



U.S. Department of the Interior PRIVACY IMPACT ASSESSMENT

Introduction

The Department of the Interior requires PIAs to be conducted and maintained on all IT systems whether already in existence, in development or undergoing modification in order to adequately evaluate privacy risks, ensure the protection of privacy information, and consider privacy implications throughout the information system development life cycle. This PIA form may not be modified and must be completed electronically; hand-written submissions will not be accepted. See the DOI PIA Guide for additional guidance on conducting a PIA or meeting the requirements of the E-Government Act of 2002. See Section 6.0 of the DOI PIA Guide for specific guidance on answering the questions in this form.

NOTE: See Section 7.0 of the DOI PIA Guide for guidance on using the DOI Adapted PIA template to assess third-party websites or applications.

Name of Project				Date	
Send Word Now (SWN)				07-28-2016	
Bureau/Office			Bureau/Office Contact Title		
Office of the Secretary/Office of Emergency Management			IT Project Manager		
Point of Contact Email	First Name	M.I.	Last Name	Phone	
Sandra_C_Rainbolt@ios.doi.gov	Sandra		Rainbolt	(202) 208-5716	
Address Line 1					
1849 C Street NW					
Address Line 2					
MS-3409					
City			State/Territory		Zip
Washington			District of Columbia		20240

Section 1. General System Information

A. Is a full PIA required?

Yes

Yes, information is collected from or maintained on

Federal personnel and/or Federal contractors

B. What is the purpose of the system?

Send Word Now (SWN) Emergency Notification Service is an emergency notification and employee accountability cloud-based application that provides organizations with the ability to quickly send critical information to recipients. SWN collects, modifies, updates, and safeguards contact information for emergency situations, including natural, environmental, or austere weather conditions affecting the Department of the Interior (DOI) mission or function, emergency contacts, and agency continuity of operations. In emergency situations where active involvement of the vendor is necessary due to the loss of DOI primary and normal means of communication, SWN may be used to facilitate

and transfer communications between agency leaders in support of continuity of operations and provide alerts and other response needs as determined by DOI.

SWN is centrally managed by the DOI Office of Emergency Management (OEM) and may be used by DOI bureaus and offices, including National Park Service, Bureau of Land Management, U.S. Fish and Wildlife Service, Bureau of Indian Affairs, Bureau of Reclamation, Bureau of Ocean Energy Management, Bureau of Safety and Environmental Enforcement, Office of Natural Resources Revenue, U.S. Geological Survey, Bureau of Indian Education, Office of Surface Mining, and the Office of the Secretary. SWN may be used in abnormal operations as defined by the Office of Personnel Management and is further restricted to use during contingency communication conditions as determined by Bureau/Office Emergency Management (EM) Coordinators. Examples of SWN uses may include notifications of response level or alert declaration, continuity events or activities, building or facility closure or access issues, weather events (severe storms, flooding, etc), security alerts/threats/incidents, exercise messaging, and communications drills.

SWN is a Software as a Service (SaaS) cloud service provider located in the United States. This assessment is being conducted while SWN is undergoing the FedRAMP certification process, and this PIA will be updated as necessary upon completion of the certification process and issuance of an authorization to operate to reflect additional risks identified or updated information regarding mitigating controls.

C. What is the legal authority?

5 U.S.C. 301; 44 U.S.C. 3101; 6 U.S.C. 101 et seq., Homeland Security Act of 2002; 50 U.S.C. App. 2062, The Defense Production Act of 1950, as amended; 31 U.S.C. §§ 1535-1536, Economy Act; 50 U.S.C. §§ 1601-1651; 42 U.S.C. 247d and 300hh, The Public Health Security and Bio-terrorism Preparedness and Response Act of 2002; Pub. L. 106-390, Robert T. Stafford Disaster Relief and Emergency Assistance Act; Executive Order 12656, Assignment of National Security and Emergency Preparedness Responsibilities; Presidential Decision Directive 67, Enduring Constitutional Government and Continuity of Operations; Federal Continuity Directive - 1, Federal Executive Branch National Continuity Program and Requirements; Federal Property Management Regulation (FPMR) 101-20.103-4, Occupant Emergency Program; Homeland Security Presidential Directive 20, National Continuity Policy; 900 Departmental Manual Chapters 1-5, Emergency Management Program; and Department of the Interior Continuity of Operations Plan.

