Affects Members Of the Public? □

Department of Energy

Privacy Impact Assessment (PIA)

MODULE I – PRIVACY NEEDS ASSESSMENT

Date	June 21, 2023
Departmental Element & Site	Office of the Chief Information Officer; DOE Headquarters and other EITS locations
Name of Information System or IT Project	Department of Energy, Alert, Warning, and Response (DOE-AWARe) Blackberry AtHoc (Major App.)
Exhibit Project UID	Purchase through GSA to AtHoc: GS-35F-0218V
New PIA □ **Update** ☒	Periodic update to the 2022 PIA for this system required for yearly assessment. No material changes to the system.

	Name, Title	Contact Information Phone, Email
System Owner	John Gossel Emergency Management Specialist Enterprise Operations and Shared Services (IM-60)	1000 Independence Avenue, S.W. Washington DC 20585 202-586-7619 John.Gossel@hq.doe.gov
Local Privacy Act Officer	Brooke Dickson Director of Privacy Management and Compliance Office of the Chief Information Officer, IM-42	1000 Independence Avenue, S.W. Washington DC 20585 202-287-5786 Brooke.Dickson@hq.doe.gov

MODULE I – PRIVACY NEEDS ASSESSMENT

Cyber Security Expert reviewing this document (e.g. ISSM, CSSM, ISSO, etc.)	Manda Shu-Nyamboli Information System Security Officer (ISSO) Security and Compliance, IM-63	19901 Germantown Road Germantown, MD 20874 301-903-0102 Manda.shu-nyamboli@hq.doe.gov
Person Completing this Document	John Gossel Emergency Management Specialist Enterprise Operations and Shared Services (IM-60)	1000 Independence Avenue, S.W. Washington DC 20585 202-586-7619 John.Gossel@hq.doe.gov
Purpose of Information System or IT Project	Department of Energy (DOE) Alert, Warning, Accountability, and Response (DOE-AWARe) (offered as a Software-as-a-Service(SaaS)) is an emergency notification system that utilizes BlackBerry AtHoc Cloud Services for government (ACSforGov). During an emergency or a critical need, BlackBerry AtHoc Services provides a seamless and trusted exchange between organizations, their people, devices, and any external entity. It provides functionality for desktop alerts as well as Continuity of Operations Plan (COOP) notifications and accountability reporting. It is utilized by DOE Headquarters, LLNL, and OROSC. The system is 100% cloud-based except for a desktop agent which provides desktop alerts to users. Other alerts provided by the system are sent via Department of Energy (DOE) or personal, email address, or telephone number. The system is a service which provides alerts to users. Alerts produced by the system are sent to a DOE email address or SMS text message device or telephone via a voice response system. Alerts can be triggered and input only by operators with alert publishing rights in the system. Alert types can be various levels of emergencies (categories in the system are Chemical, Biological, Radiological and Nuclear Defense (CBRNE), Environmental, Fire, Geophysical, Health, Infrastructure, Meteorological, Rescue, Safety, Security, Transportation, and Other) with High, Moderate, Low, and Informational severity levels. This system will hold e-mail addresses, building locations, Active Directory user IDs (logon ID's), DOE Unique Identifiers (DUID), DOEInfo GUID, business mailing address, duty station locations, building names, office/room numbers, and program office codes. Users have the option to voluntarily provide personal information such as home phone number, cell phone number and personal email address. This PII is necessary to the purpose of the system, to wit: providing alerts and notifications.	
Type of Information Collected or Maintained by	□ SSN □ Medical & Health Information	

MODULE I – PRIVACY NEEDS ASSESSMENT

the System:	☐ Financial Information ☐ Clearance Information ☐ Biometric Information ☐ Mother's Maiden Name ☐ DoB, Place of Birth ☐ Employment Information ☐ Criminal History ☒ Name, Phone, Address (work addresses only) ☒ Other – Please Specify - This system will hold e-mail addresses, building locations, Active Directory user IDs (logon ID's), DOE Unique Identifiers (DUID), DOEInfo GUID, business mailing address, duty station locations, building names, office/room numbers, and program office codes. Users have the option to voluntarily provide personal information such as home phone number, cell phone number and personal email address.

