ADAMS ML12067A167

U.S. Nuclear Regulatory Commission

Revised

Privacy Impact Assessment

Designed to collect the information necessary to make relevant determinations regarding the applicability of the Privacy Act, the Paperwork Reduction Act information collection requirements, and records management requirements.

Verizon Notification Service (VNS)

Date: March 7, 2012

A. GENERAL SYSTEM INFORMATION

1. Provide a detailed description of the system:

The Verizon Notification Service (VNS) consists of an internal ColdFusion web page that interfaces with an external notification system hosted by Verizon Business Services (Verizon) and Varolii. VNS allows the Nuclear Regulatory Commission (NRC) employees and contractors to **voluntarily** enter personal contact information in order to receive important alerts and notifications from the NRC. Notifications will include information such as office or building closures, weather related event information, and any other emergency notification information that is unrelated to licensees or other NRC business.

2. What agency function does it support?

Human Capital Management – Emergency Employee and Contractor Communication

3. Describe any modules or subsystems, where relevant, and their functions.

The VNS does not have any modules or subsystems.

4. What legal authority authorizes the purchase or development of this system?

On November 1, 2005, President George W. Bush announced the National Strategy for Pandemic Influenza ("National Strategy") and directed all Federal agencies to begin internal planning to ensure readiness in the event of an influenza pandemic.

5. What is the purpose of the system and the data to be collected?

The purpose of collecting this information is to notify NRC employees when there is an important event such as office or building closures, weather related event information, and any other emergency notification information.

6. Points of Contact:

Project Manager	Office/Division/Branch	Telephone
Bob Randall	OIS/ICOD	301-415-6242
Business Project Manager	Office/Division/Branch	Telephone
Karen Paradiso	OIS/ICOD	301-415-5852
Technical Project Manager	Office/Division/Branch	Telephone
Jonathan Feibus	OIS/ICOD	301-415-0717
Executive Sponsor	Office/Division/Branch	Telephone
Thomas Rich	OIS/ICOD	301-415-7485

7. Does this privacy impact assessment (PIA) support a proposed new system or a proposed modification to an existing system?

a. ___ **New System** __X__ **Modify Existing System** ____ **Other (Explain**)

b. If modifying an existing system, has a PIA been prepared before?
Yes

(1) **If yes, provide the date approved and ADAMS accession number**.
July 14, 2011 and ML11196A104

B. INFORMATION COLLECTED AND MAINTAINED

These questions are intended to define the scope of the information requested as well as the reasons for its collection. Section 1 should be completed only if information is being collected about individuals. Section 2 should be completed for information being collected that is not about individuals.

1. **INFORMATION ABOUT INDIVIDUALS**

a. Does this system maintain information about individuals?
Yes

(1) If yes, identify the group(s) of individuals (e.g., Federal employees, Federal contractors, licensees, general public).

Federal Employees and Federal Contractors

(2) IF NO, SKIP TO QUESTION B.2.

b. What information is being maintained in the system about an individual (be specific)?

Name, NRC e-mail address, NRC phone number, physical office location, program office, NRC division, NRC LAN ID, work cell / Blackberry, home phone, personal cell phone, personal e-mail, personal short message service (SMS)/text number, and time zone information.

c. Is information being collected from the subject individual?

Yes.

(1) If yes, what information is being collected?

The subject individual voluntarily enters their home phone, personal cell phone, personal email, and personal SMS/text number.

d. Will the information be collected from 10 or more individuals who <u>are not</u> Federal employees?

Yes

(1) If yes, does the information collection have OMB approval?

No. OMB clearance is not required for subscription to an agency notification system.

(a) If yes, indicate the OMB approval number:

e. Is the information being collected from existing NRC files, databases, or systems?

Yes

(1) If yes, identify the files/databases/systems and the information being collected.

Some of the information collected comes from the NRC's Active Directory environment. When a user logs into the VNS web page on the NRC internal network the web service will connect to the NRC's Active Directory infrastructure via secure sockets layer (SSL). It verifies the user's credentials and gathers select

information. The information pulled from the Active Directory includes data elements such as Name, NRC e-mail address, NRC phone number, physical office location, program office, NRC division, and NRC LAN ID.

f. Is the information being collected from external sources (any source outside of the NRC)?

