Privacy Impact Assessment
for the

Web Time & Attendance System

May 1, 2008

Contact Point
Cheryl Mcelroy
Human Capital Business Systems
Department of Homeland Security
202-357-8285

Reviewing Official
Hugo Teufel III
Chief Privacy Officer
Department of Homeland Security
(703) 235-0780

Abstract

The Department of Homeland Security (DHS) Office of the Chief Human Capital Officer (OCHO) has procured a COTS application and customized it to meet DHS standard requirements. This system is designed to implement an enterprise system that can efficiently automate the timesheet collection process and provide robust reporting features and a labor distribution capability. This privacy impact assessment was conducted because WebTA utilizes personally identifiable information.

Introduction

The Human Resources Information Technology Program is a collection of functions and systems centered on a core enterprise Human Resource Management System (HRMS). The Program is part of a broader "OneDHS " model where collection of disparate and redundant systems across DHS is consolidated into enterprise wide solutions.

An enterprise WebTA system is a key component of HRMS. The goal of the WebTA system is to reduce the number of existing WebTA systems within DHS and consolidate the requirements into one enterprise system. In the initial phase of the WebTA deployment, the system will focus on capturing and reporting employee time and attendance data. In the broader HRIT program, there will be a core HR system that organizational components will access for all HR functions. The WebTA system will interface with this core system as well as the United States Department of Agriculture's (USDA) National Finance Center (NFC), DHS' payroll provider. During the time and attendance week, WebTA is setup to automatically send all timecards to NFC for processing. This procedure occurs several times a day during attendance week. The WebTA system expedites the processing of data associated with Time and Attendance, payroll/personnel processing. This information could include billing from amended timecards. The system adheres to the Inter-Agency Agreement, which is designed to ensure the confidentiality, integrity, and availability of data for both parties

Typical Transaction

An employee or timekeeper enters the employee's information, hours worked, and any leave used (among other possible data) into the WebTA system. This can be done daily or any time during the pay period. When the pay period has ended, a timekeeper or employee will confirm their data entry by clicking the "Validate" button. Once the timecard passes the edit phase, the supervisor verifies the accuracy of the data and certifies the information. Once the timecard is certified, the data is transmitted to the payroll system and is again validated for accuracy.[1] Once the timecard has passed the edits, it is placed on the database so the employee's pay can be calculated.

The WebTA system will modernize time collection within DHS as employee time and attendance data will be entered interactively by DHS personnel. The program will enable DHS to implement an

[1] This second editing phase is due to not all front-end system currently being used by the components have the extensive edits built in.

enterprise system that can efficiently automate the timesheet collection process and provide robust reporting features and a labor distribution capability.

Section 1.0 Information Collected and Maintained

1.1 What information is to be collected?

Employee data: social security number (SSN), last name, first name, middle name, alternate work schedule (AWS), pay plan, tour of duty, duty hours, scd for leave,

Timesheet data, accounting codes, time off, annual leave, sick leave, comp time, leave without pay (LWOP), absence without leave (AWOL), military emergency, military regular, unapproved annual leave, and all types of premium pay.

NOTE: It is the intent of Human Capital Business Systems (HCBS) to migrate away from using SSNs in the Time & Attendance system once all DHS employees are assigned employee identification numbers. Currently, all of the agencies that have been deployed to webTA are using SSNs as employee IDs; therefore, HCBS must continue to use the SSN as the unique identifier in the application. USCG, TSA, FAMS, HQ, USSS, FLETC, FEMA and ICE have all been deployed. All other components do not have a timeframe for deployment as yet.

1.2 From whom is information collected?

When an employee begins working at DHS, the employee profile and T&A profile are established by the timekeeper of the employee. The WebTA application allows the employee or the timekeeper to enter time and attendance data in the system for each pay period.

1.3 Why is the information being collected?

The WebTA system collects this information in order to record employee hours worked, and monitor attendance and employee holiday/vacation and determine leave balances. The WebTA system will enhance the current payroll processing function by improving the employee timesheet submission process which includes work hours and other types of employee time such as leave and other absences.

1.4 How is the information collected?

The additional rolling out of data entry to the individual employee is up to each component therefore timeframes are constantly changing. The timesheet data entered for employees is transmitted via a secure communications link to the National Finance Center which hosts the WebTA application and is also the payroll service provider for DHS. After timesheet data is submitted to NFC, DHS employees or their timekeepers may make corrections to employee records if it is determined that an individual's reported hours or accounting codes were incorrect. The method of data entry is determined by each individual component.

