Affects Members Of the Public?	Mark if Applicable w/ an X

Department of Energy

Privacy Impact Assessment (PIA)

Guidance is provided in the template. See DOE Order 206.1, Department of Energy Privacy Program, Appendix A, Privacy Impact Assessments, for requirements and additional guidance for conducting a PIA: https://www.directives.doe.gov/directives-documents/200-series/0206.1-BOrder/@@images/file

Please complete form and return via email to Privacy@hq.doe.gov

No hand-written submissions will be accepted.

This template may not be modified.

MODULE I – PRIVACY NEEDS ASSESSMENT

Date	04/18/2024	
Departmental Element & Site	Fossil Energy and Carbon Management/National Energy Technology Laboratory	
Name of Information System or IT Project	RedSky E911	
Exhibit Project UID		
New PIA ☒ **Update** □		
	Name, Title	**Contact Information Phone, Email**
System Owner	Roger Rhoads	(O) 304-285-0259 roger.rhoads@netl.doe.gov
Local Privacy Act Officer	Ann Guy	(M) (202) 555-1212 Ann.Guy@netl.doe.gov

MODULE I – PRIVACY NEEDS ASSESSMENT

Cyber Security Expert reviewing this document (e.g. ISSM, CSSM, ISSO, etc.)	Justin Woodford	(O) (541) 918-4508 justin.woodford@netl.doe.gov
Person Completing this Document	Jordan Niphanprasart	(M) (541) 801-0291 jordan.niphanprasart@netl.doe.gov
Purpose of Information System or IT Project	RedSky Enhanced Emergency (E911) serves a critical function in ensuring the safety and security of individuals within National Energy Technology Labs (NETL), particularly of legislative initiatives like Kari's Law and Ray Baum's Act. It is used by many different organizations within the Federal Government. At its core, RedSky E911 provides dynamic location support and an intricate network infrastructure that effectively routes emergency 911 calls to the appropriate Public Safety Answering Points (PSAPs) across the United States. These capabilities are essential for complying with these important legal mandates and enhancing the overall emergency response system. Many organizations utilize this service; it is the recommended system to route 911 calls by Cisco for the Cisco Jabber application. Kari's Law mandates that all multi-line telephone systems in the United States must enable direct access to 911 without the need for an initial prefix or other dialing code. RedSky E911 aligns with Kari's Law by ensuring that emergency 911 calls can be placed promptly without any hindrances, helping save crucial time during critical situations. Ray Baum's Act requires organizations to transmit accurate location information to emergency service providers, ensuring that first responders can reach those in need as quickly as possible. RedSky E911 provides dynamic location support, accurately pinpointing the caller's location, and routing calls to the nearest PSAP, thus aiding compliance with Ray Baum's Act and further enhancing the safety of employees and visitors. The information is stored on-prem on NETL’s CUCM-ER as well as in the Redsky E911 cloud. The integration of RedSky E911 with the Cisco Jabber soft-phone simplifies the process of initiating an emergency call, allowing users to connect with the appropriate authorities and reducing administrative overhead. RedSky Enhanced Emergency (E911) ensures compliance with Kari's Law and Ray Baum's Act. Its features, such as the emergency call management portal and integration with Cisco Jabber, make it an indispensable tool for NETL to prioritize the safety and security of personnel.	

MODULE I – PRIVACY NEEDS ASSESSMENT

Type of Information Collected or Maintained by the System:	□ SSN Social Security number □ Medical & Health Information e.g. blood test results □ Financial Information e.g. credit card number □ Clearance Information e.g. "Q" □ Biometric Information e.g. finger print, retinal scan □ Mother's Maiden Name □ DoB, Place of Birth □ Employment Information □ Criminal History ☒ Name, Phone, Address ☒ Other – Please Specify Location

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 on the system.
If "Yes," what method was used to verify the system did not contain PII? (e.g. system scan)	N/A

Threshold Questions

1. Does system contain (collect and/or maintain), or plan to contain any information about individuals?	YES

MODULE I – PRIVACY NEEDS ASSESSMENT

2. Is the information in identifiable form?	YES
3. Is the information about individual Members of the Public?	NO
4. Is the information about DOE or contractor employees?	YES X Federal Employees X Contractor Employees

If the answer to **all** four (4) Threshold Questions is "**No**," you may **proceed to the signature page** of the PIA. Submit the completed PNA with signature page to the CPO.

