U.S. Department of Commerce
Office of Human Resources Management
(OHRM)

Privacy Threshold Analysis
for the
WebTA and Archive Time Application

U.S. Department of Commerce Privacy Threshold Analysis

WebTA and Archive Time Application

Unique Project Identifier: OS-059 Enterprise Application System DOC WebTA-ArchiveTime

Introduction: This Privacy Threshold Analysis (PTA) is a questionnaire to assist with determining if a Privacy Impact Assessment (PIA) is necessary for this IT system. This PTA is primarily based from the Office of Management and Budget (OMB) privacy guidance and the Department of Commerce (DOC) IT security/privacy policy. If questions arise or further guidance is needed in order to complete this PTA, please contact your Bureau Chief Privacy Officer (BCPO).

Description of the information system and its purpose: *Provide a general description of the information system in a way that a non-technical person can understand.*

The E-Government Act of 2002 defines "information system" by reference to the definition section of Title 44 of the United States Code. The following is a summary of the definition: "Information system" means a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information. See: 44. U.S.C. § 3502(8).

a) *Whether it is a general support system, major application, or other type of system*

The OHRM is responsible for planning, developing, administering and evaluating the human resources management programs of the Department. This enables the Department to acquire and manage a dedicated, diverse, motivated, and highly qualified workforce to accomplish its mission and achieve its goals, while ensuring compliance with pertinent Federal, Office of Personnel Management, Office of Management and Budget, and Department of Labor, policy and administrative mandates.

- WebTA is Kronos Proprietary software – Used to record DOC employee's time and attendance data. The employees enter their own time and attendance data. The data is transmitted bi-weekly to NFC for employees pay processing.
- ArchiveTime is a data archiving and report application that sits on top of the WebTA 3.8 database so DOC can access past years of historical data (WebTA 4.2, which is in production, only converted 26 prior pay periods of data) for audits and reports.

b) *System location*

The systems are primarily managed by resources located at the CBS Solution Center in Gaithersburg, MD. The system is physically located at the Federal Aviation Administration Data Center (DOT/FAA/ESC) in Oklahoma City, OK.

c) *Whether it is a standalone system or interconnects with other systems (identifying and describing any other systems to which it interconnects)*

NIST/Census Commerce Business Solutions (CBS) - NIST uses a supplemental file from WebTA to obtain a labor/cost estimate, and Census uses it to validate accounting against CBS valid accounts as well as with an interface to import Decennial Census payroll data.

d) The purpose that the system is designed to serve

This system enables the Department to acquire and manage a dedicated, diverse, motivated, and highly qualified workforce to accomplish its mission and achieve its goals, while ensuring compliance with pertinent Federal, Office of Personnel Management, Office of Management and Budget, and Department of Labor, policy and administrative mandates.

- WebTA is Kronos Proprietary software used to record DOC employees' time and attendance data. The employees enter their own time and attendance data.
- ArchiveTime is a data archiving and report application that sits on top of the WebTA 3.8 database so DOC can access past years of historical data (WebTA 4.2, which is in production, only converted 26 prior pay periods of data) for audits and reports.

e) The way the system operates to achieve the purpose

WebTA is a timekeeping system that stores PII for the purposes of passing information to the NFC Payroll system. The system collects data daily from user input. This input consists of Work Data, Leave Data and Dollar Transaction Data.

Work Data consists of weekly (and ultimately, bi-weekly pay period) input of daily labor descriptive data related to daily work duties. A daily occurrence, consists of a transaction code describing the nature of the work duty, an accounting code for where the financial system will charge this time and the actual time worked. It is also possible to include a clock time range worked within each work day. There may be multiple occurrences of work data in a given pay period, and multiple occurrence of work data in a given day.

Leave Data includes weekly (ultimately, bi-weekly pay period) input of daily time off and time off award data, a transaction code describing the type of leave being taken, an account code to trigger the correct chargeback in downstream financial systems and actual time taken as leave. There may be multiple occurrences of work data in a given pay period, and multiple occurrences of leave data in a given day.

Dollar Transactions include employee requests for reimbursement related to work-incurred expenses. This includes a transaction code describing the type of expense incurred, an accounting code to charge this expense and the actual expense amount requested.

