Privacy Impact Assessment
Web Total Cost Account System (WebTCAS)

Technology, Planning, Architecture, & E-Government

- Version: 2.02
- Date: July 29, 2013
- Prepared for: USDA OCIO TPA&E

USDA
United States Department
of Agriculture

Privacy Impact Assessment for the

Web Total Cost Account System (WebTCAS)

29 July 2013

Contact Point
Paige Niederer
Natural Resources Conservation Service
970-295-5496

Reviewing Official
Lian Jin
Acting Chief Information Security Officer
United States Department of Agriculture
202-720-8493

Abstract

The Web Total Cost Account System (WebTCAS) is a system of the Natural Resources Conservation Service (NRCS).

NRCS employees record their individual time and attendance data using the WebTCAS Internet accessible web site interface. WebTCAS processes the time and attendance data and forwards this data to produce records from which employee paychecks are derived.

A Privacy Threshold Analysis (PTA) was performed, indicating that a PIA must be completed. This PIA is being conducted to comply with the Federal Information Security Management Act of 2002 (FISMA) and the E-Government Act of 2002 (Public Law. 107-347, 116 Stat. 2899, 44 U.S.C. § 101, H.R. 2458/S. 803) Federal Law.

Overview

The Web Total Cost Account System (WebTCAS) is a system of the Natural Resources Conservation Service (NRCS). The purpose of WebTCAS is to provide consolidated, efficient and simplified reporting of employee labor hours as applied against the many various NRCS programs and projects nationwide. NRCS employees record their individual time and attendance data using the WebTCAS Internet accessible web site interface.

The data contained within the WebTCAS system includes employee name, USDA assigned employee number, labor hours, and various time charge codes (job/project activity codes, vacation/sick time codes, etc.). HR repositories (that are maintained outside of WebTCAS) also include Social Security Number (SSN) information for NRCS employees. This is PII required to transfer labor hour information to HR for payroll purposes, since the payroll system does not recognize any other employee identifier.

The information collected includes hours worked, leave hours taken, arrival and departure times, time taken for lunch, associated activity codes, and extra accrued hours. This facilitates the mission of the organization by providing necessary inputs for the generation of employee payroll, personnel scheduling, activity cost accounting, and other such labor hour related administrative requirements.

A typical system transaction involves an individual employee logging into the system, entering labor hours for a particular day into data cells for the specific appropriate activity code(s), saving the data and logging out of the system. While the NRCS employees do not enter any PII, they do record their individual time and attendance data using the WebTCAS Internet accessible web site interface. As data is submitted, several internal modules process it. These modules store the timesheet and profile information in database tables, use data to produce records from which employee paychecks are derived, and produce views and screens used for other time recordkeeping functions. Individual NRCS employees maintain their own individual WebTCAS time records. After timesheets are submitted within the application by the employees, an NRCS assigned "timekeeper" accesses all the timesheets for that timekeeper's group using authenticated web browser sessions, and verifies timesheets against the employees' job assignments, project codes, etc. Once they match, the timekeeper verifies the timesheets inside the application browser window. After the timekeeper verifies the timesheet, the supervisor then certifies that the timesheet is correct according to employee duties and responsibilities. No PII is collected from any of the user types described herein.

Certified time and attendance is linked to individual employee Social Security Number (SSN) and is periodically provided to the USDA National Finance Center (NFC). NFC then issues employee paychecks based upon the data provided. WebTCAS depends on the HR database (and the primary NFC payroll system) for employee PII (i.e., employee names). WebTCAS also depends upon the Program Maintenance Tool (PMT) for non-PII funding data and Office Information Profile (OIP) for non-PII office information.

Authority to operate CST was previously provided via the ATO granted in 2010.

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?

WebTCAS does NOT directly "collect" any PII from any individual.