Module II must be completed for all systems if the answer to any of the four (4) threshold questions is "Yes." All questions must be completed. If appropriate, an answer of N/A may be entered.

The goal of the threshold questions is to legitimately and efficiently determine whether additional assessment is necessary. If there is doubt, it is in the System Owner's best interest to complete Module II.

PIAs affecting Members of the Public are posted on the DOE Privacy website. For this reason, PIAs affecting Members of the Public should be written in plain language and at a high level so they are easily understandable and do not disclose sensitive information.

END OF PRIVACY NEEDS ASSESSMENT

MODULE II – PII SYSTEMS & PROJECTS

AUTHORITY, IMPACT & NOTICE

MODULE II – PII SYSTEMS & PROJECTS

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.
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)?**	Individuals using the RedSky E911 integration with Cisco Jabber can choose to accept or decline sharing their personal information, including location data. Declining will result in the removal of Cisco Jabber, offering users a choice while ensuring emergency service functionality.
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?**	Contractors are onboarded to assist with the design, development and maintenance of PTS and Occupational Health Management (OHM). Privacy Act clauses are included in the contracts. Depending upon the type of contract awarded, one or more of the clauses listed below is included: • Compliance with Applicable Federal, State, and Local Requirements; • Confidentiality of Information; • Security and Personnel Requirements; • 52.224-1 Privacy Act Notification (Apr 1984); • 52.224-2 Privacy Act (Apr 1984); • 52.239-1 Privacy or Security Safeguards (Aug 1996); • 952.204-77 Computer Security (Aug 2006).

MODULE II – PII SYSTEMS & PROJECTS

4. IMPACT ANALYSIS: **How does this project or information system impact privacy?**	DOE has assessed RedSky E911 as a moderate-risk system according to the criteria set forth in Federal Information Processing Standard 199 established by the National Institute of Standards and Technology (NIST). The risk rating is used to determine the effect to the agency should the system's confidentiality, integrity or availability be compromised. The unauthorized disclosure of information contained in the system is expected to have a serious adverse effect on individuals' privacy. The system contains highly sensitive PII. Should sensitive PII in the system be compromised, it would result in significant privacy harm to individuals potentially including financial harm, professional harm, and it would damage the trust between individuals and the Federal Government. Authorized users of RedSky E911 are the subject of a favorably adjudicated background investigation and receive extensive training on the use and protection of PII. The system maintains the minimum PII necessary for its business purpose to mitigate privacy harm. In addition, use of the PII in is limited to clearly defined business purposes. Security controls have been implemented and processes are in place to ensure that access is restricted. The RedSky E911 system is designed to protect PII and mitigate privacy risk via the following administrative, technical, and physical controls: • Strict access control enforcement based on need-to-know • System reviews • Encryption of data at rest and data in transit

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.**	The retrieval of data within the RedSky E911 system is input by the user and primarily based on the location information of the individual initiating an emergency call. The individuals address/building # will be sent to the PSAP based on whomever placed the call and the information that is put into the RedSky database. The information is sent using HTTP Enabled Location Delivery (HELD) protocol. This data helps route the call to the appropriate Public Safety Answering Point (PSAP). Personal Identifiable Information (PII) such as an individual's name or unique identifier is typically not used to retrieve information within the system, and would only be used by an administrator to assist with updating user information on their request.. Instead, location data, often determined through the phone number of the device, is the primary identifier for routing the emergency call. The system prioritizes privacy and data protection by avoiding the unnecessary use of PII for routing and handling emergency calls. Only System Administrators can access PII information from the RedSky database. The focus is on efficient and accurate location-based routing to local authorities, which is a fundamental component of E911 services. However, specific implementations and organizational practices may vary, so it's essential to review the system's policies and practices to understand how PII is handled and if it is used as an identifier for any specific purposes. If an administrator were to search for individuals the search result would show full name, current address, phone number, email address, and business affiliation.
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*.**	OPM GOVT-1 General Personnel Records DOE-2 DOE- Personne; Supervisor Maintained Personnel Records DOE-11 Emergency Operations Notification Call List DOE-60 General Correspondence Files

