Feasibility and Demonstration of a Cloud-Based RIID Analysis System

Michael C. Wright^a, Kristin L. Hertz^b, William A. Johnson^b, Eric D. Sword^a,
James R. Younkin^a, Lorraine E. Sadler^b

^a*Oak Ridge National Laboratory, Oak Ridge, TN 37831, USA*

**Corresponding author. Tel.: +1 865 574 5604 Email: wrightmc@ornl.gov*

^b*Sandia National Laboratories, Livermore, CA 94551, USA*

Abstract

A significant limitation in the operational utility of handheld and backpack radioisotope identifiers (RIIDs) is the inability of their onboard algorithms to accurately and reliably identify the isotopic sources of the measured gamma-ray energy spectrum. A possible solution is to move the spectral analysis computations to an external device, the cloud, where significantly greater capabilities are available. The implementation and demonstration of a prototype cloud-based RIID analysis system have shown this type of system to be feasible with currently available communication and computational technology. A system study has shown that the potential user community could derive significant benefits from an appropriately implemented cloud-based analysis system and has identified the design and operational characteristics required by the users and stakeholders for such a system. A general description of the hardware and software necessary to implement reliable cloud-based analysis, the value of the cloud expressed by

the user community, and the aspects of the cloud implemented in the demonstrations are discussed.

Key Words: Radiation detection, gamma-ray spectroscopy, isotope identification, cloud computing

1. Introduction and motivation

In an effort to interdict threat material, the United States has broadly implemented the use of radiation detectors[1]. Radiation detectors are used by federal response teams at national events, customs officers at ports of entry, local law officials on routine patrol, etc. Currently, deployed portable radiation detectors used for isotope identification have onboard analysis software that commonly provides information on the isotope(s) identified and the confidence of the identification, and less often provides the category (medical, industrial, special nuclear material) and threat level of the isotopes. Although the algorithms are continually improving, they still have difficulty accurately and reliably separating threat from benign or background sources. They also have limited ability to use additional contextual information in making an assessment.

One possible solution to this problem is to incorporate cloud-based analysis algorithms into the Concept of Operations (CONOPS) of radioisotope identifier (RIID) use. The National Institute of Standards and Technology (NIST) has defined cloud computing as “a model for enabling ubiquitous, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications,

and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction”[2]. Cloud computing affords the radiation detection community an opportunity for tremendous leverage of private sector developments. The challenge of a cloud-based system is that it must provide accurate results in a timely, secure, and reliable manner that decreases the cost and increases the analysis effectiveness of the response to radiation detection events. Additionally, carrying out analysis and archiving in the cloud provides a number of inherent advantages beyond the simple performance and accurate identification gains of advanced data processing codes.

We have performed an investigation of the strengths and weaknesses of an envisioned cloud-based system to determine if the operational performance of RIIDs could be improved by applying these developments in a way that meets the needs of the national security community.

2. A cloud-based RIID system

The broad use of RIIDs defines a wide range of uses and needs for these devices. The cloud-based system needs to be flexible enough to accommodate these differences. The general work flow of a cloud-based portable detector analysis system is shown in Figure 1. A cloud-based RIID analysis system can take a variety of forms. At the simplest level, the system implementation requires 1) spectra transmission by the RIID to the cloud, 2) automatic analysis of the spectra by the cloud, and 3) isotopic identification and threat rating transmission by the cloud back to the RIID. A more sophisticated process that provides a more rigorous analysis includes the ability to transfer additional

information to the cloud either by user input or peripheral devices. Information could include a background spectrum, calibration spectrum, the distance to the source, the source size, multiple detector readings, etc. The information required for this level of analysis may still be transmitted from the detector, or from an intermediate device like a tablet, to the cloud and back to the detector. Finally, a detailed analysis may be conducted by the user, or a different user located elsewhere, using the state-of-the-art analysis software on the cloud, accessed from a computing device separate from the detector.