D. Why is this PIA being completed or modified?

New Information System

E. Is this information system registered in CSAM?

No

F. List all minor applications or subsystems that are hosted on this system and covered under this privacy impact assessment.

Subsystem Name	Purpose	Contains PII	Describe
None	None	No	

G. Does this information system or electronic collection require a published Privacy Act System of Records Notice (SORN)?

Yes

List Privacy Act SORN Identifier(s)

DOI-58, Employee Administrative Records, April 20, 1999 (64 FR 19384) and DOI-85, Payroll, Attendance, Retirement, and Leave Records, April 8, 2008 (73 FR 19090). Some information in this system may be covered under OPM/GOVT-1, General Personnel Records, June 19, 2006 (71 FR 35341).

H. Does this information system or electronic collection require an OMB Control Number?

No

Section 2. Summary of System Data

A. What PII will be collected? Indicate all that apply.

- | | | |
|--|--|--|
| <input checked="" type="checkbox"/> Name | <input type="checkbox"/> Religious Preference | <input type="checkbox"/> Social Security Number (SSN) |
| <input type="checkbox"/> Citizenship | <input type="checkbox"/> Security Clearance | <input checked="" type="checkbox"/> Personal Cell Telephone Number |
| <input type="checkbox"/> Gender | <input checked="" type="checkbox"/> Spouse Information | <input type="checkbox"/> Tribal or Other ID Number |
| <input type="checkbox"/> Birth Date | <input type="checkbox"/> Financial Information | <input checked="" type="checkbox"/> Personal Email Address |
| <input type="checkbox"/> Group Affiliation | <input type="checkbox"/> Medical Information | <input type="checkbox"/> Mother's Maiden Name |
| <input type="checkbox"/> Marital Status | <input type="checkbox"/> Disability Information | <input checked="" type="checkbox"/> Home Telephone Number |
| <input type="checkbox"/> Biometrics | <input type="checkbox"/> Credit Card Number | <input type="checkbox"/> Child or Dependent Information |
| <input type="checkbox"/> Other Names Used | <input type="checkbox"/> Law Enforcement | <input type="checkbox"/> Employment Information |
| <input type="checkbox"/> Truncated SSN | <input type="checkbox"/> Education Information | <input type="checkbox"/> Military Status/Service |
| <input type="checkbox"/> Legal Status | <input type="checkbox"/> Emergency Contact | <input type="checkbox"/> Mailing/Home Address |
| <input type="checkbox"/> Place of Birth | <input type="checkbox"/> Driver's License | |
| <input checked="" type="checkbox"/> Other | <input type="checkbox"/> Race/Ethnicity | |

Specify the PII collected.

SWN may also contain employee job title, work email address, office phone number, work cell phone number, organization code, group name and membership for roles in emergency management groups, username, and internet protocol (IP) address. Information may also include spouse contact information such as phone numbers, email address, and alternate address.

B. What is the source for the PII collected? Indicate all that apply.

- | | | | |
|--|--|---|---|
| <input checked="" type="checkbox"/> Individual | <input type="checkbox"/> Tribal agency | <input checked="" type="checkbox"/> DOI records | <input type="checkbox"/> State agency |
| <input type="checkbox"/> Federal agency | <input type="checkbox"/> Local agency | <input type="checkbox"/> Third party source | <input checked="" type="checkbox"/> Other |

Describe

Information may be extracted from DOI employee records with Emergency Response Official (ERO) designations within the Federal Personnel Payroll System (FPPS). Bureau/Office Continuity of Operation (COOP) officials vet the extracted data and identify any records that should not be uploaded to SWN. Data may also be manually added to the application or updated by authorized managers or by the employee through an email request via the internal DOI Contact Management System (CMS) a program interface that leverages official email addresses in Active Directory (AD). Email requests generated by CMS are sent to the EROs to review their contact record and make the necessary updates. This request may be initiated by DOI OEM staff with access to CMS. After a contact record is added, deleted, or updated it is pushed to SWN via an application program interface (API). If a contact record is added or deleted from a group in CMS, it is also pushed to SWN, as well as the associated AD group. These AD updates are processed every four hours or other bureau/office schedule.

