Privacy Impact Assessment
for the

RadResponder Network

DHS/FEMA/PIA-054

August 15, 2019

Contact Point
Sean Crawford
Chemical, Biological, Radiological, Nuclear Office
Federal Emergency Management Agency
(202) 646-8269

Reviewing Official
Jonathan R. Cantor
Acting Chief Privacy Officer
Department of Homeland Security
(202) 343-1717

Abstract

The U.S. Department of Homeland Security (DHS), Federal Emergency Management Agency (FEMA), Chemical, Biological, Radiological, and Nuclear Office (CBRN), supports the RadResponder program. RadResponder is a free web-based platform that standardizes how all federal, state, local, tribal, and territorial disaster response organizations collect, store, use, and manage radiological data following a disaster or manmade event. RadResponder collects data at radiological sites for the purpose of analyzing the dangers of the site and to help emergency personnel determine how to mitigate the disaster's impact and save lives. FEMA has conducted this privacy impact assessment (PIA) to cover how RadResponder collects, stores, uses, and protects users' personally identifiable information (PII).

Overview

The FEMA CBRN mission is to respond effectively to a nuclear disaster. After the nuclear disaster in Fukushima, Japan, in 2011, DHS recognized that the United States lacked a national standard on how to collect radiological data following nuclear disasters. In response, FEMA CBRN, the Department of Energy/National Nuclear Security Administration (DOE/NNSA), and the Environmental Protection Agency (EPA) collaborated to build RadResponder, a web-based platform that supports the sharing and management of radiological data among the emergency responder community. RadResponder is a contractor-provided service that enables federal, state, local, tribal, and territorial (FSLTT) disaster response organizations to rapidly share and aggregate large quantities of data, while managing their equipment, personnel, interagency partnerships, and multijurisdictional event spaces.

Prior to the creation of RadResponder, no common platform existed for sharing radiological data across FSLTT organizations. RadResponder provides this common platform, and is codified in the latest edition of the Nuclear/Radiological Incident Annex to the Response and Recovery Federal Interagency Operational Plans (NRIA)[1] as the "National Standard and Whole Community solution for the management of radiological data." RadResponder consists of the RadResponder web portal and a mobile application that is available for iOS, Android, and Windows.[2] The RadResponder web portal is the central repository for members from FSLTT response organizations to share radiological information and resources of common interest (e.g., field teams, equipment, documents) during both preparatory exercises and actual radiological disasters. The mobile application enables response personnel to collect and transmit radiological data from the field into the RadResponder portal. In the event of a radiological disaster, emergency

[1] Nuclear/Radiological Incident Annex to the Response and Recovery Federal Interagency Operational Plans, (October 2016), *available at* https://www.fema.gov/media-library-data/1488825883577-fb52b6b7fd784dfb64aaee1fd886393a/NRIA_FINAL_110216.pdf.

[2] FEMA users access the mobile application on FEMA-issued mobile devices, and first responders, who are members of the public, access the application on their own mobile devices.

responders will use radiological detection equipment to survey the environment and will record the readings and relevant information in RadResponder. Once the data is uploaded into the portal, members of the emergency response community can review the data to support response efforts and decision-making.

In the case of a radiological event that results in a Stafford Act Declaration,[3] designated Stafford Act Administrators within FEMA will be granted access to view the data collected for the relevant event. Additionally, site administrators have access to view all events in RadResponder, in order to provide technical support to end users.

RadResponder Portal

A response to a radiological release or detonation is often a multijurisdictional effort, involving response organizations from all levels of government and industry. The RadResponder portal provides a collaborative space where these disparate organizations can upload and share information and data in real time. While the portal was built with emergency response activities in mind, it is most often used for training, drills, and exercises during which organizations practice and prepare for responding to a radiological disaster.

All collected radiological data and its associated metadata (e.g., location, date/time, height, type of equipment) are compartmentalized in different "events" within the RadResponder portal. An event is simply the name given to a space where data can be uploaded and shared with designated groups. Types of events can include: emergency response, special event, testing/training, exercise/drill, or routine monitoring. There are over a thousand organizations in RadResponder, and segregating data into events is necessary for the management and organization of the data. The creation of an event also allows organizations to determine which other organizations can upload and have access to the data. Within an organization, only individuals with an "Event Manager" role can create events. Event Managers determine the sharing permissions for their organization's events, and can choose to make an event "Network Wide," allowing all RadResponder organizations to view the data, for "My Organization Only" so that only organization personnel can view the data, "Private" so that only the event creator can view the data, or for "Partners Only," which allows only partner organizations to view the data. On top of these broad data sharing settings, Event Managers can customize access for individual responders or organizations.

An organization's Event Manager creates an event by filling out a short form with the event name, event type (testing/training, exercise/drill, special event, routine monitoring, or emergency response), start date, and data sharing setting (my organization only, partners only, private, or network-wide). Once the event has been saved, responders using the mobile application will be able to see the event name and can begin submitting data if they have been granted access to the

[3] 42 U.S.C. § 5121.

event. Responders using the web portal may also submit data, and can view incoming data geospatially or in a tabular format. Event Managers may customize data sharing settings throughout the duration of the event, for example granting access to state, regional, or federal organizations as a response grows in scope. Data assessors (with the "data assessor" role assigned by the organization's Event Manager), may approve or reject data to indicate which data should be used in decision-making. Although RadResponder encourages data assessment and shares Federal Radiological Monitoring and Assessment Center (FRMAC) data quality standards in training and RadResponder drills, it is ultimately up to the state/local organization to determine if and how to assesses its data.

The data in RadResponder is owned by the organization that collected it. Unless there is a Stafford Act Declaration, that data cannot be accessed by any other organization, including FEMA, unless the originating organization's Event Manager chooses to grant other organizations access to that event's data. In the event of a Stafford Act Declaration, contractor system administrators will share information related to relevant event(s) with FEMA if the current event managers have not already done so. FEMA may then share this data with the EPA and/or DOE/NNSA, as necessary.

To access the RadResponder site, users must apply for and be granted RadResponder accounts. An individual must provide the following information to the RadResponder administrative team: work email; work phone number; first and last name; citizenship status;[4] the organization to which they belong; and user-configurable security questions for password resets.

