Pay Specialist	USDA FS HCM WO Arlington, VA	703 605-0822



TABLE OF CONTENTS

1	PRIVACY IMPACT ASSESSMENT.....	1
1.1	Introduction.....	1
1.2	Summary of Results of the Privacy Impact Assessment.....	1
	USDA Privacy Impact Assessment Form.....	2
1.2.1	DATA COLLECTION.....	5
1.2.2	DATA USE.....	6
1.2.3	DATA RETENTION.....	8
1.2.4	DATA SHARING.....	9
1.2.5	DATA ACCESS.....	11
1.2.6	CUSTOMER PROTECTION.....	11
1.2.7	SYSTEM OF RECORD.....	13
1.2.8	TECHNOLOGY.....	13
	PRIVACY IMPACT ASSESSMENT AUTHORIZATION MEMORANDUM.....	15



1 PRIVACY IMPACT ASSESSMENT

1.1 Introduction

The objective of the PIA is to assist USDA FS employees in identifying information privacy when planning, developing, implementing, and operating agency owned applications. The PIA will help USDA FS employees consider and evaluate whether existing statutory requirements are being applied to systems that contain personal information. These requirements are drawn from the Privacy Act of 1993, Children's Online Privacy Protection Act of 1998, Freedom of Information Act, Paperwork Reduction Act of 1995, Office of Management and Budget Memoranda M-99-18 dated June 2, 1998 and M-00-13 dated June 22, 2000 and OCIO memorandum, Use of Cookies on Web Pages, DR 3410-1, Information Collection Activities, and DR 3080-1, Records Disposition

The PIA is a Government requirement that helps to ensure that system owners and developers consider and evaluate existing statutory information management requirements that must be applied to new or modified applications that contain personal information. The goals accomplished in completing this PIA include:

- Providing USDA FS management with the tools to make informed policy and system design decisions.
- Ensuring accountability for privacy issues.
- Ensuring a consistent format and structured process for analyzing both technical and legal compliance of the application.
- Providing basic documentation on the flow of personal information within the application.

1.2 Summary of Results of the Privacy Impact Assessment

A review of the application, as installed by USDA FS, indicates that the Paycheck7 application does maintain identifiable form of information on individual employees. A completed USDA Privacy Impact Assessment Form is provided below.



USDA Privacy Impact Assessment Form

Agency: USDA Forest Service

System Name: Paycheck7

System Type: Major Application

System Categorization (per FIPS 199): Moderate

Description of the System:

Paycheck7 is an agency developed application for employees to report time and attendance. It provides agency employees with access to input daily hours worked for a bi-weekly period. It is designed to support field-level users in national forests with a common set of business rules and data standards in a common computing environment. Business processes using Paycheck7 are executed at the Washington Office and all Regional Offices; these support the Areas, Stations and Lab.

As Paycheck7 gathers time and attendance data from users, it validates the data against a set of business rules, obtains user and supervisor verification, and creates files which are transferred to the National Finance Center (NFC) for processing in the production of payroll reports.

Paycheck7 is presently a partially centralized database whose server components are installed on Domino cluster servers. Data resides in Oracle databases on IBM AIX servers located in the Washington Office, Region 3 Regional Office, Region 6 Regional Office and Region 9 Regional Office. There are 10 Domino server clusters storing application data which is managed from 1 master Domino server and 4 Domino servers are used to manage the approval process.

Who owns this system? (Name, agency, contact information)

Name: Laree Edgecombe
Title: Assistant Director, Human Capital Technology,
Agency: USDA Forest Service
Address: 1601 N. Kent Street, Arlington, VA 22209
Telephone number: 703-605-0820
E-mail: ledgecombe@fs.fed.us

Who is the security contact for this system? (Name, agency, contact information)

Name: Ginger Nethery, Paycheck7
Title: Program Manager,
Agency: USDA-Forest Service
Address: 1601 N. Kent Street, Arlington, VA 22209
Telephone Number: 703-605-0850



E-mail: gnethery@fs.fed.us

Who completed this document? (Name, agency, contact information)

Xacta Corporation
19886 Ashburn Road
Ashburn, Virginia 20147

Reviewed by:

Name: Ginger Nethery, Paycheck7
Title: Program Manager
Agency: USDA – Forest Service
Address: 1601 N Kent Street, Arlington, VA 22209
Telephone Number: 703-605-0850
E-mail: gnethery@fs.fed.us



DOES THE SYSTEM CONTAIN INFORMATION ABOUT INDIVIDUALS IN AN IDENTIFIABLE FORM?

