Department of the Treasury
BUREAU OF ENGRAVING AND PRINTING

AtHoc Mass Notification System

November 5, 2015

A. Contact Information

[redacted]

B. System Application/General Information

1. **Does this system contain any PII? [ ] No [X] Yes**

2. **What is the purpose of the system/application?**

   The Bureau of Engraving and Printing (BEP), DCF's Office of Security - Emergency Management Division and WCF's Security Division will establish an emergency notification system utilizing the cloud-based AtHoc Mass Notification System (AtHoc) a unified crisis interactive communication solution suite. Authorized personnel will use a web-based interface to compose emergency broadcast notices, messages, and instructions to BEP employees and contractors. Emergency notifications will be sent to work and/or personal email, cell, office, or home phones (or any combination as deemed appropriate for the emergency situation). Message recipients will be able to acknowledge receipt of the notifications. AtHoc will have the capability to aggregate metrics associated with responses and determine individuals who have not responded to the notification.

   An interactive emergency notification capability is necessary in response to natural disasters, work place violence, and terrorist threats. This capability will allow WCF's Security Division and the DCF's Office of Security personnel to inform personnel of the adverse situation, coordinate user response (e.g. shelter-in-place, evacuate, etc.), and, if necessary, identify personnel who might be trapped or require assistance responding to the incident.

3. **What legal authority authorizes the purchase or development of this system/application?**

   5 U.S.C. § 301; 31 U.S.C. § 321

4. **Under which SORN does the system operate? (Provide name and number)**

   OPM/GOVT-1, General Personnel Records, 77 Fed. Reg. 73694 (December 11, 2012). Treasury .015 – General Information Technology Access Account Records, 80 Fed. Reg. 1988 (January 14, 2015).

C. Data in the System

1. **What categories of individuals are covered in the system? (e.g., employees, contractors, taxpayers, other)**

   Covered individuals include BEP employees and contractors working at the DCF and WCF.

2. **What are the sources of information in the system?**

a. Is the source of the information from the individual or is it taken from another source? If not directly from the individual, then what other sources?

The BEP Windows Active Directory (AD) will provide the following information about BEP employees and contractors for AtHoc:

- Individual's name;
- Individual's home phone number;
- Personal cell phone number;
- Personal email address;
- BEP office phone number;
- BEP cell phone number and
- BEP email address.

BEP employees and contractors will provide the home phone number, personal cell phone number, and personal email address voluntarily in the BEP Windows AD. AtHoc will ingest a manually derived, user initiated extract from AD on a monthly basis.

b. What Federal agencies are providing data for use in the system?

The BEP Windows Active Directory System will provide the contact information of employees and contractors to populate AtHoc. No other Federal agency will provide data for use in this system.

c. What state and/or local agencies, tribal governments, foreign governments, or international organizations are providing data for use in the system?

No state and/or local agencies, tribal governments, foreign governments, or international organizations will provide data for use in this system.

d. From what other third party sources will data be collected?

No third party sources will provide data to AtHoc.

e. What information will be collected from employees, government contractors and consultants, and the public?

The data AtHoc will collect from BEP Windows Active Directory is:

- Name;
- BEP Office Phone Number;
- BEP Cell Phone Number; and
- BEP Email Address.
- Home Phone Number (provided voluntarily);
- Personal Cell Phone Number (provided voluntarily); and

- Personal Email Address (provided voluntarily).
  The AtHoc system will collect the following information:

- Number of Times of Attempted Contact;
- Time Attempt Was Made;
- Date and Time Employee or Contractor Response Received;
- Employee or Contractor Response Status; and
- Employee or Contractor Response during the Incident.

  The AtHoc system will also track the following information:

- BEP employee (User) who executed a scenario including the date and time of execution; and
- BEP employee (User) who edited personnel information in the system including the date, time, and what object was modified.

3. Accuracy, Timeliness, and Reliability

a. How is data collected from sources other than from Treasury records going to be verified for accuracy?

There is no data collected from other sources.

b. Is completeness required? [X] No [] Yes

c. What steps or procedures are taken to ensure the data is current and not out-of-date?

Each individual is responsible for maintaining changes to his/her name or personal contact information within Windows AD. The data in AtHoc will be updated based on these events in one of two ways: by an AtHoc Administrator or an updated file extraction from Windows AD.

d. Are the data elements described in detail and documented? [ ] No[X] Yes

If yes, what is the name of the document?