C. How will the information be collected? Indicate all that apply.

- | | | | |
|---|--|--------------------------------|--|
| <input type="checkbox"/> Paper Format | <input checked="" type="checkbox"/> Face-to-Face Contact | <input type="checkbox"/> Fax | <input checked="" type="checkbox"/> Telephone Interview |
| <input checked="" type="checkbox"/> Email | <input checked="" type="checkbox"/> Web Site | <input type="checkbox"/> Other | <input checked="" type="checkbox"/> Information Shared Between Systems |

Describe

Information in the contact records may be collected from FPPS and updated by authorized managers or by the employee through a CMS email request.

D. What is the intended use of the PII collected?

The PII collected in the contact records is necessary for the DOI COOP, EM, Employee Accountability, and Occupant Emergency Programs to have multiple methods of contacting EROs and Crisis Management Teams during an emergency to ensure emergency contacts and operations sustain a continuity of operations. This information will be used for emergency alerts and notifications to DOI employees who are on or off duty regarding incidents, emergencies, office closures, tests, and/or exercises.

E. With whom will the PII be shared, both within DOI and outside DOI? Indicate all that apply.

Within the Bureau/Office

Describe the bureau or office and how the data will be used.

Contact information is provided to the OS COOP Team members or EM Coordinators to verify members on the contact lists.

Other Bureaus/Offices

Describe the bureau or office and how the data will be used.

Contact information is provided to the Bureau/Office COOP Team members or EM Coordinators to verify members on the contact lists. Employee lists may be shared with authorized personnel for the purposes of employee accountability, recall, and other contingency operations.

Other Federal Agencies

Tribal, State or Local Agencies

Contractor

Describe the contractor and how the data will be used.

SWN contract support staff have access to the records in order to determine causes related to issues with communications. The staff analyzes the message history and logs to determine where a failure may have occurred, such as an incorrect phone number or email address. DOI/OCIO contractors also have access to records in order to provide the support for the CMS to resolve issues between AD, the CMS, and SWN. For example, the contractor will manually remove the records for an employee that left the agency.

Other Third Party Sources

F. Do individuals have the opportunity to decline to provide information or to consent to the specific uses of their PII?

Yes

Describe the method by which individuals can decline to provide information or how individuals consent to specific uses.

Individuals may verbally or in writing decline to provide the contact information. During a routine self-update, individuals have the option to provide all, some, or none of the non-work contact information. As a member of the DOI emergency management community, each contact must ensure their information is current to perform their role as an ERO. A Privacy Act Statement will be placed in the self-update email message. The message is sent to contacts through CMS from SWN.

G. What information is provided to an individual when asked to provide PII data? Indicate all that apply.

Privacy Act Statement

Privacy Notice

Other

None

Describe each applicable format.

A Privacy Act Statement will be included in the self update email request. In some cases, a privacy notice may be added to phone trees or emergency contact lists used in parallel with SWN and as an alternate if SWN is unavailable. Individuals are also provided notice through the publication of this privacy impact assessment and related assessments, and applicable DOI system of records notices, DOI-58 and DOI-85.

H. How will data be retrieved? List the identifiers that will be used to retrieve information (e.g., name, case number, etc.).

Data is retrieved manually by an administrator or other privileged user or message sender. Contact record information is retrieved by last name and group name or membership. Group membership is identified in group membership reports generated manually or programmed.

I. Will reports be produced on individuals?

Yes

What will be the use of these reports? Who will have access to them?

OEM Watch Officers, Warning Specialists, and authorized COOP/EM staff can produce reports which are uploaded to the EM Roster Subsite in DOI Safetalk. DOI Safetalk is a repository for DOI COOP Plans and EM documents located in the DOI SharePoint Portal. These reports are separated by EM groups and accessible by authorized personnel as approved by the DOI COOP staff. The reports contain names and contact information of the DOI EM community. Reports from

SWN regarding contact responses to alerts, message history, receipt of emergency notifications, and participation status are used for employee accountability. Reports may be generated to determine the effectiveness of emergency response, exercises, or contingency which will be shared with authorized personnel at bureaus/offices in order to provide feedback and corrective actions.