Once an account has been created, the user may log into the RadResponder portal using his or her unique username and password. From there, he or she is able to view radiological data that is collected by or shared with his or her organization. Information stored and shared in the portal includes: field surveys, spectra,[5] samples, observations, documents, location information, and photographs collected through the RadResponder mobile application. Appendix B of this PIA provides a complete list of radiological data and associated metadata recorded in RadResponder.

RadResponder Mobile Application

Emergency personnel deployed during a radiological disaster use the RadResponder mobile application to collect radiological data (see Appendix B).[6] The radiological data and associated information are compartmentalized in "Events" within the RadResponder portal.

[4] Only U.S. citizens are granted full access to RadResponder. Non-U.S. citizens may be granted temporary and restricted access after being screened and approved. See Appendix C.

[5] Spectra readings are taken by specialized radiological detection equipment that read the energy levels (in counts) per channel. Scientists can interpret this graph or "signature" to identify which radioactive isotopes are being detected.

[6] Generally, FEMA only uses the RadResponder portal for situational awareness; FEMA personnel generally do not collect data through the mobile application (the data collection features are actually disabled for FEMA personnel currently, though the option is available should it be necessary).

RadResponder uses the Global Positioning System (GPS) function on mobile devices for two distinct purposes: 1) to collect the location of radiological measurements, and 2) to track location information of personnel in the field. Documenting the location of radiological measurements is crucial to assessing data and understanding where elevated levels of radiation are present. All radiological measurements are required to have a location identified; by default, the mobile application uses GPS to populate the location field; however, responders can disable this and choose to manually enter a location by selecting from a map, entering a latitude and longitude, entering a street address, or choosing from a list of pre-identified sampling locations. The mobile application also uses GPS to track responder locations via the Responder Tracking feature, which provides leadership with insight into where to direct personnel to continue collection efforts. Responder Tracking updates GPS location after the device has moved at least 10 meters or 10 seconds have passed. GPS location is associated with radiological measurements only when the responder records GPS data.

Responder Tracking provides situational awareness for emergency managers, and allows field team coordinators to re-direct the closest field team to an area where new measurements need to be taken, or previously-uploaded measurements need to be verified. A pop-up appears when the user first downloads the application, asking the user's permission to use the mobile device's GPS features. If the user declines, GPS cannot be associated with measurements nor can responders be tracked. If the user accepts, by default, a prompt appears every time users open an event in the mobile application that permits users to opt in to or out of Responder Tracking. If users opt in, then RadResponder tracks their geospatial location information (latitude/longitude) and uploads this information to the RadResponder web portal. If users opt out, then Responder Tracking does not collect their geospatial location information. Users may change the default setting at any time, within the application, either to always allow Responder Tracking for events or never allow Responder Tracking for events. Within an event on the mobile application, users can pause and resume tracking at any time via a bar that is always displayed across the bottom of the screen. If users send the application to the background without closing the application or exiting the event, they will receive a push notification indicating whether or not their location is still being tracked. Users can click on the notification to re-enable or disable tracking without re-entering the application. Additionally, users can opt out of using GPS entirely via the general location settings on their device. The purpose of Responder Tracking is not to analyze the movements of individual responders during an emergency, but rather for the data they are collecting and directing them for further analysis.

After the user selects whether to opt in or opt out of Responder Tracking, he or she may begin to collect radiological data. Individual members' usernames are associated with the radiological data they collect, which is uploaded from the mobile application into the RadResponder web portal. When entering a radiological measurement, the application by default

pulls the mobile device's current geospatial location, but the responder may choose an alternate location mode, such as manually entering a latitude and longitude, entering an address, selecting a pre-defined sampling location, or selecting from a map. Opting out of Responder Tracking within the application does not affect the default use of current geospatial location when entering a radiological measurement. However, if a user disallows the RadResponder application from using the mobile device's GPS function, Responder Tracking will not function, and the user will have to manually enter a location for each radiological measurement.

The location information collected by RadResponder is necessary for the proper analysis of radiological data; if elevated readings are collected, it is crucial to know where those elevated readings are to identify the source, or if the source is known, to determine how and where radiation has spread. Knowing the location of the data helps data assessors determine data quality and accuracy. For example, if a reading of zero is recorded within feet of a radiological detonation, it would lead assessors to re-examine the data's accuracy. This function also provides situational awareness for emergency managers or decision makers monitoring the disaster through the RadResponder portal, who are granted access to a particular event by the eventmanager and can view incoming data geospatially or in a tabular format. By having a clear operational picture of the location of RadResponder mobile application users, emergency managers can direct them to specific locations in order to more optimally capture radiological data during an emergency.

As soon as the radiological data collection is completed, it is automatically uploaded to the RadResponder web portal. If a cellular or Wi-Fi connection is unavailable, the data is cached locally on the mobile device until a connection is re-established, at which point the data is uploaded automatically. Users are instructed not to submit photographs or comments that contain any type of PII, including pictures of individuals. When required for scale and perspective, RadResponder application users may take photographs of individuals. However, users will be instructed to have all persons included in a photograph to stand backwards with their faces away from the camera.

Data Sharing

All data collected in RadResponder about a specific event, is owned by the organization that collected it, and cannot be accessed by any other organization, including FEMA, unless the originating organization chooses to grant access to that event's data to other individuals or organizations. In the case of a Stafford Act Declaration,[7] designated Stafford Act Administrators within FEMA will be granted access to view the data collected for the relevant event. Additionally, system administrators have access to view all events in RadResponder, in order to provide technical support to end users.

RadResponder interfaces with the DOE's FRMAC Radiological Assessment and

[7] 42 U.S.C. § 5121.

Monitoring System (RAMS).[8] RAMS is used by DOE to analyze, monitor, and map radiological data. RadResponder's interface with this system enables DOE to pull RadResponder data into their own systems for further analysis, but only for events to which DOE has been granted access by the originating organization's Event Manager. The data sent to DOE includes: radiological data, names and contact information associated with those members who collected the data, and the location at which the radiological reading was collected. The radiological data shared can support decision-making during response and mitigation efforts. FEMA is the only DHS component that uses RadResponder.