AtHoc is a commercial product and the data elements are described in the AtHoc User's Manual.

D. Attributes of the Data

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

The WCF's Security Division and the DCF's Office of Security need the data to inform BEP personnel of any emergency and identify personnel who might require assistance during the incident, if necessary.

2. **Will the system derive new data or create previously unavailable data about an individual through aggregation from the information collected, and how will this be maintained and filed? [] No [X] Yes**

   The system will be able to create new data about BEP employees and contractors such as logs of when the alert was sent, when the individual viewed the alert, when they responded to the alert, and the response. AtHoc will have the capability to aggregate metrics associated with the individual's responses and determine who have not responded to the notification. This data will be used to generate reports on who has received and responded to notifications.

3. **Will the new data be placed in the individual's record?** [] No [X] Yes

   New data is event centric, meaning as an alert is sent, a list of each individual it is sent to is maintained within the event record. An individual's record contains the originally extracted data from Windows AD plus the event records participation, which can be reported.

4. **Can the system make determinations about employees/members of the public that would not be possible without the new data?**

   Yes. The AtHoc system can determine whether an individual has received / viewed the message and can determine if the individual has responded to the message.

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

   The new data will not be verified for relevance and accuracy. The data collected in the execution of a notification event is assumed to be accurate. However, as is often the case, a notification event will uncover required changes in an individual's contact information when an individual is unable to be contacted with the existing information. The System Manager of AtHoc will request the individual to make any corrections or changes to their contact information provided in Windows AD.

6. **If the data is being consolidated, what controls are in place to protect the data from unauthorized access or use?**

   Access to the on-line data is limited to approved WCF's Security Division and the DCF's Office of Security personnel with a system of user IDs and passwords. Access to any hardcopy reports generated is limited to the WCF's Security Division and the DCF's Office of Security personnel. Records are maintained in locked file cabinets. Only authorized users have access to the area that houses the file cabinets. Rooms are locked when not manned by cleared personnel.

7. **If processes are being consolidated, are the proper controls remaining in place to protect the data and prevent unauthorized access? Explain.**

   N/A. Processes are not being consolidated.

8. **How will the data be retrieved? Is the data retrieved by a personal identifier? If yes, explain and list the identifiers that will be used to retrieve information on the individual.**

   The data in AtHoc will be retrieved by the individual's name or contact information to include BEP email, BEP phone number, BEP cell phone number, personal email, personal cell or home phone number.

9. **What kinds of reports can be produced on individuals? What will be the use of these reports? Who will have access to them?**

   Reports are generated during an event execution at specific time periods and at the conclusion of the event showing the status of the notification. The reports produced during the event will provide the name of the individual, number of attempted contacts by device, (i.e., personal/work phone number, personal/work email), time attempt was made, time response received and the employee/contractor response. There is also summary data presented for that time period showing number of personnel to be notified, number of notifications attempted and number of responses received. The report generated at the end of the event is summary data including number of personnel to be contacted, number of contacts attempted, and number of responses received.

   These reports will be used to determine what further actions need to be taken to reach the individual and the success of the notification event.

   A report showing the name and contact information can also be brought up on the screen in order to edit an individual's data.

   Approved WCF's Security Division and the DCF's Office of Security personnel can generate these reports based on the role they have been assigned.

E. Maintenance and Administrative Controls

1. **If the system is operated in more than one site, how will consistent use of the system and data be maintained in all sites?**

   The system is operated at a single contractor facility with a back-up location. The AtHoc service provided ensures the data is consistent at both sites.

2. **What are the retention periods of data in the system?**

Records are retained and disposed in accordance with the National Archives and Records Administration (NARA), General Records Schedule No. 18, (items 26 and 28).

3. **What are the procedures for disposition of the data at the end of the retention period? How long will the reports produced be kept? Where are the procedures documented?**

   Paper records beyond their retention period are destroyed by shredding or burning. Electronic records beyond their retention period are electronically erased using accepted techniques. Reports generated are retained in accordance with NARA GRS 18, Items 26 or 28.

   The procedures used to facilitate this process are documented in BEP Circular No. 80-05, Records Management Program (2006); BEP Circular No. 80-05.3, Records Storage (2007); and BEP Circular No. 80-05.4, Policies and Procedures for Electronic Records and Email (2006).

