Privacy Impact Assessment
for the

Web Time and Attendance

October 31, 2006

Contact Point
Mr. Mark Danter
Bureau of Alcohol, Tobacco, Firearms and Explosives
Office of Management/ Financial Management Division
202-927-8589

Reviewing Official
Jane C. Horvath
Chief Privacy Officer and Civil Liberties Officer
Department of Justice
(202) 514-0049

Introduction

WebTA is a web-based software application that supports federal time and attendance reporting requirements. The application has been configured to ATF specifications. WebTA's purpose is to facilitate the payroll data being transmitted to United States Department of Agriculture (USDA)'s National Finance Center (NFC) in order to generate payroll for the Bureau and provide reports to aid employees and managers in interpreting the Time and Attendance (T&A) information into financial – related data.

Section 1.0
The System and the Information Collected and Stored within the System.

The following questions are intended to define the scope of the information in the system, specifically the nature of the information and the sources from which it is obtained.

1.1 What information is to be collected?

Information on the employee is recorded directly into WebTA when the employee joins the agency. The information recorded is listed below:

- Employee's Userid
- Employee's Name
- Employee's Social Security Number
- Employee's Supervisor's Name
- Employee's Timekeeper's Name
- Organization Code
- Employee's Role in the System
- Active Status indicator

1.2 From whom is the information collected?

The information is being collected from the employee (and approved by the supervisor) and entered into WebTA via an internal-agency form titled Information Systems Access form; identified as ATF Form 7200.1. This is a standard form that every employee uses to request access to specific applications within the agency's information systems network.

Section 2.0
The Purpose of the System and the Information Collected and Stored within the System.

2.1 Why is the information being collected?

The information being collected is required to compensate the employees for their hours worked on the various assignments within the agency. The hours worked are entered on the timecards on a bi-weekly or weekly basis and get transmitted to NFC. This information is processed within NFC's database, and the employees are compensated by the bi-weekly paycheck for carrying out the department's missions.

2.2 What specific legal authorities, arrangements, and/or agreements authorize the collection of information?

The primary documents that authorize this collection of information are the Service Level Agreements and Memorandums of Understanding between NFC and ATF, in addition to the ATF orders; ATF O 2550.1B and ATF O 2600.2A.

2.3 Privacy Impact Analysis: Given the amount and type of information collected, as well as the purpose, discuss what privacy risks were identified and how they were mitigated.

The risk of exposure of employee name and social security number are mitigated by the following controls:

1. Employee social security numbers are not displayed on any screen or report in the WebTA system except for the security profile screen, to which application access is severely limited via role-based security.
2. All access privileges to the WebTA system are reviewed annually by ATF managers.
3. The WebTA system is maintained within the DOJ and ATF technical and security infrastructures, and operated according to all DOJ and ATF Information System polices and procedures, including Certification and Accreditation.
4. There are also network systems at work to protect the privacy of information contained in WebTA. Intrusion Detection Software (IDS), which is part of the UNIX server configuration, is installed on the UNIX servers. IDS confidentiality, integrity and availability are protected with UNIX access controls. In addition, the Operations Systems Branch (OSB) Security Team performs penetration testing, risk assessments, vulnerability testing and password cracking periodically in accordance with the OSB General Support System (GSS) Security Plan.

Section 3.0
Uses of the System and the Information.

The following questions are intended to clearly delineate the intended uses of the information in the system.

3.1 Describe all uses of the information.

The information in WebTA is primarily used to maintain the employee's personal information, leave balances and record work hours spent on carrying out the agency's missions via the timecard (T&A). In addition, when (and only when) the T&A has been both validated (by the employee) and certified (by the supervisor), the T&A is automatically sent to NFC to be processed into a payroll disbursement for the employee.