Figure 1: Work flow of a cloud-based system. (1) The portable detector collects data. (2) The data are communicated to the cloud using the detector, cell phone, the detector base, or a local computer. (3) Analysis is performed. (4) The results are sent back to the user. (5) Interested parties are notified of the results and/or the data are added to a cloud-accessible database.

Direct linking of RIIDs to the cloud offers a number of potential benefits over the built-in capabilities currently available on the detectors themselves, including the following.

- Improved Analysis – More accurate analysis of the measured data, using software and algorithms that exceed the capabilities of the built-in algorithms
- Streamlined Operation – Ability to directly interact with centralized information systems used by team leaders, incident commanders, headquarters, or analysts

- 90 • Greater situational awareness – Ability to provide a centralized database of all
91 data for user communities that do not already use appropriate centralized
92 information systems
- 93 • Easy updating – Ability to more easily update and maintain the analysis engine,
94 without requiring firmware upgrades by the manufacturer
- 95 • Customizable analysis – Ability to customize the user interface or the algorithm
96 parameters to the specifics of a user or situation, while still relying on the same
97 advanced analysis engine on the back end
- 98 • Data fusion – Ability to incorporate nonspectral information into the analysis
- 99 • Monitoring of RIIDS – Ability to track device firmware; manage energy
100 calibration and detector characterization, history, and state of health; and provide
101 on-line help and instructions
- 102 • Information Security – Algorithms can contain or use sensitive information that is
103 not appropriate for wide dissemination on devices themselves, while the reported
104 results may be sanitized of these sensitivities.

105 The greatest concern to a cloud-based system is its reliance on having access to
106 the cloud, which makes the system susceptible to outages due to network blackouts,
107 network congestion, or just poor connectivity conditions. Most emergency responders
108 have access to a variety of communication systems that will mitigate this problem.
109 However, there is always the possibility that connectivity will not be possible. When the
110 cloud is not available, the RIIDs must rely on their onboard algorithms for analysis and
111 local analysts. The cloud does not replace the existing methods; rather, it enhances them.

A field-deployable processing and analysis server is one option to mitigate internet connectivity loss. Certain processes to maintain and secure a field-deployable server would be necessary to ensure it is up to date with the current cloud implementation and to physically protect its algorithms. Providing the information security barriers to prevent misuse is paramount to a cloud-based implementation; mutual authentication between the cloud servers and the fielded devices and data authentication are proven approaches to deny access by unauthorized users and prevent malicious alteration of transmitted results.

Finally, an important note critical to all radiation detection is that analysis results are highly dependent on good-quality data being collected by the user and provided to the analysis engine. The proposed cloud system may be used to assist in the collection of high-quality data from the user community by encouraging standardized data formats and good data collection techniques. Advanced pre-processing algorithms to perform auto calibration and background estimation and analysis prior to spectral analysis of the RIID data and the incorporation or fusion of the results of multiple analysis algorithms can also be performed in a cloud paradigm.

3. Architecture and technical issues

The technology can be separated into three sections: 1) data collection, transmission, and user interface; 2) data analysis algorithms and archiving on the cloud; and 3) security and account management. A proposed architecture for implementation of cloud-based analysis is shown in Figure 2. The system must be flexible enough to support

a wide range of device types that may send data to the cloud in a number of ways. This includes the device itself sending data to and editing data on the cloud, the device sending data through a bridge device such as a cell phone, or the data being extracted from the device and uploaded manually. The cloud system should include the ability to receive raw data electronically and provide analysis results that can be read either by requesting the data from the server and displaying it on the device or by requesting and viewing it using a web interface. Additionally, the cloud system should support authentication strong enough to protect the integrity of the data, but general enough to be compatible with a wide range of devices.

Figure 2. Architecture for cloud-based RIID system for the use-case of a RIID device coupled with a network bridge device.