This data is collected, maintained and used for payroll generation via downstream system, ad-hoc research and reporting and leave-related reporting and tracking.

WebTA has its own credential assignment function. Each user receives a unique user ID and password. The password is required to adhere to Federal IA standards. Each user can be assigned a variety of roles that allow varying levels of data access. These permissions range from basic employee-related time and leave entry to Master User and Administrator, who can

see and manipulate much larger data populations and affect system administration-type changes to system operational parameters and functions.

WebTA collects bi-weekly payroll data from this input to create and transmit a payroll time and attendance file to NFC, the payroll processor at USDA. This is a secure SFPT transmission configured and monitored by a WebTA Administrator, with password maintenance and access provided by NFC.

CENSUS and NIST extract a version of this payroll file via a vendor provided custom process, and upload it to downstream financial systems for budget analysis.

CENSUS receives remote input from WebTA to timesheets via a vendor provided custom interface from a system called WebFRED. The remote users do not have direct access to WebTA's timesheet entry and maintenance functions, so this system replaces it to the extent that the remote offices need it to. This remote system also has assigned and restricted access and is limited to timesheet and code-related maintenance.

f) *A general description of the type of information collected, maintained, use, or disseminated by the system*

WebTA is a timekeeping system that stores PII for the purposes of passing information to the NFC Payroll system. The system collects data daily from user input. This input consists of Work Data, Leave Data and Dollar Transaction Data.

g) *Identify individuals who have access to information on the system*

Access to WebTA and Archive Time are role based. Security is provided by granting and revoking privileges on a person-by-person and role-by-role basis.

WebTA – It is the responsibility of the WebTA Security Officers/Timekeepers Keep a record of all WebTA accesses that they granted resulting from the SHRO's established enter-on-duty procedures.

Archive Time – It is the responsibility of the Archive Time Security Officers to keep a record of the HR employees they provided system access to. Information to be recorded include: name, user ID, date access was granted, and the level of access. This record must be made available to the Office of Human Resources Management, auditors, and other authorized persons upon request.

h) *How information in the system is retrieved by the user*

Users can print reports containing only data that is allowed by their role within all of WebTA and Archive Time. It is the responsibility of the users to handle printed media in accordance with established policies/procedures/rules of behavior and governmental record retention regulations of their bureau and DOC. Users can download information, again based on their assigned user role within WebTA and Archive Time, to removable media and it is their responsibility to handle

digital media in accordance with established policies/procedures/rules of behavior and governmental record retention regulations of their bureau and DOC.

i)   How information is transmitted to and from the system

Information is transmitted across approved encryption protocols such as HTTPS, SSH, and SFTP. Sensitive data transmissions are encrypted according to NIST 800-18, Federal Information Processing Standards (FIPS) 186, Digital Signature Standard and FIPS 180-1, and Secure Hash Standard issued by NIST when necessary.

Questionnaire:

1. What is the status of this information system?

    _____   This is a new information system. *Continue to answer questions and complete certification.*

    _____   This is an existing information system with changes that create new privacy risks.
    Complete chart below, continue to answer questions, and complete certification.

Changes That Create New Privacy Risks (CTCNPR)					
a. Conversions		d. Significant Merging		g. New Interagency Uses	
b. Anonymous to Non-Anonymous		e. New Public Access		h. Internal Flow or Collection	
c. Significant System Management Changes		f. Commercial Sources		i. Alteration in Character of Data	
j. Other changes that create new privacy risks (specify):					

    _____   This is an existing information system in which changes do not create new privacy risks, and there is not a SAOP approved Privacy Impact Assessment. *Continue to answer questions and complete certification.*

    _X__   This is an existing information system in which changes do not create new privacy risks, and there is a SAOP approved Privacy Impact Assessment (version 01-2015 or later). *Skip questions and complete certification.*

2. Is the IT system or its information used to support any activity which may raise privacy concerns?
    NIST Special Publication 800-53 Revision 4, Appendix J, states "Organizations may also engage in activities that do not involve the collection and use of PII, but may nevertheless raise privacy concerns and associated risk. The privacy controls are equally applicable to those activities and can be used to analyze the privacy risk and mitigate such risk when necessary." Examples include, but are not limited to, audio recordings, video surveillance, building entry readers, and electronic purchase transactions.

