Privacy Impact Assessment

Template

Technology, Planning, Architecture, & E-Government

- Version: 1.3
- Date: March 30, 2020
- Prepared for: USDA OCIO TPA&E

United States Department
of Agriculture

Privacy Impact Assessment for the

Enterprise Web Application and Platform Services (eWAPS)

March 30, 2020

Contact Point
Steve Hou
USDA, Departmental Administration Information Technology Office (DAITO)
202-720-2914

Reviewing Official
Cedric Bragg
Assistant Chief Information Officer
Authorizing Official
USDA, Departmental Administration Information Technology Office
202-720-4490

Abstract

The abstract should be a minimum of three sentences and a maximum of four, if necessary, and conform to the following format:

- First sentence should be the name of the component and system.
- Second sentence should be a brief description of the system and its function.
- Third sentence should explain why the PIA is being conducted.

The Departmental Administration Information Technology Office (DAITO) eWAPS is a public facing web service providing connectivity via HTTPS for Federal Government websites. DAITO provides hosting and maintenance for software infrastructure and services made available to multiple agencies. The PIA is being conducted as the system stores and processes Name and E-mail PII data during routine operations.

Overview

The overview is the most important section of the PIA. A thorough and clear overview gives the reader the appropriate context to understand the responses in the PIA. The overview should contain the following elements:

- The system name and the name of the Department component(s) who own(s) the system;
- The purpose of the program, system, or technology and how it relates to the component's and Department's mission;
- A general description of the information in the system;
- A description of a typical transaction conducted on the system;
- Any information sharing conducted by the program or system;
- A general description of the modules and subsystems, where relevant, and their functions; and
- A citation to the legal authority to operate the program or system.

The Departmental Administration Information Technology Office (DAITO) eWAPS is a public facing web service providing connectivity via HTTPS for Federal Government websites. DAITO provides hosting and maintenance for software infrastructure and services made available to multiple agencies. Standard functionality provided to Federal Government users includes Docker-containerized services on isolated virtual networks. Containerized services include HAproxy, Caching (Redis, Varnish, Memcached, etc), Search (Apache Solr, ElasticSearch, etc), Web Services (Nginx, Apache Web Server with PHP and PHP-FPM, etc), Database Services (MariaDB, Postgre, etc), and maintenance services (backup, cron, networking, logging, and monitoring). An elastic (variable number) of servers provide the pre-production and production infrastructure. The systems rely on a centralized master *orchestration and configuration management server to provision and deprovision servers in the environment. Services implemented use an "infrastructure as code" model using Salt and Rancher allowing auditable and testable configurations to be deployed on test environments prior to production release. Systems operate within the USDA's Digital Infrastructure Services Center (DISC), Data Center Hosting Services (DCHS). Pre-production services are currently being migrated from OpenStack to DISC's PaaS Base Linux service. Production servers operate on the VMware vSphere PaaS Base Linux service. DAITO provides 4-hour emergency business hours SLA support backed by agency staff, USDA Office of the CIO, and support contracts for Rancher and Docker. Typical transactions include authenticated and non-authenticated presentation of webpages for US Federal Agency staff and the general public.*

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?

Full Name, E-mail address, Full address + zipcode and telephone number; herein referred to as "contact information"

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

eAuth Integration and Form Submission

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

Contact Information is used for account maintenance, program administration and communication activities. Contact information is disseminated via privileged and authenticated user account access for staff office activities. Contact information is maintained within database for access by program area and support staff.

1.4 How is the information collected?

Contact information is collected via eAuth integration and web form submission.

1.5 How will the information be checked for accuracy?

Contact Information collected will validated through manual staff review when used for mission efforts.

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

Paperwork Reduction Act of 1995 (44 U.S.C. 3501 et seq.)

OMB CONTROL NUMBER: 0506-0005
EXPIRATION DATE: 07/31/2020
The agency is required to display the OMB Control Number and inform respondents of its legal significance in accordance with 5 CFR 1320.5(b).

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

Risks: Minimal risk; eWAPS gives customers, producers, partners, and others ability to submit forms related to USDA programs. Limited data as defined in the PTA is produced.

Mitigation: Applications are located behind the NITC secure midrange infrastructure. See the System Security Plan (SSP) security controls: Accountability, Audit and Risk Management (AR), Data Quality and Integrity (DI) and Data Minimization and Retention (DM). These applications are behind eAuthentication (eAuth) with a Level 2 access authority. Users of the system are required to complete annual privacy act training to ensure the proper handling of privacy data.

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.

Communication of non-sensitive program related information, authenticated account access, automated notifications from website.

