

Privacy Impact Assessment

Technology, Planning, Architecture, & E-Government



Privacy Impact Assessment for the Civil Rights Enterprise System (CRES)

February 18, 2020

Contact Point

Michele A. Washington
OCIO/OASCR ISSPM
202-205-3369

Reviewing Official

Michele A. Washington
ISSPM and Project Manager
United States Department of Agriculture
(202) 205-3369

Abstract

This PIA is for the Civil Rights Enterprise System (CRES). It is a Web-based enterprise-wide suite of applications supporting USDA and all Departmental Agencies by tracking, processing, and managing employment, and program complaints, as well as meeting regulatory reporting requirements.

The PIA is being conducted to maintain ATO.

Overview

CRES is a major application—an enterprise system sponsored by the USDA Office of the Assistant Secretary for Civil Rights (OASCR). It is a Web-based enterprise-wide suite of applications supporting USDA and all Departmental Agencies by tracking, processing, and managing employment, and program complaints, as well as meeting regulatory reporting requirements. The system provides core support for the mission of Civil Rights (CR) offices both at the Departmental and Agency levels, and it serves management needs of Agency Heads who by law are charged with the responsibility for Agency compliance with Equal Employment Opportunity (EEO) and CR. The initiative encompasses Employment Complaint Processing and Reporting and Program Complaint Processing and Reporting. In addition to the complaint processing CRES also handles Alternative Dispute Resolution (ADR) which is offered prior to making a complaint, both a formal and informal process. CRES is a server based application that users connect to via their web browser application. There is no client side portion of software that must be installed. CRES itself is a COTS package of software called iComplaints. CRES is co-located at MicroPact Engineering, Inc. MicroPact Engineering provides system, network, development, and administrative security under contract with The Assistant Secretary for Civil Rights (OASCR). The CRES server environment is interconnected to the public Internet via a MicroPact managed gateway that includes a Cisco routers and switches, Fortigate and Firebox Firewall appliances, and Linksys switches. Other than the Internet, CRES has no interconnections or information sharing with other systems.

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 application is for USDA employees. The information includes complaints of discrimination against USDA programs and services and employee complaints. It uses complainant personal information such as names, addresses, phone numbers, and miscellaneous identification numbers (generates a case number).

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

Civil Rights Complaints involving programs and services administered by USDA, and employees are entered into the system by civil rights staff.

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

To track the Civil Rights complaint process, eliminate manual data gathering, improve the accuracy of data in reports and respond promptly and consistently on a Department-wide basis to changes in laws, regulatory guidance, and reporting requirements.

1.4 How is the information collected?

The information is received by mail, email, telephone or interviews. It is then inputted into the system by approved users.

1.5 How will the information be checked for accuracy?

The Equal Opportunity Assistants review and check the documents and verifies for accuracy.

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

Both the Office of Management and Budget (OMB) Circular A-130, Appendix II and the Federal Information Security Modernization Act of 2014 (FISMA) (Title III, Pub. L. No. 107-347) require that all users of a system be uniquely identified to be able to use a Federal information system. Remedy, a critical component of CRES, implements this requirement by using the individual's name as part of the unique identification process.

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

Only the individual's name, email address, and telephone number is used within CRES and not shared with other systems and applications. Risks associated with data collection in the CRES are minimal. Additional risks to the system data are mitigated through the use of regular system scans, testing, and reviews.

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.

Agencies use the data to track the number of complaints and trends. It supports the complaint process.

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

N/A. CRES does not use any type of tools to analyze data and there is no type of data that may be produced.

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

N/A. The system does not use 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.

N/A. Since the above describes uses, are N/A (there are no types of controls that may be in place to ensure that information is handled in accordance with the uses).

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?

CRES's files are destroyed, based on the judicial's regulations.

3.2 Has the retention period been approved by the component records officer and the National Archives and Records Administration (NARA)?