Other uses for the information in WebTA are for research, storage or configuration purposes:

- Conducting leave audits to certify work hours entered on the T&A are correct and the employee was paid correctly,
- Running reports to confirm hours worked by project codes,
- Determining the agency's status of what T&As have been sent, received, processed at NFC,
- Determining the user role assignment for each employee in WebTA,
- Determining the overtime amount earned and hours worked for employees or an employee,
- Determining the leave requests submitted/ approved for employees in WebTA,
- Determining the hour totals for LEAP and AUO Report Certification for Agents,
- Maintaining the Leave Transfer Program in WebTA,
- Ability to view the T&A Summary data for each employee,
- Ability to store the leave and premium pay requests for each employee,
- Ability to store the employee's locator information to facilitate the email notification process within WebTA,
- Ability to validate and certify the T&A information in preparation for transmittal to NFC for pay disbursement to the employee,

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

No.

3.3 How will the information collected from individuals or derived from the system, including the system itself be checked for accuracy?

The initial data collected from new employees is validated against the ATF O 7200.1 form; Information Systems Access form. Employee information, time utilization data and leave data is validated by the employee and verified by the supervisor each pay period.

3.4 What is the retention period for the data in the system? Has the applicable retention schedule been approved by the National Archives and Records Administration (NARA)?

Data retention meets or exceeds that required by the applicable retention schedules (6 years, 3 months).

3.5 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.

ATF employees read and agree (in writing) to follow official ATF Rules of Behavior governing use of ATF workstations and the safeguarding of ATF data and information system resources on an annual basis. All ATF employees are required to complete Information Security Awareness training on an annual basis. Access to WebTA is governed by role-based security. Timecards are validated by employees and approved by supervisors.

The banner page for the system displays a notice stating that "WebTA is an official U.S. Government system, which is to be used for authorized purposes only. This system contains sensitive but unclassified data. Falsification of any data in this system is subject to disciplinary action. The Govt may monitor usage of this system, & usage of it constitutes consent to such monitoring. Unauthorized attempts to access the data on this web site are strictly prohibited and subject to prosecution."

A hot link to ATF's privacy notice is also prominently displayed on the banner page of the WebTA system.

A further list of controls in place governing how the data is used within WebTA are listed below:

1. Employee social security numbers are not displayed on any screen or report in the WebTA system except for the security profile screen, to which application access is severely limited via role-based security.
2. All access privileges to the WebTA system are reviewed annually by ATF managers.
3. The WebTA system is maintained within the DOJ and ATF technical and security infrastructures, and operated according to all DOJ and ATF Information System polices and procedures, including Certification and Accreditation.
4. There are also network systems at work to protect the privacy of information contained in WebTA. Intrusion Detection Software (IDS), which is part of the UNIX server configuration, is installed on the UNIX servers. IDS confidentiality, integrity and availability are protected 1 with UNIX access controls. In addition, the Operations Systems Branch (OSB) Security Team performs penetration testing, risk assessments, vulnerability testing and password cracking periodically in accordance with the OSB General Support System (GSS) Security Plan.

Section 4.0
Internal Sharing and Disclosure of Information within the System.

The following questions are intended to define the scope of sharing both within the Department of Justice and with other recipients.

4.1 With which internal components of the Department is the information shared?

The information in WebTA is not shared with any component of the Department.

4.2 For each recipient component or office, what information is shared and for what purpose?

N/A

4.3 How is the information transmitted or disclosed?

N/A

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

N/A

Section 5.0
External Sharing and Disclosure

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

5.1 With which external (non-DOJ) recipient(s) is the information shared?

The certified T&A information is shared with NFC.

5.2 What information is shared and for what purpose?

The certified T&A records are the only elements shared and are electronically transmitted to NFC. The purpose of the transmission is to provide NFC with the data so that the bi-weekly payroll disbursements may be issued to the employees of the agency.