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

Manual review by program staff, review by site administrators.

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

Not using 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.

Information gathered is retained in web application with privileged access granted via eAuth authentication. Communication of program information using Contact Information is only completed when reviewed by program staff prior to delivery. Authenticated account access occurs once a user has authenticated via eAuth service. Automated website notifications are only delivered when triggered by automated webservice task queue.

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?

Until no longer necessary for program or administrative activities.

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.

System may retain Contact Information for extended periods as necessary for program administration and application authentication. Application patching is consistently applied. When data is in use, information is transmitted via SSL encryption using Forward Secrecy. Accounts are automatically logged after 30 minutes of inactivity.

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?

Contact Information is shared with numerous agency users from a broad cross-section of agency staff including, but not limited to, FNS, OCIO, DAITO, and DM.

4.2 How is the information transmitted or disclosed?

SSL Encrypted connection via web browser after authentication with eAuth.

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

The NIST 800-53 controls for the eWAPS system are discussed in detail in the System Security Plan and specifically the System and Communication (SC) controls are in place to provide integrity and confidentiality. Interconnection Service Agreement (ISA) and Memorandum of Understanding (MOU) agreements are in place [in Cyber Security Assessment and Management (CSAM)] and maintained by the Information Systems Security Staff (ISSS).

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?

No external sharing.

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

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

N/A

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

N/A

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?

Yes.

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

Yes

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

No. The information required and how it will be used is documented in agency regulations and published on the USDA Privacy Policy of the website.

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 is provided to customers at the time of their inquiry submission. It is during this process that the customer has the opportunity to cancel the request.

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?

Users may view Contact Information via eAuth system.

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

Users may update Contact Information via eAuth system. Data is automatically synchronized when updated within eAuth system.

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

Information is provided via e-mail when support request is received.

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

N/A

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 are limited to those associated with eAuth system. No heightened risk to agency for redress.

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?

PIV card is required to access eWAPS. Generally, the National Institute of Standards and Technology (NIST) 800-53 controls for Common Call Components are discussed in detail in the System Security Plan and specifically the Access Control (AC), Identification and Authentication (IA) and Systems and Communication Protection (SC) controls are in place to prevent unauthorized access. Access control is also addressed in the individual systems desk procedures. Desk Procedures document the process for establishing, activating, and modifying IDs. This process is defined by

System Owners. System Owners define Groups and account types. System Point of Contact assigns group membership and determines Need to know validation. The POC is responsible for verifying user identification; the User Access Management (UAM) Team relies on a POC supplying the correct UserID and password to UAM to identify themselves. Support tickets are the tool used to track authorized requests by approving Point of Contact (POC). The organization employs automated mechanisms to support the management of information system accounts. Temporary and emergency accounts are restricted to limited usage. Guest and Anonymous accounts are not managed by the DAITO Team. POCs (empowered by DAITO IT support) are responsible for notifying UAM Team if access or roles need to be modified and periodically reviewing and certifying established access.

8.2 Will Department contractors have access to the system?

Yes.

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

Users are required to complete USDA IT Security training prior to access.

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

Yes. eWAPS has an ATO.

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

eAuth limits access to Contact Information to only program administrative users. Users must be granted appropriate access to each program application in order view Contact Information. Accounts automatically expire within application once terminated within eAuth service.

8.6 <u>Privacy Impact Analysis</u>: 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?

Privacy risk is limited due to limited privileged account usage within each program area.

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?

Hosted enterprise-wide web application shared service system.

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

N/A

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?

DigitalGov Analytics, Social Media Analytics Service

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

None. Services collect anonymized, generic information for use when assessing program success.

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

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

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

N/A

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

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

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

10.10 Does the system use web measurement and customization technology?

Yes, web measurement.

If so, is the system and procedures reviewed annually to demonstrate compliance to OMB M-10-23?

Yes

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

Yes, users may elect to set "Do Not Track" settings within browsers.

If so, does the agency provide the public with alternatives for acquiring comparable information and services?

Yes.

10.12 <u>Privacy Impact Analysis</u>: 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.

PII data is not collected via 3rd party websites and/or applications.

Responsible Officials

Steve Hou

eWAPS System Owner

Departmental Administration Information Technology Office

United States Department of Agriculture

Approval Signature

CEDRIC BRAGG

Digitally signed by CEDRIC BRAGG
Date: 2020.09.02 14:28:36 -04'00'

Cedric Bragg
Assistant Chief Information Officer
eWAPS Authorizing Official
Departmental Administration Information Technology Office
United States Department of Agriculture