

# Privacy Impact Assessment Photo Gallery

Technology, Planning, Architecture, & E-Government

- Version: 1.2
- Date: August 25, 2010
- Prepared for: USDA OCIO TPA&E





# Privacy Impact Assessment for the Photo Gallery

May 16, 2012

Contact Point  
George Schrader  
NRCS  
970-295-5421

Reviewing Official  
*Mr. Ray Coleman*  
*Director of IT Security*  
United States Department of Agriculture  
(202)205-7712

## 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.

*This assessment is for the PhotoGallery Web application for NRCS. PhotoGallery houses and hosts NRCS photos and is available to the public via the Web. This PIA is being conducted to determine the security level of the application.*

## 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 NRCS Photo Gallery is the NRCS National website used as the agency's source of natural resource and conservation related photos from across the USA. It is a public facing website that is used as a source for high quality imagery by all levels of the public sector business and general public communities, as well as internally by NRCS employees meeting their public information responsibilities. The public can find Photo Gallery via a Google search. If one were to Google "NRCS Photo Gallery," NRCS Photo Gallery would be the first "hit." The NRCS Photo Gallery provides the primary visual representation of the agency and its business, and therefore is linked to a wide assortment of other NRCS websites, including the National and most State websites. It is a very prominent website for NRCS.*

*Users may download a copy of an image. They may view metadata regarding an image.*

---

## 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?

*Photos and their metadata (e.g., name and geographical data). Contact feature in Section 7 may request: phone number, fax number or email address.*

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

*Photos taken by NRCS employees USDA photographers, and contract photographers.*

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

*For high quality imagery to be used by all levels of the public sector business and general public communities, as well as internally by NRCS employees meeting their public information responsibilities. Office of Communication (OC) has a waiver option before photo taken. Presently, both adults and minors are offered waivers.*

### 1.4 How is the information collected?

*Photographers send images via a disk to trained NRCS employees. The disks are not encrypted but are not handled outside of NRCS employees. Other ways exist that images are transferred. Contract photographers will take photos this summer and mail them directly to NRCS. Headquarters is dragnetting states to collect appropriate photos for Photo Gallery—these photos would be submitted via Share Point (which is secure and becoming more secure).*

### 1.5 How will the information be checked for accuracy?

*Trained NRCS employees ensure that photos meet NRCS guidelines.*

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

*None.*

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

*The design of this application ensures that only the minimum required amount/type of data is collected to meet the public relations requirement. The only PII elements involved is a photo/facial image and in some instances a name (not sensitive PII)—the photos are provided subject to a waiver and release.. The photo subject information is stored in a secure SQL Server database in the USDA enterprise data center in Kansas City. This public facing site is secure (i.e., uses secure https protocol). HTTPS is another design element which ensures this system merits a moderate classification.*

*Notice and or consent are to be provided to photo subjects who are both adults and minors.*

*Mitigation: Common mitigation is provided by the USDA-OCIO-eAuthentication application, which provides user Authentication for NRCS. When required by the application business, Role-based Access Control, granted through the NRCS Delegation of Authority and using eAuthentication to verify user authentication.*

## **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.**

*It is used by all levels of the public sector business and general public communities, as well as internally by NRCS employees meeting their public information responsibilities. It is a public facing site, so it is available to everyone.*

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

*NRCS employees manually analyze the photos. They may use post-processing tools, such as Adobe Photoshop, to ensure they meet NRCS guidelines. For example, they may change the size of the image.*

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

*It is used by all levels of the public sector business and general public communities, as well as internally by NRCS employees meeting their public information responsibilities. It is a public facing site, so it is available to everyone.*

**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.**

*As the photos are available to the public, no controls are in place. Notice and or consent will be provided in the form of a waiver and release to photo subjects who are both adults and minors. If a photo is taken of an adult, notice should be provided to the adult that "your photo has been taken and it may appear in/on USDA Photo Gallery site <http://photogallery.nrcs.usda.gov/>."*

*This application is in compliance with the Federal Information Security Management Act of 2002 (FISMA), USDA Office of the Chief Information Officer (OCIO) Directives, and U.S. National Institute of Standards and Technology (NIST) Special Publication 800-53, Revision 3 guidance. Security Certification and Accreditation (C&A) is underway for this application.*

- *Access Control (AC)*
- *Security Awareness and Training Policy and Procedures (AT)*
- *Identification and Authentication (IA)*
- *Media Protection (MP)*
- *Physical Access (PE)*
- *Personnel Security (PS)*

