Privacy Impact Assessment
DamWatch

Policy, E-Government and Fair Information Practices

- Version: 1.8
- Date: August 27, 2020
- Prepared for: USDA OCIO-Policy, E-Government and Fair Information Practices (PE&F)

Privacy Impact Assessment for the

DamWatch (DamWatch)

August 5, 2020

Contact Point

Charles Sorenson
Dam Watch Project Manager
Farm Production and Conservation Business Center
816-926-6944

Reviewing Official

James Flickinger
Chief Information Security Officer, FPAC
United States Department of Agriculture
(816) 926-6010

Table of Contents

Abstract

The Natural Resources Conservation Service (NRCS) is required by United States Department of Agriculture (USDA) Department Regulation DR-1043-18 to make every reasonable and prudent effort to enhance the safety of dams under the agency's jurisdiction. DamWatch is a commercially developed product that enables NRCS to monitor more than 11,300 watershed dams more efficiently and effectively.

This PIA is being conducted to comply with Federal Information Security Management Act (FISMA) of 2002 and the E-Government Act of 2002 (Public Law. 107-347, 116 Stat. 2899, 44 U.S.C. § 101, H.R. 2458/S. 803) Federal Law.

Overview

DamWatch provides web-based storage and retrieval of electronic files of dam information including as-built drawings, inspection reports, breach inundation maps, and photos. The system links to outside sources to access weather radar, rainfall data, weather alerts, and seismic activity alerts. These links provide data and information to DamWatch; however, no data or information are sent from DamWatch to any of these outside sources. The system will also include emergency contact information for each dam. DamWatch is not publicly accessible.

Legal Authority: This system is regulated by privacy laws, regulations and government requirements, including the Privacy Act (5 U.S.C. §552a); the E-Government Act of 2002 (Pub. Law. 107-347, 44 U.S.C. §101); the Paperwork Reduction Act of 1995 (44 U.S.C. §3501); the Federal Information Security Modernization Act of 2014 (FISMA) (44 U.S.C. §3551 to §3559); Office of Management and Budget (OMB) Memos M-03-22, M-10-23, M-16-24, and M-17-12; and OMB Circular A-130, Appendix I.

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?

DamWatch contains Emergency Action Plans (EAPs) that will be activated in the event of an emergency involving an NRCS-managed dam. EAPs contain the name, home address, and telephone number of emergency responders, as well as the names and addresses of property owners that could be impacted by an emergency involving a dam.

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

The PII can be obtained from publicly accessible information resources, from organizations involved in emergency response, or submitted voluntarily by individual responders or property owners.

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

The information is collected, maintained, and used for the successful execution of EAPs.

1.4 How is the information collected?

EAPs are created by NRCS or dam project sponsors, who coordinate with state and local officials to gather the appropriate PII required to satisfy EAP execution requirements.

1.5 How will the information be checked for accuracy?

PII contained in each EAP is verified by the author of the EAP, by cross-checking the information with other resources, and/or by obtaining verification of accuracy from individuals. EAPs are routinely checked for accuracy and updated as needed.

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

The following regulations are applicable:

- *Privacy Act (5 U.S.C. §552a)*
- *E-Government Act of 2002 (Pub. Law. 107-347, 44 U.S.C. §101)*
- *Paperwork Reduction Act of 1995 (44 U.S.C. §3501)*

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

Minimal privacy risks have been identified. Names, physical addresses, and telephone numbers are readily available via open source, therefore, should a compromise of the system occur, the potential impact to individual privacy would be minimal.

Please see Sections 2 and 8 for a further discussion of security controls that are in place to mitigate privacy risks.

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.

PII collected is only used during the execution of an EAP following the authorized activation of the EAP.

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

No automated tools are used to analyze PII data in the EAPs. EAPs are manually created and maintained.

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

All DamWatch EAP PII is publicly available, with the possible exception of telephone numbers that may not be publicly listed. This data is provided by the individual, or the individual's organization. PII collected is only used during the execution of an EAP following the authorized activation of the EAP.

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.

This application is in compliance with the FISMA and the security and privacy controls provided in the U.S. National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, Revision 4.

