U.S. Securities and Exchange Commission

Assurance Notification Manager (NM)
PRIVACY IMPACT ASSESSMENT (PIA)

February 18, 2016

Office of Information Technology

Privacy Impact Assessment

Assurance Notification Manager (NM)

Publishing History

Document Publication Number	Revision	Date	Changes Made
Initial Document	Initiation	12/23/2015	Document Creation (Replacement for NOTIFIND)
Document update	1		
Document update	2		
Document update	3		
Document update	4		
Document update	5		
Document update	6		

Privacy Impact Assessment
Assurance Notification Manager (NM)

General Information

1. **Name of Project or System.**
   Assurance Notification Manager (NM)

2. **Describe the project and its purpose or function in the SEC's IT environment.**
   Assurance Notification Manager (NM) is an automated alerting service that provides high-speed message delivery to all Commission personnel. The system uses communications devices (such as phone, text messages, email messages, and desktop alerts) to share important information. This system provides alerts, notifications, warnings, and other similar operations in the event of a scheduled exercise or an actual emergency. Messages are either critical in nature, routine, or for testing purposes with appropriate authorization. Messages are generated in response to threat alerts issued by the Department of Homeland Security, weather related emergencies, or other critical situations that disrupt the operations and accessibility of a worksite. The system provides for personnel accountability during an emergency through personnel sign-in and rapid alert notification. Assurance NM will replace the current agency emergency notification system (NOTIFIND, approved March 30, 2007) and will consist of records used by the SEC to maintain emergency contact information on current employees. The system will be externally hosted via SunGard Availability Services, the vendor.

3. **Requested Operational Date?**
   1/15/16

4. **System of Records Notice (SORN) number?**
   Information collected, stored and shared by the Assurance NM System is covered by SEC-51, Emergency Contingency Plan System and SEC-53, Automated Emergency Notification System.

5. **Is this an Exhibit 300 project or system?**
   ☒ No
   ☐ Yes

6. **What specific legal authorities, arrangements, and/or agreements allow the collection of this information?**
   5 U.S.C. allows agency heads to make rules for managing agency employees and permits the collection of this information. The information is collected for inclusion in a Continuity of Operations Program, as described in Executive Order 12656 (November 18, 1988) for the purposes of facilitating contact with personnel in case of an emergency.

Privacy Impact Assessment
Assurance Notification Manager (NM)

Specific Questions

SECTION I - Data in the System

1. **What data about individuals could be collected, generated, or retained?**
   Full name, office phone number, home phone number, SEC issued cell phone number, Blackberry phone number and PIN, SEC email address, and personal email address.

2. **Does the project/system use or collect the social security number (SSN)? (This includes truncated SSNs)**
   ☒ No.
   ☐ Yes. If yes, provide the function of the SSN and the legal authority to collect.

3. **What are the sources of the data?**
   After the initial import of information from the legacy system (NOTIFIND) individual users are responsible for updating their own PII to ensure its accuracy. Information from new users is collected directly from the individual. Users input their contact information using a secure webpage.

4. **Why is the data being collected?**
   Data is being collected to provide alerts, notifications, warnings, and other similar operations in the event of a scheduled exercise, or an actual hazard, threat, or emergency. The PII is used to notify and account for employees in the event of an exercise or an actual emergency situation. The system uses communications devices (such as phone, text messages, email messages, and desktop alerts) as multiple ways to share important information and contact personnel.

5. **What technologies will be used to collect the data?**
   Information is collected directly from SEC personnel. Users login to the system using a secure webpage and input their contact information.

SECTION II - Attributes of the Data (use and accuracy)

1. **Describe the uses of the data.**
   The data is used to notify and account for employees and contractors during emergency situations. Assurance NM provides alerts, notifications, and warnings during all hazards, threats and emergencies.

