Privacy Impact Assessment

Operating System for Customer Access and Requests (OSCAR)

Policy, E-Government and Fair Information Practices

- Version: 1.4
- Date: May 29, 2020
- Prepared for: USDA Office of Operations - Privacy Office

Privacy Impact Assessment for the

Operating System for Customer Access and Requests (OSCAR)

May 29, 2020

Contact Point

Duane Williams
System Owner
202-720-3937

Reviewing Official

Lisa McFerson
Interim Information Systems Security Program Manager
United States Department of Agriculture
202-720-8599

Abstract

This Privacy Impact Assessment (PIA) is for the USDA, Departmental Management (DM) Office of Operations (OO) Operating System for Customer Access and Requests (OSCAR) System. The DM-OO OSCAR system provides a web-based tool that enables and support multiple business processes across the Office of Operations. This PIA is being conducted to determine the potential impact of data collected via DM-OO OSCAR.

Overview

DM-OO OSCAR supports multiple business processes across the Office of Operations, including:

- Hotline 2.0, a service desk accepting work orders and service requests from USDA employees. It handles the routing and is the clearing house for all activities through WASC.
- Waste Management handles the disposal of recyclable and non-recyclable items. Recycled waste is collected through various methods throughout the facility. They include hallway containers cafeteria receptacles and office recycle bins. Waste is collected and weighed by the janitorial staff. Record on a form and tuned into the WASC for system entry.
- AM-PM Center is responsible for generating equipment PM requests at an assigned frequency.
- Executive Limousine Service provides dispatch limousine service to USDA executives. It is also responsible for recording maintenance requests for vehicles.
- Minor Repairs System processes work order requests for tickets that cost between $500 and $25,000. It will also track the total costs (such as labor and material) costs for work order tickets below $500.
- Project Management module will combine 3 different modules in the current system: Maintenance Control System, Building Project Management, and Repairs and Alteration. These will become 3 different project types in the new system. The processes for this module will vary by project type.
- Building Permit Management center handles requests for building permits. An application for a request is submitted by a customer, which is routed through a process where various reviewers across different disciplines can be assigned to approve the request.
- Mechanical Equipment module currently holds information about various equipment; such as water heater, pump, chiller, and AHU.

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?

The system uses the following information about users of the system:
- Name
- Address information
- Miscellaneous identification numbers (Parking permit number and building permit number)
- Photographic image (photographs are at the discretion of the user and are not required), and
- Other information that may be seen as personal (there is an "About Me" section within the Salesforce model that is not restricted as to what the user can input.

Conceivably, a user could enter any data into the form that is PII).

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

The sources of information in the system come from the users of the system themselves.

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

The information is collected to issue parking permits to various personnel, and to identify individuals making requests within the OSCAR application and managing the data within OSCAR. It is also used to maintain the integrity of the system through ACLs (Access Control Lists). PII is not required for the proper operation of the OSCAR system, and is provided solely at the discretion of the user.

1.4 How is the information collected?

The information is collected by email from each user initially to create the account within Salesforce. Upon Salesforce user access, the user has the option to update their profile within Salesforce to include a photo, which is considered PII when combined with a name.

1.5 How will the information be checked for accuracy?

Information provided by the user is cross-checked with Federated User IDs through Active Directory.

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

Departmental Regulation (DR) 1633-001, "Parking - USDA Headquarters Complex Washington, D.C." states that all applicants must submit the appropriate forms, and that Agency Parking Representatives are specifically instructed to return incomplete or improperly prepared applications to the applicant.

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

The Office of Operations has become aware of the need for policies and procedures governing input of PII into DM cloud systems, and these policies/procedures are under development.

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.

Information within the DM-OO OSCAR application is used to provide parking permits, and to dispatch limousine service to USDA executives.

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

There is no analysis of the data that occurs.

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

The system does not use commercially 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.

The information is protected through various levels of security and policy. The system itself is protected by role-based access layers and positive identification techniques to ensure that only people authorized to view and act on information about others can do so.

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?

Items are retained per the General Records Schedule 24: Information Technology Operation and Management Records. Records are destroyed based on the subject matter.

http://www.archives.gov/records-mgmt/grs/grs24.html

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.

The retention period is in line with standard retention schedules for similar data and is long enough that any likelihood of having issues associated with the archiving or disposal of data is minimal.

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?