If any residual risks are identified, they will be managed and reported via the FISMA mandated risk assessment processes.

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?

All information will be retained in compliance with NARA Guidelines, which vary on average in years from less than one year to more than ten years according to the NARA General Records Schedules Transmittal 29, issued December 2017.

Per the NRCS-1 System of Record Notice (SORN), "Records are maintained as long as the owner, operator, producer, or participant qualifies for conservation programs."

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

Yes. Per NARA Code of Federal Regulations - 36 CFR 1220, Subchapter B – Records Management and USDA OCIO Department Regulation 3080-001 accessible at: http://www.ocio.usda.gov/document/departmental-regulation-3080-001

NARA Approval: NARA approval is required for all official records schedules. SF-115 shall be submitted to NARA for approval. External approval has already been granted for records covered by the General Records Schedules (GRS). No external approval is required for the disposition of non-record materials. An informational copy of the SF-115, in both hard copy and electronic format, shall be provided to the Departmental Records Officer at the same time that the original is sent to NARA.

Electronic Records: Electronic records should be scheduled in the context of entire information systems, along with appropriate documentation and related indexes, and provide the necessary elements:

- *All input records or source documents.*
- *All information recorded on electronic media.*
- *All output records.*
- *The documentation associated with the system.*
- *Any related indexes.*

As with audiovisual and microform records, permanent electronic records should not be proposed for long-term storage at Federal records centers but should be transferred directly to the National Archives.

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 primary privacy risk is that a data breach could result in the release of information on members of the public. This is mitigated by limited access to the data, non-portability of the data and controlled storage of the data located in controlled facilities.

Retention of application-specific data is required to meet business and organizational requirements for this particular information system. The risks associated with retaining application-specific information are mitigated by the controls discussed above.

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?

N/A. Information is not shared with other internal USDA organizations. DamWatch does not share PII data with any other system. NRCS personnel may access EAPs containing PII, as needed; however, the USDA and NRCS does not share this PII outside the scope of DamWatch operations.

4.2 How is the information transmitted or disclosed?

N/A. Information is not shared with other internal USDA organizations. PII contained within EAPs will be disclosed via hardcopy or electronic copy during EAP review cycles or when an EAP is activated.

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.

Privacy risks are mitigated by not sharing information with other internal USDA organizations. Any residual risks are mitigated by the controls discussed in Section 2.4.

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?

The EAPs within DamWatch are created and maintained by NRCS and other state and local dam project sponsors. The PII contained within the EAPs is shared with state and local emergency responders in the event of activation of an EAP.

5.2 Is the sharing of Personally Identifiable Information (PII) outside the Department compatible with the original collection? If so, is it covered by an appropriate routine use in a System of Records Notice (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.

Yes. The sharing of PII within DamWatch EAPs is compatible with the original collection authority. This application is subject to the NRCS-1 SORN accessible at: https://www.ocio.usda.gov/sites/default/files/docs/2012/NRCS-1.txt

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

PII contained within EAPs will be disclosed via hardcopy or electronic copy during EAP review cycles or when an EAP is activated. DamWatch does not have the capability to directly share PII with other systems. EAPs are considered controlled documents and will be shared via secure communications methods at all times.

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

There are minimal risks identified with external sharing since sharing is at the discretion of emergency responders, the NRCS, and dam project sponsors. DamWatch is secured by the USDA Common Computing Environment (CCE) user authentication process and eAuthentication (eAuth) login and password protection. Offices are locked during non-business hours. Any residual risks are mitigated by the controls discussed in Section 2.4.

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?

Yes. This application is subject to the NRCS-1 SORN accessible at: https://www.ocio.usda.gov/sites/default/files/docs/2012/NRCS-1.txt

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

Yes. Notification of the collection of PII occurs when an emergency responder is assigned to a particular dam and the EAP is created for that dam. Property owners that may be at risk during a dam emergency are notified by state and local emergency responders as needed.

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

Yes. Disclosure of responder's PII is voluntary when they are assigned under an EAP. Property owners at risk are not notified, as the PII contained within EAPs is sourced from publicly available records.

