Privacy Impact Assessment Form

SEND WORD NOW

This document is only used when the Chief Privacy Officer determines that the system contains personally identifiable information and a more in depth assessment is required.

Complete and sign this form and forward to the Chief Privacy Officer.

David A. Lee
Federal Housing Finance Agency
1700 G Street NW
Washington, DC 20552
(202) 414-3804
David.Lee@fhfa.gov

Guidance for Completing the Privacy Impact Assessment

A Privacy Impact Assessment (PIA) is an analysis of how information in identifiable form is handled. PIAs are to be completed when FHFA: 1) develops or procures IT systems or projects that collect, maintain, or disseminate information in identifiable form from or about members of the public; or 2) initiates a new electronic collection of information in an identifiable form for 10 or more members of the public. System owners and developers are responsible for completing the. The guidance below has been provided to help the system owners and developers complete the PIA.

Overview

- This section should provide a thorough and clear overview of the system and give the reader the appropriate context to understand the system owner's responses in the PIA. What is the purpose of the IT system? What will be the primary uses of the system? How will this support the program's mission?
- This section fulfills the E-Government Act's requirement for an introduction for members of the public who may be reading the PIA. PIAs will be made publicly available (unless a determination is made to not make the PIA available because publication would raise security concerns and/or reveal classified or sensitive information).

Section 1.0 Characterization of the Information

- Identify if the system contains information about individuals, versus statistical, geographic, or financial, with no link to a name or other identifier, such as name, home address, social security number, account number, home telephone number and fax numbers, or personal e-mail address.
- Examples of sources of the information include information that comes from individuals applying for loans, mortgages, and forms individuals completed. Where does the data originate? (e.g., the FHA, Office of Personnel Management, and Financial Institutions). A third party is usually a non-Federal person or entity, which may be a source of data/information (e.g., a bank, an internet service provider, an organization).
- If the system collects information from 10 or more members of the public, ensure that the agency has received OMB's approval to do so or determine whether OMB's approval is needed to collect the information in accordance with the Paperwork Reduction Act of 1980.

Section 2.0 Uses of the Information

- Identify the primary uses of the information and how the information supports the program's mission.
- Identify the controls that are in place to ensure the information will be used for the manner for which it was collected. For example, access to the information will be restricted a limited number of program staff who use the data for their specific program use.

Section 3.0 Retention

- The Privacy Act requires agencies to address the retention and disposal of information about individuals. (The retention information is published in the Privacy Act system of records notice).

- The retention periods of data/records that the agency manages are contained in either the NARA General Records Schedule or agency Records Schedule. For the data being created/ maintained in the system, the records schedules are the authoritative sources for this information.
- Disposing of the data at the end of the retention period is the last state of life cycle management. Records subject to the Privacy Act have special disposal procedures (e.g. shredding of paper documents).

Section 4.0 Notice, Access, Redress and Correction

- The Privacy Act at 5 U.S.C. 552a(e)(1) requires that "each agency that maintains a system of records shall maintain in its records only such information about an individual as is relevant and necessary to accomplish a purpose of the agency required to be accomplished by statute or by executive order of the President."
- Data can be retrieved in a number of ways, but there is usually a personal identifier associated with a record. If the system retrieves information by an individual's name or other personal identifier it is a Privacy Act system and may need a system of records notice (SORN published in the Federal Register. The system may already have a Privacy Act SORN that applies to it. If you do not have a published SORN, contact the Privacy Act Officer. The Privacy Act requires that amendments to an existing system must also be addressed in a Federal Register notice. Any employee who knowingly and willfully maintains a systems of records without meeting the Privacy Act notice requirements (5 U.S.C. 552a(e)(4)) is guilty of a misdemeanor and may be fined up to $5,000.
- If a name or other personal identifier is not used to retrieve information, it is possible that the system is not a Privacy Act system. However, even though information may not fall under the Privacy Act's protection and requirements, certain information may be protected from disclosure under the Freedom of Information Act.
- The agency has developed and published an agency specific Privacy Act Rule in the Federal Register (12 CFR Part 1204) that explains how individuals can gain access to information about themselves and correct errors if appropriate.
- The Privacy Act of 1974 requires that agencies only maintain data that is accurate, relevant, timely, and complete about individuals. These requirements are statutory and need to be addressed. If the data does not meet any one of these four components, then fairness in making any determination is compromised.