   The WCF's Security Division, the DCF's Office of Security and the Office of Critical Infrastructure and IT Security are responsible for ensuring that records are preserved, records no longer of current use are promptly destroyed, retention schedules are implemented and that the BEP complies with the recordkeeping requirements issued by the Department of the Treasury, National Archives and Records Administration, Office of Management and Budget, and the National Institute of Standards and Technology.

4. **Is the system using technology in ways the office or bureau has not previously employed (e.g., monitoring software, Smart Cards, Caller-ID)? If yes, explain.**

   Yes. This is the first time BEP has used a cloud based model for performing emergency notification functions. In this model, the PII data and the application acting on the PII data to perform and track notification events are located on computers owned and operated by a contractor. Authorized BEP employees from WCF's Security Division and the DCF's Office of Security manage the data, scenarios, and event execution.

5. **How does the use of this technology affect public/employee privacy?**

   The cloud based model stores a set of individual's contact information in a secure location not on the BEP's IT infrastructure and uses this data under the control of approved BEP personnel. The cloud infrastructure and application has been designed specifically for this purpose and is used by numerous Government and Military organizations. AtHoc Cloud Services is certified per NIST SP 800-53 Rev 4 (at a moderate FIPS 199 classification), complying with government and DoD security mandates. BEP employees and contractors will be notified that their personal information in AtHoc will be stored in Windows AD and a cloud service owned by the contractor.

6. **Will the system provide the capability to identify, locate, and monitor individuals? If yes, explain.**

Yes. The AtHoc Mass Notification System has the capability to identify and monitor whether an individual has received and responded to an emergency notification.

7. **What kind of information is collected as a function of the monitoring of individuals?**

   AtHoc collects information on attempts to contact an individual and their response.

8. **What controls will be used to prevent unauthorized monitoring?**

   Only approved WCF's Security Division and the DCF's Office of Security personnel are provided access to the data.

9. **Under which SORN does the system operate? (Provide name and number)**

   OPM/GOVT-1, General Personnel Records, 77 Fed. Reg. 73694 (December 11, 2012). Treasury .015 – General Information Technology Access Account Records, 80 Fed. Reg. 1988 (January 14, 2015).

10. **If the system is being modified, will the SORN require amendment or revision? Explain.**

    The system is not being modified.

F. Access to Data

1. **Who will have access to the data in the system? (e.g., contractors, users, managers, system administrators, developers, others).**

   Approved WCF's Security Division and the DCF's Office of Security personnel are provided access to the data.

2. **How is access to the data by a user determined? Are criteria, procedures, controls, and responsibilities regarding access documented?**

   Users must complete the BEP System Access Request Identity Manager Form requesting access to the system and be approved for access by an authorized BEP personnel. Users are granted access based on their roles and need- to- know. Criteria, procedures, controls, and responsibilities regarding access to the system are documented in the access control portion of the AtHoc system security plan.

3. **Will users have access to all data on the system or will the user's access be restricted? Explain.**

   Users are granted restricted access based on their roles and need -to -know.

4. **What controls are in place to prevent the misuse (e.g., unauthorized browsing) of data by those having access? List procedures and training materials.**

   Users participate in the mandatory Annual Privacy Awareness Training sponsored by the Department of the Treasury, Office of Privacy and Civil Liberties (OPCL) and the Records Management-Employees and Contractors Training sponsored by the Department of the Treasury, Office of Privacy, Transparency, and Records (OPTR).

5. **Are contractors involved with the design and development of the system and will they be involved with the maintenance of the system?**

   AtHoc is a commercial off-the-shelf capability developed and maintained by Blackberry.

6. **Do other systems share data or have access to the data in the system? If yes, explain.**

   No.

7. **Who will be responsible for protecting the privacy rights of the public and employees affected by the interface?**

   N/A

8. **Will other agencies share data or have access to the data in this system?**

   [] Federal **[] State** **[X] Local** **[ ] Other**

   Local authorities may have access to AtHoc data as first responders to an emergency situation.

9. **How will the data be used by the other agency?**

   Local authorities may utilize the data to assist the BEP in urgent situations.

10. **Who is responsible for assuring proper use of the data?**

    Chief, DCF Office of Security
    Manager, WCF Security Division

The Following Officials Have Approved This Document