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

N/A. No PII is directly collected from any individual landowner (i.e., members of the public). Members of the public do not have access to DamWatch.

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.

The use notice is provided to emergency responders when they provide their PII for inclusion in an EAP. Property owners at risk are not notified, as the PII contained within EAPs is sourced from publicly available records.

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?

Emergency responders identified within a given EAP can contact their Emergency Response Coordinator at the state or local level if access to PII is required. Property owners at risk can also contact their state, county, or local emergency response offices; however, such contact is not anticipated as the property owner PII contained within EAPs is sourced from publicly available records.

As published in SORN USDA/NRCS-1: "Any individual may request information regarding this system of records, or information as to whether the system contains records pertaining to him/her by contacting the respective district conservationist or other designee. If the specific location of the record is not known, the individual should address his/her request to the Director, Management Services Division, USDA-Natural Resources Conservation Service, P. O. Box 2890, Washington, DC 20013, who will refer it to the appropriate field office. A request for information pertaining to an individual should contain: Name, address, and other relevant information (e.g., name or nature of program, name of cooperating body, etc.)."

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

Emergency responders identified within a given EAP can contact their Emergency Response Coordinator at the state or local level if access to PII is required. Property owners at risk can also contact their state, county, or local emergency response offices; however, such contact is not anticipated as the property owner PII contained within EAPs is sourced from publicly available records.

As published in SORN USDA/NRCS-1: "Any individual may request information regarding this system of records, or information as to whether the system contains records pertaining to him/her by contacting the respective district conservationist or other designee. If the specific location of the record is not known, the individual should address his/her request to the Director, Management Services Division, USDA-Natural Resources Conservation Service, P. O. Box 2890, Washington, DC 20013, who will refer it to the appropriate field office. A request for information pertaining to an individual should contain: Name, address, and other relevant information (e.g., name or nature of program, name of cooperating body, etc.)."

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

N/A. No notification is provided related to procedures to allow individual landowners to correct their PII, because no PII is collected from any landowner. Individual landowners do not have access to DamWatch.

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

N/A. Refer to Section 7.3.

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

No privacy risks have been identified associated with the redress of incorrect information within DamWatch.

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?

Access to DamWatch is determined via a Level 2 eAuth ID and password on a valid need-to-know basis, determined by requirements to perform applicable official duties.

Access is also limited to NRCS employees and contractors support of the DamWatch project as well as state and local emergency responders assigned to a particular dam site.

DamWatch has documented Access Control (AC) Procedures, in compliance with FISMA and USDA directives. Please refer to Section 2.4 for further information.

8.2 Will Department contractors have access to the system?

Yes. Department contractors with a need-to-know will have access to DamWatch as part of their regular assigned duties. Contractors are required to undergo mandatory background investigations commensurate with the sensitivity of their responsibilities, in compliance with Federal requirements. Access is also limited to state and local emergency responders assigned to a particular dam site.

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

Annual organizational Privacy Awareness Training is mandatory for all NRCS personnel. NRCS requires that every employee and contractor receive information security awareness training before being granted network and account access, per General Manual, Title 270, Part 409 - Logical Access Control and Account Management. Annual Security Awareness and Specialized Training is also required, per FISMA and USDA policy, and is tracked by USDA.

8.4 Has Certification & Accreditation (C&A) been completed for the system or systems supporting the program?

Yes. DamWatch has an ATO that expires on 01/04/2021.

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

NRCS complies with the FISMA of 2014. Assessment and Accreditation (A&A), as well as annual key control self-assessments and continuous monitoring procedures are implemented for PDS per the requirements given in NIST SP 800-53 Revision 4. The system also provides technical safeguards to prevent misuse of data including the following:

- *Confidentiality: Encryption is implemented to secure data at rest and in transit for PDS [e.g., by Federal Information Processing Standards (FIPS) 140-2 compliant HTTPS and end-user hard disk encryption]. The documents that are passed to, and maintained in, DamWatch are encrypted in transit.*
- *Integrity: Masking of applicable information is performed for PDS (e.g., passwords are masked by eAuth).*
- *Access Control: PDS implements least privileges and need-to-know to control access to PII [e.g., by Role-Based Access Control (RBAC)].*
- *Authentication: Access to the system and session timeout is implemented for PDS (e.g. by eAuth and via multi-factor authentication for remote access).*
- *Audit: Logging is implemented for PDS [there is a logging infrastructure including Application Audit Log Solution (AALS)]. PDS logs events from various devices within its accreditation boundary to include web servers and database servers. NRCS logs data transactions from devices adjacent to the PDS accreditation boundary to include the legacy databases and the CA Application Programming Interface (API) Gateway. Logged events will be stored in the NRCS Security Information and Event Management (SIEM) server.*
- *Attack Mitigation: The system implements security mechanisms such as input validation.*

Note: For the privacy notice control, please see Section 6 which addresses notice. For the privacy redress control, please see Section 7 which addresses redress.

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?

DamWatch does not directly collect any PII from any individual landowner (i.e., member of the public); however, it does utilize PII within the system which is obtained from other sources (refer to Section 1.0). Data extracts containing PII are not regularly obtained from the system, therefore, privacy risk from this area is limited and addressed through IT Data Extract processes controls.

No PII is shared by DamWatch with any other system. PII contained within DamWatch EAPs has been determined to be of minimal sensitivity. Minimal risks have been identified for the PII data types within DamWatch. Mitigation occurs through Separation of Duties (SOD) and access control policies which ensure that system operators, system administrators, emergency responders, and associated personnel have limited, if any, access to PII.

Any privacy risks identified in this system are mitigated by the security and privacy safeguards provided in Section 8.5 and by the security controls discussed in Section 2.4. Remediation of privacy risks associated with internal/external sharing are addressed in Sections 4 and 5 respectively. Remediation of privacy risks associated with notice and redress are addressed in Sections 6 and 7 respectively.

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?

DamWatch is a commercially developed application hosted on devices using Commercial-Off-The-Shelf (COTS) hardware and software configured in accordance with USDA baseline configurations for servers and web portals.

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

No. DamWatch utilizes Agency-approved technologies and these technology choices do not raise privacy concerns.

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 "M-10-22 Guidance for Online Use of Web Measurement and Customization Technologies" 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. DamWatch does not use third-party websites and/or applications.

10.3 What Personally Identifiable Information (PII) will become available through the agency's use of 3rd party websites and/or applications?

N/A. DamWatch does not use third-party websites and/or applications.

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. DamWatch does not use third-party websites and/or applications.

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. DamWatch does not use third-party websites and/or applications.

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

N/A. DamWatch does not use third-party websites and/or applications.

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. DamWatch does not use third-party websites and/or applications.

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. DamWatch does not use third-party websites and/or applications.

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 SORN?

N/A. DamWatch does not use third-party websites and/or applications.

10.10 Does the system use web measurement and customization technology?

N/A. DamWatch does not use web measurement and customization technology.

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. DamWatch does not use web measurement and customization technology.

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.

Privacy risks of DamWatch data becoming available via 3rd party websites are nominal. In addition, DamWatch does not use web measurement or customization technology.

There is the unlikely event that data which falls within the PII definition may be erroneously released. At that point, the security/privacy training administrator/operator would dispose of this rarely encountered PII immediately.

Disaster recovery related error may also occur. PII is collected only for inclusion in EAPs. Only NRCS personnel/administrators (with background checks and training), state and local emergency responders, and associated support staff, will have access to the PII contained in the EAPs.

Agency Responsible Official

JAKE ZEBELL

Digitally signed by JAKE ZEBELL
Date: 2020.10.13 12:08:56 -06'00'

Jake Zebell
DamWatch Information System Owner
United States Department of Agriculture

Agency Approval Signature

LANITA THOMAS

Digitally signed by LANITA THOMAS
Date: 2020.10.23 14:18:14 -04'00'

Lanita Thomas
Information Systems Security Program Manager
United States Department of Agriculture

Agency Privacy Approval Signature

Digitally signed by AMBER ROSS
Date: 2020.10.19 12:12:27 -05'00'

Amber Ross
FPAC Privacy Officer
United States Department of Agriculture