Section 5.0 Sharing and Disclosure

- If it is unknown to you whether or not systems share data, you can either contact the business owner of the data, or you can contact the IT specialist who knows what other interface goes on between the systems/applications. As an example, if your system/application shares data with another system/application, ask yourself whether you have access to the data in the interfaced system/application. If so, then your answer is yes and an explanation is needed.
- Also consider "other" users who may not be obvious as those listed, such as the GAO or the Inspector General. "Other" may also include database administrators or IT Security Officers. Also include organizations listed in the Privacy Act system of records notice

under the "Routine Use" section when a Privacy Act system of records notice is required. The more comprehensive the list, the better it is.

- You must first review appropriate SORN to determine whether any information that may come from an existing SORN allows that information to be exchanged and used for these new purposes or uses. There are statutory restrictions on use and disclosure of information that comes from a SORN.

Section 6.0 Technical Access and Security

- For the most part, access to data by a user within FHFA is determined by the "need-to-know" requirements of the Privacy Act (this means to authorized employees within the agency who have a need for the information to perform their duties). Care should be taken to ensure that only those employees who need the information have access to that information. Other considerations are the user's profile based on the user's job requirements and managerial decisions.
- The criteria, procedures, controls and responsibilities regarding access must be documented to comply with the intent of the Federal Information Security Management Act of 2002 for standards and guidelines on security and privacy. What criteria will the manager and system security person use to decide on access to the data, for example?
- The system owner is responsible for ensuring that access to information and data is restricted to authorized personnel. Usually, a user is only given access to certain information that is needed to perform an official function. Care should be given to avoid "open systems" where all information can be viewed by all users. System administrators may be afforded access to all of the data depending upon the system and/or application. However, restrict access when users may not need to have access to all the data.
- When a contract provides for the operation of a system on behalf of FHFA, the Privacy Act requirements must be applied to such a system.
- The IT Security C&A process requires a system security plan that identifies the technical controls associated with identification and authentication of users. Certain laws and regulations require certain monitoring for authorized reasons by authorized employees. What is in place to ensure that only those authorized can monitor use of the system? For example, business rules, internal instructions, posting Privacy Warning Notices address access controls and violations for unauthorized monitoring and access. It is the responsibility of managers of systems to ensure no unauthorized monitoring is occurring.
- The IT Security Plan describes the practice of applying logical access controls. Logical access controls are system-based means by which the ability is explicitly enabled or restricted. It is the responsibility of managers of systems to ensure no unauthorized access is occurring.
- The IT Security Plan describes the practice of audit trails. Audit trails maintain a record of system activity and user activity including invalid logon attempts and access to data. The C&A process requires a system security plan outlining the implementation of the technical controls associated with identification and authentication.
- According to OMB Circulars A-123 and A-130, every system/application/process that uses data must have some sort of control to prevent the misuse of the data by those having access to the data. For instance, in computerized systems the Security Information Record

(SIR) is part of the Core Storage Terminal Table. The SIR is the automated tool that identifies and authenticates an individual for the system and is transparent to the user. Describe these in response to this question.

- Are there privacy and security awareness controls such as training materials for personnel? All employees, including contractors, have requirements for protecting information in Privacy Act systems
- Describe the controls in place to protect the information.

SUMMARY INFORMATION

Date submitted for review:

Name of System: **Send Word Now**

System Owner(s): Tom Davy

Name	E-mail	Telephone number
Tom Davy	Thomas.Davy@FHFA.gov	202-577-9925

Overview

The overview section provides an overview of the system and addresses the following elements:

- The system name and the division/office that owns the system;
- The purpose of the program, system, or technology and how it relates to FHFA's mission; and
- A general description of the information in the system.