RadResponder only pushes data out to DOE; RadResponder does not receive any information from these two systems. All data is associated with specific events, and sharing is done at the event level, on an event-by-event basis. Access to these events is controlled by the designated event manager, and only those individuals that are granted access to a specific event may view the data collected for that event. FRMAC can only pull data for events in which the event sponsor specifically enabled the "Shared with FRMAC" setting when configuring the event. The EPA and DOE can only pull data for events that they themselves create, or events in which they have been added as a partner by the event's manager. Only systems administrators have access to all of the data collected for every event. FEMA CBRN personnel can only view the data captured for an event if and when the event manager grants FEMA access or during a Stafford Act event when the system administrator grants access.

Exercises

Although RadResponder is an emergency response tool intended to facilitate real-time sharing of radiological data across FSLTT response organizations, actual radiological disasters are extremely rare. To date, there have been zero instances of an Improvised Nuclear Device (IND) detonation or Radiological Dispersal Device (RDD) detonation on U.S. soil; the last accident involving a U.S. Nuclear Power Plant (NPP) was at Three Mile Island in 1979. As a result, the overwhelming majority of radiological data collected in RadResponder consists of simulated readings entered by first responders during training, drills, and exercises. These measurements do not reflect the actual levels of radiation at the location/time for which they were recorded. However, frequent use of the site in a simulated environment helps establish a standard and reinforces FSLTT interoperability in the event that RadResponder might be used for an actual response.

[8] For more information about FRMAC, please *see* https://www.nnss.gov/pages/programs/FRMAC/FRMAC.html and the FRMAC Operations Manual (May 2010), *available at* https://www.nnss.gov/docs/docs_FRMAC/FRMAC%20Operations%20Manual%202010.pdf. RAMS is an online data repository used by DOE Consequence Management to store and view data from measurements and field samples during a radiological response.

In addition to simulated data collected during trainings, drills, and exercises, some organizations use RadResponder to monitor background radiation levels in their jurisdictions. Radiation is naturally occurring and omnipresent, although background levels vary from region to region.

None of the radiological data collected in RadResponder is considered "sensitive" in any way, be it simulated data or actual background radiological measurements. Outside of RadResponder, background radiation data is easily obtained via several public-facing websites (Safecast, EPA's RadNet, etc.), by taking measurements using radiation detection equipment (available for public purchase), or by formally requesting records from a nuclear power utility or state agency. Even data collected in the aftermath of a radiological disaster is not considered sensitive. This is data that will be used to inform protective action decisions, and thus will ultimately be released to the public once it has been assessed, scrubbed for PII, aggregated, and accompanied by proper messaging.

After Action Review to Scrub PII

At the end of a disaster or exercise, the event manager, or designated personnel, will review the photographs, documents, and comments sections to ensure that no PII has been collected, to include faces of individuals. In the event that PII has been inadvertently collected, the event manager or designated personnel will scrub or obfuscate any faces or PII. FEMA does not modify or delete any other data or events unless explicitly requested to by the collecting organization.

Section 1.0 Authorities and Other Requirements

1.1 What specific legal authorities and/or agreements permit and define the collection of information by the project in question?

Section 502 of the Homeland Security Act of 2002, as amended by the Department of Homeland Security Appropriations Act of 2007, defines the Nuclear Incident Response Team (NIRT) as a resource composed of specialized radiological response capabilities from DOE and the EPA.[9] Section 504 of that act further mandates that FEMA must manage the NIRT, including establishing standards, conducting exercises, and providing training and equipment support.[10] The programmatic requirements derived from this authority include developing policy, plans, training, and exercises related to NIRT operations including accident response, search response, advisory, and technical operations functions as well as radiation exposure functions and radiological assistance functions. Additionally, the NIRT program must provide funding to the EPA and DOE for training, equipping, and exercising NIRT assets which are managed by these entities on a daily basis. Operationally, it must also be prepared to deploy the NIRT as an organizational unit of DHS.

[9] 6 USC § 312.
[10] 6 USC § 314(a)(2).

In the event of a declaration of a major disaster, FEMA's Federal Coordinating Officer (FCO) may activate and implement the Federal Response Plan (FRP) and coordinate and direct emergency assistance and disaster relief of impacted individuals, business, and public services under the Stafford Act.[11]

FEMA is also required during preparedness planning or in actual response to an emergency to provide guidance, policy and program advice, and technical assistance in hazardous materials, chemical, and radiological emergency preparedness activities (including planning, training, and exercising).[12]

National Security Presidential Directive (NPSD) 28[13] identifies FEMA as the office of primary responsibility for consequence management activities in response to a U.S. nuclear weapon incident or accident. Additionally, FEMA must develop, implement, maintain, and regularly exercise integrated consequence management and counterterrorism response plans, procedures, and capabilities relevant to a U.S. nuclear weapon incident or accident and engage with state, local, tribal, and territorial authorities, as appropriate.

The DHS Integrated Planning Guidance Fiscal Year 2011-2015 directed FEMA to develop and execute the DHS Strategy for Improving the National Response and Recovery from an IND Attack (DHS IND Strategy) and establish the IND Response and Recovery Program to address capability gaps and to coordinate solutions. The DHS IND Strategy identifies the critical core capabilities, objectives, and targets for effective response and recovery from an IND attack. FEMA must act as the coordinating agency for incidents of IND/RDD attacks domestically as well as lead coordination and execution of the DHS IND Strategy.

As part of the DHS IND Strategy, FEMA is required to coordinate with interagency and "Whole Community" partners to identify and address critical radiological/nuclear (R/N) capability gaps and develop plans, policies, and procedures unique to R/N incidents that allow for an effective and credible response to support impacted survivors and communities. FEMA coordinates with DHS Science and Technology (S&T) as the technical lead for R/N response and recovery research and development to identify and fill the technology needs to accomplish effective response and recovery in an R/N incident.