Has there been any attempt to verify PII does not exist on the system? **DOE Order 206.1, *Department of Energy Privacy Program,* defines PII as** *any information collected or maintained by the Department about an individual, including but not limited to, education, financial transactions, medical history and criminal or employment history, and information that can be used to distinguish or trace an individual's identity, such as his/her name, Social Security number, date and place of birth, mother's maiden name, biometric data, and including any other personal information that is linked or linkable to a specific individual.*	PII exists.
If "Yes," what method was used to verify the system did not contain PII? (e.g. system scan)	Not Applicable

Threshold Questions

1. Does system contain (collect and/or maintain), or plan to contain any information about individuals?	Yes
2. Is the information in identifiable form?	Yes

MODULE I – PRIVACY NEEDS ASSESSMENT

3. Is the information about individual Members of the Public?	No
4. Is the information about DOE or contractor employees?	Yes ☒ Federal Employees ☒ Contractor Employees

END OF PRIVACY NEEDS ASSESSMENT

MODULE II – PII SYSTEMS & PROJECTS

AUTHORITY, IMPACT & NOTICE

1. AUTHORITY **What specific authorities authorize this system or project, and the associated collection, use, and/or retention of personal information?**	• Department of Energy Authorization Act, Title 42, United States Code (U.S.C), Section 7101 et. seq. • Federal Information Security Modernization Act of 2014
2. CONSENT **What opportunities do individuals have to decline to provide information (e.g. where providing information is voluntary) or to consent only to particular uses of the information (other than required or authorized uses)?**	Work contact information is a requisite of the system and of employment for safety and accountability purposes. Users may decline to provide additional personal information.

MODULE II – PII SYSTEMS & PROJECTS	
3. CONTRACTS **Are contractors involved with the design, development and maintenance of the system? If yes, was the Privacy Order CRD or Privacy Act clauses included in their contracts?**	No. This is a service provided as Software as a Service (SaaS). DOE does not design, develop, or maintain any part of the system (i.e, we do not design or maintain any of the code nor do we operate any infrastructure on which the product runs). DOE merely operates the system. All system design, development, and maintenance is done by the vendor.
4. IMPACT ANALYSIS: **How does this project or information system impact privacy?**	The system contains work-related PII consisting primarily of low sensitivity administrative employment information. Should PII in the system be compromised, it could result in a moderate adverse impact to individuals. The compromise could cause personal harm to individuals including embarrassment and professional harm which may translate into financial or social harm. DOE AWARe observes a number of protections to protect privacy and via the Fair Information Practice Principles (FIPPs). DOE AWARe maintains the minimum PII necessary for its business purpose to mitigate privacy harm. In addition, use of the PII in DOE AWARe is limited to clearly defined business purposes. Access to and use of PII in the system is protected by a series of controls including role and permission-based monitoring controls. Users have access to their information to ensure the accuracy and currency of PII in the system. DOE AWARe system administrators/operators have access to the information. The Office of the Chief Information Officer (OCIO) provides technical support and system administration support for the DOE AWARe system. Approved OCIO system administrators have access to the user data. DOE AWARe operators are assigned by the NNSA Continuity Office or the Headquarters Office of Environment, Safety, and Health. Operators are assigned access rights via role based security. The application roles limit access to view or modify user data, to publish alerts, and to perform system administrative functions to authorized operators. The Office of the CIO tracks and documents user requests for access.

MODULE II – PII SYSTEMS & PROJECTS

5. SORNs **How will the data be retrieved? Can PII be retrieved by an identifier (e.g. name, unique number or symbol)?** **If yes, explain, and list the identifiers that will be used to retrieve information on the individual.**	PII can be retrieved by individual name. For each individual alert, data can be queried or displayed in reports. Information on users can be queried by name or attribute (e.g., building name, routing symbol, work address, etc.)
6. SORNs **Has a Privacy Act System of Records Notice (SORN) been published in the *Federal Register*?** **If "Yes," provide name of SORN and location in the *Federal Register*.**	• DOE-11, Emergency Operations Notification Call List, 74 FR 1011 • DOE-17, DOE Alert System, 74 FR 1019
7. SORNs **If the information system is being modified, will the SORN(s) require amendment or revision?**	N/A
DATA SOURCES	
8. What are the sources of information about individuals in the information system or project?	Active Directory, ESS/MIS/DOEInfo, and optional user-provided personal contact information.
9. Will the information system derive new or meta data about an individual from the information collected?	Yes, the system collects metadata. The system records the date and time the user last responded to an alert and what method they used to respond (i.e., phone, SMS text, e-mail). Metadata regarding the user's last logon to a computer running the AtHoc desktop client is also collected, including logon time, IP address, system name, and operating system logon id.
10. Are the data elements described in detail and documented?	Yes. See System Security Plan.

MODULE II – PII SYSTEMS & PROJECTS

DATA USE

11. How will the PII be used?	PII is only used to target alerts to users.
12. If the system derives meta data, how will the new or meta data be used? **Will the new or meta data be part of an individual's record?**	The metadata is used to verify personnel accountability status for the employee or contractor. This information becomes part of the user's record.
13. With what other agencies or entities will an individual's information be shared?	None.