System Overview
• Send Word Now (SWN) falls under the Deputy Chief Operating Officer in the area of emergency preparedness and continuity of operations (COOP). SWN allows FHFA to communicate with FHFA personnel and contractors, especially those who have not been issued an FHFA Blackberry (BB) in an emergency. It allows FHFA to reach multiple employees at multiple points of contact quickly and efficiently. It also notifies FHFA if and how an employee received that message. SWN aids FHFA's communications capabilities in a crisis and supports FHFA ability to determine if an employee needs help after an emergency and can be used to push information to employees and contractors, and to perform mission-essential functions in an emergency situation. • SWN takes information available on FHFA servers (BB and FHFA "desk" telephone number numbers work e-mail addresses) as well as voluntarily provided personal information (personal mobile telephone number and e-mail).

Section 1.0 Characterization of the Information

The following questions 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. The questions address all information collected, with more emphasis provided on the collection of personally identifiable information (PII), such as name, address, social security number, date of birth, financial information, etc.

#	Question	Response
1.1	What information is collected, used, disseminated, or maintained in the system?	Name, work telephone number, work e-mail address, work BB telephone number; and for people who wish to be contacted on their personal device, their personal telephone number, personal e-mail address.
1.2	What are the sources of the information in the system?	The information comes from two sources. Work information (i.e., FHFA-issued e-mail address, office desk telephone number and BB telephone number) is taken from Windows active directory on FHFA servers. Personal information is user-generated on the FHFA Access Control Module (ACM).
1.3	Why is the information being collected, used, disseminated, or maintained?	The primary purpose is to contact employees and contractors in an emergency situation in order to deliver a message or to account for FHFA employees and contractors in an emergency. Additionally, it may be used in non-emergency situations, such as informing FHFA personnel and contractors of office closures due to inclement weather. While FHFA can send targeted or All Hands e-mails, many FHFA personnel do not have an issued BB. SWN bridges this gap.
1.4	How is the information collected?	Work information is taken from the Windows Active Directory on FHFA servers. Personal information is voluntarily provided through ACM. ACM is a portal that allows users to input personal information, such as personal telephone number, personal e-mail, and the names, telephone numbers, and e-mail addresses of emergency contacts. SWN
1.5	Given the amount and type of data collected, what risks to an individual's privacy are associated with the data?	In the event the SWN data was lost or mishandled, the risk to personal privacy of FHFA personnel is that their personal information, specifically their name, work phone numbers (desk and BB) and work e-mail could be compromised. Additionally, those who chose to give a "home" phone number and/or e-mail could also have that information compromised. This could result in unwanted contacts.

Section 2.0 Uses of the Information

The following questions clearly delineate the use of information and the accuracy of the data being used.

#	Question	Response
2.1	Describe the uses of information.	Used to contact all or a select group of employees and contractors (personnel) in emergency and non-emergency situations. This might include office closure, natural disaster, or a man-made threat. It will give notice to employees and contractors of what to do, and will provide confirmation of whether an employee or contractor has received the notification. Many FHFA personnel do not have an issued BB. Many with an issued do not carry them 24/7, carrying their personal cell phone only – including during work hours.
2.2	Describe any types of controls or safeguards in place to ensure that information is only used in the manner for which it was collected.	Only authorized users will have access to the information, specifically the System Owner – the Continuity Program Manager, the DepCOO and other assistants to the DepCOO. FHFA uploads the data to SWN two ways: 1. A spreadsheets of all FHFA personnel with data generated from the OTIM ACM is sent to SWN, Inc. by an encrypted e-mail. This will be done as soon as SWN has been approved and annually as a system update. 2. Most updates will be done by hand directly in to the SWN database by the System Owner or other authorized person as people enter / leave the Agency. Once the information has been compiled, the only way that SWN will issue an emergency notification is if an authorized user calls or e-mails SWN and states the correct password. The System Owner has discretion when choosing authorized users. In selecting authorized users, the System Owner weighs the potential misuse of SWN against the possibility that limiting the number of authorized users may render the system obsolete in an emergency where a limited number of persons may activate the system.

Section 3.0 Retention

The following questions outline how long information will be retained after the initial collection.