3.1. Data Collection, Transmission, and User Interface

The success of the RIID cloud-based analysis system is dependent on its ability to accept data from a broad field of possible detectors used to acquire data. For example, this feasibility study includes spectroscopic detectors only, but the protocols should be

defined broadly such that gross counting devices and neutron analysis may be added as well. Ideally, the cloud will support a wide range of detectors and CONOPS in a manner that is relatively simple from the user's viewpoint. Thus, it is necessary to ensure that there is consistency in the way data are transmitted and formatted so that they may be used by the cloud server.

Furthermore, detector outputs vary widely depending on the vendor and type of the device. Many vendors format the detector data in a proprietary format. Even in the set of devices that produce ANSI N42.42[3] compatible XML files, there is much variation in how information is presented due to that standard being very broadly defined. The recent update (2006 N42.42 to 2012 N42.42) of the standard is more strictly defined and will reduce variations. Therefore, the cloud must either be able to accept this varied output or the cloud may restrict the structure of the data, requiring some adjustment to data produced by existing devices. In the end, it may be necessary to consider adding extensions to the existing standard to add support for quantities not explicitly included. The N42.42 format accommodates extensions to allow incorporating additional or vendor-specific information.

By the nature of the cloud-based solution, a data link to the server must be provided. Most RIIDs built today have the ability to send data via Bluetooth or some other wireless mechanism to a nearby device. Thus, a data file may be sent from the detector directly to the cloud or to an intermediate bridge device and then to the cloud for analysis. This data transmission is commonly accomplished using a local Wi-Fi network or a cellular connection. In areas without such connectivity, a portable satellite connection may be used, although its bandwidth is significantly lower. The transfer speed

may be improved by compressing the data on upload and download. Field-deployable “personal cell towers” known as cellular base stations are being used in areas that have poor cellular coverage or in large buildings and malls to provide better signals. One significant advantage of these base stations is that they can be configured to only associate with specific communications devices.

Of primary importance to a user in the field is how quickly analysis results are returned. This depends primarily on two factors: the connection speed and the time required by the analysis algorithm running on the cloud server. In areas where the link to the cloud is fast, such as areas with Wi-Fi or 3G/4G data service, the analysis algorithm execution time will be the dominant factor. During surge activities, the cloud server could be a possible bottleneck if it is not adequately provisioned to handle the upload, analysis, and download of varying quantities of data in a timely manner.

Often additional information is useful for the analysis, such as the type of spectrum (background, calibration, or unknown), source-to-detector distance, description of intervening materials, etc. Generally, detectors themselves do not handle this type of information, so the data must be supplied using a web-connected portable device. This is the most problematic step in the process to automate. Currently, most methods in use are time-consuming and awkward if performed with a small screen on the RIID itself. Discussions with end users and integration with current systems will influence the method in which this is handled by the cloud-based systems.

Interaction with the cloud-based system will also be available via a website or tablet application to allow an authorized user to access uploaded data or analysis results whether the user is part of the measurement team or is remotely located.

199

200 3.2. Analysis Algorithms and Archiving on the Cloud

201

202 The cloud can offer either minimal services or highly sophisticated services,
203 depending on the user and the situation. At a minimum, when the data are sent to the
204 cloud, it must be able to receive the gamma spectral data, parse the data, analyze the data,
205 and send the results back to the user. Isotope identification is a necessary result, followed
206 by a threat/no threat assessment. Other results such as isotope quantity or other
207 information based on comparisons to previous data may be of value as well.

208 For most current, widely used detectors, the detector specifications and nonstandard
209 data file formats are already understood and parsed by tools such as Cambio[4], whose
210 parsing capabilities are utilized by GADRAS[5]. For the remainder, this information
211 needs to be provided by the detector's designer, reverse engineered, or converted to an
212 accepted format externally before it can be used with the cloud.

213 In addition to the unknown spectrum, accurate automated analysis generally
214 requires a background spectrum and a calibration spectrum. Analysis results are
215 improved, particularly confidence levels, with the additional information and detector
216 characterization, as depicted in Table 1. To determine isotope quantities, it is necessary to
217 provide the source-to-detector distance. The analysis algorithm may estimate intervening
218 materials, but greater accuracy and confidence are achieved when external knowledge of
219 these materials is available. In some cases, this is easily measured and may be sent to the
220 cloud. Sometimes the source is behind a wall or in a container and the distance is

unknown. The cloud could be configured to prompt the user to take the multiple measurements necessary to use the inverse square law to determine the distance.