The Chemical, Biological, Radiological, and Nuclear (CBRN) Incident Annexes to the Response and Recovery Federal Interagency Operational Plans provide incident-specific roles and responsibilities for federal response and recovery operations under the National Response

---

[11] 40 CFR 300.130(i); *see also* Robert T. Stafford Disaster Relief and Emergency Assistance Act, Pub. L. No. 93-288 (as amended primarily at 42 U.S.C. §§ 5121-5207), *available at* https://www.fema.gov/media-library-data/1519395888776-af5f95a1a9237302af7e3fd5b0d07d71/StaffordAct.pdf.

[12] 40 CFR 300.175(b)(3).

[13] National Security Presidential Directive 28, "United States Nuclear Weapons Command and Control, Safety, and Security," June 20, 2013.

Framework and National Disaster Recovery Framework. FEMA must establish concepts for integrating response operations with law enforcement operations based on the Terrorism Incident Law Enforcement and Investigations Incident Annex.[14] FEMA is also responsible for maintaining the capability to coordinate all federal response and recovery operations in response to a CBRN incident. Additionally, the Nuclear/Radiological Incident Annex (NRIA) identifies the requirement for a Nuclear/Radiological Incident Task Force (NRITF) advising the National Response Coordination Center (NRCC) on response operations and impacts of the Radiological/Nuclear hazard affecting response operations, priorities, and decisions; FEMA's CBRN coordinates this task force. The NRIA also codifies RadResponder as "the national standard and Whole Community solution for the management of radiological data," and states that "RadResponder should never be locked or turned off during an incident; organizations should always be able to access their input data."[15]

1.2 What Privacy Act System of Records Notice(s) (SORN(s)) apply to the information?

RadResponder's collection of geospatial location information will be covered by DHS/ALL-014 Department of Homeland Security Personnel Contact Information.[16] The information collected to access the RadResponder portal is covered by DHS/ALL-004 General Information Technology Access Account Records System (GITAARS).[17]

1.3 Has a system security plan been completed for the information system(s) supporting the project?

RadResponder is a service, not a system, and as such does not require a security plan or Authority to Operate.

1.4 Does a records retention schedule approved by the National Archives and Records Administration (NARA) exist?

NARA has determined that data accumulated in the absence of a Stafford Act radiological incident do not meet the threshold of a record under the Federal Records Act. If FEMA does use reports or data from the RadResponder network because of a Stafford Act radiological incident,

---

[14] Terrorism Incident Law Enforcement and Investigation Annex (December 2004), *available at* https://www.fema.gov/media-library-data/20130726-1825-25045-5502/terrorism_incident_law_enforcement___investigation_annex_2004.pdf.

[15] Nuclear/Radiological Incident Annex to the Response and Recovery Federal Interagency Operational Plans, (October 2016), p. 52, *available at* https://www.fema.gov/media-library-data/1488825883577-fb52b6b7fd784dfb64aaee1fd886393a/NRIA_FINAL_110216.pdf.

[16] DHS/ALL-014 Department of Homeland Security Personnel Contact Information, 83 FR 11780 (March 16, 2018).

[17] DHS/ALL-004 General Information Technology Access Account Records System (GITAARS), 77 FR 70792 (November 27, 2012).

the records would at that point meet the threshold definition of a federal record, and FEMA would need to schedule the records. The actual data collected during a Stafford Act radiological incident, the use of that data, and the nature of the incident would all factor into a NARA appraisal decision; therefore, a schedule for these records cannot yet be determined.

In accordance with General Records Schedule 3.2, item 31, system access records are retained for six (6) years after password is altered or user account is terminated.

1.5 If the information is covered by the Paperwork Reduction Act (PRA), provide the OMB Control number and the agency number for the collection. If there are multiple forms, include a list in an appendix.

FEMA is working with its Records Management Branch to develop an Information Collection Request package for registering users for RadResponder. When complete, the package will be routed to the Office of Management and Budget for approval and an official form number. When this package is approved, FEMA will update the appendix of this PIA.

Section 2.0 Characterization of the Information

2.1 Identify the information the project collects, uses, disseminates, or maintains.

RadResponder collects the following information from users:

- First name (associated with collected data);
- Last name (associated with collected data);
- Work email (associated with collected data);
- Work phone number (associated with collected data);
- Employer/Organization name (used to associate the user's account with an organization in RadResponder);
- U.S citizenship (yes or no button); if no, country of citizenship (used to determine access to the network);[18]
- User-configurable security questions (used to reset passwords);
- Geospatial location information of users (latitude/longitude, used to track responders who opt in to Responder Tracking);

[18] See Appendix C for additional information related to foreign national access to RadResponder.

- Geospatial location information of radiological measurements (either automatically entered as the current device latitude/longitude, or manually entered if a user has disabled GPS functions on their device or chooses manual entry for another reason).

Along with the radiological measurements, users can take photographs and upload them into RadResponder. Users are cautioned to not include PII in photographs, and in the event that a person is needed for scale, RadResponder users will instruct the individual to stand facing away from the camera.

2.2 What are the sources of the information and how is the information collected for the project?

RadResponder collects user registration information directly from the individual through the portal registration page.

The location information that is used to track responders comes directly from the RadResponder mobile application's Responder Tracking function. When a user opens an event on the mobile application to begin collecting data, he or she is prompted to opt in or opt out of the Responder Tracking for that event. If the user opts in, then the user's location (latitude/longitude) is collected and uploaded to the RadResponder web portal at user-selected intervals between every one and every ten minutes. Location information is also associated with each radiological data point collected by the user—this can be the "Current Location" (determined by the mobile device's GPS signal, separate from Responder Tracking, and available only if the user has permitted the application to pull the mobile device's GPS location), street address, manually entered latitude/longitude, or pre-defined sampling location (e.g., "A2").

2.3 Does the project use information from commercial sources or publicly available data? If so, explain why and how this information is used.

No. RadResponder does not use information from commercial sources or publicly available data.

2.4 Discuss how accuracy of the data is ensured.

Since individuals directly provide their PII to obtain an account, it is presumed that the information obtained is correct. Once the user's information is submitted, the individual will receive an email that confirms he or she has been granted an account. If the individual needs to amend his or her information, he or she can directly amend his or her account, contact the event manager, or technical support.