    _____   Yes. *Please describe the activities which may raise privacy concerns.*

    _____   No

3. Does the IT system collect, maintain, or disseminate business identifiable information (BII)?

    As per DOC Privacy Policy: "For the purpose of this policy, business identifiable information consists of (a) information that is defined in the Freedom of Information Act (FOIA) as "trade secrets and commercial or financial information obtained from a person [that is] privileged or confidential." (5 U.S.C.552(b)(4)). This information is exempt from automatic release under the (b)(4) FOIA exemption. "Commercial" is not confined to records that reveal basic commercial operations" but includes any records [or information] in which the submitter has a commercial interest" and can include information submitted by a nonprofit entity, or (b) commercial or other information that, although it may not be exempt from release under FOIA, is exempt from disclosure by law (e.g., 13 U.S.C.)."

    _____   Yes, the IT system collects, maintains, or disseminates BII about: *(Check all that apply.)*

    _____   Companies
    _____   Other business entities

    _____   No, this IT system does not collect any BII.

4. Personally Identifiable Information

4a. Does the IT system collect, maintain, or disseminate personally identifiable information (PII)?

    As per OMB 07-16, Footnote 1: "The term 'personally identifiable information' refers to information which can be used to distinguish or trace an individual's identity, such as their name, social security number, biometric records, etc... alone, or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, mother's maiden name, etc..."

    _____   Yes, the IT system collects, maintains, or disseminates PII about: *(Check all that apply.)*

    _____   DOC employees
    _____   Contractors working on behalf of DOC
    _____   Members of the public

    _____   No, this IT system does not collect any PII.

If the answer is "yes" to question 4a, please respond to the following questions.

4b. Does the IT system collect, maintain, or disseminate PII other than user ID?

    _____   Yes, the IT system collects, maintains, or disseminates PII other than user ID.

    _____   No, the user ID is the only PII collected, maintained, or disseminated by the IT system.

4c. Will the purpose for which the PII is collected, stored, used, processed, disclosed, or disseminated (context of use) cause the assignment of a higher PII confidentiality impact level?

Examples of context of use include, but are not limited to, law enforcement investigations, administration of benefits, contagious disease treatments, etc.

_____ Yes, the context of use will cause the assignment of a higher PII confidentiality impact level.

_____ No, the context of use will not cause the assignment of a higher PII confidentiality impact level.

If any of the answers to questions 2, 3, 4b, and/or 4c are "Yes," a Privacy Impact Assessment (PIA) must be completed for the IT system. This PTA and the approved PIA must be a part of the IT system's Assessment and Authorization Package.
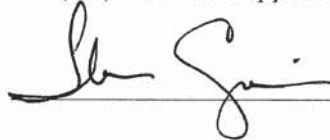
CERTIFICATION

__X__ I certify the criteria implied by one or more of the questions above **apply** to the DOC WebTA-ArchiveTime system and as a consequence of this applicability, I will perform and document a PIA for this IT system.

_____ I certify the criteria implied by the questions above **do not apply** to the DOC WebTA-ArchiveTime system and as a consequence of this non-applicability, a PIA for this IT system is not necessary.

Name System Owner (SO): Teresa Coppolino

Signature of SO: _____ Date: ___3/7/19___

Name of Information Technology Security Officer (ITSO): Jun Kim

Signature of ITSO: _____ Date: _____

Digitally signed by JUN KIM
DN: c=US, o=U.S. Government, ou=Department of Commerce,
ou=Office of the Secretary, cn=JUN KIM,
0.9.2342.19200300.100.1.1=13001001483988
Date: 2019.03.11 14:37:38 -04'00'

Name of Authorizing Official (AO): Stephen Kunze

Signature of AO: _____ Date: __4/12/19__

Name of Bureau Chief Privacy Officer (BCPO): Wes Fravel

WESLEY FRAVEL
Digitally signed by WESLEY FRAVEL
Date: 2019.04.16 15:27:04 -04'00'

Signature of BCPO: _____ Date: _____