Table 1. Measurement requirements for various automated analysis results

	Isotope ID	ID Confidence	Threat/No Threat	Quantification	Masking
Unknown spectrum	Need	Need	Need	Need	Need
Background spectrum	Better	Better	Better	Need	Need
Calibration spectrum	Better	Better	Better	Best	Best
Source-to-detector distance	Best	Best	Best	Need	Need
Intervening Material	Best	Best	Best	Best	Best

Full spectrum analysis algorithms used by software such as GADRAS provide higher quality results when the detector response function is well characterized. In the cloud it is possible for a detector characterization to be customized for each detector by registering the device and providing the necessary measurements. Submission of a series of spectrum uploads could be defined (sources and distances), and the analysis service may be able to carry out the characterization automatically. Energy calibration needs to be done with each submission and may be accomplished either by sending energy calibration coefficients to the server or by uploading appropriate spectra along with source information and having the analysis service carry out calibration automatically.

As the complexity and accuracy of the analysis algorithms are increased, the computational time available to make a decision with the given data will be increased. Harnessing the distributed and expandable computing available with the cloud significantly reduces this limitation by allowing many computers to work together to

239 solve a problem using algorithms that otherwise would not be viable. Current algorithms
240 may be altered to search for a larger number of isotopes and shielding configurations,
241 make full use of the detector's resolution, as well as relax some of the simplifying
242 assumptions used. New algorithms that will become computationally feasible may not
243 only be able to be intrinsically more sensitive or accurate but may be able to provide
244 more information than currently available from the analysis algorithms. For example, an
245 algorithm may apply computationally expensive statistical methods to determine the most
246 likely source and shielding information as well as provide more rigorous confidence
247 levels about the maximum amount of a dangerous material that could be present, a
248 process that may require thousands of forward simulations.

249 Beyond the ability to increase the fidelity of the analysis algorithms, there is the
250 possibility of storing data sent to the cloud for archiving and further analysis. This adds
251 powerful features to the overall system. The cloud-based analysis may pull information
252 and metadata from other sources such as weather, cargo manifests, data trending for the
253 region, etc. In addition, the cloud can be manipulated to assist with training exercises, in
254 which previously acquired data could easily be substituted for, or injected into real data,
255 to facilitate training scenarios.

256 The analysis features that could be implemented by the cloud are numerous. The
257 features rely on various characteristics that the cloud may provide. Some examples are as
258 follows.

- 259 • Integration of analysis tools developed and maintained by national labs
- 260 • Ability to perform analysis from multiple algorithms and weigh the results
- 261 • Tracking individual devices including device history and state of health

- Automated sharing of data based on user preferences
- Pushing of software updates to detectors
- Assist with training scenarios
- Dynamic adjustments to decision thresholds based on situational awareness
- A large database of diverse data sets and cases for testing and validating new and refined algorithms

3.3. Security and Account Management

A necessary component of a cloud-based system will be information security. Various approaches to user authentication and data encryption involve a trade-off between security and ease-of-use on mobile devices. The primary layer will be user authentication. This could consist of a simple password or more secure methods such as access tokens or detector hardware address verification. Users will have accounts on the cloud that they can access from the detector directly or from a computer of some type. The user will be able to set up and manage their accounts. User groups may be formed to allow for various levels of information sharing and access.

Gamma-ray spectra by themselves are generally not considered to be sensitive. However, when combined with other information, such as user location or name of user, then the data may become sensitive and require encryption. Many standard encryption techniques are widely available.