RadResponder uses Responder Tracking, a GPS function, to provide user location information. Once activated, the GPS application tracks users' latitude and longitude in one- to

ten-minute intervals. The GPS function of RadResponder is not intended to and does not provide real-time location data. The location information is only used to provide situational awareness to emergency managers to inform decision-making in response efforts.

2.5 Privacy Impact Analysis: Related to Characterization of the Information

Privacy Risk: RadResponder may contain inaccurate data.

Mitigation: This risk is mitigated because RadResponder collects account information directly from individuals for the purpose of gaining an account. Since the individual provides the information it is presumed the information provided is correct. However, if necessary, users can correct their information in the RadResponder portal, contact the event manager, or contact technical support to correct any erroneous PII.

Privacy Risk: RadResponder may contain an inaccurate picture of where an individual is or was, due to the limitations of GPS location information.

Mitigation: This privacy risk is mitigated. When turned on, Responder Tracking tracks users' location information (longitude/latitude) using GPS. The location information is collected directly from the user. Moreover, FEMA CBRN, in conjunction with DOE and the EPA, conducts engineering reviews to ensure the accuracy of the location data provided.

Section 3.0 Uses of the Information

3.1 Describe how and why the project uses the information.

RadResponder collects PII from users to provide access to the portal and mobile application. After an account is created, users' PII is also associated with the radiological measurements and photographs that they collect during an event. PII, such as work phone or work email address, is useful to data assessors who may need to verify certain data elements with the person that recorded the data. Responder Tracking uses GPS to track users' location information as they collect radiological data.

The Responder Tracking function provides an operational picture of the location of RadResponder users, which allows emergency managers to better direct response personnel and more-optimally capture radiological data during an emergency. The radiological measurements and photographs provide emergency management personnel with situational awareness of the levels of radiological activity in a given area. RadResponder does not provide real-time location data, and is not used to ensure the safety of its users during an emergency.

RadResponder users may opt out of location tracking at any time either in the application itself, or in the device location settings.

3.2 Does the project use technology to conduct electronic searches, queries, or analyses in an electronic database to discover or locate a predictive pattern or an anomaly? If so, state how DHS plans to use such results.

No. RadResponder does not conduct electronic searches, queries, or analyses to discover or locate predictive patterns or anomalies.

3.3 Are there other components with assigned roles and responsibilities within the system?

No. No other DHS component has an assigned role or responsibilities within RadResponder. However, a number of FSLTT agencies use RadResponder.

3.4 Privacy Impact Analysis: Related to the Uses of Information

Privacy Risk: Any individual with access to an event may misuse information collected during a disaster for purposes beyond those that are stated in this PIA.

Mitigation: Users only have access to radiological information collected by or explicitly shared with their organization, and only the contractor technical support teams have access to all of the data within RadResponder. If a Stafford Act Declaration occurs, FEMA Stafford Act Administrators will be granted view-only access to data associated with that specific disaster. These FEMA Stafford Act Administrators may then choose to grant view-only access to select EPA and DOE/NNSA personnel. FEMA has developed Rules of Behavior (see Appendix A) to which all users must agree that restrict the use of user location data and work contact information to only event-related and incident management activities.

Privacy Risk: Responder Tracking may allow management and others to track RadResponder users outside of the scope of their work or to take inappropriate personnel actions against an employee based on the location data stored in RadResponder.

Mitigation: Before users can collect radiological data, a prompt allows the individual to opt in or opt out of location sharing. If the user opts out, then RadResponder will not record the user's location.

In addition, a user's location is never recorded outside of an event. Within an event on the mobile application, users can pause and resume tracking at any time via a bar that is always displayed across the bottom of the screen. If users send the application to the background without closing the application or exiting the event, they will receive a push notification (assuming notifications are allowed) indicating whether or not their location is still being tracked. Users can click on the notification to re-enable or disable tracking without re-entering the application. Additionally, users can disable the application from accessing the mobile device's location through

the mobile device's factory setting. Doing so would prevent the application from collecting Responder Tracking information, and from automatically collecting location information associated with a radiological record.

Privacy Risk: Photographs and other radiological measurements may capture PII.

Mitigation: This risk is partially mitigated. While users are instructed not to collect PII, PII may inadvertently be collected during an exercise or incident, and this PII may be stored for a limited amount of time until an after-action scrub can be performed. FEMA has instructed users not to input PII into RadResponder and there are reminders provided within the application. However, when required for scale and perspective, RadResponder mobile application users may take photographs of individuals. Users will be instructed to have all persons included in a photograph stand backwards with their face away from the camera. In the event that PII is inadvertently collected, the event manager or a designated person will scrub, obfuscate, or redact any faces or PII following the incident or exercise. Any inadvertent PII is never linked to nor used to identify the individuals whose PII was collected.

Section 4.0 Notice

4.1 How does the project provide individuals notice prior to the collection of information? If notice is not provided, explain why not.

RadResponder has a mobile Privacy Policy that is provided to all users. There is also a Privacy Notice on the web portal that tells users how and why their PII is collected.

Moreover, users are prompted to opt in or opt out of sharing their location information each time they use the application. By opting in, the users are notified of and consenting to having their location information captured as they use the application.

4.2 What opportunities are available for individuals to consent to uses, decline to provide information, or opt out of the project?

Prior to obtaining an account, responders are shown a Privacy Policy that explains how and why their PII is being collected. Since obtaining a RadResponder account is entirely voluntary, responders may choose not to provide this information and thus not receive an account. Responders may also use RadResponder strictly for situational awareness without submitting any radiological data. In these cases, responder names, contact information, and location information is never associated with any radiological measurements. However, when a user does take radiological measurements, each measurement is associated with the user's current location (if enabled), as well as the user's name to enable additional information gathering from the individual who took the measurement. The Responder Tracking function on the mobile application collects first responder movements at select intervals, as determined by the user. When a user opens an event

on the mobile application to begin collecting data, he or she will be prompted to opt in or opt out of Responder Tracking for that event. If the user opts in, the user's location (latitude/longitude) is collected and uploaded to the RadResponder portal, along with the radiological data he or she captures.

