UNITED STATES

FEDERAL COMMUNICATIONS COMMISSION

PRIVACY IMPACT ASSESSMENT FOR WEB TIME & ATTENDANCE (WEBTA)

May 19, 2021

OFFICE OF THE GENERAL COUNSEL

WASHINGTON, DC 20554

Record of Approval

Document Approval		
Drafter Name: A. Marie Dorsey		**Bureau/Office: OMD/IR**
SAOP Approval		
Printed Name: Margaret Drake		**Senior Agency Official for Privacy**
Signature: Margaret E Drake Digitally signed by Margaret E Drake DN: cn=Margaret E Drake, o=Federal Communications Commission, ou=Privacy, email=margaret.drake@fcc.gov, c=US Date: 2021.05.19 15:13:38 -04'00'	**Date** 5/19/21	

Record of Approval

Date	Description	Name
05/12/2021	Validation of information – System Owner	Carol Edwards
05/19/2021	Validation of completeness – IT Compliance Lead	Liem Nguyen

Web Time & Attendance

1.1. Introduction

Section 208 of the E-Government Act of 2002[1] requires agencies to conduct a **Privacy Impact Assessment (PIA)** whenever they procure or develop an information technology system that will collect, maintain, or disseminate information about individual people. The PIA must document how the system will use information it collects about individuals and, unless it contains classified or sensitive information, it must be made available to the public. The PIA was intended to be a tool for agencies to protect personal information throughout a technology system's life cycle. The Office of Management and Budget (OMB) has commented: "*In general, PIAs are required to be performed and updated as necessary where a system change creates new privacy risks.*"[2]

The FCC is subject to the requirements of the E-Government Act and is committed to identifying and addressing privacy risks whenever it develops or makes changes to its information systems. The questions below explore important privacy issues identified in the Act and in later guidance by the Office of Management and Budget (OMB) and the National Institute of Standards and Technology (NIST). A longer discussion of the FCC's PIA policies can be found in Chapter 9 of the FCC's Privacy Act Manual (FCC Inst. 1113.1).

System owners, in collaboration with the Information System Security Officers (ISSOs) should complete the **Initial Privacy Assessment (IPA)** prior to filling out the PIA. The FCC Senior Agency Official for Privacy (SAOP) uses the IPA to determine whether a system will collect the kind of information that would make it subject to the requirements of Section 208, including a PIA. A PIA should not be completed until an IPA is completed and the SAOP makes a determination..

If you have any questions, please contact the Privacy Team at privacy@fcc.gov.

[1] 44 U.S.C. § 3501 note.

[2] OMB Memorandum No. M-03-22 (Sep. 26, 2003), https://www.whitehouse.gov/sites/whitehouse.gov/files/omb/memoranda/2003/m03_22.pdf.

1.2. Authority To Operate (ATO) Boundary Overview

For each IT system that resides within the ATO Boundary, please use the table below to provide the system name, a brief description of the what the system does, whether it contains Personally Identifiable Information (PII) and a brief description of the PII (if applicable), the applicable System of Records Notice, the legal authorities to collect and maintain the PII, and whether the PII is shared with other systems (internal or external).

Please copy the table as necessary to complete the information for each system within the boundary.

INFORMATION ABOUT THE SYSTEM
NAME OF THE SYSTEM Web Time & Attendance (webTA)
DOES THE SYSTEM CONTAIN PII? Yes.
PLEASE PROVIDE A BRIEF DESCRIPTION OF THE PII (IF APPLICABLE) Full Name, alias, email address, medical information, social security number, and user id.
IN WHAT SYSTEM OF RECORDS (SORN) IS THE INFORMATION CONTAINED (IF APPPLICABLE)?
WHAT ARE THE LEGAL AUTHORITIES FOR THE COLLECTION OF THIS PII? 5 U.S.C. chapters 53, 55, 61, 63, and 65; Executive Order 9397, as amended (Nov. 20, 2008); Personal Responsibility and Work Opportunity Reconciliation Act of 1996 (Pub. L. 104-193); 10 U.S.C. 1408; and 42 U.S.C. 659.
DOES THIS SYSTEM SHARE THE PII WITH OTHER SYSTEMS? Yes. USDA National Finance Center (NFC).

A. Is this a new ATO Boundary or an existing ATO Boundary?

☒ New Boundary

☐ Existing Boundary

B. If the ATO Boundary is/will consist of cloud-based computing system(s),[3] please check the box that best describes the service the FCC receives/will receive from the cloud computing provider:

☒ The FCC uses provider-supported application/s on the provider's cloud network (Software as a Service or SaaS) [list applicable system(s)]

Amazon Web Services (AWS)

☐ The FCC has deployed application/s on the provider's cloud network and the provider supports the applications (Platform as a Service or PaaS) [list applicable system(s)]

☐ The FCC has deployed its own application/s on the cloud network and controls how these application/s are configured and operate (Infrastructure as a Service or IaaS) [list applicable system(s)]

C. **If the IT systems in the ATO Boundary are in the cloud, are the they FedRAMP certified?**

☒ Yes, all the IT systems are FedRAMP certified
☐ No, none, or only some, of the IT systems are FedRAMP certified

Web Time & Attendance is a software as a service, externally hosted on FedRAMP Amazon Web Services (AWS).