MODULE II – PII SYSTEMS & PROJECTS

7. SORNs **If the information system is being modified, will the SORN(s) require amendment or revision?**	No
DATA SOURCES	
8. What are the sources of information about individuals in the information system or project?	A user's home address is pulled from Cisco emergency responder. If a user connects to a new WiFi network, they will be prompted to enter their physical location.
9. Will the information system derive new or meta data about an individual from the information collected?	No
10. Are the data elements described in detail and documented?	N/A
DATA USE	
11. How will the PII be used?	PII used for routing emergency calls and aiding emergency responders in identifying and assisting individuals during critical situations. Its use is limited to the specific purpose of emergency response, ensuring privacy and data security.
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?**	N/A
13. With what other agencies or entities will an individual's information be shared?	Shared with authorized emergency response agencies, including Public Safety Answering Points (PSAPs), to ensure an effective response during emergencies.
Reports	

MODULE II – PII SYSTEMS & PROJECTS	
14. What kinds of reports are produced about individuals or contain an individual's data?	N/A
15. What will be the use of these reports?	N/A
16. Who will have access to these reports?	N/A
Monitoring	
17. Will this information system provide the capability to identify, locate, and monitor individuals?	Yes, based on the information that is entered in manually by the individuals.
18. What kinds of information are collected as a function of the monitoring of individuals?	Name, Phone, Address/Location
19. Are controls implemented to prevent unauthorized monitoring of individuals?	Yes, controls are implemented within RedSky E911 to prevent unauthorized monitoring of individuals. These controls include strict access permissions, encryption measures, and audit trails to ensure that only authorized personnel can access and monitor the system, thus safeguarding against unauthorized monitoring or privacy breaches. The system is designed to prioritize individual privacy and data protection while enabling effective emergency response.
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.	Information is entered in manually by the individuals as needed. Users will be prompted to update their information when they change locations.
21. If the information system is operated in more than one site, how will consistent use of the information be ensured at all sites?	Redundancy and replication occur within RedSky E911, this is provided within the Everbridge Cloud Solution Provider.

MODULE II – PII SYSTEMS & PROJECTS

Records Management

22. Identify the record(s).	Full name, address/location
23. Identify the specific disposition authority(ies) that correspond to the record(s) noted in no. 22.	☐ Unscheduled ☒ Scheduled *(cite NARA authority(ies) below)* GRS 5.5 Item 10 Staff and office directories, contact lists, and locators for mail deliveries GRS 5.5 Item 20 Mail, printing, and telecommunication services control records GRS 3.2 Item 30 System access records GRS 3.2 Item 36 Cybersecurity event logs GRS 5.3 Employee emergency contact information
24. Records Contact	Ryan Morrone, ryan.morrone@netl.doe.gov (O) (412) 386-4693

ACCESS, SAFEGUARDS & SECURITY

25. What controls are in place to protect the data from unauthorized access, modification or use?	Controls are implemented within RedSky E911 to prevent unauthorized access or modification to data. These controls include strict access permissions, encryption measures, and audit trails to ensure that only authorized personnel can access and monitor the system, thus safeguarding against unauthorized modification of data.
26. Who will have access to PII data?	Access will be limited only to RedSky E911 system administrators which will only be four individuals (all of which are NETL employees).
27. How is access to PII data determined?	System Administrators will have access to all data and individuals will have access to their own data.
28. Do other information systems share data or have access to the data in the system? If yes, explain.	Data will be pushed to authorized emergency response agencies as needed, including Public Safety Answering Points (PSAPs), to ensure an effective response during emergencies.

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?	NETL Privacy Officer NETL Authorizing Official

END OF MODULE II

SIGNATURE PAGE

	Signature	Date
System Owner	**Roger Rhoads** **(Print Name)** **(Signature)**	
Local Privacy Act Officer	**Ann Guy** **(Print Name)** **(Signature)**	
Ken Hunt **Chief Privacy Officer**	**(Print Name)** William K. Hunt Digitally signed by William K. Hunt Date: 2024.05.14 16:16:50 -04'00' **(Signature)**	