4.3 Privacy Impact Analysis: Related to Notice

Privacy Risk: A RadResponder user may be unaware that their location is tracked while he or she is using the application.

Mitigation: RadResponder member training explains how user PII will be tracked on the application and how to opt out of location tracking. When a user opens an event on the RadResponder application, he or she will be prompted to opt in or opt out of the Responder Tracking for that event.

Privacy Risk: A RadResponder mobile application user may be unaware that his or her PII will be linked to any radiological measurements the user submits, and will be viewable by other users on the web portal who are part of the same event.

Mitigation: This risk is mitigated because the Privacy Notice and mobile application Privacy Policy both inform mobile application users that other users in the same event will be able to see their PII. RadResponder member training also explains how PII is associated with their measurements, who has access to PII in RadResponder, how their PII will be used, and how to limit the collection of their PII.

Section 5.0 Data Retention by the project

5.1 Explain how long and for what reason the information is retained.

NARA has determined that the data accumulated in the absence of a Stafford Act radiological incident do not meet the threshold of a record under the Federal Records Act. If FEMA does use reports or data from the RadResponder network because of a Stafford Act radiological incident, the records would at that point meet the threshold definition of a federal record, and FEMA would need to schedule the records. The actual data collected during a Stafford Act radiological incident, the use of that data, and the nature of the incident would all factor into a NARA appraisal decision; therefore, a schedule for these records cannot yet be determined. Since organizations own the data they collect, they choose when/if that data is ever deleted. RadResponder does not delete FSLTT data without the explicit permission of the collecting organization. In accordance with General Records Schedule 3.2, item 31, system access records are retained for six (6) years after password is altered or user account is terminated.

Section 6.0 Information Sharing

6.1 Is information shared outside of DHS as part of the normal agency operations? If so, identify the organization(s) and how the information is accessed and how it is to be used.

Yes. The data in RadResponder is owned by the organization that collects it, and it is shared with other non-DHS entities in RadResponder according to the collecting organization's preferences. DHS/FEMA does not have access to view the majority of the data collected in RadResponder, unless the collecting organization has explicitly chosen to share that data with DHS/FEMA. In the event of a Stafford Act Declaration, FEMA will have access to view all data associated with the disaster, and can elect to share that data with the EPA and DOE, memorialized in an Interconnection Security Agreement (ISA), as appropriate. The data includes: radiological data, names and contact information associated with those members who collected the data, any photographs or Responder Tracking taken, and the location where the radiological reading was recorded. Location data would be used to make deployment decisions and reduce duplication of efforts. The radiological data shared can support decision-making during response and mitigation efforts. PII associated with radiological data allows participating organizations to reach out to personnel to verify findings. FEMA is the only DHS component that uses RadResponder.

In day to day operations, DOE FRMAC RAMS may receive radiological data associated with specific events in RadResponder if the sharing of data is approved by the organization that created the event, or in the event of a Stafford Act Declaration if FEMA chooses to share the information. The radiological data provided to FRMAC contains names, email, and phone numbers associated with the individual user who collected the data.

FEMA is in the process of memorializing its information sharing practices with DOE through an ISA with the agency.

6.2 Describe how the external sharing noted in 6.1 is compatible with the SORN noted in 1.2.

RadResponder collects and uses PII to provide access to DHS information technology resources and to allow DHS to track the use of DHS IT resources. The routine uses within the RadResponder Web Portal are covered by DHS/ALL-004 General Information Technology Access Account Records System (GITAARS).[19] Routine Use H allows for sharing of information with sponsors, employers, contractors, facility operators, grantees, experts, and consultants in connecting with establishing an access account for an individual. Routine Use K allows for the

[19] DHS/ALL-004 General Information Technology Access Account Records System (GITAARS), 77 FR 70792 (November 27, 2012).

sharing of business contact information in order to facilitate collaboration for official business. Each of these Routine Uses are necessary for account creation purposes, as individuals must supply this information, in order to be granted a RadResponder account.

RadResponder collects, shares, and uses location information of individuals who participate in or who respond to all-hazards emergencies, including technical, manmade, or natural disasters, and to support DHS all-hazard emergency response for the limited purposes of situational awareness during a disaster and to mitigate the human exposure to radiological material, in accordance with the DHS/ALL-014 Personnel Emergency Contact Information System of Records, Routine Uses I and J.[20] Routine Use I allows for the sharing of personnel location data with FSLTT, if the information is relevant and necessary, for the purpose of providing support in an all hazards emergency included technical, manmade, or natural disasters. Routine Use J allows for information sharing with the identified emergency contacts of current and former DHS personnel (including federal employees and contractors), individuals who participate in or conduct exercises, or individuals who respond to all hazards emergencies including technical, manmade, or natural disasters.

6.3 Does the project place limitations on re-dissemination?

DOE and the EPA may be granted access to information in RadResponder during a Stafford Act Declaration. The FEMA Stafford Act Administrators (the FEMA CBRN Director and FEMA Program Manager), however, will determine what information DOE and the EPA will be able to access.

RadResponder collects, shares, and uses information only pursuant to the routine uses outlined in the SORNs listed under Sections 1.2 and 6.2 above or through an approved ISA such as the sharing described in Section 6.1.

Event managers will also perform a post-event scrub of all of the data collected during an event to ensure that no PII has been inadvertently captured. In the event that PII has been captured, it will be scrubbed, obfuscated, or redacted.

6.4 Describe how the project maintains a record of any disclosures outside of the Department.

Access to information within RadResponder is generally segregated by "event" and access to the "event" is controlled by the participating organization's event manager. Although RadResponder does not maintain records of which users access particular pages and information, the system does keep a record log of user access to an event. Therefore, while RadResponder

[20] DHS/ALL-014 Personnel Emergency Contact Information System of Records, 81 FR 48832 (August 25, 2016).

records which individual users access an event, it does not maintain a record of what information that individual user accesses within the event.

6.5 Privacy Impact Analysis: Related to Information Sharing

Privacy Risk: The information collected in RadResponder may be shared beyond the intended organizations and shared beyond the intended purpose for which it was collected.