Information may be shared with senior leadership across USDA through a series of Tableau dashboards and reports for the purpose of promoting data-driven decisions. The information shared will span data from different various administrative domains including IT, Finance, HR, Property, Operations, Homeland Security, and Property & Fleet.

4.2 How is the information transmitted or disclosed?

The information will be transmitted to the USDA Data Lake via secure file transfer methods such as SFTP, API, and Web Service. Once in the USDA data Lake, data will be shared via a series of Tableau dashboards.

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.

Risk when sharing within USDA is considered low-moderate. Should data sharing include sources of the network, encryption protocols ensure PII is not inadvertently shared in an unencrypted format. Data is encrypted in motion and at rest. In addition, access to data is limited to only those persons with a need-to-know using internal, granular governance process. Dissemination of information is governed by internal policy. Access to information is monitored, tracked, logged and audited using tools such as Cloudera Navigator and Cloudera Manager.

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?

Given that information is not shared with any other organizations, internal or external, there is no privacy risks associated.

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.

The information is not shared with any other organizations, internal or external.

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

The information is not shared with any other organizations, internal or external.

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

Given that information is not shared with any other organizations, internal or external, there is no privacy risks associated.

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 Does this system require a SORN and if so, please provide SORN name and URL.

No

6.2 Was notice provided to the individual prior to collection of information?

Notice is not provided, as PII is not is not required to use the OSCAR system and is provided solely at the discretion of the user.

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

Yes, PII is not required to use the OSCAR system.

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

Yes, they can change their information in their profile at any time, and PII is not required to use the OSCAR system. There is no policy that specifies how their information is used.

6.5 Privacy Impact Analysis: Describe how notice is provided to individuals, and how the risks associated with individuals being unaware of the collection are mitigated.

PII is not required to use the OSCAR system, and PII is provided solely at the user's discretion. Each individual has access to their profile page within Salesforce to edit or remove any PII that is listed.

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?

Each individual has access to their profile information within Salesforce.

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

Each individual can edit their profile within Salesforce to correct inaccurate or erroneous information.

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

User guides within Salesforce provide information on how to edit a user's profile.

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

Each individual can edit their profile within Salesforce to correct inaccurate or erroneous information.

7.5 Privacy Impact Analysis: Please discuss the privacy risks associated with the redress available to individuals and how those risks are mitigated.

User profiles are not monitored for PII input by the agency and is not required for the proper use of the OSCAR system. Individuals have redress by virtue of access to their profile to correct, or delete any information that they have input.

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?

DM-OO implements a Rules of Behavior (ROB) to which all users must consent before being granted system credentials for access. The system inherits the USDA implementation of User Security Awareness training, which is provided annually by the Department. Additionally, user accessing the system must have an eAuth account.

8.2 Will Department contractors have access to the system?

Only specifically authorized Department contractors have access to the system. Those individuals must first obtain relevant security clearances along with specific authorization to access information at various levels.

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

Annual Security Awareness training is offered through the AgLearn+ system, and "Protecting Personally Identifiable Information" is offered as a training module as well.

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

Yes

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

All users are required to have an individual account, and role-based access is in place.

8.6 Privacy Impact Analysis: 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?

The information is protected through various levels of security and policy. The system itself is protected by role-based access layers and positive identification techniques to ensure that only personnel authorized to view and act on information about others can do so.

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?

DM-OO OSCAR is a web-based information system on a cloud-based platform.

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

The system does not use any technologies that would raise a privacy risk.

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?

N/A, no third party websites are used.

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

N/A, no third party websites are used.

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, no third party websites are used.

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, no third party websites are used.

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

N/A, no third party websites are used.

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, no third party websites are used.

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, no third party websites are used.

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, no third party websites are used.

10.10 Does the system use web measurement and customization technology?

N/A, no third party websites are used.

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?

N/A, no third party websites are used.

10.12 Privacy Impact Analysis: 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.

N/A, no third party websites are used.

Agency Responsible Officials

Duane Williams
System Owner
Department Administration/Office of Operations
United Stated Department of Agriculture

Agency Approval Signature

LISA MCFERSON Digitally signed by LISA MCFERSON
Date: 2020.06.11 09:02:18 -04'00'

Lisa McFerson
Information System Security Program Manager
Departmental Administration Information
Technology Office
United States Department of Agriculture

CEDRIC BRAGG Digitally signed by CEDRIC BRAGG
Date: 2020.06.11 16:39:16 -04'00'

Cedric Bragg
Authorizing Official
Departmental Administration Information
Technology Office
United States Department of Agriculture