1.5 What specific legal authorities/arrangements/agreements define the collection of information?

The Homeland Security Act of 2002 called for the establishment of a new human resources system for the DHS that is flexible and contemporary. In related legislation, the E-Government Act of 2002 called for the use by the Government of web-based Internet applications and other information technologies, combined with processes that implement these technologies, to bring about improvements in Government operations that may include effectiveness, efficiency, service quality, or transformation. It also called for the adoption of innovative information technology, including the appropriate use of commercial best practices. Authority for Maintenance of the System: 5 U.S.C. 1302, 3109, 3301, 3302, 3304, 3305, 3306, 3307, 309, 3313, 3317, 3318, 3319, 3326, 4103, 4723, 5532, and 5533, and Executive Order 9397.

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

Recognizing that employee's Social Security Numbers (SSNs) are of particular sensitivity, WebTA is working to phase out the use of the SSN as a personal identifier. Once the remaining DHS components have been completely converted to WebTA identifier instead of the SSN as an identifier, the risk of use of the SSN will be eliminated. This PIA will be updated once SSN has been phased out of DHS operations.

Section 2.0 Uses of the System and the Information

2.1 Describe all the uses of information.

The time and attendance data will be compiled for use in processing payroll through the NFC based on hours worked and leave taken. In addition to payroll efforts, the information will be used to accurately record work hours, and monitor attendance and employee holiday/vacation and determine leave balances.

2.2 Does the system analyze data to assist users in identifying previously unknown areas of note, concern, or pattern (Sometimes referred to as data mining)?

The capability exists to capture project codes, project name, and locator information in WebTA that supports labor distribution accounting which is not available in the NFC system of record. However, this data is voluntary. Additionally, DHS wide reports are not possible at this time because all components are not using the system. Usage of the WebTA system is not mandatory.

2.3 How will the information collected from individuals or derived from the system be checked for accuracy?

Edit checks are built into the system. Timesheets will also be reviewed by supervisors to further ensure accuracy. NFC will run the data through their T&A Validation Edit and Messaging, which will produce error reports. If the component has enabled data entry to employees, they can make changes to

the historical timesheet. The corrected timesheet will have to be validated by the employee and certified by the supervisor. At that time, the timecard is locked in preparation of transmission to the Payroll system. Additionally they can update other items such as their default schedule, leave and premium pay requests, etc. If the component has enabled entry to the employees, generally they do not provide the employee with the user ID and password to access the system.

2.4 Privacy Impact Analysis: Given the amount and type of information collected, describe any types of controls that may be in place to ensure that information is used in accordance with the above described uses.

The scope of the information collection (detailed above) is narrowly tailored to ensure that the information collected matches the uses. Information collected will not be used for any other purpose. The reporting and analytical tools help the Department better refine HR practices. The accuracy of the information is ensured by both employee input and supervisor verification.

Section 3.0 Retention

3.1 What is the retention period for the data in the system?

Data will be retained on-line for six years in accordance with the NARA General Records Schedule which stipulates that, for Time and Attendance Input Records "records in either paper or machine readable form used to input time and attendance data into a payroll system, maintained either by agency or payroll processor" can be destroyed after a General Accountability Office (GAO) audit or when 6 years old, whichever is sooner. Active employee records require on-line access for the duration of employment.

3.2 Has the retention schedule been approved by the National Archives and Records Administration (NARA)?

NARA will evaluate records in system by 2007 after DHS completes its scheduling. All records are considered permanent until full evaluation is complete.

3.3 Privacy Impact Analysis: Given the purpose of retaining the information, explain why the information is needed for the indicated period.

The information is retained for a time that is reasonable considering government reporting functions and auditing while respecting an individual's right to have their information deleted once it is no longer needed for the purpose for which it was collected. Any shorter period would compromise the Department's reporting and auditing requirements, while a longer period would be a potential harm to the individual by unnecessarily retaining their information.

Section 4.0 Internal Sharing and Disclosure

4.1 With which internal organizations is the information shared?

The USCG, TSA, FAMS, HQ, USSS, FLETC, FEMA and ICE are using the WebTA application to input time attendance. The data for each component is only accessible by the individual component. .

4.2 For each organization, what information is shared and for what purpose?

Information contained in WebTA is not shared with other components except in the case of employee transfer from one component to another. Even with this, the limitation of what is seen is limited to uses associated with human resources functions..

4.3 How is the information transmitted or disclosed?

There is a single system which the above-noted components use to enter WebTA data. The system communications are handled in the highly secure environment contained within NFC's infrastructure which has a current Certification and Accreditation (C&A). The information is not shared with other agencies except in the case of employee transfer. Other DHS components can only view their respective data.