On a continuing basis, non-PII labor hour information is provided by employees. This includes the hours worked on specific projects, leave hours, arrival / departure times, time taken for lunch, activity codes, and extra accrued hours. This non-PII data is collected, used, disseminated and maintained by the WebTCAS system.

WebTCAS connects to the Human Resources (HR) database that is maintained outside the accreditation boundary by HR. PII obtained from HR is used to populate WebTCAS.

- Employee name is the only type of HR PII that is maintained in WebTCAS.
- Employee ID is also obtained from the HR database, but this is considered a business identifier rather than personal identifier.

WebTCAS also creates a "transmit file" that is used to disseminate timesheets to NFC.

- The records in this file "link" to employee SSN that is stored in the HR database.
- SSN information is protected by encryption (i.e., hashing) by WebTCAS.

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

PII obtained from HR is used to populate WebTCAS. Employee name is the only type of HR PII that is maintained in WebTCAS. WebTCAS does not directly "collect" any PII from any individual.

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

WebTCAS does not directly "collect" any PII from any individual.

PII data is used, disseminated and maintained by WebTCAS to A) obtain time and attendance data, and B) to send a "transmit file" containing timesheets to NFC.

Note that non-PII data is collected by WebTCAS from employees to produce records from which employee paychecks are derived. This data is also used to produce views and screens used for other time recordkeeping administrative functions.

1.4 How is the information collected?

N/A – WebTCAS does not directly "collect" any PII from any individual.

1.5 How will the information be checked for accuracy?

N/A – Applicable procedures to allow individuals to check the accuracy of their PII are maintained outside the accreditation boundary for WebTCAS by the HR systems that are the source of the PII used by this application.

For non-PII information, after the timesheets are submitted within the application by the employees, an NRCS assigned "timekeeper" accesses all the timesheets for that timekeeper's group using authenticated web browser sessions, and verifies timesheets against the employees' job assignments, project codes, etc. Once they match, the timekeeper verifies the timesheets inside the application browser window. After the timekeeper verifies the timesheet, the supervisor then certifies that the timesheet is correct according to employee duties and responsibilities.

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

While WebTCAS does not directly "collect" any PII information from any individual, these references pertain:

- Federal Register /Vol. 75, No. 27 /Wednesday, February 10, 2010/Rules and Regulations
- Paperwork Reduction Act of 1995 (44 U.S.C. 3501 et seq.)

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

WebTCAS does not directly collect any PII information from any individuals.

The PII that is used by WebTCAS includes only employee names that are obtained from HR. This PII data presents minimal privacy risks. Employee timesheets must include individual names for obvious reasons. The only other identifier used by WebTCAS is the USDA generated employee number, which is considered to be a business identifier, not a personal identifier. Privacy risks associated with the minimal PII maintained by WebTCAS are mitigated because access to the information is limited to authorized NRCS personnel by the use of the USDA-OCIO-eAuthentication application, which provides user authentication for NRCS. Role-Based Access Control (RBAC) provides access enforcement.

External privacy risks exist with respect to individual SSNs. SSNs are maintained in the HR database (outside of the WebTCAS accreditation boundary) for the sole purpose of facilitating transfer of individual time and attendance information to NFC. NFC requires SSN usage because NFC currently does not recognize any other means of individual identity validation. Per NFC policy, this privacy risk is mitigated by the use of independently generated password protection for the "transmit" batch files that contain SSN information, which provides further specific encryption protection for this particularly sensitive information.

Note: SSN PII data is **NOT** maintained within the WebTCAS application database.

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 information is used, disseminated and maintained by WebTCAS to A) obtain time and attendance data, and B) to send a "transmit file" containing timesheets to NFC. As discussed in Section 1, WebTCAS uses PII that was obtained from HR:

- Employee name is the only type of HR PII that is maintained in WebTCAS.
- Employee ID is also obtained from the HR database, but this is considered a business identifier rather than personal identifier.

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

N/A – WebTCAS does not use any type of tools to "analyze/produce" any type of PII.