The detail included in results sent back to the user could be customized based on who the user is, what information the user needs, and the security implications of

285 providing that information. At the simplest level, a law enforcement officer may only
286 receive a threat/no threat response. This response could include isotope identification,
287 confidence, and a threat assessment. A more advanced user may receive more
288 information than an average user. This could include an energy-calibrated, background-
289 subtracted spectrum with the gamma peaks corresponding to the identified isotopes
290 highlighted in some way. A user at the command center would have access to situational
291 information beyond just the radiation detection information.

292 For some applications, proper data security during transmission must be enabled.
293 This may involve encryption of the data while in transit and in storage, authorized
294 authenticated access, access controls, etc. Some of these capabilities may require
295 hardware support (encryption hardware, access tokens, etc.), or they may be implemented
296 in software.

298 **4. User needs for a cloud-based RIID system**

300 A systems study was performed to look at the radiation detection mission
301 architecture and determine the benefits, risks, and costs, as well as a guide for
302 development of a cloud-based RIID system. The cloud system would optimize the
303 already substantial amount of money that has been spent to train and equip federal, tribal,
304 state, and local agencies in order to increase the system capabilities without placing
305 additional burdens on the users. The impact of a cloud-based RIID analysis capability
306 was considered for the various users of such a system, as well as the necessary steps and
307 objectives required for its implementation.

Various potential users of the system were interviewed and observed in order to assess the potential benefits and impacts on field operations of a cloud-based analysis system. First responders want rapid analysis results and quick rejection of clearly innocuous alarms, compatibility with existing CONOPS, easier communications with incident commanders, retention of onboard capabilities supplemented by reanalysis in the cloud, and field operation readiness. Operation managers, who may be on site or located remotely, want high-confidence adjudication of the alarms, robust and accurate decision-making tools, fast decisions and communication with the cloud, and the ability to train and guide first responders to take accurate data. Data analysts, who also may be on site or located remotely, want streamlined data transfer for rapid access to the spectral data, fusion of nonspectral data into the analysis, the ability to promote good data collection in the field, and training via the use of historical data and analysis. Some potential user communities already have centralized information management systems, and the cloud-based RIID system should be able to work in cooperation with those systems rather than being a replacement for them.

5. Demonstration of a prototype cloud-based analysis system

A small-scale prototype cloud-based analysis system demonstrating most of the aspects of the architecture in Figure 2 was implemented to show its feasibility and to gain practical experience. The system was demonstrated using three widely deployed commercial off-the-shelf (COTS) systems, as well as a custom-built detection system, to take data and send it to the cloud for analysis. Two different algorithms were used to

analyze the data. Analysis results were then returned to the detector for those devices which had the ability to receive results onboard. For the other systems, the results could be viewed on smartphones, tablets, or laptop computers. Using a web interface, additional information could be added to the analysis, the full-spectrum regression fits could be viewed, and the data could be downloaded for further analysis.

The model for a cloud-based analysis system for RIIDs consists of five components: 1) the detector, 2) the link between the detector and a bridge device, 3) the bridge device, 4) the link to the cloud, and 5) the cloud server, as shown in Figure 3. The server incorporates the analysis software, storage of data, and any additional tools that may enhance the cloud's capabilities. The technology integration demonstrations showed an implementation of the five components of the detector-to-cloud communications model. The specific components selected for the five different configurations that were demonstrated are shown in Figure 3.

Detector	Link to Bridge	Bridge	Link to Cloud	Security Barrier	Server
DigiBase	-	Embedded	Wi-Fi	HTTPS	GADRAS /
Identifinder2	Bluetooth	Phone	Cellular	HTTPS	DHSIsotopeID
Detective	Ethernet	PDA	Wi-Fi	Password	HPGeFSA
Falcon 5000	Ethernet	XP Tablet	Wi-Fi	Password	Database
(Viewer)	-	Tablet	Wi-Fi	Password	

Figure 3. The components of a cloud-based RIID analysis system implemented in the small-scale demonstrations.