Indicate whether the following types of personal data are present in the system.

QUESTION 1 Does the system contain any of the following type of data as it relates to individual:	Citizens	Employees
Name	No	Yes
Social Security Number	No	Yes
Telephone Number	No	No
Email address	No	Yes
Street address	No	No
Financial data	No	No
Health data	No	No
Biometric data	No	No
QUESTION 2 Can individuals be uniquely identified using personal information such as a combination of gender, race, birth date, geographic indicator, biometric data, etc.? NOTE: 87% of the US population can be uniquely identified with a combination of gender, birth date and five digit zip code ¹	No	No
Are social security numbers embedded in any field?	No	Yes
Is any portion of a social security numbers used?	No	No
Are social security numbers extracted from any other source (i.e. system, paper, etc.)?	No	No



If all of the answers in Questions 1 and 2 are NO,

You do not need to complete a Privacy Impact Assessment for this system and the answer to OMB A-11, Planning, Budgeting, Acquisition and Management of Capital Assets, Part 7, Section E, Question 8c is:

3. No, because the system does not contain, process, or transmit personal identifying information.

If any answer in Questions 1 and 2 is YES, provide complete answers to all questions below.

¹ Comments of Latanya Sweeney, Ph.D., Director, Laboratory for International Data Privacy Assistant Professor of Computer Science and of Public Policy Carnegie Mellon University To the Department of Health and Human Services On "Standards of Privacy of Individually Identifiable Health Information". 26 April 2002.



1.2.1 DATA COLLECTION

3. Generally describe the data to be used in the system.

Customer Data: None

Employee Data:

Personally Identifiable Information: (PII)

The application mandatorily maintains the following information:

- Last and First Name
- Social Security Number (SSN)

The following mandatory non-PII is maintained within the Paycheck7 application:

- Employee E-mail address
- Approver E-mail address
- Transaction Codes
- Override Codes
- Job Codes
- Appointment Limits
- Service Year Dates
- Annual Leave, Sick Leave and other leave balances if other than zero.
- Number of Hours Associated with Codes

4. Is the use of the data both relevant and necessary to the purpose for which the system is being designed? In other words, the data is absolutely needed and has significant and demonstrable bearing on the system’s purpose as required by statute or by Executive order of the President.

YES

NO

5. Sources of the data in the system.

5.1 What data is being collected from the customer?

Employee information includes the following:

- Number of Hours Associated with Codes

5.2 What USDA agencies are providing data for use in the system?

There are no other agencies that provide data for Paycheck7.

5.3 What state and local agencies are providing data for use in the system?

None



5.4 From what other third party sources is data being collected?

None

6. Will data be collected from sources outside your agency? For example, customers, USDA sources (i.e. NFC, RD, etc.) or Non-USDA sources.

YES

NO

If **NO**, go to Question 7

6.1 How will the data collected from customers be verified for accuracy, relevance, timeliness, and completeness?

6.2 How will the data collected from USDA sources be verified for accuracy, relevance, timeliness, and completeness?

6.3 How will the data collected from non-USDA sources be verified for accuracy, relevance, timeliness, and completeness?

1.2.2 DATA USE

7. Individuals must be informed in writing of the principal purpose of the information being collected from them. What is the principal purpose of the data being collected?

The principal purpose is to provide the National Finance Center, the proper number of hours to pay an employee for a given 2 week pay period.

8. Will the data be used for any other purpose?

YES

NO

If **NO**, go to Question 9

8.1 What are the other purposes?



9. Is the use of the data both relevant and necessary to the purpose for which the system is being designed? In other words, the data is absolutely needed and has significant and demonstrable bearing on the system's purpose as required by statute or by Executive order of the President

YES

NO

10. Will the system derive new data or create previously unavailable data about an individual through aggregation from the information collected (i.e. aggregating farm loans by zip codes in which only one farm exists.)?