4.4 Privacy Impact Analysis: Given the internal sharing, discuss what privacy risks were identified and how they were mitigated.

The risks associated with internal sharing are minimal because WebTA does not share information with any component other than the component which provided information.

Section 5.0 External Sharing and Disclosure

5.1 With which external organizations is the information shared?

The WebTA system shares information with the USDA's NFC (bi weekly payroll data).

5.2 What information is shared and for what purpose?

The system will only share time and attendance and payroll processing data. The following fields are shared:

Name (First, middle, and last name)
SSN
Pay Plan
Duty of hours

Tour of Duty
Service Computation date
Agency code
Accounting Code
Transaction Codes

This allows WebTA and the NFC to operate on the same set of information in order to pay employees and account for leave. The information shared is to expedite the processing of data associated with time and attendance, payroll/personnel processing. This information could include billing from amended timecards. The system is designed to provide labor distribution data to assist with financial management activities in DHS; TSA is the only component that is using project based accounting at this time.

5.3 How is the information transmitted or disclosed?

The timesheet data entered for employees is transmitted via a secure communications link to the National Finance Center which hosts the WebTA application and is also the payroll service provider for DHS. After timesheet data is submitted to NFC, DHS personnel may make corrections to employee records if it is determined that an individual's reported hours or accounting codes were incorrect.

5.4 Is a Memorandum of Understanding (MOU), contract, or any agreement in place with any external organizations with whom information is shared, and does the agreement reflect the scope of the information currently shared?

Yes. The Department and USDA are partners to an Interconnection Service Agreement.

5.5 How is the shared information secured by the recipient?

NFC, which services many other federal agencies, has undergone a C&A. The Interconnection Service Agreement is designed to ensure the confidentiality, integrity, and availability of data for both parties. The agreement covers data sensitivity, information exchange security, trusted behavior, incident reporting, audit trail responsibilities, security parameters, and security awareness and training. The security of the information being passed on the two-way connection is protected through the use of 128bit SSL that is then passed through firewalls and VPN connection points to the receiving data. Anti-virus and intrusion detection systems are deployed for the Department. The connections at each end are located with controlled access facilities. Individual users will not have access to the data except through their systems security software inherent to the operating system. All access is controlled by identification and authentication methods to validate approved users.

5.6 What type of training is required for users from agencies outside DHS prior to receiving access to the information?

Each DHS component and the NFC are required to administer security and privacy training.

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

Although there are risks inherent with any external sharing such risks have been mitigated to the fullest extent possible in WebTA's sharing with the NFC. DHS and USDA operate under an ISA which details the sharing of information between Departments. Each system has completed a C & A package and each system transmits information in a secure manner. Inasmuch as risks cannot be completely nullified, all risks associated with external sharing are reasonably mitigated.

Section 6.0 Notice

6.1 Was notice provided to the individual prior to collection of information? If yes, please provide a copy of the notice as an appendix. A notice may include a posted privacy policy, a Privacy Act notice on forms, or a system of records notice published in the Federal Register Notice. If notice was not provided, why not?

Notice of the system and the system's operation is provided in two ways.

First, WebTA is covered by the Office of Personnel Management government-wide system of records notice (SORN) OPM-GOVT1, General Personnel Records (June 19, 2006, 71 FR 35356). DHS is in the process of developing a DHS-specific system of records notice to cover DHS time and attendance systems, but until that time OPM-GOVT1 appropriately notifies individuals of the collection of general personnel data, including time sheets.

Second, when logging into WebTA users are notified that they are accessing a government system and that any information submitted or retrieved on the system is subject to monitoring and recording by DHS system security officers.

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

Employee timesheet submission is required by policy and is a condition of employment. Compensation is determined by timesheet data.

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

Accounting for employee hours is part of the terms of employment. Employees can discuss concerns with their supervisors who will address them accordingly. The use of employee information is limited to what is required for proper time and attendance, leave, and payroll calculation (see Section 2.0 and 5.0).

6.4 Privacy Impact Analysis: Given the notice provided to individuals above, describe what privacy risks were identified and how you mitigated them.

The notice provided regarding the existence and operation of the system is adequate for the needs of government employees who are, by virtue of employment, under notice that all actions undertaken for personnel purposes is recorded and logged. Once the DHS-specific SORN is drafted, this notice will be refined for the DHS employee audience.

Section 7.0 Individual Access, Redress and Correction

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

Timekeepers can verify and amend employee information as necessary directly through the system. Employees are, capable of entering their own time, changing their default schedule and processing amended timecards, if necessary.