5.1. The Detectors

The four detectors chosen for the demonstrations are either traditional RIID devices or a portion of a larger device that includes a built-in data router. The technology demonstrated included building a device specifically for integration with the cloud as well as tying currently deployed detectors to the cloud analysis server. The laboratory-built system makes use of a NaI detector with an ORTEC digiBASE multi-channel analyzer (MCA) integrated with a small form factor computer and a touchscreen for the user interface. The commercially available systems used were a FLIR NaI identiFINDER 2 and two HPGE systems, the ORTEC Detective and a Canberra Falcon 5000.

5.2. Link to the Bridge Device

The link to the bridge device provides an exposed communications interface between the detector counting electronics, MCA, or instrument and a bridge device responsible for uploading data to the cloud. A separate bridge device is not required for every RIID, though most currently fielded detectors will not have a native ability to send data to the cloud. The link to the bridge device may be accomplished by wireless methods, such as short-range Bluetooth or Wi-Fi, or in the case of older detectors, wired methods such as serial ports, USB, or Ethernet. The laboratory-built detector has an integrated computer with Wi-Fi capability; therefore, no bridge device is needed. The identiFINDER 2 natively passes N42.42 files via Bluetooth or USB link through a bridge device, using its built-in “reachback” functionality. The Detective’s built-in controller, a

Windows Mobile PDA, is capable of Wi-Fi communications; therefore, no separate bridge device is needed. The networked controller for the Falcon 5000 is a Windows XP tablet with various internet connectivity options: Wi-Fi, Bluetooth and USB tethering, and Ethernet. The Falcon 5000 controller is the bridge device for the acquired Falcon 5000 spectrum files.

5.3. Bridge Device

The bridge device is responsible for providing connectivity between the RIID device and the cloud. In some cases it is also used to append metadata, such as user information, to the acquired spectrum. It is critical that the implementation of the bridge device be as unobtrusive as possible. A separate bridge device is required in many cases because most currently available detectors are not designed to work with the cloud natively. A deployed system will need to be able to accommodate older detector designs while optimizing the value of the cloud for newer detectors that are able to integrate directly with it. The laboratory-built detector makes use of its built-in computer as the bridge to the cloud, as well as the data acquisition controller and processor. The software packages the measurement with a background, calibration, and user identification information in 2006 N42.42 format. Results are retrieved automatically and displayed in real time along with the live data acquisition. The identiFINDER2 system can utilize any device that has network connectivity and can share that network connection via a Bluetooth personal area network as its bridge device. The Bluetooth tether to 3G/4G/Wi-Fi gateway solution used here was tested with iOS, OSX, and Windows. The bridge

device can use its own sensors and other capabilities to incorporate supplemental data such as GPS, inclinometer, gyro, compass, and mapping information.

A software bridge is used for a class of instruments that is integrated at some level with a controller that runs the vendor's data acquisition package and has hardware network connectivity but does not know how to send its files to the cloud. The two software bridges that were developed for this project share a common code base with minor differences attributed to tailoring the graphical user interface to the respective PDA and tablet screen sizes and navigation differences. The software bridge for the Detective is targeted for the Windows Mobile operating system and gives it the ability to upload data to the cloud for analysis directly from the PDA. The software bridge for the Falcon 5000 is targeted for its data acquisition controller—a Windows XP tablet.

5.4. Link to the Cloud and Security

The link to the cloud is made through Wi-Fi, 3G/4G data network, or satellite communication to a remote server located at ORNL and/or Sandia National Laboratories (SNL). Encryption, authentication, and data compression occur across this link. There are two primary concerns when considering the secure transfer of data over a network. The first concern is the security and integrity of the data itself, and the second is the security and integrity of the transfer method. For the purposes of this discussion, data security is focused on preventing unauthorized access to the data, while data integrity is concerned with ensuring that the data are not corrupted in transit or storage. Although the purpose of this document is to discuss the transfer of files, it is important to keep in mind the

security of files on both the server and the device. In the proof-of-concept system, security is accomplished using HTTPS, which makes use of SSL/TLS as the security protocol. The initial communication to post data and get analysis results is made via a web application due to familiarity with the process and the ability to collect user input in a unique format for analysis (i.e., background spectrum labeled as such).