Section 3. Attributes of System Data

A. How will data collected from sources other than DOI records be verified for accuracy?

Bureau/Office COOP officials vet the extracted data from FPPS and identify any records that should not be uploaded to SWN. After records are uploaded, other records will be manually added to the application by authorized managers through the internal DOI CMS system. Updates to the records are manually entered by the authorized managers or by the employee through a CMS email request. Email requests generated by CMS are sent to the EROs to review their contact record and make the necessary updates. This request may be initiated by DOI OEM staff with access to CMS. After a contact record is added, deleted, or fields updated via CMS, it is pushed to SWN via the Group/Contact Management Web Services API. If a contact record is added or deleted from a group in CMS, it is also pushed to SWN, as well as the associated AD group. AD updates are processed every four hours. An email update request is sent to employees with instructions on how to update contact records to ensure accuracy of emergency management contact information.

B. How will data be checked for completeness?

The contact information is checked for completeness during the SWN alert notification for events such as fire drills, shelter-in-place, building evacuations, National Level Exercises, and office closures. If the message history for the alert for each contact indicates the message was not received, the contact information such as email address, phone numbers, and text message will be manually checked to confirm the information is correct or needs to be updated.

C. What procedures are taken to ensure the data is current? Identify the process or name the document (e.g., data models).

Individuals are sent the self update email requests at least once a year. Account administrators, data owners, units, groups, or office managers using the SWN account are responsible for keeping the data in their accounts current. To accomplish this task, SWN supports a number of data maintenance methods which include direct entry, a flat file (csv, xls, xlsx) import process, a batch extensible markup language file of contact data that is transmitted to SWN via an automatable secure fill transfer, and a Web Services API using a simple object access control connection. All data maintenance methods used by SWN require administrative authentication.

D. What are the retention periods for data in the system? Identify the associated records retention schedule for the records in this system.

Contact records in SWN are maintained under the DOI Departmental Records Schedule 1 - DAA-0048-2013-0001-0003, Administration Records of Specific Temporary Value, which was approved by the National Archives and Records Administration (NARA). The disposition is temporary. Records are cut off when the object or subject of the record is removed or discontinued, and records are destroyed when no longer needed.

E. What are the procedures for disposition of the data at the end of the retention period? Where are the procedures documented?

SWN uses software for data deletion or destruction that complies with the U.S. Department of Defense 5220.22-m standards. Approved disposition methods include shredding or pulping for paper records, and degaussing or erasing for electronic records, in accordance with NARA Guidelines and 384 Departmental Manual 1. Disposition procedures are outlined in the SWN Information Security Policy.

F. Briefly describe privacy risks and how information handling practices at each stage of the "information lifecycle" (i.e., collection, use, retention, processing, disclosure and destruction) affect individual privacy.

There are risks to the privacy of individuals due to the PII contained in the system related to individual's work phone number, home phone number, work and personal cell phone numbers, and work or personal email addresses. These risks are mitigated by a combination of administrative, physical and technical controls. The contact information is used to communicate with COOP, emergency management personnel, and individuals with occupant emergency responsibilities. These individuals must be reachable by several methods. In addition, group email lists need to be current. During COOP training, individuals are informed that their contact information must be current in the system.

SWN is a Software as a Service (SaaS) cloud service provider located in the United States. This assessment is being conducted while SWN is undergoing the FedRAMP certification process, and this PIA will be updated if necessary upon completion of the certification process and issuance of an authorization to operate to reflect additional risks identified or updated information regarding mitigating controls. SWN has a Moderate system security categorization based upon the type of data and the requirement for security and privacy controls to protect the confidentiality, integrity, and availability of the sensitive PII contained in the system in accordance with National Institute of Standards and Technology (NIST) standards and FIPS 199, and the Federal Information Security Modernization Act (FISMA). A system security plan was developed for the SWN application to ensure appropriate security controls were implemented to safeguard DOI information transmitted, processed or stored, including access controls, password management, firewalls, segregation of duties, and encryption of database, media and communications. This application uses the principle of least privilege access for authorized users to perform duties, and government information is managed and safeguarded in accordance with FISMA, Office of Management and Budget policies, NIST standards, and DOI security and privacy policies. The SWN system is subject to monitoring consistent with applicable security and privacy laws, regulations, OMB policy, and DOI policies and procedures.