7.2 What are the procedures for correcting erroneous information?

Edit checks are built into the system and allow employees to make changes interactively, however employee entered corrections have a limited processing cycle within that pay period or they will have to wait until the following pay period for submission. Timekeepers will also be able to correct erroneous information or submit correct timecards. Corrections in this system will be consistent with NFC processes. Historical updates are limited to specific user roles

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

In WebTA, timekeepers, as well as, employees are authorized to make corrections. The procedures for making corrections are in the User's Guide and the training material. This information follows federal regulations and NFC's directives regarding processing corrections. If an employee requires a correction to his/her timecard, they must either contact their timekeeper or if participating in employee based time entry they can enter a correction themselves. The corrected timecard must be certified by their supervisor.

Employees are allowed to correct historical records and not missing records, and the corrected timesheet will have to be validated by the employee or timekeeper and then certified by their supervisor. DHS approval of changes ensures information accuracy integrity.

7.4 If no redress is provided, are alternatives are available?

Redress is provided by direct amending of records by supervisors and employees.

7.5 Privacy Impact Analysis: Given the access and other procedural rights provided for in the Privacy Act of 1974, explain the procedural rights that are provided and, if access, correction and redress rights are not provided please explain why not.

WebTA is premised on the idea of the importance of accurate employee information. Because WebTA controls accurate timekeeping and, in its relationship with the NFC, employee paychecks, robust information correction measures are in place. Not only do WebTA and NFC synchronize every two weeks but timesheet information is verified at least twice before being submitted to NFC. The multiple levels of input into the employee's information ensure accurate information as well as employee involvement in their record and timekeeping. Procedural mechanisms for access and correction are included within the application. The application tracks all corrections through a history table, which displays who and what changes were made to an employee time record.

Section 8.0 Technical Access and Security

8.1 Which user group(s) will have access to the system? (For example, program managers, IT specialists, and analysts will have general access to the system and registered users from the public will have limited access.)

The WebTA system will allow users, supervisors, timekeepers, approvers, and/or administrators to retrieve employee information based on their Login Name, subject to role-based data access controls. The convention for the Login Name uses a combination of the user's last name, first initial, and the last four digits of their social security number in reverse (e.g., DoeJ4321). DHS has determined the role assignments, and the roles are noted in application and documentation.

8.2 Will contractors to DHS have access to the system? If so, please submit a copy of the contract describing their role to the Privacy Office with this PIA.

The contractor selected to manage the application, will provide system administrators to perform administration tasks to include add/delete users, and administer the application and database.

8.3 Does the system use "roles" to assign privileges to users of the system?

Yes, the roles restrict users to what actions or system functions they have access to. There are two levels of data security within WebTA, the agency code and the organization tree restricts users to the data they can see.

1. **Employee** – WebTA is designed as a self service system and every employee record is assigned a login ID, password and the employee role as the most basic role in WebTA and is restricted to agency and organization. Not all agencies use WebTA as a self service application.

2. **Timekeeper** – The timekeeper role is used to add new employee data, edit, correct and validate time and attendance data, time and attendance profiles, employee profiles and locator information for their assigned employees. This role is restricted by agency and organization.

3. **Master Timekeeper *Restricted*** – The master timekeeper role is used to add new employee data, edit, correct and validate time and attendance data, time and attendance profiles, employee profiles and locator information. This role is restricted by agency only. If there are several organizations within an agency, this role is at the top of the organization tree within a specific agency.

4. **Master Timekeeper *Read only*** – The master timekeeper role is used to view time and attendance data, time and attendance profiles, employee profiles and locator information only. This role is restricted by agency only. If there are several organizations within an agency, this role is at the top of the organization tree within a specific agency.

5. **HR Administrator** – HR Administrators manage the leave transfer program, manage role assignments, edit and add organizations to the organizational chart, edit and add accounting data and manage employees within their agency. This role is restricted by agency and can be restricted by organization.

6. **Supervisor** – The supervisor role can only review and certify time and attendance reports for their assigned employees. This role is restricted by agency and organization.

7. **Master Supervisor *Restricted*** – The supervisor role can only review and certify time and attendance reports for any employee within an agency. If there are several organizations within an agency, this role is at the top of the organization tree within a specific agency.

8. **Project Manager** – The project manager administers the project hierarchy of the accounting codes. This role is restricted by agency and can be restricted by organization.

9. **Master Timekeeper** – The master timekeeper role is used to add new employee data, edit, correct and validate time and attendance data, time and attendance profiles, employee profiles and locator information globally. This role is not restricted by agency or organization and is kept at the System Administrator level.

10. **Master Supervisor** – The supervisor role can only review and certify time and attendance reports for any employee globally. This role is not restricted by agency or organization and is kept at the System Administrator level.