#	Question	Response
3.1	How long is information retained?	The Records Office at OTIM is currently working with a vendor to implement a new records management system. The new system anticipates three or four different classifications of records. Each classification will be subject to a retained for a specific time period. The SWN System Owner will comply with any requirements they publish. As long as FHFA administers SWN, the records created by FHFA will be kept until superseded by a new record that reflects the most up-to-date information. The General Records Schedule governs how long FHFA will maintain this information. Currently, SWN retains only retains the information that reflects the most current updates. For instance, when the System Owner sends a new database from the ACM and Windows Active Directory via encrypted e-mail, SWN does not retain the previous database. The information at SWN is retained until superseded/changed. As people leave the Agency, their information is removed from both the FHFA and SWN, Inc. databases. The System Owner will maintain data as long as required in any media recommended by either the CPO or Records Management office.
3.2	Has the retention schedule been approved by the component records officer and the National Archives and Records Administration (NARA)?	As discussed above, the Records Office at OTIM is in the process of implementing a new records retention system. Thus, the retention schedule has not explicitly been approved. Once the new system is in place, it is anticipated that will be approved by the component records officer.
3.3	Please discuss the risks associated with the length of time data is retained and how those risks are mitigated.	Once the initial SWN database has been setup, the system owner will update the SWN database on a weekly basis to ensure that departing employees & contractors are removed as quickly as new ones are added. SWN, Inc. does not keep old data and deletes outdated data.

Section 4.0 Notice, Access, Redress and Correction

The following questions are directed at notice to the individual, the individual's right to consent to uses of the information, the individual's right to decline to provide information, and an individual's ability to ensure the accuracy of the information collected about them.

#	Question	Response
4.1	Has a System of Record Notice (SORN) been created?	Yes. OPM publishes a government wide SORN OPM GOVT-1 for general personnel records.
4.2	Was notice provided to the individual prior to collection of information?	Notice is not provided for their work information from the information collected from Windows Active Directory. Notice is provided before users input their personal information in ACM.
4.3	Do individuals have the opportunity and/or right to decline to provide information?	Yes. FHFA employees may choose whether or not to enter their personal information in the ACM. We can remove anyone's work information from SWN if the employee/contractor requests, with the understanding that they would not receive important information from the system.
4.4	What are the procedures that allow individuals to gain access to their information?	The ACM application is only accessible while connected to the FHFA local area network. Employees may access their information in the system. System Administrators and the System owner may also see and update the information. Employees may inform the system owner that they have recently updated their personal information in order to expedite the delivery of that updated information to SWN. Otherwise, the system owner will update all information at least quarterly to reflect any changes made. There is no mechanism whereby FHFA personnel may communicate directly with SWN to gain access to their information.
4.5	What are the procedures for correcting inaccurate or erroneous information?	Employees and contractors are the only individuals allowed to enter and maintain their information. They may be asked to periodically update that information on ACM, which will then be re-sent to SWN. There is no mechanism whereby FHFA personnel may communicate directly with SWN to gain access to their information.

Section 5.0 Sharing and Disclosure

The following questions define the content, scope, and authority for information sharing.

#	Question	Response
5.1	With which internal organization(s) is the information shared, what information is shared and for what purpose?	The information gathered from the ACM will be available to the OTIM, the System Owner, SWN, Inc. and other authorized FHFA employees. It will be shared with OTIM because OTIM administers the ACM and will be in charge of administering that system and providing the System Owner with periodic updates. It will be available to the System Owner for the purpose of aggregating the data from the Windows Active Directory and ACM and compiling that into a single spreadsheet which will then be sent via encrypted e-mail to SWN.
5.2	With which external organization(s) is the information shared, what information is shared, and for what purpose? External organization(s) include Federal, state and local government, and the private sector.	The aggregated information from ACM and Windows Active Directory will be sent via encrypted e-mail to SWN, Inc. SWN, Inc. is the vendor who administers the emergency contact notification system. It will be sent to SWN so that they can input the information into their system. Once they have done this, SWN will have the ability to send out a message when directed to do so by the System Owner. The primary purpose of acquiring SWN is its ability to send out a message to FHFA personnel during an emergency situation.
5.3	Is the sharing of PII outside the FHFA compatible with the original information 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 authority the program or system is allowed to share the PII outside of the FHFA.	Yes. OPM GOVT-1 allows sharing of this information with government contractors like SWN.