2. **Does the system analyze data to assist users in identifying previously unknown areas of note, concern or pattern?** ☒ No ☐ Yes If yes, please explain: not applicable

3. **How will the data collected from individuals or derived by the system be checked for accuracy?**
   The SEC assumes the initial accuracy of the PII provided by SEC personnel through import from the legacy system NOTIFIND. After the initial input/import, SEC personnel are responsible for updating their own PII to ensure its accuracy. Periodic (quarterly) emergency exercises are conducted, which require employees to login to the system following an alert from the system via one or more communication devices, to verify and/or update their own information.

SECTION III - Sharing Practices

1. **Will the data be shared with any internal organizations?**
   ☐ No
   ☒ Yes If yes, please list organization(s):

Information from the system will only be shared with authorized internal organizations for a purpose compatible with the purpose of the collection, including the Office of Human Resources, Office of Support Operations, Safety, Emergency Management and COOP Office and the Office of Information Technology. Information may also be shared with the Office of the Inspector General for an authorized purpose.

2. **Will the data be shared with any external organizations?**

☐ No
☒ Yes If yes, please list organizations(s):
SEC does not routinely share Assurance NM information outside of the SEC as part of the normal course of operations. SEC may share information with other federal, state, or local government agencies with mission-specific ties. Any sharing of information from Assurance NM is covered by SORN SEC-51, Emergency Contingency Plan System and SEC-53, Automated Emergency Notification System. These SORNs allow SEC to contact necessary external organizations in the event of an actual emergency, including technical, manmade, or natural disasters, or to participate in exercises. This purpose is consistent with the published routine uses therein, which are compatible with the original purpose of collection.

How is the data transmitted or disclosed to external organization(s)?
Data may be transmitted electronically via secure email (reports), or secure file transfer (data), or encrypted media.

3. **How is the shared data secured by external recipients?**
Prior to sharing data with an external recipient, the recipient must accept and sign a Memorandum of Understanding (MOU). The MOU will delineate specific information security requirements.

4. **Does the project/system process or access PII in any other SEC system?**

☒ No
☐ Yes. If yes, list system(s).

SECTION IV - Notice to Individuals to Decline/Consent Use

1. **What privacy notice was provided to the different individuals prior to collection of data? (Check all that apply)**

☒ Privacy Act Statement: The Assurance NM web portal displays a Privacy Act Statement that must be acknowledged before users input data into the system.
☒ System of Records Notice: Information collected, stored and shared by the Assurance NM System is covered by SEC-51, Emergency Contingency Plan System and SEC-53, Automated Emergency Notification System.
☒ Privacy Impact Assessment: Publishing this PIA mitigates the privacy risk that individuals will not receive notice that their PII is being used for Assurance NM system at the time it is collected.
☐ Web Privacy Policy
☐ Notice was not provided to individuals prior to collection

2. **Do individuals have the opportunity and/or right to decline to provide data?**

☐ Yes ☒ No ☐ N/A Please explain.
SEC employees do not have the opportunity to opt-out of providing PII associated with their SEC-issued devices, such as an SEC cell phone and Blackberry, or their SEC issued email or telephone number. All other personal contact information is provided voluntarily and may be amended at any

time. Personnel who choose not to provide other personal contact information will have fewer methods of contact, which may limit their ability to receive notification messages from certain communication devices.

3. **Do individuals have the right to consent to particular uses of the data?**
☐ Yes ☒ No ☐ N/A Please explain.
SEC employees do not have the opportunity to consent to uses of the data. Information provided voluntarily will be used in accordance with the purpose of the collection for emergency broadcasting.

SECTION V - Access to Data (administrative and technological controls)

1. **Has the retention schedule been established by the National Archives and Records Administration (NARA)?**
☐ No If no, please explain:
☒ Yes If yes, list retention period: Data is maintained for a 2 year period in accordance with the records retention period established by the National Archives and Records Administration (NARA)

2. **What are the procedures for identification and disposition of the data at the end of the retention period?**
Records will be maintained until they become inactive, at which time they will be destroyed in accordance with records schedules of the United States Securities and Exchange Commission and as approved by the National Archives and Records Administration.