YES

NO

10.1 Will the new data be placed in the individual's record (customer or employee)?

YES

NO

10.2 Can the system make determinations about customers or employees that would not be possible without the new data?

YES

NO

10.3 How will the new data be verified for relevance and accuracy?

11. Individuals must be informed in writing of the routine uses of the information being collected from them. What are the intended routine uses of the data being collected?

The routine use is to provide the National Finance Center the number of hours by which to properly pay an employee for a given 2 week pay period

12. Will the data be used for any other uses (routine or otherwise)?

YES

NO

If NO, go to Question 13

12.1 What are the other uses?



13. Automation of systems can lead to the consolidation of data – bringing data from multiple sources into one central location/system – and consolidation of administrative controls. When administrative controls are consolidated, they should be evaluated so that all necessary privacy controls remain in place to the degree necessary to continue to control access to and use of the data. Is data being consolidated?

YES

NO

If NO, go to Question 14

13.1 What controls are in place to protect the data and prevent unauthorized access?

14. Are processes being consolidated?

YES

NO

If NO, go to Question 15

14.1 What controls are in place to protect the data and prevent unauthorized access?

1.2.3 DATA RETENTION

15. Is the data periodically purged from the system?

YES

NO

If NO, go to Question 16

15.1 How long is the data retained whether it is on paper, electronically, in the system or in a backup?

Paper copies of T&A's are mandated to be stored up to 6 years or after a GAO Audit, whichever comes first.

Electronic data is retained for a period of 3 years, the NFC can only accept corrected T&A's up to 25 pay periods prior.



Backup files are maintained by the IRM/ISO staffs.

15.2 What are the procedures for purging the data at the end of the retention period?

Paper copies are destroyed by means of shredding.

Electronic data is maintained for a period of 3 years and then deleted from the database.

Per FSM 6683.82 - Media Sanitization and Disposal use sanitization and disposal methods appropriate for the information's FIPS 199 security categorization following guidelines found in National Institute of Standards and Technology (NIST) SP 800-88.

15.3 Where are these procedures documented?

Paper copies are retained and destroyed per National Archives and Record Administration and General Records (NARA) Schedule 2 and Schedule 20.

Electronic data is retained and destroyed per the USDA FS Paycheck7 System Features User Guide (SFUG).

16. While the data is retained in the system, what are the requirements for determining if the data is still sufficiently accurate, relevant, timely, and complete to ensure fairness in making determinations?

The hardcopy/paper T&A is the official documentation. Electronic data is validated/verified with the hardcopy/paper T&A. If changes to the data are made that affect the pay received than a corrected T&A would need to be submitted to the NFC within one year of completing the original T&A. If changes to the data are necessary after one year then a personnel action must be completed and processed through the NFC. Leave audits are performed yearly on all employees to ensure leave data is accurately reflected. The NFC is the database of record and is considered correct unless the employee can proof otherwise.

17. Is the data retained in the system the minimum necessary for the proper performance of a documented agency function?

YES

NO

1.2.4 DATA SHARING

18. Will other agencies share data or have access to data in this system (i.e. international, federal, state, local, other, etc.)?



- YES
 NO

If **NO**, go to Question 19

18.1 How will the data be used by the other agency?

18.3 Who is responsible for assuring the other agency properly uses of the data?

19. Is the data transmitted to another agency or an independent site?

- YES
 NO

If **NO**, go to Question 20

19.1 Is there the appropriate agreement in place to document the interconnection and that the PII and/or Privacy Act data is appropriately protected?

Yes, there is an agreement in place with the National Finance Center to accept time information by which to accurately make salary payments to USDA Forest Service employees. This agreement is maintained through Green Book procedures and at the USDA department level.

20. Is the system operated in more than one site?

- YES
 NO

If **NO**, go to Question 21

20.1 How will consistent use of the system and data be maintained in all sites?

Software versions are maintained and updated through one server.

Updates/changes/edits are all maintained on one server and this information is replicated throughout the Lotus Notes environment. The oracle databases are maintained and upgraded through the Database Administration group of IRM/ISO and they follow specific procedures to maintain consistency. Controls that enforce the consistent use of the Paycheck application and its data include:

- Use of specific roles depending on the need of each user
- User Identification and Authentication to the system through an LDAP
- Encryption during transmission to NFC



- Intrusion detection at the network level

1.2.5 DATA ACCESS

21. Who will have access to the data in the system (i.e. users, managers, system administrators, developers, etc.)?

Employees, Paycheck Administrators, Application Managers, Oracle Database Administrators.