## **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?**

*Indefinitely at the interim until archival determination made. Photo collection is periodically culled, and images found to be dated are sent to the National Archives. Determination is based on perceived value of the image at the time of the culling.*

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

*The photo collection contains two primary PII elements: facial recognition and name. The photo collection is not subject to this type of regulation, but we do work with the National Archives to consign dated elements of the collection to their keeping.*

**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 sensitivity and scope of the information collected is MODERATE since some minors are in photos and per NIST 800-60, Volume 1, Revision 1, pages 29-30.*

*This is MODERATE because the minimal risks that exist related to this PII are mitigated by the design of this application, and the fact that only two related items of PII are collected. However, the two items are perhaps the most sensitive PII elements needed to identify someone, their facial image combined with their name (including that of minors).*

*Some records management NARA guidelines are followed when photos sent to archives. Risks may also include those related to technical disaster recovery. Human error such as leaked data exists. Hackers may intentionally attempt to break through system security.*

*The ability to track the individual is limited since the individual's information is stored in a secure SQL Server database in the USDA NITC enterprise data center in Kansas City.*

## **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?**

*As the application is available to the public, photos and their metadata are available to any internal and external organization to be used by all levels of the public sector business and general public communities, as well as internally by NRCS employees meeting their public information responsibilities.*

**4.2 How is the information transmitted or disclosed?**

*Via a Web application. A COTS software product, Extensis Portfolio Server, is used to host the photos.*

**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.**

*Facial images with accompanying name of subject's facial image is PII. The sharing of this information is necessary as part of the public relations function. Risks also include the internal threat—are all people handling the address labels (electronic or physical hard copies) background checked? Human error and natural disasters are also risks.*

## **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?**

*As the application is available to the public, photos and their metadata are available to an internal and external organization to be used by all levels of the public sector business and general public communities, as well as internally by NRCS employees meeting their public information responsibilities.*

**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 name of the photographer is included in the metadata. Photos may include members of the public such as farmers, ranchers, Earth Day volunteers, etc.*

*The Photo Gallery public relations function could be argued to be “necessary for implementation of conservation programs” to ensure effectiveness. And, this NRCS public relations/communications analysis could be argued “as necessary to provide NRCS technical services to landowners... for which contractors or technical services provider is hired” to ensure NRCS mission is being carried out satisfactorily. This falls within NRCS-1 SORN routine uses (1) and (7). As a matter of federal government services/public policy, this is a reasonable request (as long as the necessary federal laws and regulation compliance exists). Notice and consent are also provided by a waiver and release to both adults and minors.*

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

*As Photo Gallery is a public facing Web application, there are no security measures in place other than those employed by ITS. This is a public facing site in the public domain. Protection from hacking exists; other ITS National Information Technical Center (NITC) (hosted in Kansas City) security measures are in place.*

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

*Yes, facial images with accompanying name of subject's facial image is PII. The moderate risks that exist related to sharing of this PII externally are mitigated because typically only photographic images are available and if another element of PII is available in addition to the photographic image, it may only be a name. Human error and natural disasters are also risks. These elements are mentioned in the NRCS-1 SORN.*

*The electronic data retrieval system is secured by the USDA Common Computing Environment user authentication process and USDA eAuthentication login and password protection. Offices are locked during non-business hours. Some applications may also have user roles using the NRCS Photo Gallery systems.*

## **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?**

*Notice must be provided to individuals whose names accompanied by facial images appear in the public domain. Notice and or consent provided only to photo subjects who are both adults and minor.*

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

*Yes. Notice and or consent provided to photo subjects who are both adults and minors. Both a waiver and release and the NRCS-1 provide notice. The SORN talks about key points such as the right to decline and that incorrect information may be pulled.*

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

*Not non-minors. Notice and or consent provided only to photo subjects who are both adults and minors.*

**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 via the NRCS SORN mentioned herein. However, notice is provided to both adults and minors at this time. While more mitigation could take place, predominantly non-PII data is collected. An NDA may be provided any time someone may appear in a Photo Gallery site photo.*

## **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 may use the Photo Gallery "contact feature" to request that system administrators access their information. The PhotoGallery application includes a comments page that allows the user to send information to the business owner to correct any misinformation displayed on the Website concerning the individual. In order for the system administrator to respond to the requester, the requester may provide: phone number, fax number or email address.*

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

*Individuals may use the Photo Gallery "contact feature" to request that system administrators correct inaccurate or erroneous information.*

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

*Individuals may use the Photo Gallery "contact feature" to request that system administrators correct their information.*

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

*In the field, photo subjects would be asked to double check their information to confirm the accuracy of their information.*