3. **Describe the privacy training provided to users, either generally or specifically relevant to the program or system?**
All SEC staff and contractors are required to take annual privacy awareness training, which outlines their roles and responsibilities for properly handling and protecting PII. Assurance NM system managers, and end users are also required to take system-oriented training related to accessing the system and data maintenance.

4. **Has a system security plan been completed for the information system(s) supporting the project?**
☐ Yes If yes, please provide date SA&A was completed:
☒ No If no, please explain: The SA&A in accordance with the requirements of the Federal Information Security Act of 2002 (FISMA) is pending.

5. **Is the system exposed to the Internet without going through VPN?**
☐ No
☒ Yes If yes, Is secure authentication required? ☐ No ☒ Yes; and
Is the session encrypted? ☐ No ☒ Yes

6. **Are there regular (i.e. periodic, recurring, etc.) PII data extractions from the system?**
   ☒ No
   ☐ Yes If yes, please explain:
   A quarterly statistical report is generated from scheduled exercises or an actual emergency. The report does not include PII. The statistics of responders and non-responders will be generated based on information in the system. This report is provided to only authorized users.

7. **Which user group(s) will have access to the system?**
   The SEC Office of Information Technology system managers, Office Human Resources authorized staff, and staff in the OSO, Safety, Emergency Management and COOP Office will have access to the data in the system.

8. **How is access to the data by a user determined?**
   The system uses a role-based access control mechanism for data and functionality. Permissions for the data and functions used to manipulate the data have been pre-defined for each type of user based on the principles of separation of duties and "need to know". SEC employees will have restricted, role-based, access limited to the extent necessary to perform official duties associated with operations and maintenance of the system. SunGard employees (i.e., contractors) will also have limited access to support the troubleshooting of technical system issues encountered on a day-to-day basis. SEC end users will have access only to the extent necessary to perform their official duties, including the ability to review and update their own information.

   Are procedures documented? ☒ Yes ☐ No

9. **How are the actual assignments of roles and rules verified?**
   The Office of Human Resources or the head of an office/division will assign a sub-administrator who will be responsible for reviewing the list of users in that office/division. If an employee no longer works for the SEC or otherwise no longer needs access to the system, their access/password will be deleted by the Office of Human Resources. Individual users are only able to review and update their own information.

10. **What auditing measures/controls and technical safeguards are in place to prevent misuse (e.g., unauthorized browsing) of data?**
    The Assurance NM system utilizes Principles of Least Privilege, Separation of Duties, and Business Need to Know for access to production servers and information collected on behalf of the SEC. The system logs all changes made to the information collection. The logs are maintained throughout the lifecycle of the system. Additionally, the system maintains an audit history of access activity, which SEC staff can review and run activity reports, as needed, for internal auditing and compliance requirements. Access activity logs consist of date and timestamp, and all logins to the system by username, including password resets. Role-based access controls are also included, as additional technical safeguards.

SECTION VI - Privacy Analysis

Given the amount and type of data being collected, discuss what privacy risks were identified and how they were mitigated.

Privacy risks associated with Assurance NM is the possibility of unauthorized use of PII, unauthorized disclosure of PII, and inaccurate data. The SEC mitigates the risks of unauthorized use and unauthorized

disclosure by: limiting the data in Assurance NM to data that is necessary, limiting access to the system to only persons with a business need to know and implementing role-based access controls, maintaining audit logs of all access activity, and requiring sharing with external parties to be governed by written Memoranda of Understanding (MOU) and limited to the routine uses set forth in System of Records Notices (SORN) SEC-51, Emergency Contingency Plan System and SEC-53, Automated Emergency Notification System. The SEC mitigates the risk of inaccurate data by having each individual maintain their own information.