Data will be used for emergency alert and notification of DOI employees on incidents, emergencies, tests and/or exercises. EM COOP officials and bureau/office EM Coordinators notify OEM when a member should be deleted. Authorized users will immediately delete the individual's record and from groups in CMS. An authorized user may confirm the record has been deleted in SWN. Within a four hour cycle, the contact is removed from the AD group. Contact data within a SWN account will not be removed from the account without a specific request from an authorized EM official. After the termination of a client contract or service, a legal review will be completed on the contract to determine further actions necessary for this data and whether the data will be destroyed, retained, or returned.

The use of DOI information and information technology (IT) systems is conducted in accordance with the appropriate DOI use policy. IT systems, in accordance with applicable DOI guidance, will maintain an audit trail of activity sufficient to reconstruct security relevant events. The audit trail will include the identity of each entity accessing the system; time and date of access; activities performed using a system administrator's identification; and activities that could modify, bypass, or negate the system's security controls. Audit logs will be reviewed on a regular, periodic basis and any suspected attempts of unauthorized access or scanning of the system are reported to IT Security. The least amount of access is given to a user to complete their required activity. All access is controlled by authentication methods to validate the authorized user. DOI employees and contractors are required to complete security and privacy awareness training, and DOI personnel authorized to manage, use, or operate the system information are required to take additional role-based training and sign DOI Rules of Behavior.

Section 4. PIA Risk Review

A. Is the use of the data both relevant and necessary to the purpose for which the system is being designed?

Yes

Explanation

The application is relevant and necessary for collecting, modifying and safeguarding contact information for emergency situations affecting the DOI mission or function, emergency contacts, and agency continuity of operations.

B. Does this system or electronic collection derive new data or create previously unavailable data about an individual through data aggregation?

No

C. Will the new data be placed in the individual's record?

No

D. Can the system make determinations about individuals that would not be possible without the new data?

No

E. How will the new data be verified for relevance and accuracy?

SWN does not derive new data or create previously unavailable data about an individual through data aggregation.

F. Are the data or the processes being consolidated?

No, data or processes are not being consolidated

G. Who will have access to data in the system or electronic collection? Indicate all that apply.

- Users Developers System Administrator
 Contractors Other

H. How is user access to data determined? Will users have access to all data or will access be restricted?

COOP/EM leadership identify who is authorized to access SWN. Currently, all of the Watch Officers have access to initiate alerts for closures, testing, drills, and emergencies. They also have access to view and edit contact records, as a backup, when the CMS is down. COOP, IT and authorized staff have rights to create users, input or initiate updates to contact information and generate roster reports. Authorized staff personnel are responsible for rebuilding DOI operations at different locations when operations have been incapacitated. EM IT staff can assign access rights to view or edit records.

I. Are contractors involved with the design and/or development of the system, or will they be involved with the maintenance of the system?

Yes

Were Privacy Act contract clauses included in their contracts and other regulatory measures addressed?

Privacy Act contract clauses were included in the SWN contract.

- Federal Acquisition Regulation (FAR) 52.224-1, Privacy Act Notification (Apr 1984)
- FAR 52.224-2, Privacy Act (Apr 1984)
- FAR 52.239-1 Privacy or Security Safeguards (Aug 1996)

J. Is the system using technologies in ways that the DOI has not previously employed (e.g., monitoring software, SmartCards or Caller ID)?

No

K. Will this system provide the capability to identify, locate and monitor individuals?

Yes

Explanation

SWN contains a Message History with a Summary, Delivery Status, Recipient Status, and Report. The Reports and Audit Trail is a reporting tool with the ability to generate reports and view when groups or contacts were created or modified, the username of the individual that changed the record, and the date and time the record was updated. Information in the history and audit log may include contact person responses, date/time, mode of contact such as Short Message Service, cell, or email. The SWN application administration system logs all changes to customer accounts for auditing purposes, and are only accessed by administrative/manager staff to track the date, IP address, and time. The auditing feature does not allow for the application to be used or changed without administrative notification.

L. What kinds of information are collected as a function of the monitoring of individuals?

Information collected is used to monitor user access (username) and activity (logins, record changes, deletions, additions, date and time-stamp) for auditing purposes.