- Non-PII data in WebTCAS is simply collected, and is then validated and verified.
- Data is not manipulated or reformatted (other than being summarized).
- No type of PII data is "produced."

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

N/A – WebTCAS 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.

This application is in compliance with the Federal Information Security Management Act of 2002 (FISMA) as reflected in CSAM, USDA Office of the Chief Information Officer (OCIO) Directives, and National Institute of Standards and Technology (NIST) guidance, including applicable controls provided in these NIST Special Publication 800-53 Revision 3 control families: Per conference call 8/9 at 11:45 EST.

Audit log (AU)

- Access Control (AC)
- Security Awareness and Training (AT)
- Identification and Authentication (IA)
- Media Protection (MP)
- Physical and Environmental Protection (PE)
- Personnel Security (PS)
- Risk Assessment (RA)
- System and Communication Protection (SC)
- System and Information Integrity (SI)

If any residual risks are identified, they will be managed and reported via the FISMA mandated risk assessment processes.

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?

Per NARA General Records Schedule 20, this application-specific information has been authorized by the NRCS Records Manager for erasure or deletion when the agency determines that this information is no longer needed for administrative, legal, audit, or other operational purposes.

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

Yes.

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 primary privacy risk is that a data breach could result in the release of time and attendance information associated with NRCS employees. This is mitigated by limited access to the data, non-portability of the data and controlled storage of the data located in controlled facilities.

Retention of application-specific data is required to meet business and organizational requirements for this particular information system. The risks associated with retaining application-specific information are mitigated by the controls discussed 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?

WebTCAS shares (receives) PII from the Human Resources (HR) database, which is maintained outside the accreditation boundary by HR. The employee name is the only type of HR PII that is maintained within WebTCAS.

WebTCAS automatically shares (transmits) the time and attendance data via batch process output to the NFC.

4.2 How is the information transmitted or disclosed?

Transmission of time and attendance data via batch process output to the NFC is accomplished via password-protected (encrypted) files sent that are over a dedicated line for security purposes. Passwords for connecting to NFC to enable transmitting the files are handled by the WebTCAS coordinators to ensure separation of duties (SOD).

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

Privacy risks are mitigated by ensuring that the sharing of sensitive PII with the NFC (which holds such data independently) is only performed by means of password protected (encrypted) transmissions. Any residual risks are mitigated by the controls discussed in Section 2.4 above.

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?

N/A – PII is <u>not</u> shared or disclosed with organizations that are external to the USDA.

Note that WebTCAS does <u>not</u> share, disclose or transmit <u>any</u> information to the IRS.

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.

N/A – PII is <u>not</u> shared or disclosed with organizations that are external to the USDA.

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

N/A – PII is <u>not</u> shared or disclosed with organizations that are external to the USDA.

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

Privacy risks are mitigated by virtue of NOT sharing information external to the USDA. Any residual risks are mitigated by the controls discussed in Section 2.4 above.

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?

N/A – No notice is provided, because no PII is collected from any individual by this application.

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

N/A – No PII is collected from any individual by this application.

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

N/A – No PII is collected from any individual by this application.

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.

Notice does not need to be provided to individuals. There is no risk that an individual would be unaware of "collection," because no PII is collected from any individual by this application.

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?

N/A – Applicable procedures to allow individuals to gain access to their information are maintained outside of the accreditation boundary of this application by Human Resources (HR), which is the source of the PII used by this application.

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

N/A – Applicable procedures for correcting inaccurate or erroneous information are maintained outside of the accreditation boundary of this application by Human Resources (HR), which is the source of the PII used by this application.

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

N/A – Applicable notification is provided by Human Resources (HR), which is the source of the PII used by this application.

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

NA – see 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.

Privacy risks associated with "redress that is available to individuals" are fully mitigated since individuals can use applicable HR procedures to update their original records in the HR source systems.

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?