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

*eAuthentication is not on the public site. Four users nationwide can upload photos into a Photo Gallery proprietary catalog. These four users use the authorization scheme within COTS software used for Photo Gallery site. Human error is possible. However, with both the system "contact feature" and the "in the field request for confirmation of accuracy," most all is being done to mitigate privacy risks.*

*Additional possible risks are: human error, the internal human threat, and disaster recovery related error may occur.*

*N/A*

## **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?**

*Photo Gallery is a public facing site. Five NRCS employees access a separate Web application via an SSL connection and an authentication/authorization scheme proprietary to Extensis Portfolio Server to upload photos and metadata.*

**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?**

*Privacy issues may be involved. PII is collected in the form of facial recognition and names. Privacy (PII) training is available via AgLearn. For public, system has Privacy Policy Statement.*

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

*In progress. N/A*

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

*Photos served by Photo Gallery are public domain. The PhotoGallery application has been scanned via a security scanning application to ensure that no security holes are present in the application. ITS also monitors the site to ensure the availability and integrity of the server.*

**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 sensitivity and scope of the information collected is MODERATE since some minors are in photos and per NIST 800-60, Volume 1, Revision 1, pages 29-30.*

*This is MODERATE because the minimal risks that exist related to this PII are mitigated by the design of this application, and the fact that only two related items of PII are collected. However, the two items are perhaps the most sensitive PII elements needed to identify someone, their facial image combined with their name (including that of minors).*

*Mitigation occurs through separation of duties policies which ensures both system operators and system administrators have limited, if any, access to PII. Identification numbers keep customer PII ephemeral. Photo Gallery does not collect/retain sensitive PII (e.g., social security numbers). Also, NIST 800-53 A.U. audit controls are used to prevent data misuses.*

## **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?**

*A public facing Web application. This application contains photos of USDA activities.*

**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.*

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

*N/A... because no third party Web sites/applications are employed.*

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

*None, because no third party Web sites/applications are employed.*

**10.4 How will the PII that becomes available through the agency’s use of 3<sup>rd</sup> party websites and/or applications be used?**

*N/A... because no third party Web sites/applications are employed.*

**10.5 How will the PII that becomes available through the agency’s use of 3<sup>rd</sup> party websites and/or applications be maintained and secured?**

*N/A... because no third party Web sites/applications are employed.*

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

*N/A... because no third party Web sites/applications are employed.*

*If so, is it done automatically?*

*N/A*

*If so, is it done on a recurring basis?*

*N/A*

**10.7 Who will have access to PII that becomes available through the agency's use of 3<sup>rd</sup> party websites and/or applications?**

*N/A... because no third party Web sites/applications are employed.*

**10.8 With whom will the PII that becomes available through the agency's use of 3<sup>rd</sup> party websites and/or applications be shared - either internally or externally?**

*N/A... because no third party Web sites/applications are employed.*

**10.9 Will the activities involving the PII that becomes available through the agency's use of 3<sup>rd</sup> party websites and/or applications require either the creation or modification of a system of records notice (SORN)?**

*N/A, because no third party Web sites/applications are employed.*

**10.10 Does the system use web measurement and customization technology?**

*No*

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

*N/A*

**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... because no third party Web sites/applications are employed.*

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

*N/A*

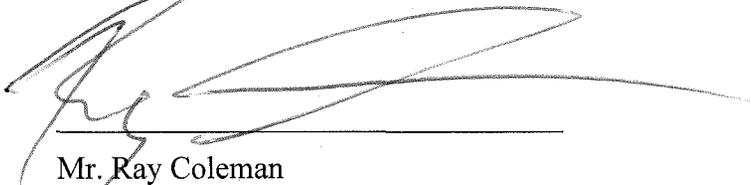
**10.12 Privacy Impact Analysis: Given the amount and type of PII that becomes available through the agency's use of 3<sup>rd</sup> party websites and/or applications, discuss the privacy risks identified and how they were mitigated.**

*Privacy risks are nominal. HTTPS secure transfer. Application exists behind firewall; however, data is always subject to human error. There is the unlikely event that data which falls within the PII definition may be erroneously engaged. The security/privacy training administrator/operator would dispose of such rarely encountered PII immediately. Disaster recovery related error may occur*

## **Responsible Officials**

*Robert Gresh, Web and Design Team Lead (acting), Public Affairs Division, NRCS  
United States Department of Agriculture*

## **Approval Signature**



Mr. Ray Coleman  
Director of IT Security  
United States Department of Agriculture  
Natural Resources Conservation Service