M. What controls will be used to prevent unauthorized monitoring?

Access to this program is only provided to the necessary authorized employees and is applied on the principle of least-privilege access to allow authorized employees access to the tracking information. Audit features track user activity and the SWN application administration system logs all changes to customer accounts for auditing purposes.

N. How will the PII be secured?

(1) Physical Controls. Indicate all that apply.

- | | | | |
|--|---|---|---|
| <input checked="" type="checkbox"/> Security Guards | <input checked="" type="checkbox"/> Secured Facility | <input checked="" type="checkbox"/> Identification Badges | <input checked="" type="checkbox"/> Combination Locks |
| <input type="checkbox"/> Key Cards | <input checked="" type="checkbox"/> Closed Circuit Television | <input checked="" type="checkbox"/> Safes | <input checked="" type="checkbox"/> Locked Offices |
| <input checked="" type="checkbox"/> Locked File Cabinets | <input checked="" type="checkbox"/> Cipher Locks | <input type="checkbox"/> Other | |

(2) Technical Controls. Indicate all that apply.

- | | |
|---|--|
| <input checked="" type="checkbox"/> Password | <input type="checkbox"/> Intrusion Detection System (IDS) |
| <input checked="" type="checkbox"/> Firewall | <input checked="" type="checkbox"/> Virtual Private Network (VPN) |
| <input checked="" type="checkbox"/> Encryption | <input checked="" type="checkbox"/> Public Key Infrastructure (PKI) Certificates |
| <input checked="" type="checkbox"/> User Identification | <input checked="" type="checkbox"/> Personal Identity Verification (PIV) Card |
| <input type="checkbox"/> Biometrics | |
| <input type="checkbox"/> Other | |

(3) Administrative Controls. Indicate all that apply.

- | | |
|--|--|
| <input checked="" type="checkbox"/> Periodic Security Audits | <input checked="" type="checkbox"/> Regular Monitoring of Users' Security Practices |
| <input checked="" type="checkbox"/> Backups Secured Off-site | <input checked="" type="checkbox"/> Methods to Ensure Only Authorized Personnel Have Access to PII |
| <input checked="" type="checkbox"/> Rules of Behavior | <input checked="" type="checkbox"/> Encryption of Backups Containing Sensitive Data |
| <input checked="" type="checkbox"/> Role-Based Training | <input checked="" type="checkbox"/> Mandatory Security, Privacy and Records Management Training |
| <input type="checkbox"/> Other | |

O. Who will be responsible for protecting the privacy rights of the public and employees? This includes officials responsible for addressing Privacy Act complaints and requests for redress or amendment of records.

The Director, Office of Emergency Management, is the SWN Information System Owner and the official responsible for oversight and management of the SWN security controls and the protection of agency information processed and stored in the SWN application. The Information System Owner and SWN Privacy Act System Manager, in collaboration with the DOI Senior Management Team, are responsible for ensuring adequate safeguards are implemented to protect individual privacy in compliance with Federal laws and policies for the data managed, used, and stored in the SWN application. These officials, DOI bureau and office emergency response officials, and authorized SWN personnel are responsible for protecting individual privacy for the information collected, maintained, and used in the system, and for meeting the requirements of the Privacy Act, including providing adequate notice, making decisions on Privacy Act requests for notification, access, and amendments, as well as processing complaints, in consultation with DOI Bureau and Office Privacy Officers.

P. Who is responsible for assuring proper use of the data and for reporting the loss, compromise, unauthorized disclosure, or unauthorized access of privacy protected information?

The SWN Information System Owner is responsible for oversight and management of the SWN security and privacy controls, and for ensuring to the greatest possible extent that agency data is properly managed and that all access to agency data has been granted in a secure and auditable manner. The Information System Owner is also responsible for ensuring that any loss, compromise, unauthorized access or disclosure of agency PII is reported to US-CERT within 1-hour of discovery in accordance with Federal policy and established procedures.

Customer communications are managed through an initial point of contact service model. SWN Customer Support Managers (CSMs) serve as the initial point of contact for assuring the proper use of client data, as well as informing clients of the loss, compromise, unauthorized disclosure, or unauthorized access of privacy protected information. The SWN Customer Support management team will also be involved in this process as necessary.