#	Question	Response
5.4	Given the external sharing, explain the privacy risks identified and describe how they were/are mitigated.	The primary risk is that an FHFA employee or contractor will have his or her work and (if given, personal) telephone numbers and e-mail address exposed should the information be lost or otherwise compromised. Currently, the risks are mitigated by allowing only the System Owner and a few others authorized to retrieve information from ACM. Initial transmission of the information from FHFA to SWN will be done via encrypted e-mail. After this initial transmission, the System owner will update the SWN database on a weekly basis. The information taken from Windows Active Directory is the Work information. Not all the information generated by the user in the ACM is transmitted to SWN, Inc.; only the user's e-mail and telephone numbers will be transmitted. No information about third-party emergency contacts of FHFA employees or contractors will be sent to SWN. Data is maintained and stored at SWN, Inc. Please see Attachment #1 "SWN Security Measures" for a detailed analysis of the procedures that the contractor uses to protect FHFA employees' personal information.

Section 6.0 Technical Access and Security

The following questions describe technical safeguards and security measures.

#	Question	Response
6.1	What procedures are in place to determine which users may access the system and are these procedures documented?	Only authorized users of SWN (and OTIM), as assigned by the System Owner, may view employee SWN information. Additionally, employee's supervisors may view personal information from Windows Active Directory and/or the spreadsheet of personal information from the ACM. Procedures are currently be drafted.

#	Question	Response
6.2	Will contractors have access to the system? If yes, how will contractors gain access to the system? How will the FHFA control their access and use of information?	Yes. Contractors will have access to SWN in two ways. First, contractors working within FHFA (i.e. Help Desk Staff) will have access to the ACM. This will allow their personal information to be sent to SWN in the same way that FHFA employees' personal information is given to SWN so that they may be contacted in an emergency. FHFA will control their access to the system in the same way that FHFA employees' access is controlled, i.e., they may only log on to the ACM while logged on to an FHFA computer, they may not see other employees' personal information, and they may choose to decline to upload any personal information to the ACM. The second way that contractors have access refers to the contractors at SWN, i.e., the vendors who provide the service. Their access to SWN refers to the information that we provide them via encrypted e-mail. They have the ability to use that information to send out an emergency notification when instructed to do so by an authorized user of SWN. SWN as a vendor is contractually obligated not to divulge or misuse the information FHFA provides to them. Other than the contractual relationship between FHFA and SWN, there is no auditing or enforcement mechanism currently in place to ensure compliance.
6.3	Describe what privacy training is provided to users either generally or specifically relevant to the program or system?	All FHFA employees are required to participate in annual Information System Security Awareness and Privacy Training.
6.4	What technical safeguards are in place to protect the data?	SWN data is maintained by OTIM and SWN, Inc. The System Owner maintains a copy of the SWN data on the shared drive at S://Continuity, which only members of the Continuity Team have access to. For information on the technical safeguards put in place by SWN, see Attachment #1.
6.5	What auditing measures are in place to protect the data?	The System Owner and a few others, under the direction of the DepCOO have the ability to send out a notification using SWN. Additionally, the System Owner may designate others as authorized users.

#	Question	Response
		These individuals will be given the username and password for web- and telephone number-based access to SWN. This will allow only authorized individuals to send out a notification. For information on auditing measure in place at SWN, see Attachment #1.
6.6	Has a Certification & Accreditation been completed for the system or systems supporting the program?	No.