Access to the WebTCAS application is determined via a valid eAuthentication ID and password (level II) on a valid "need to know" basis, determined by requirements to perform applicable official duties. The application has documented Access Control Procedures, in compliance with FISMA and USDA directives. See Section 2.4.

8.2 Will Department contractors have access to the system?

No.

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

NRCS requires that every employee and contractor receives information security awareness training before being granted network and account access, per General

Manual, Title 270, Part 409 - Logical Access Control and Account Management. Annual Security Awareness and Specialized Training are also required, per FISMA and USDA policy, and this training is tracked by USDA.

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

Yes. Recertification in progress; scheduled to be complete by 9/2013.

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

NRCS complies with the "Federal Information Security Management Act of 2002" (FISMA). Assessment and Accreditation, as well as annual key control self-assessments, and continuous monitoring procedures are implemented for this application per the requirements given in National Institute of Standards and Technology (NIST) Special Publication 800-53. Additionally, NRCS complies with the specific security requirements for "auditing measures and technical safeguards" provided in OMB M-07-16. Finally, the system provides technical safeguards to prevent misuse of data including:

- Confidentiality: encryption is implemented to secure data at rest and in transit for this application (e.g., by FIPS 140-2 compliant HTTPS and end-user hard disk encryption).
- Integrity: Masking of applicable information is performed for this application (e.g., passwords are masked by eAuth).
- Access Control: The systems implements least privileges and need to know to control access to PII (e.g., by RBAC).
- Authentication: Access to the system and session timeout is implemented for this application (e.g. by eAuth and via multi-factor authentication for remote access).
- Audit: logging is implemented for this application (e.g. by logging infrastructure).
- Attack Mitigation: The system implements security mechanisms such as input validation.

Notice: For the privacy notice control, please see Section 6 which addresses notice. For the privacy redress control, please see Section 7 which addresses redress.

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?

WebTCAS does not directly collect any PII from any individual, but WebTCAS does utilize PII within the system which is obtained from HR and transmitted to NFC (see

Section 1.0 above). Data extracts containing PII are not regularly obtained from the system, therefore, privacy risk from this area is limited and addressed through IT Data Extract processes controls.

Any privacy risks identified in this system are mitigated by the security and privacy safeguards provided in Section 8.5, and by the security controls discussed in Section 2.4 above. Remediation of privacy risks associated with internal/external sharing are addressed in PIA Sections 4 and 5 respectively.

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?

This is a legacy application that is hosted on devices using common COTS hardware and software configured in accordance with USDA baseline configurations for servers and web portals.

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

No. The project utilizes Agency approved technologies, and these technology choices do not raise privacy concerns.

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?

N/A – 3rd party websites / applications are not used.

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

N/A – 3rd party websites / applications are not used.

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

N/A – 3rd party websites / applications are not used.

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?

N/A – 3rd party websites / applications are not used.

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

N/A – 3rd party websites / applications are not used.

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

N/A – 3rd party websites / applications are not used.

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?

N/A – 3rd party websites / applications are not used.

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)?

N/A – 3rd party websites / applications are not used.

10.10 Does the system use web measurement and customization technology?

No. The system does not use web measurement and customization technology.

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

N/A – See 10.10.

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.

Privacy risks are nominal. WebTCAS does not provide access or link to Third Party Applications. In addition, the system does not use web measurement and/or customization technology.

Responsible Officials

paige.niederer
@usda.gov

Digitally signed by
paige.niederer@usda.gov
DN: cn=paige.niederer@usda.gov
Date: 2013.07.30 16:54:02 -06'00'

Paige Niederer
NRCS
United States Department of Agriculture
This signature certifies that the above PIA responses are provided to the best of my knowledge and understanding.

Date

Approval Signature

8/9/13

Mr. Lian Jin
Acting Chief Information Security Officer
United States Department of Agriculture
This signature certifies that the PTA analysis and PIA determination due diligence has been conducted pursuant to Department guidance and NIST regulations.

Date