1.3. Collection of Data

A. Please explain why it is necessary to collect PII to carry out the purpose of each of the system(s) that maintain PII within this Boundary.

Records are used to prepare time and attendance records, to record employee pay rates and status, including overtime, the use of leave, and work absences; to track workload, project activity for analysis and reporting purposes; for statistical reporting on leave and overtime use/usage patterns, number of employees teleworking, etc.; and to answer employee queries on leave, overtime, and pay.

[3] *See* NIST, *The NIST Definition of Cloud Computing*, Special Pub. No. 800-145 (Sep. 2011), https://csrc.nist.gov/publications/detail/sp/800-145/final.

B. For each system within this Boundary, will this PII be collected from individuals themselves, or from third-parties? If collected from individuals themselves, link to the Privacy Act Statement[4] for each system that is included with the online or paper form the system(s) use(s) to collect the PII.

Individuals themselves.

C. What steps is the FCC taking to limit the collection of PII to only that which is necessary?

FCC HRM only collects the needed PII from the individuals themselves to set up profile and personnel record.

D. What steps will the FCC take to make sure this PII is accurate, complete, and up-to-date?

FCC HRM verifies all PII from issued Government identification or documents.

1.4. Use of the Data

A. Please explain the data flow, including whether the PII will be ingested from, or shared with, another system. Are internal connections reflected in the Cyber Security Asset Management tool (CSAM)? Are Information Sharing Agreements (ISAs) in CSAM for external connections?

PII will be shared with the USDA National Finance Center (NFC). There are no internal connections to be reflected within the Cyber Security Asset Management tool (CSAM). An Inter-Agency Security Agreement (ISA) has been developed and is fully executed by both organizations. The connection and documentation is reflected in the Cyber Security Asset Management tool (CSAM).

B. Will the information be shared with third-parties as part of the operations of the information system (e.g., through an application programming interface or "API")?

No

[4] A Privacy Act Statement must inform individuals about (1) the authority to solicit information, (2) the principal purpose(s) for collecting the information, (3) the routine uses for disclosing the information, and (4) whether providing the information is mandatory or voluntary.

C. How long will the PII be retained and how will it be disposed of?

PII will be retained and disposed of in accordance with the National Archives and Records Administration (NARA) General Records Schedule 2.4 (GRS 2.4). Which indicates to destroy when 3 years old, but longer retention is authorized if required for business use. Additionally, once documents containing PII have been manually entered into the HRM database, the PII documents are shredded.

1.5. Data Security and Privacy

A. What are the system's ratings for confidentiality, integrity, and availability?

Confidentiality	**__High**	**_X_Moderate**	**___Low**
Integrity	**__High**	**_X_Moderate**	**___Low**
Availability	**__High**	**_X_Moderate**	**___Low**

B. Discuss the physical, administrative, and technical controls in place to protect the data in the system.

The FCC protects its information resources with a dynamic set of security measures. Some of these measures (e.g., network firewalls, physical security) protect the entire FCC enterprise, while other measures (e.g., user access restrictions, encryption) are applied to specific information systems. Following the risk-based policy established in the Federal Information Modernization Act (FISMA), the FCC applies more security measures (also known as security "controls") to information systems that present higher operational risks. Consistent with this policy, the FCC applies specific security controls to systems that collect and process PII. A comprehensive list of the security and privacy controls the FCC may apply to its information systems can be found in National Institute of Standards and Technology (NIST) Special Publication No. 800-53 (revision 4), ttps://csrc.nist.gov/publications/detail/sp/800-53/rev-4/final.

C. Does the system inherit privacy controls from an external provider? If an Interconnection Security Agreement (ISA) , Memorandum of Understanding (MOU) , or similar document is in place, please summarize the privacy applicable portions of the document.

Web Time & Attendance (webTA) does not inherit privacy controls from an external provider.

1.6. Access to the Information

A. Which FCC employees and contractors will have access to the PII in this information system?

FCC employees and contractors within the Human Resource Management department will have access to the PII in Web Time & Attendance (webTA).

B. Does this system leverage Enterprise Access Controls?

Yes.

C. Does the system leverage the FCC's Accounting for Disclosure control?

Yes. The Privacy Team keeps an accurate accounting of disclosures of information.