Employee information that is transmitted to NFC is:

- Employee's Name
- Employee's Social Security Number
- Organization Code

5.3 How is the information transmitted or disclosed?

The certified T&A records are transmitted by a routine file transfer to the NFC that is enabled by a batch job initiated by the WebTA server. The file transfer is via secure link shared by both DOJ and NFC (and no other parties). This link is owned and established by the NFC and is dedicated to use for the purpose of sending Time and Attendance records from DOJ to NFC. This link is encrypted using SecureFTP software.

5.4 Are there any agreements concerning the security and privacy of the data once it is shared?

The agreement concerning the security and privacy of the transmitted data is the Service Level Agreements and Memoranda of Understanding between NFC and DOJ.

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

The most recent review of NFC internal controls provided to ATF indicates that the Department of Agriculture's OIG found that internal control objectives related to training of its employees were suitably designed, were in place and were operating effectively. The OIG reviewed the training records for a sample of employees with significant security responsibilities and determined that the training provided was adequate.

5.6 Are there any provisions in place for auditing the recipients' use of the information?

In accordance with the Service Level Agreements and Memorandums of Understanding between NFC and DOJ, any routine audits shall be subject to prior approval by DOJ.

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

In accordance with the Service Level Agreement and the Memorandums of Understanding between NFC and DOJ, paragraph J.1 and J.2 states that USDA agrees to provide the degree of protection (administrative, technical and physical safeguards) for the payroll/ personnel databases as prescribed by the Privacy Act of 1974, 5 U.S.C. Section 552A. No DOJ payroll or personnel data shall be released to any requestor unless approved in advance in accordance with criteria furnished by DOJ and the provisions of the Privacy Act, except for normal use or audits by USDA personnel incidental to providing payroll/ personnel services to DOJ. Access by other government agencies, such as the GAO, OMB and OPM for routine audits shall be subject to prior approval by DOJ.

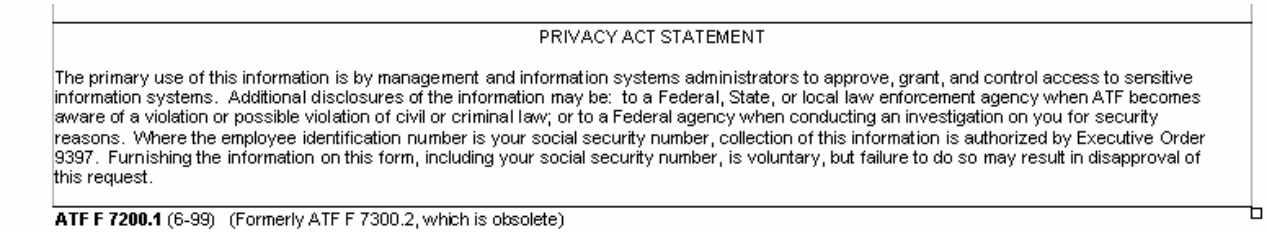
The USDA agrees to provide the same degree of protection as specified in Paragraph J.1 for any data on DOJ personnel that may be furnished while developing conversion procedures, implementing or maintaining the system; and in accordance with Paragraph J.1 and J.2, USDA shall process all DOJ-related Freedom of Information Act requests with the approval of the appropriate DOJ Personnel Office.

Section 6.0 Notice

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

6.1 Was any form of 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?

Yes. The following Privacy Act notice appears on the bottom of the Information Systems Access form (ATF F 7200) signed by the employee.



PRIVACY ACT STATEMENT

The primary use of this information is by management and information systems administrators to approve, grant, and control access to sensitive information systems. Additional disclosures of the information may be: to a Federal, State, or local law enforcement agency when ATF becomes aware of a violation or possible violation of civil or criminal law; or to a Federal agency when conducting an investigation on you for security reasons. Where the employee identification number is your social security number, collection of this information is authorized by Executive Order 9397. Furnishing the information on this form, including your social security number, is voluntary, but failure to do so may result in disapproval of this request.

ATF F 7200.1 (6-99) (Formerly ATF F 7300.2, which is obsolete)

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

Yes.