No

(1) If yes, identify the source and what type of information is being collected?

g. How will information not collected directly from the subject individual be verified as current, accurate, and complete?

Every time a user logs into the VNS, the interface system will check to ensure that the user's NRC information from the Active Directory is complete and accurate. If data from the Active Directory needs to be updated the VNS system will automatically update the information. It will be the responsibility of the individual user to validate the personal information they have voluntarily entered into the VNS. The Office of Information Services (OIS) will send out periodic messages to those who have registered in the system to verify and update their information.

h. How will the information be collected (e.g. form, data transfer)?

When a user accesses the internal web page it presents the user's NRC Active Directory (AD) information on the page, retrieves any information from the Verizon/Varolii system over the internet, and allows the user to enter/update their personal information. Once the user enters/updates their information they press the Update button and all of the user information is sent via SSL to the Verizon/Varolii system. All traffic to and from the internal NRC VNS web page is secured and encrypted with SSL technology. The AD is part of NRC internal network infrastructure and is completely separate from VNS. AD is a Microsoft special purpose database and is responsible for authenticating all users in a network.

2. INFORMATION NOT ABOUT INDIVIDUALS

a. Will information not about individuals be maintained in this system?

No

(1) If yes, identify the type of information (be specific).

b. What is the source of this information? Will it come from internal agency sources and/or external sources? Explain in detail.

Not Applicable

C. USES OF SYSTEM AND INFORMATION

These questions will identify the use of the information and the accuracy of the data being used.

1. Describe all uses made of the data in this system.

This information will be used to notify NRC employees and contractors who voluntarily register in the system when there is an important event to provide information such as office or building closures, weather related event information, and any other emergency notification information.

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

Yes

3. Who will ensure the proper use of the data in this system?

The system administrators will ensure that the information in the system is used properly.

4. Are the data elements described in detail and documented?

Yes

a. If yes, what is the name of the document that contains this information and where is it located?

The VNS documentation is available on the OIS Service Catalog page.

5. Will the system derive new data or create previously unavailable data about an individual through aggregation from the information collected?

No

a. If yes, how will aggregated data be maintained, filed, and utilized?
N/A

b. How will aggregated data be validated for relevance and accuracy?
N/A

c. If data are consolidated, what *controls* protect it from unauthorized access, use, or modification?
N/A

6. How will data be *retrieved* from the system? Will data be retrieved by an individual's name or personal identifier? (Be specific.)

Contact information will be used based on organization or office location. VNS is designed so that an announcement can go out to a specific geographical location if the emergency situation warrants that. This system is developed for not targeting any specific people, but targets are currently grouped by Regions, HQ, Different building in HQ, Divisions etc. An individual's name or personal identifier will not be used to retrieve information from the system.

7. Will this system provide the capability to identify, locate, and monitor (e.g., track, observe) individuals?

No

a. If yes, explain.

(1) What controls will be used to prevent unauthorized monitoring?

8. List the report(s) that will be produced from this system.

The system can produce reports on the success and failure of different types of messages sent from VNS.

a. What are the reports used for?

Reports generated from this system will be used to track the number of successful and failed communications and methods for individual alerts that are sent.

b. Who has access to these reports?

Only VNS system administrators can access the reports that are generated on the Back-end Verizon/Varolii part of VNS. Only select people in each NRC program office that have access to the back end of the system will be allowed to run reports.

D. ACCESS TO DATA

1. Which NRC office(s) will have access to the data in the system?

Only select staff in OIS, the Office of Administration, the Office of Human Resources, the Office of Nuclear Security and Incident Response and the Regional Offices will have access to the VNS.

(1) For what purpose?

The staffs that have access to the information in the system will use it to create groups based on location, office, or other criteria in order to send out approved notifications to NRC staff and contractors.

(2) Will access be limited?

Yes, access will be limited to how many people can administer the back end of the VNS system and send out communications. At this time the limitation is for two to three people in each program office.

2. Will other NRC systems share data with or have access to the data in the system?

No

(1) If yes, identify the system(s).

(2) How will the data be transmitted or disclosed?

3. Will external agencies/organizations/public have access to the data in the system?

No

(1) If yes, who?