REPORTS

14. What kinds of reports are produced about individuals or contain an individual's data?	Personnel accountability reports, user account information (which can include all data elements), alert status reports, alert response reports . The reports can show (1) when the alert was sent; (2) to which devices the alert was sent (e.g., telephone, SMS text device, email address); (3) if and when the user responded to the alert (date and time); (4) the specific response from the user selected from a list of pre-defined responses; (5) the device the user responded from (e.g., e-mail, phone).
15. What will be the use of these reports?	To provide for personnel accountability during an emergency, to verify user data in the system, to report on the response rate for a sent alert, AND to verify if and how a user responded to an alert.
16. Who will have access to these reports?	DOE AWARe administrators will have access. Access is granted upon approval for the Office of the Chief Human Capital Officer (HC), Advanced Alert Manager, Advanced Alert Publisher, Alert Manager, Alert Publisher, Distribution Lists Manager, Draft Alert Creator, End Users Manager, Report Manager ,SDK User, Accountability Manager, and Accountability Officer and is restricted based on role-based security rules.

MODULE II – PII SYSTEMS & PROJECTS

MONITORING

17. Will this information system provide the capability to identify, locate, and monitor individuals?	The system contains work location information and monitors alert responses.
18. What kinds of information are collected as a function of the monitoring of individuals?	The system records the date and time the user last responded to an alert and what method they used to respond (i.e., phone, SMS text, e-mail). Information regarding the user's last logon to a computer running the AtHoc desktop client is also collected, including logon time, IP address, system name, and operating system logon id.
19. Are controls implemented to prevent unauthorized monitoring of individuals?	The system implements a series of administrative and technical controls to prevent unauthorized monitoring and data use including role-based access controls with technical safeguards.

DATA MANAGEMENT & MAINTENANCE

20. How will records about individuals be kept current and verified for accuracy, relevance and completeness? Include PII data collected from sources other than DOE records.	The work information is collected exclusively from individuals and DOE sources including ESS/MIS/DOEInfo and Active Directory. These systems have protocols in place to ensure the accuracy of information. Please see system-specific compliance documentation for more information. User self-service information is manually entered and verified via correlation with authoritative data sources. Additional personal information is provided at the discretion of the user. The user has access to update their personal information, as appropriate.
21. If the information system is operated in more than one site, how will consistent use of the information be ensured at all sites?	N/A

RECORDS MANAGEMENT

MODULE II – PII SYSTEMS & PROJECTS

22. Identify the record(s).	Data within AtHoc are held in the form of alert recipient records. The primary record types in AtHoc are: (1) User records – retained until the employee separates from the Department (2) Alert response history – retained until the alert history is cleared from the system by an administrator (3) Alerts (4) Employee emergency contact information
23. Identify the specific disposition authority(ies) that correspond to the record(s) noted in no. 22.	GRS 5.3, item 020 Emergency alerts and all emergency response records are currently unscheduled records.
24. Records Contact	Christie Flora christie.flora@hq.doe.gov 301-903-2560
ACCESS, SAFEGUARDS & SECURITY	
25. What controls are in place to protect the data from unauthorized access, modification or use?	The system implements a series of administrative and technical controls to prevent unauthorized access and data use including role-based access controls with technical safeguards.The AtHoc System Security Plan (SSP) details the controls to protect the data following the NIST RMF guidance.
26. Who will have access to PII data?	AtHoc system operators (COOP Coordinators, Human Capital personnel, and system vendor) have access to user PII based on approved role-based permissions. Users will have access to their own PII via their system user profile.
27. How is access to PII data determined?	Access is determined through account management using groups and roles based on a need to know.
28. Do other information systems share data or have access to the data in the system? If yes, explain.	No.

MODULE II – PII SYSTEMS & PROJECTS

29. For connecting information systems, is there an Interconnection Security Agreement (ISA) or other agreement between System Owners to ensure the privacy of individuals is protected?	N/A
30. Who is responsible for ensuring the authorized use of personal information?	AtHoc Operators, COOP Coordinators, and operators from the Office of Human Capital.

END OF MODULE II

SIGNATURE PAGE

	Signature	Date
System Owner	**John Gossel** **(Print Name)** John C. Gossel Digitally signed by John C. Gossel Date: 2023.06.26 12:56:31 -04'00' **(Signature)**	
Local Privacy Act Officer	**Brooke Dickson** **(Print Name)** Brooke J. Dickson Digitally signed by Brooke J. Dickson Date: 2023.06.26 12:46:39 -04'00' **(Signature)**	
Chief Privacy Officer	**Ken Hunt** **(Print Name)** William K. Hunt Digitally signed by William K. Hunt Date: 2023.06.23 16:06:34 -04'00' **(Signature)**	