6.3 Do individuals have an opportunity to consent to particular uses of the information, and if so, what is the procedure by which an individual would provide such consent?

Yes, however partial submission of the information would not provide the employee with the full amount of compensation for the hours worked over the pay period. Employees consent to use of the provided information by requesting access to the WebTA system on the access form.

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

The risk of exposure of employee name and social security number are mitigated by the following controls:

1. Employee social security numbers are not displayed on any screen or report in the WebTA system except for the security profile screen, to which application access is severely limited via role-based security.

2. All access privileges to the WebTA system are reviewed annually by ATF managers.

3. The WebTA system is maintained within the DOJ and ATF technical and security infrastructures, and operated according to all DOJ and ATF Information System polices and procedures, including Certification and Accreditation.

Section 7.0
Individual Access and Redress

The following questions concern an individual's ability to ensure the accuracy of the information collected about him/her.

7.1 What are the procedures which allow individuals the opportunity to seek access to or redress of their own information?

If information from the signed ATF O 7200.1 form is incorrect after the data has been entered into WebTA, the employee may notify either the timekeeper or the WebTA Administrators. The corrected information should be corrected by submitting another signed ATF O 7200.1 form. The information can then be corrected in WebTA upon approval from their supervisor.

7.2 How are individuals notified of the procedures for seeking access to or amendment of their information?

The employees are notified of the procedures when they contact either their timekeeper or the WebTA Administrator.

7.3 If no opportunity to seek amendment is provided, are any other redress alternatives available to the individual?

The opportunities are made available for making amendments to the employee's data.

7.4 Privacy Impact Analysis: Discuss any opportunities or procedures by which an individual can contest information contained in this system or actions taken as a result of agency reliance on information in the system.

In the event that data provided by the employee which is stored in WebTA is incorrect, submission of a correct ATF O 7200.1 form is the approved procedure for correction. ATF employees have full access to review their timecard data in the system and request corrected timecards to be submitted at any time, with supervisor approval

Section 8.0
Technical Access and Security

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

8.1 Which user group(s) will have access to the system?

All ATF employees have access to WebTA in order to record and monitor their own T&A being validated and certified. In addition, employees can access their leave balances and premium pay usage.

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

We are not currently aware of any contractors with access to WebTA.

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

Yes. The roles are: Employee, Timekeeper, Master timekeeper, Supervisor, Master supervisor, Administrator and Human Resource Administrator. In addition, there is also an inquiry-only role to be used exclusively for auditors and contractors who need limited and controlled access for research purposes only.

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

All access to the system must be requested and approved via an Information Systems Access form (ATF F 7200). All access privileges to the WebTA system are reviewed annually by ATF managers. Other procedures are defined and described in the Web Time and Attendance System Security Plan.

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

Actual roles assigned to employees in WebTA are verified via the ATF O 7200.1 forms where the approved user role is written on the form. The form is signed by both the employee and supervisor. All access privileges to the WebTA system are reviewed annually by ATF managers.

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

Based on internal functionality settings per the specific WebTA role, the employee is restricted to only that WebTA role and level of system access. Each employee is assigned a unique userid. All data processed in WebTA are tagged with the userid that is stored on each record in the application. Employees are notified with warning message banners upon attempting certain tasks to alert them that these functions should only be taken with the knowledge that the employee is being held 100% responsible. In addition, access privileges to the WebTA system are reviewed annually by ATF managers. An auditing table tracks all changes, update and create actions performed within WebTA.

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

Before being granted access to ATF systems, all employees must read ATF Rules of Behavior and sign the Customer Agreement for ATF Workstation Users. On an annual basis, ATF employees are required to take the ATF Information Security Awareness Course.

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

WebTA data is secured in accordance with FISMA requirements. The date of the last Certification and Accreditation was December 28, 2005.