22. How will user access to the data be determined?

Role based access controls ensure only the individual employee and individuals authorized to review, approve, and process records can view details.

22.1 Are criteria, procedures, controls, and responsibilities regarding user access documented?

YES

NO

23. How will user access to the data be restricted?

Access to Paycheck7 is granted through Lotus Notes accounts and Oracle Admin instance accounts.

Are procedures in place to detect or deter browsing or unauthorized user access?

YES

NO

24. Does the system employ security controls to make information unusable to unauthorized individuals (i.e. encryption, strong authentication procedures, etc.)?

YES

NO

1.2.6 CUSTOMER PROTECTION

25. Who will be responsible for protecting the privacy rights of the customers and employees affected by the interface (i.e. office, person, departmental position, etc.)?

The USDA Forest Service HCM is responsible for protecting the privacy rights.



26. How can customers and employees contact the office or person responsible for protecting their privacy rights?

Employees may contact the ASC-HCM regarding their privacy rights.

27. A "breach" refers to a situation where data and/or information assets are unduly exposed. Is a breach notification policy in place for this system?

YES

NO

If YES, go to Question 28

27.1 If NO, please enter the POAM number with the estimated completion date:

28. Consider the following:

- Consolidation and linkage of files and systems
- Derivation of data
- Accelerated information processing and decision making
- Use of new technologies

Is there a potential to deprive a customer of due process rights (fundamental rules of fairness)?

YES

NO

If NO, go to Question 29

28.1 Explain how this will be mitigated?

29. How will the system and its use ensure equitable treatment of customers?

All employees are to be paid for their hours worked, so all employees are provided access to input their time and submit it for payment either through a Lotus Notes account provided for them or individuals who have the role of Paycheck Administrator can submit time for an employee without a Lotus Notes account.

30. Is there any possibility of treating customers or employees differently based upon their individual or group characteristics?

YES

NO



If **NO**, go to Question 31

30.1 Explain

1.2.7 SYSTEM OF RECORD

31. Can the data be retrieved by a personal identifier? In other words, does the system actually retrieve data by the name of an individual or by some other unique number, symbol, or identifying attribute of the individual?

YES

NO

If **NO**, go to Question 32

31.1 How will the data be retrieved? In other words, what is the identifying attribute (i.e. employee number, social security number, etc.)?

The Lotus Notes short name or the employee's last name is used for data retrieval.

31.2 Under which Systems of Record notice (SOR) does the system operate? Provide number, name and publication date. (SORs can be viewed at www.access.GPO.gov)

Privacy Act SOR USDA/OP-1 Personnel and Payroll System for USDA Employees.

31.3 If the system is being modified, will the SOR require amendment or revision?

No

1.2.8 TECHNOLOGY

32. Is the system using technologies in ways not previously employed by the agency (e.g. Caller-ID)?

YES

NO

If **NO**, the questionnaire is complete.

32.1 How does the use of this technology affect customer privacy?



Upon completion of this Privacy Impact Assessment for this system, the answer to OMB A-11, Planning, Budgeting, Acquisition and Management of Capital Assets, Part 7, Section E, Question 8c is:

1. Yes.

PLEASE SUBMIT A COPY TO
THE OFFICE OF THE ASSOCIATE CHIEF INFORMATION OFFICE/CYBER SECURITY



PRIVACY IMPACT ASSESSMENT AUTHORIZATION MEMORANDUM

I have carefully assessed the Privacy Impact Assessment for the

Paycheck7
(System Name)

This document has been completed in accordance with the requirements of the E-Government Act of 2002.

~~We fully accept the changes as needed improvements and authorize initiation of work to proceed. Based on our authority and judgment, the continued operation of this system is authorized.~~ (statement not required for recertification)

Ginger Anthony 3 APR-2008
System Manager/Owner Date
OR Project Representative
OR Program/Office Head.

Cassie M Rice 5-1-2008
Agency's Chief FOIA officer Date
OR Senior Official for Privacy
OR Designated privacy person

[Signature] 5/15/08
Agency OCIO Date