Signatures:

Thomas E. Davy, III
System Owner (Printed Name)

System Owner (Signature)

4 May 2011
Date

N/A – COTS
System Developer (Printed Name)

N/A
System Developer (Signature)

Date

Ralph Mosios
Chief Information Security Officer
(Printed Name)

Ralph Mosios
Chief Information Security Officer
(Signature)

17 May 2011
Date

R. Kevin Winkler
Chief Information Officer
(Printed Name)

Chief Information Officer
(Signature)

5/20/11
Date

David A. Lee
Chief Privacy Officer
(Printed Name)

Chief Privacy Officer
(Signature)

5/24/2011
Date

Attachment #1

SWN Security Measures

[Note: The following information was provided by Amelia Koethen, who is the account the Account Manager for FHFA's SWN account. Ms. Koethen can be reached at akoethen@sendwordnow.com]

1. What procedures are in place to determine which users at SWN may access FHFA data?

All privileges to FHFA data are based on the need-to-know. Usernames and passwords are created by SWN Customer Support Managers, or by privileged customer administrators. Initial passwords are randomly generated; new customers are then required to change their initial password upon first login. This is for security purposes and is one of SWN's SAS 70 Type II internal controls.

Authentication for the User Interface is performed by a server-side PHP module that calls an application layer routine to validate the Username/Password pair entered by the user. Client-side validation is never performed.

All privileged accounts are controlled by senior operations management. Separation of duties is in place, when possible, and user access is role-based and need-based for all SWN customers. Role-based access is restricted by username and password.

2. What technical safeguards are in place to protect the data?

1. USER-LEVEL SECURITY
   a. All traffic to and from the Web interfaces to the SWN application is encrypted using 128-bit SSL.
   b. Login credentials to the SWN application are created by customer administrators; new customers are required to change their initial password to the SWN web portal upon first login. Passwords are neither visible nor accessible by SWN personnel. To prevent key-logging/password interception, no username/password validation is performed at the client.
   c. SWN provides customer-configurable password security with minimum complexity requirements. In addition to periodic reviews, automatic controls for password strength include:
      i. Password History: 6
      ii. Minimum Password Age: 1
      iii. Account Lockout Duration: 0
      iv. Account Lockout Threshold: 5
      v. Reset Account Lockout Counter: 15
2. NETWORK-LEVEL SECURITY

a. Redundant Cisco firewalls block all but the necessary categories of traffic (HTTP, HTTPS, VPN, etc.) entering a service complex (data center), and limit the traffic between servers within the complex. The firewalls also reduce vulnerabilities to denial of service attacks.

b. SWN also uses Network Intrusion Detection Systems (NIDS) to monitor network traffic for known malicious or suspicious traffic. SWN NIDS are placed just behind the firewall in the DMZ and just behind the firewall in the internal network. This provides full coverage of all traffic entering and exiting the DMZ.

c. All Web applications within the service are hardened to eliminate known classes of vulnerabilities to malicious attacks. Classes against which Web applications are hardened include:

   i. Backdoors and Debug Options
   ii. Buffer Overflows
   iii. Cookie Poisoning
   iv. Cross-site Scripting
   v. Hidden Field Manipulation
   vi. Null Parameter Exploitation
   vii. Parameter Tampering
   viii. Stealth Commanding
   ix. Third-party Configurations

3. <u>PHYSICAL-LEVEL SECURITY</u>

a. Onsite security guards are present 24/7, supplementing both indoor and outdoor security monitoring.

b. Access to a facility requires a Hosting Facility photo ID badge and inclusion on the list of authorized personnel for that facility.

c. Biometric hand scans and pulse detection are required for entry to a facility; this limits hosting customers from moving from one co-location area to another within the facility.

d. Only SWN personnel have either physical or logical access to SWN resources.

3. What auditing measures are in place to protect the data?

SWN strongly believes that full logging is the cornerstone to providing the greatest amount of transparency into all aspects of the system. This includes every aspect of the infrastructure from the data center to the application itself. To achieve this end, SWN uses a product called Splunk to collect and aggregate available logs. Splunk simplifies the collection and manipulation of logs, making searching, reviewing and auditing very easy. Splunk also provides a means of non-repudiation.

4. Are the procedures relating to safeguarding and protecting private information documented?

SWN's privacy policy is posted on our website (http://www.sendwordnow.com/) towards the bottom of the page.