(2) Will access be limited?

(3) What data will be accessible and for what purpose/use?

(4) How will the data be transmitted or disclosed?

E. RECORDS RETENTION AND DISPOSAL

The National Archives and Records Administration (NARA), in collaboration with federal agencies, approves whether records are temporary (eligible at some point for destruction/deletion because they no longer have business value) or permanent (eligible at some point to be transferred to the National Archives because of historical or evidential significance). These determinations are made through records retention schedules and are required under 36 CFR 1234.10. The following questions are intended to determine whether the records in the system have an approved records retention schedule or if one will be needed.

1. Can you map this system to an applicable retention schedule in NUREG-0910, or the General Records Schedules at http://www.archives.gov/records-mgmt/grs ?

Yes

a. **If yes, please cite the schedule number, approved disposition, and describe how this is accomplished. For example, will the records or a composite thereof be deleted once they reach their approved**

retention or exported to a file for transfer based on their approved disposition?

General Records Schedule 25, Item 7, Transitory Files. Disposition: Destroy immediately, or when no longer needed for reference, or according to a predetermined time period or business rule (e.g., implementing the auto-delete feature of electronic mail systems)

b. If the answer to question E.1 is yes, skip to F.1. If the response is no, complete question E.2 through question E.7.

2. If the records cannot be mapped to an approved records retention schedule, how long do you need the records? Please explain.

3. Would these records be of value to another organization or entity at some point in time? Please explain.

4. How are actions taken on the records? For example, is new data added or updated by replacing older data on a daily, weekly, or monthly basis?

5. What is the event or action that will serve as the trigger for updating, deleting, removing, or replacing information in the system? For example, does the information reside in the system for three years after it is created and then is it deleted?

6. Is any part of the record an output, such as a report, or other data placed in ADAMS or stored in any other location, such as a shared drive or MS SharePoint?

7. Does this system allow for the deletion or removal of records no longer needed and how will that be accomplished?

F. TECHNICAL ACCESS AND SECURITY

1. Describe the security controls used to limit access to the system (e.g., passwords).

All of the system data is maintained and protected in the back-end of the VNS system which is hosted at Verizon/Varolii.The internal NRC Web page does not save or maintain any PII. All to and from traffic is secured and encrypted with SSL technology. The NRC has one “Super Administrator (ADMIN)” account that has access to all aspects of the NRC instance of VNS on their servers and that account can provide elevated rights to other accounts on the system when necessary. Verizon/Varolii limits the number of “Sub-Admin” accounts on the system to 10 to also help control elevated access to the system.

2. What controls will prevent the misuse (e.g., unauthorized browsing) of system data by those having access?

Only the single “Super Administrator account has full access to all data in system and assigns the level of access to all other sub-administrators” which limits system access and limits misuse.

3. Are the criteria, procedures, controls, and responsibilities regarding access to the system documented?

Yes

(1) If yes, where?

Yes, standard operating procedure from Verizon/Varolii for the VNS system. These are maintained on the Varolii web site and our internal SharePoint site for VNS.

4. Will the system be accessed or operated at more than one location (site)?
Yes, the system will be accessed and operated from NRC Headquarters as well as the Regional offices.

a. If yes, how will consistent use be maintained at all sites?

Consistent use will be maintained by limiting the number of Admin accounts on the system and only allowing people to have Admin rights to the production system after they have learned how to use the system and send test notifications on the development portal that Verizon/Varolii provides on their servers. That development server does not have the production database on it and it allows full scale testing of scenarios on the system without impacting live users.

5. Which user groups (e.g., system administrators, project managers, etc.) have access to the system?

System Administrators

6. Will a record of their access to the system be captured?

No

a. If yes, what will be collected?

7. Will contractors be involved with the design, development, or maintenance of the system?|

Yes

If yes, and if this system will maintain information about individuals, ensure Privacy Act and/or PII contract clauses are inserted in their contracts.

- *FAR clause 52.224-1 and FAR clause 52.224-2 should be referenced in all contracts, when the design, development, or operation of a system of records on individuals is required to accomplish an agency function.*

- *PII clause, "Contractor Responsibility for Protecting Personally Identifiable Information" (June 2009), in all contracts, purchase orders, and orders against other agency contracts and interagency agreements that involve contractor access to NRC owned or controlled PII.*

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

The Super Admin is the only person will full access to all data. This person assigns the level of access to all other Sub Admins. OIS will send out periodic messages to registered users to verify and update their contact information. Super Admin also has the capability to monitor even logs in the system.