Mitigation: Information sharing will occur according to the SORNs listed in this PIA. In addition, the event manager determines what information will be shared and with whom. In general, event managers only share information with emergency managers and entities that are involved in a disaster response effort for a specific event.

Section 7.0 Redress

7.1 What are the procedures that allow individuals to access their information?

Users may access their own information through their RadResponder profile page using the mobile application or web portal. In addition, any users who are U.S. citizens or lawful permanent residents may make a Privacy Act request to the FEMA Disclosure Branch. Non-U.S. citizens may make a Freedom of Information Act (FOIA) request through the FEMA Disclosure Branch.

Requests for Privacy Act-protected information must be made in writing, and clearly marked as a "Privacy Act Request." FOIA requests should be marked accordingly. The request must include the name of the requester, the nature of the records sought, and the required verification of identity must be clearly indicated. Requests should be sent to:

Chief, Disclosure Branch
Information Management Division
500 C Street, SW, Mailstop 3172
Washington, DC, 20472

Additionally, individuals may request their records by going to the DHS FOIA website[21] and completing the online form.

7.2 What procedures are in place to allow the subject individual to correct inaccurate or erroneous information?

To correct inaccurate or erroneous information, individuals may use the procedures outlined in Section 7.1. Additionally, users can correct their information in the RadResponder portal, contact the event manager, or contact technical support.

[21] *See* https://www.dhs.gov/freedom-information-act-foia.

7.3 How does the project notify individuals about the procedures for correcting their information?

Individuals are notified of the procedures for correcting their information through this PIA, as well as the SORNs discussed in Sections 1.2 and 6.1. A Privacy Notice is on the landing page of the portal and a privacy policy is accessible to all users of the mobile application.

7.4 Privacy Impact Analysis: Related to Redress

Privacy Risk: A RadResponder user may not be able to correct inaccurate information.

Mitigation: This risk is mitigated in several ways. As noted in Section 7.1 above, RadResponder users can access and correct their PII at any time through the RadResponder mobile application and web portal. Individuals can also review their information by sending a Privacy Act/FOIA request as outlined in Section 7.1. Additionally, FEMA minimizes this risk by informing RadResponder users of procedures for correcting their information through this PIA and the SORNs listed in Section 1.2.

Section 8.0 Auditing and Accountability

8.1 How does the project ensure that the information is used in accordance with stated practices in this PIA?

All responders are assigned roles and associated permissions in RadResponder that correspond to their job functions and provide access to the appropriate functionality in RadResponder. Differentiating roles also serves to limit the number of users who can create, edit, and share events on behalf of their organization (see Section 8.3 for more information on roles), so that data is not shared unnecessarily. Within events, designated Data Assessors routinely review the collected radiological data and mark data as approved or rejected. Adherence to FRMAC data quality standards is encouraged in RadResponder training and drills. Pursuant to these standards, irrelevant, inaccurate, or poor quality data are marked “rejected” and excluded from decision-making. The mobile application, the mobile privacy policy, and the after-action scrub for PII all provide measures to limit PII from being captured or stored within RadResponder and to ensure that the practices outlined in this PIA are followed. PII could be incidentally captured during a training exercise or during an actual disaster, and this risk is not fully mitigated. While users are instructed to avoid collecting PII, in an actual scenario this may not be practical.

The contractor regularly performs scans to monitor the logs to ensure that individuals are not attempting to gain access to RadResponder in excess of their assigned privileges, or attempt to gain access to RadResponder without a RadResponder account.

Users are also held to the Rules of Behavior, to which they agree when they initially request an account.

8.2 Describe what privacy training is provided to users either generally or specifically relevant to the project.

The RadResponder site administrators receive role-based training according to DHS and FEMA policies. This includes what PII is, how the service uses PII, the implications of misuse of PII, how to protect it and how to inform users of their ability to opt out of GPS tracking. RadResponder members are trained while attending in-person training, online training, webinars, outreach and exercises pertaining to the topic of PII. They are provided with the definition of PII, how the service uses this PII, and how to shut off the option to share PII. RadResponder member training also explains who has the ability to see PII in RadResponder, the responsibilities of those that have access to the PII, and how to appropriately handle this PII.

8.3 What procedures are in place to determine which users may access the information and how does the project determine who has access?

In order to gain an account, a new user must visit www.radresponder.net and select "Request an Account." The new user must then be approved by the Organization Administrator associated with his or her organization, as well as by a RadResponder site administrator. At the initial request for an account, the user must agree to adhere to the RadResponder Rules of Behavior.

All users that are granted accounts with RadResponder have designated roles and associated permissions. Available roles include (in descending order of control): Organization Administrator, Planner, Event Manager, Personnel Manager, Equipment Manager, Data Collector, Data Assessor, and Data Viewer. By default, users are only granted Data Collector and Data Viewer roles unless the organization's existing Administrator or Personnel Manager upgrades those permissions. All users only have access to the data collected in events created by their organization's Event Managers or in events that have been shared with their organization. Event Managers have full control over if and how their events' data is shared with other users or organizations. Event Managers may grant other organizations or specific users access to their events' data. Similarly, they can revoke individual or organizational access at any time, including removing access for individuals within their own organization. In addition, site administrators have access to view all data in RadResponder to provide technical support for users.

The only scenario under which users from other federal agencies may access state, local, tribal, and territorial agency data without explicit permission is during a Stafford Act Declaration. In such a scenario, FEMA Stafford Act Administrators would receive view-only access to data collected as part of the relevant disaster, and could provide view only access to the EPA and DOE/NNSA in order to fulfil their statutory obligations.

8.4 How does the project review and approve information sharing agreements, MOUs, new uses of the information, new access to the system by organizations within DHS and outside?

Most of the user base of RadResponder is from outside of DHS, as RadResponder is a portal to allow smaller organizations to collect and share standardized radiological data. Access to the site by organizations within and outside of DHS is determined via a multi-step process. An individual submits a request for his or her organization to be created in RadResponder with an explanation of that organization's role in a radiological emergency response. Upon doing so the individual must select a "sponsor" that is an organization that already exists in RadResponder. The administrator of the sponsor organization must validate that this new organization is a member of the radiological/nuclear emergency response community who should have access to RadResponder. After the sponsor approves, the request is forwarded to the RadResponder Administrative Team for final approval and creation. New organizations that are not connected to any existing organizations in RadResponder are instructed to select FEMA CBRN as the sponsor. In this case, the FEMA CBRN office and contractor administrative team work together to adjudicate the request.