11. **Administrator** – Administrators manage the Time and Attendance System. This includes system configuration, build management, and managing employee's roles and role assignment on a global level. This role is not restricted by agency or organization.

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

The WebTA servers primarily use traditional user ID's and passwords for authentication. All users including administration, use separate accounts as to provide individual accountability and traceability for actions performed. WebTA is a role based application and restricts the view of data even within the component depending on the role that is granted. In addition to user ID's and passwords, the NFC has capability to restrict access to WebTA resources based on IP address. Logical access controls requires the requests for access are standardized and implemented by ISSO personnel. Access requests are maintained on microfilm and stored indefinitely. Access is enabled only for what is required for each job function. The principle of least privilege is adhered to closely. As an example, users in the accounting group do not have access enabled for personnel data. Reassignment of employees to another branch requires their access/profile setting be updated. Unauthorized attempts to access resources are automatically denied and logged. Authorized users of certain sensitive resources are logged for subsequent review.

Separation of administrator duties is defined in NFC ADP Directive 75, *Network Security Policy*. The ISSO, a separate security organization, defines security policies and monitors security-related activities throughout the NFC. This group does not have direct administrative rights on NFC systems; therefore no single individual would be able to modify important configuration settings without detection. No public access to the WebTA application or its information. All access is controlled and is only available to approved agency personnel

8.5 How are the actual assignments of roles and rules verified according to established security and auditing procedures?

The WebTA system is role-based and has username and passwords for access controls. Application level security will not allow unauthorized users to access data.

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

The NFC Automated Data Processing ADP Directives provide much of the policy and responsibilities for auditing activities including what audit logging is needed, auditing procedures, reporting, and the follow-up of suspect activity. As the Operating System EnvironmentOSE General Service System DHS Application Hosting environment includes two dramatically different types of servers UNIX and Microsoft Windows, the types of events are audited vary considerably by server type. The WebTA application history table captures auditing events within the system. The application has auditing to capture events for which system auditing is activated, when the audit event occurred, audit the primary key of the table modified as a result of an audit event, audit the emp_id of the person that generated the audited event, specifies the type of audit event and a full description or explanation of the audited event.

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

DHS employees, supervisors, and timekeepers receive security and privacy training.

8.8 Is the data secured in accordance with FISMA requirements? If yes, when was Certification & Accreditation last completed?

WebTA Major Application C & A signed on November 13, 2006.

NFC GSS WebTA C & A ATO signed on August 19, 2005.

8.9 Privacy Impact Analysis: Given access and security controls, what privacy risks were identified and describe how they were mitigated.

WebTA uses established DHS protocols to ensure the risks associated with data misuse and unauthorized access is mitigated. Additionally, OCHCO has ensured that the National Finance Center, as a sharing partner, has met its security and privacy obligations as well. As WebTA incorporates more components into its operations these system security measures will be readjusted and re-verified to ensure data and system security.

Section 9.0 Technology

9.1 Was the system built from the ground up or purchased and installed?

The WebTA system is a Commercial-off-the-Shelf (COTS) package by Kronos. The vendor will use the COTS package to modernize the time collection process.

9.2 Describe how data integrity, privacy, and security were analyzed as part of the decisions made for your system.

The data housed at NFC is sensitive and critical in nature. None of the data stored on NFC's hardware is classified. Numerous NFC applications store names, Social Security Numbers, addresses, all of which are covered by the Privacy Act of 1974. Some of these applications reside or store private information on OSE servers, but privacy-related decisions about this information is managed by the applications themselves rather than at the GSS level.

Employee responsibilities in terms of data integrity/validation controls are outlined in the Rules of Behavior (RoB). The NFC Directive 67, Protection against Computer Viruses, details the reporting and investigation of incidents involving malicious code on personal computers. Virus detection and eradication software installed on servers and user workstations detects, identifies, and removes software viruses to

ensure system and data integrity. UNIX, Linux, and Novell servers are generally not susceptible to viruses themselves, but virus-checking software is used on Netware servers on behalf of end users who use Microsoft Windows.

9.3 What design choices were made to enhance privacy?

A market survey was conducted and four products were evaluated for their privacy handling capabilities. The WebTA package selected has been used in many federal agencies and has robust privacy handling capabilities. The vendor was chosen partly because it has extensive knowledge of federal privacy requirements.

Responsible Officials

John Allen
Human Capital Business Systems
Department of Homeland Security
202-357-8285

Original signed and on file with the DHS Privacy Office

John Kropf
Acting Chief Privacy Officer
Department of Homeland Security