9. Are the data secured in accordance with FISMA requirements?

Yes

a. If yes, when was Certification and Accreditation last completed?

VNS is protected by the NRC Telecommunications Infrastructure and is covered under that Certification and Accreditation boundary.

PRIVACY IMPACT ASSESSMENT REVIEW/APPROVAL
(For Use by OIS/IRSD Staff)

System Name: Verizon Notification Service (VNS)

Submitting Office: Office of Information Services

A. PRIVACY ACT APPLICABILITY REVIEW

_X_ Privacy Act is not applicable.

___ Privacy Act is applicable.

Comments:
VNS will maintain personally identifiable information on those employees and or contractors who voluntarily enter their personal contact information into the system. VNS will be used to send broadcast notifications/messages to these individuals that have signed up regarding events or emergency situations based on their office location.

Reviewer's Name	Title	Date
Sally Hardy	Privacy Act Program Analyst	March 13, 2012

B. INFORMATION COLLECTION APPLICABILITY DETERMINATION

_X_ No OMB clearance is needed.

___ OMB clearance is needed.

___ Currently has OMB Clearance. Clearance No._____

Comments:
No OMB clearance is needed for an electronic subscription to an agency notification system; therefore, no OMB clearance is required for the Verizon Notification System.

Reviewer's Name	Title	Date
Kristen Benney	Information Management Analyst	3/12/12

C. RECORDS RETENTION AND DISPOSAL SCHEDULE DETERMINATION

___ No record schedule required.

___ Additional information is needed to complete assessment.

___ Needs to be scheduled

_X_ Existing records retention and disposition schedule covers the system - no modifications needed.

Comments:

The VNS maintains records that are routine requests or quasi-official notices that do not serve as the record of actions; therefore, these records are scheduled under General Records Schedule 23, Item 7, Transitory Files. Disposition: Destroy immediately, or when no longer needed for reference, or according to a predetermined time period or business rule (e.g., implementing the auto-delete feature of electronic mail systems). No modifications to the retention schedule are needed; however, these retentions are mandatory under 44 U.S.C 3303a and retention functionality, or a manual process, must be developed to meet this requirement.

Reviewer's Name	Title	Date
Mary Haynes	Records Management Analyst	March 13, 2012

D. BRANCH CHIEF REVIEW AND CONCURRENCE

_X_ This IT system **does not** collect, maintain, or disseminate information in identifiable form from or about members of the public.

___ This IT system **does** collect, maintain, or disseminate information in identifiable form from or about members of the public.

I concur in the Privacy Act, Information Collections, and Records Management reviews:

/RA/ ***03/27/2012***

_____ Date _____

Russell A. Nichols, Chief
Information Services Branch
Information and Records Services Division
Office of Information Services

TRANSMITTAL OF PRIVACY IMPACT ASSESSMENT/
PRIVACY IMPACT ASSESSMENT REVIEW RESULTS

TO: **Thomas Rich, Director, Infrastructure and Computer Operations Division, OIS**	
Name of System: **Verizon Notification Services (VNS)**	
Date IRSD received PIA for review: **March 7, 2012**	Date IRSD completed PIA review: **March 27, 2012**
Noted Issues: VNS will maintain personally identifiable information on those employees and or contractors who voluntarily enter their personal contact information into the system. Broadcast notifications/messages to these individuals regarding events or emergency situations will be based on their office location. No OMB clearance is needed for an electronic subscription to an agency notification system; therefore, no OMB clearance is required for the Verizon Notification System.	
Russell A. Nichols, Chief Information Services Branch Information and Records Services Division Office of Information Services	Signature/Date: ***/RA/ 03/27/2012***
Copies of this PIA will be provided to: *James Shields, Director(Acting)* *Business Process Improvement and Applications Division* *Office of Information Services* *Paul Ricketts,* *Senior IT Security Officer (SITSO)* *FISMA Compliance and Oversight Team* *Computer Security Office*	