Responsible Officials

William Holzerland
Senior Director for Information Management
Federal Emergency Management Agency
Department of Homeland Security

Approval Signature

Original, signed copy on file with the DHS Privacy Office.

_____

Jonathan R. Cantor
Acting Chief Privacy Officer
Department of Homeland Security

Appendix A: RULES OF BEHAVIOR

By accessing an event in RadResponder, users will have access to other responders' Personally Identifiable Information (PII), including full name, organization, work email address, work phone number, and Responder Tracking geolocation information, if applicable. This information is collected and shared within an event for the purposes of providing situational awareness to field team coordinators and incident commanders, and providing contact information for data assessors to follow-up with data collectors. Users may not record, copy, share, or act upon this information in a way that is outside the scope of their duties during incident response activities.

By submitting this request, you agree to the RadResponder Rules of Behavior.

Appendix B: METADATA

Radiological Data Type	**Associated Metadata**													
Field Survey	Data Collector	Field Team	Organization	Date/ Time	Location	Comment	Photo	Equipment	Height	Raw Value & Unit	Window Open/ Closed	Orientation		
Field Sample	Data Collector	Field Team	Organization	Date/ Time	Location	Comment	Photo	Equipment	Type	Type-specific info	Volume & Unit	Mass	Sample #	Rate & Unit
Spectrum	Data Collector	Field Team	Organization	Date/ Time	Location	Comment	Photo	Equipment	Height	Dwell Time	Background	Isotope & Confidence Levels	Exposures	
Observation	Data Collector	Field Team	Organization	Date/ Time	Location	Comment	Photo							

Appendix C: FOREIGN ACCESS POLICY

Updated 2/6/2019

Note: The below policy has been approved by the RadResponder FEMA Program Manager and is subject to change at any time following new guidance from FEMA CBRN, other DHS/FEMA offices, or as required by the community and approved by the FEMA Program Managers.

Foreign nationals seeking access to RadResponder fall under one of the following three categories, each of which has unique procedures for approving access. Foreign nationals that do not fall under one of these categories are **not** granted access to the system.

- Foreign nationals working for U.S. emergency response organizations:

  These users may be granted access to the Network via our typical account request process with some additional steps (* indicates additional requirement for foreign nationals).

  1. User submits an account request via the RadResponder website with his/her reason for needing access, basic personal information (organization affiliation, work email, work phone number) and citizenship.
  2. User must validate user's email address via a link sent to user's inbox before proceeding in the process.
  3. The organization's administrator or personnel manager must approve the user's access and indicate the minimum roles/permissions necessary for the user to do his/her job vis-à-vis the Network.

  *4. The RadResponder Administrative Team consults export control and prohibited countries lists to verify that the user's country of citizenship does not disqualify the user from accessing the Network.

  *5. The RadResponder Administrative Team verifies that the user is not on the Consolidated Screening List for export-controlled individuals: (https://www.export.gov/article?id=Consolidated-Screening-List)

  *6. The RadResponder Administrative Team requests verification from the user's organization that s/he is legally employed in that state. An email or other written correspondence from the organization's RadResponder administrator or HR department will fulfill this requirement.

  7. The RadResponder Administrative Team creates the user's account.

  If any of the above conditions are not met, the user's access will be denied. If all of the above conditions are met, the user will be granted access. The following additional restrictions apply to the foreign national after his/her account has been approved:

- The user cannot become a member of an organization other than the one to which s/he originally requested access (cannot hold multiple organization memberships in RadResponder)
- The user cannot access Network-Wide events
- The user cannot access events on which his/her organization is partnered; can only access events sponsored by his/her organization

Note: Unlike foreign nationals working for equipment manufacturers, individuals in this category are not required to re-submit access requests every 90 days.

➢ Foreign nationals working for U.S.-based **OR** non U.S.-based equipment manufacturers seeking to integrate their radiological detection equipment with the Network:

These users may be granted access to the Network via our typical account request process with some additional steps (* indicates additional requirement for foreign nationals).

1. User submits an account request via the RadResponder website with his/her reason for needing access, basic personal information (organization affiliation, work email, work phone number), and citizenship.
2. User must validate user's email address via a link sent to user's inbox before proceeding in the process.
3. The organization's administrator or personnel manager must approve the user's access and indicate the roles/permissions necessary for the user to do his/her job vis-à-vis the Network.

*4. The RadResponder Administrative Team consults export control and prohibited countries lists to verify that the user's country of citizenship does not disqualify the user from accessing the Network.

*5. The RadResponder Administrative Team verifies that the user is not on the Consolidated Screening List for export-controlled individuals: (https://www.export.gov/article?id=Consolidated-Screening-List)

6. The RadResponder Administrative Team creates the user's account.

If any of the above conditions are not met, the user's access will be denied. If all of the above conditions are met, the user will be granted temporary, 90-day access (this duration can be changed on a case-by-case basis at the discretion of the FEMA CBRN Office). The following additional restrictions apply to the foreign national after his/her account has been approved:

- When the account expires, the user must submit a request to extend access for another 90 days (or other pre-determined duration), and provide a reason. The RadResponder Administrative Team will review the request and make a determination on whether or not to approve the extension.

- The user cannot become a member of an organization other than the one to which s/he originally requested access (cannot hold multiple organization memberships in RadResponder)
- The user cannot access Network-Wide events
- The user cannot access events on which his/her organization is partnered; can only access events sponsored by his/her organization
- The user, by virtue of being an equipment manufacturer, cannot view the list of personnel who have RadResponder accounts.

➢ Foreign nationals working for foreign governments or non-U.S. emergency response organizations:

These users are **not** granted access at this time, and are instead encouraged to submit a letter to the FEMA Administrator stating their country's need for a separate instance of RadResponder. The RadResponder Team is awaiting final approval before beginning development on these separate instances.