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

The risk of exposure of employee name and social security number are mitigated by the following controls:

1. Employee social security numbers are not displayed on any screen or report in the WebTA system except for the security profile screen, to which application access is severely limited via role-based security.
2. All access privileges to the WebTA system are reviewed annually by ATF managers.
3. The WebTA system is maintained within the DOJ and ATF technical and security infrastructures, and operated according to all DOJ and ATF Information System polices and procedures, including Certification and Accreditation.
4. There are also network systems at work to protect the privacy of information contained in WebTA. Intrusion Detection Software (IDS), which is part of the UNIX server

configuration, is installed on the UNIX servers. IDS confidentiality, integrity and availability are protected with UNIX access controls. In addition, the Operations Systems Branch (OSB) Security Team performs penetration testing, risk assessments, vulnerability testing and password cracking periodically in accordance with the OSB General Support System (GSS) Security Plan.

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, RFID, biometrics and other technology.

9.1 Were competing technologies evaluated to assess and compare their ability to effectively achieve system goals?

Yes, ATF compared and evaluated a total of nine systems prior to making the decision to use WebTA.

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

Data integrity, privacy and security were analyzed on a whole in addition to system flexibility and user-friendliness of the system for the agency. Other security implications and system complexities were examined by our Information Systems Security Office (ISSO) to ensure it complied with additional security measures and other network implications.

9.3 What design choices were made to enhance privacy?

There was several design choices made to enhance WebTA's privacy. Namely, the user roles that distinguish and control the defined permissions of each role. The roles are: Employee, Timekeeper, Master timekeeper, Supervisor, Master supervisor, Administrator and Human Resource Administrator. In addition, there is also an inquiry-only role to be used exclusively for auditors and contractors who need limited and controlled access for research purposes only.

There is also the usage of the (non-SSN based) userid that is used to identify the employee as well as track all user actions (updates, changes, etc.), to the specific employee.

Concerning the storage of any financial information, all media are identified, labeled and handled as sensitive but unclassified containing Privacy Act data.

Employee social security numbers are not displayed on any screen or report in the WebTA system except for the security profile screen, to which only privileged users with approved access roles are able to access.

There are also network systems at work to protect the privacy of information contained in WebTA. Intrusion Detection Software (IDS), which is part of the UNIX server configuration, is installed on the UNIX servers. IDS confidentiality, integrity and availability are protected with UNIX access controls. In addition, the Operations Systems Branch (OSB) Security Team performs penetration testing, risk assessments, vulnerability testing and password cracking periodically in accordance with the OSB General Support System (GSS) Security Plan.

As a part of WebTA, but maintained under a different partition, there is a Password Management Application (PMA) where the authentication mechanisms are managed preventing unauthorized people or processes from entering the system. The PMA is administered by a PMA Administrator who can change the employee's passwords in the event of lockouts. The PMA Administrator does not have access to the application, can only view an employee's userid and user name. Also, the password configuration sequence requires stringent password complexity rules are enforced to prevent break-ins to the system with weak passwords. There are configurations for requiring the employee's passwords to be changed every 30, 60, 90, 120, or 365 days–these are set by the Administrator in compliance with ISSO standards. WebTA contains a feature to limit concurrent user logins.

Conclusion

Data integrity, privacy and security were analyzed on a whole in addition to system flexibility and user-friendliness of the system for the agency. Other security implications and system complexities were examined by our Information Systems Security Office (ISSO) to ensure it complied with additional security measures and other network implications.

Responsible Officials

(signed)

Hans E. Heidenreich, Financial Manager/Deputy Chief Financial Officer

(signed)

Mark T. Danter, Assistant Financial Manager, Financial Systems Branch/ Designated Security Officer of WebTA

Bureau of Alcohol, Tobacco, Firearms and Explosives

Department of Justice

Approval Signature Page

(signed)

Jane Horvath
Chief Privacy and Civil Liberties Officer
Department of Justice