5.5. Cloud Server

A demonstration cloud-based server architecture was developed in order to allow testing the practical aspects of the platform, as well as to facilitate the automatic analysis of recorded spectra by DHSIsotopeID[6] and HPGeFSA. The server implementation shown in Figure 4 provides five functions: the web-based user interface, an HTTP file upload and results transmission mechanism, database storage, an analysis queue, and detector support. A single computer instance could host any combination of the parts, or multiple computer instances could host the same part to distribute the load across multiple servers, provided each of the four parts are hosted on at least one instance. For the demonstration, a Linux virtual machine hosted on the Sandia cloud, physically in New Mexico, ran the user interface and detector upload portions, while the database was hosted on a Macintosh desktop located at Sandia California, and the analysis queue was hosted on both the Sandia cloud located in New Mexico and on a Linux virtual machine hosted on a Macintosh laptop located in California. For the demonstration, the ability to dynamically add and remove server instances was not implemented since the load was not expected to exceed the fixed resources.

442

443

444 Figure 4. Software available on the cloud server to accommodate data analysis, data archiving, and detector
445 support.

446

447 6. Conclusions

448

449 The implementation and demonstration of a prototype cloud-based RIID analysis system
450 have shown this to be feasible with currently available communication and computational
451 technology. The system study has shown that the potential user community could derive
452 significant benefit from an appropriately implemented cloud-base analysis system and
453 has identified the design and operational characteristics required by the users and
454 stakeholders for such a system. The cloud-based system is proposed as an addition to,
455 rather than a replacement for, existing systems and CONOPS. An architecture was
456 defined for a production-level system for field testing by actual users in operationally

relevant environments. A spiral development process is envisioned to prioritize implementation of new functionality based on results of user testing and evaluation.

Acknowledgments

The authors would like to thank Dr. Matthew Kiser of the Remote Sensing Laboratory at Andrews Air Force Base for his advice, support, and encouragement during the execution of the project and for providing the host location for the final project demonstration. This work was supported by the U.S. Department of Energy National Nuclear Security Administration Office of Defense Nuclear Nonproliferation Research and Development. This support does not constitute an express or implied endorsement on the part of the Government.

Sandia National Laboratories is a multi-program laboratory managed and operated by Sandia Corporation, a wholly owned subsidiary of Lockheed Martin Corporation, for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-AC04-94AL85000.

This manuscript has been authored by Oak Ridge National Laboratory, managed by UT-Battelle LLC under contract no. DE-AC05-00OR22725 with the US Department of Energy. The US government retains and the publisher, by accepting the article for publication, acknowledges that the US government retains a nonexclusive, paid-up, irrevocable, worldwide license to publish or reproduce the published form of this manuscript, or allow others to do so, for US government purposes.

480

481 **References**

- 482 [1] *Preventing Nuclear Terrorism: Does DHS Have an Effective and Efficient Nuclear*
483 *Detection Strategy*, 2012 (testimony of Dr. Huban Gowadia, Domestic Nuclear
484 Detection Office Acting Director). Print.
- 485 [2] National Institute of Standards and Technology, US Department of Commerce,
486 Special Publication 600-145, “The NIST Definition of Cloud Computing,” September
487 2011.
- 488 [3] ANSI 42.42-2012, American National Standard Data Format for Radiation Detectors
489 used for Homeland Security.
- 490 [4] “Capabilities, Methodologies, and Use of the Cambio File-Translation Application”,
491 George P. Lasche, Sandia National Laboratories, March 2007. SAND-2007-1841.
- 492 [5] “GADRAS User Manual,” Dean J. Mitchell and David R. Waymire, SNL,
493 November 2009.
- 494 [6] “DHSIsotopeID and Full-Spectrum Analysis Methods in GADRAS”, Dean J.
495 Mitchell, Sandia National Laboratories, April 3, 2009. SAND 2009-2544P.