Yes. The OASCR Records Manager has met with the department Records Manager to discuss, the Presidential Memorandum, *Managing Government Records Directive*, which was signed by President Obama on November 28, 2011. This directive marks the beginning of an Executive Branch-wide effort to reform records management policies and practices and to develop a 21st century framework for the management of government records. The OASCR Records Manager and Department Records Manager have developed the goals and timelines for reporting and adhering to records management requirements issued by the National Archive Records and Administration, the Office of Management and Budget, and the Office of Personnel Management.

3.3 Privacy Impact Analysis: Please discuss the risks associated with the length of time data is retained and how those risks are mitigated.

A daily, weekly, and monthly review of the reports generated by the application allows for management review and the correction of data if necessary.

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?

There is no internal sharing of information.

4.2 How is the information transmitted or disclosed?

N/A

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.

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 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?

N/A

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. An acceptance letter is sent to the individual indicating the OASCR has received their letter and a complaint number has been assigned to the individual. The letter indicates the complaint issue, how OASCR has advised the agency of the complaint and that an investigation will examine the case.

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

N/A. When the individual contacts OASCR, they provide the information necessary for OASCR to investigate the case.

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

The data collected is used for the sole purpose of mitigating and tracking complaints within CRES. All complainants sign a Consent/Release form prior to all investigations.

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.

For the USDA Program Discrimination Complaint Form, it states that the form is provided in accordance with the Privacy Act of 1974, 5 U.S.C. 552, and concerns the information requested in the form to which this Notice is attached. The USDA's OASCR requests the information pursuant to 7 CFR Part 15.

For the individual submitting an EEO complaint, the individual refers to the link for the USDA Privacy Policy, located at the bottom of the site. The site states "if you choose to provide us with personal information, as in an e-mail to the Secretary or other USDA staff, or by filling out a form and submitting it to us through our website, we use that information to respond to your message. This also helps us to locate the information you have requested. We treat e-mails the same way that we handle paper-based correspondence sent to USDA. We are required to maintain many documents under the Federal Record Act for historical purposes, but we do not collect personal information for any purpose other than to respond to you. We only share the information you give us with another government agency if your inquiry relates to that agency or as otherwise required by law. Moreover, we do not create individual profiles with the information you provide, nor will the information you provide be shared with any private organizations. USDA does not collect information for commercial marketing."

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?

Individuals can gain access to their information by contacting the Customer Service unit at USDA headquarters. They can also make a FOIA request.

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

Reports are run to determine the accuracy of data. If erroneous information is found, the user community responsible for entering the data is charged with making the corrections.

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

Individuals are contacted in person or by email.

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

The individual has a right to appeal.

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

All information is entered into CRES, which is not shared with any other system or entity. All employees are mandated to take the Security Awareness Training, which covers PII.

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?

Support staff security requirements are based on public trust requirements. The Program Directorate management determines levels for users of CRES. Department head calls the administrators.

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?

Security awareness and rules of engagement training are mandatory for all users. Administrators are required to take specialized training.

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 activity within the system is tracked by audit logs and reviewed for tracking purposes.

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 on this system is not shared with any other system or entity. And, only name, address and phone number is collected, so the critically in minimal. Risks to the system data are mitigated through the use of regular system scans, testing, and reviews.

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?

It is a tracking and reporting system.

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

No

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, the ISSPM has reviewed the referenced data.

10.2 What is the specific purpose of the agency’s use of 3rd party websites and/or applications?

One of the applications is an off the shelf product, and after much research and testing this product was selected as the best suited to complete our task. The system is hosted by the contractor to facilitate easy of upgrades and version changes.

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

The information contained in this system is not available to anyone outside USDA approved personnel and contractors.

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, but access to the system is userid and password protected and the system is behind firewalls.

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?

Only designated/approved users have access to the system

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?

NO

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

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.

No PII becomes available through the agency's use of 3rd party websites or applications.

NOTE: POA&M 24325 created for SORN revision.



Responsible Official

Kenneth J. Baisden
Director, Data and Records Management Division
Office of the Assistant Secretary for Civil Rights
United States Department of Agriculture

Approval Signature

Kenneth J. Baisden
Director, Data and Records Management Division
Office of the Assistant Secretary for Civil Rights
United States Department of Agriculture

Date