Statement for the Record, September 14, 2009

Hearing before the Homeland Security Subcommittee on Emerging Threats, Cybersecurity, Science and Technology

Respectfully submitted by: IP Radiation Security Associates
Stamford, CT 06902

Dear Chairwoman Clarke and Members of the Subcommittee:

My name is Keith Reynolds and I am the founder and principal of IP Radiation Security Associates. I am also a co-founder of a company that develops software to improve response procedures in the case of a radiological event. I continue to work with Internet Protocol-based security and radiation instrumentation companies to make our world safer from criminal use of radiological materials. We are employing Internet Protocol (IP) technologies to tie commercial, off-the-shelf (COTS) security systems together with a variety of radiation detectors.

By networking radiation and various other COTS security systems we can enhance the security of radiological sources, improve first responder's ability to react to a radiological event and reduce costs compared to proprietary detection systems. The implementation of IP Radiation Security (IPRS) systems is especially important to the programs like the Global Threat Reduction Initiative (GTRI) and those considered under House Bill HR 2070, the Radiological Materials Security Act introduced by Chairwoman Clarke. As taxpayers we will be afforded greater protection for the money spent in this critical area.

The threat of terrorists abusing radioactive materials is grave. The sheer availability of sources in facilities employing less than optimal security programs creates a need for more public and private investment in new security systems. We must also rethink how security is implemented based on the improvements new technologies enable. Such changes necessitate new knowledge and training to be sure. However, the risk posed by the status quo is high. In my own work over the last several years I have been in situations where I have had access to significant amounts of radiological materials in facilities I would consider less than secure.

I submit this Statement for the Record to highlight the threats posed by radiological sources and offer a cost-effective solution for government and private efforts to secure them.

The Threat Posed By Legitimate Radiological Materials

In the USA alone, there are nearly 23,000 licensees using radiological materials. These users are charged with the security of roughly 2 million sources. There are some 10 million sources worldwide.

Radiological materials can uniquely help solve the world's food, energy, environmental and cancer problems. However, growing use of radiological material in these sectors, combined with the global threat of terrorism, has increased the risk of unwanted radiation exposure. Accordingly, radiation security has become as important, if not more important, than the traditional Radiation Safety model, which has existed for over 50 years.

A small amount of conventional explosives combined with stolen radiological material is enough to create a "dirty bomb" (or RDD, short for Radiological Dispersion Device). 1,000 curies of Cesium-137 (Cs-137) could fit in a soda can. Between 50 and 100 curies of Cs-137 is enough to make a RDD that could shut a Grand Central Station-sized building for a year or more as crews clean up the facility to achieve federally mandated background radiation levels.

A dirty bomb would not likely kill large numbers of people from radiation poisoning. Such a device would certainly cause massive economic disruption. Estimates are for up to $100 Billion to clean up dispersed material[(1)] and as high as Trillions in economic losses[(2)]. A "Radiological Emissions Device," where a relatively small amount of radiological material is left in a public facility, presents a scenario that could potentially injure or kill hundreds of people. Widespread societal panic will surely ensue in both cases.

The Problem of Lost or Stolen Sources and Illicit Trafficking

The International Atomic Energy Agency (IAEA) has recorded 1,562 nuclear trafficking incidents from 1993 through 2008. Worldwide, the number of reported cases of lost and stolen radiological materials has been increasing according to the IAEA. These incidents range from illegal efforts to dispose of radioactive materials, to discovery of "orphaned" nuclear material of unknown origin. In its 2008 annual report released in August of this year, the IAEA received reports of 15 cases of clandestine nuclear possession, or related incidents and 16 cases involving theft or loss of sensitive substances. According to the IAEA, these incidents are part of 119

events that were added to the IAEA's Illicit Trafficking Database in 2008, while this year to June, the agency has received reports of 215 incidents. That is up from 85 two years prior, though the IAEA does have participation by additional countries.

In an August 1, 2007 NY Times editorial entitled "Seize the Cesium" by PETER D. ZIMMERMAN, JAMES M. ACTON and M. BROOKE ROGERS: "In the United States, commercial users lose about one radioactive source a Day… through theft, accidents or poor paperwork. One of these is recovered perhaps every two days, either because the radioactive materials are voluntarily returned or because of good detective work."

I have been studying the daily incident report activity posted on the Web site of the Nuclear Regulatory Commission (NRC). Besides Cs-137, of greatest concern to me is the number of incidents involving significant amounts (30-100 Curies) of Iridium-192 (Ir-192) being deployed in the field of radiography for applications such as verifying pipeline welds. This survey of the NRC database of reported incidents over the last several months show just how prone to human error security is and highlights there is room for improvement. I submit for the record one of these incidents where an improved security system that integrates radiation detection, surveillance and communications could have helped. More are posted with comments on our Web site, www.IPradiationsecurity.com (with commentary) and at www.nrc.gov.

Weapons of Mass Destruction

The Commission on the Prevention of Weapons of Mass Destruction Proliferation and Terrorism's Report to US Congress submitted December 3, 2008, quoted Dr. Mohamed ElBaradei, Director General of the International Atomic Energy Agency (IAEA) speaking to the United Nations General Assembly on October 28, 2008: "The possibility of terrorists obtaining nuclear or other radioactive material remains a grave threat… It is more likely than not that a weapon of mass destruction will be used in a terrorist attack somewhere in the world by the end of 2013." In my own opinion, a RDD is probably the most likely weapon to be used.

Programs to mitigate "loose," or under-protected source materials are growing at home and abroad. In the USA, we have seen the NRC promulgate the Orders of Increased Control, GTRI has seen increased funding and the Radiological Materials Security Act has been introduced a second time. Abroad, radiological security has become a way for President Obama

to engage the world from a foreign policy standpoint. Not only does the president advocate for the reduction of nuclear weapons through arms reduction agreements, but there is also a significant effort underway through these discussions to increase security of all other radiological material that are at risk.

Funding security enhancements and implementing networked radiation-monitoring systems that are interoperable with the security systems already in place are two large challenges that we face in addressing these security questions. Internet Protocol (IP)-based radiation detection systems can help make our nation safer from radiological abuse by lowering costs and facilitating systems integration -- Just as the Internet has revolutionized many aspects of our society, we can apply these technologies to do a better, faster and more cost-effective job protecting ourselves from the threats of radiological terrorism.

What is IP Radiation Security?

A fully integrated enterprise security system provides near real time monitoring of persons who enter facilities that house radiological materials and enhances control and reporting capabilities. Such systems integrate and utilize information from many discreet security systems.

IPRS combines digital, or "IP-enabled" radiation monitoring systems with other IP security tools, such as video surveillance, access control, motion detection, and the enterprise security management software in an integrated solution, or "systems of systems" approach. By combining specialized tools it is possible to better manage response procedures or “CONOPS” in case of a radiological event. Beyond better procedural response, IP Radiation Security tools can improve things such as forensic analysis, security policy, training and reporting. IPRS video systems can even automatically save video of an incident in a court-admissible format for evidentiary purposes.

There are three major categories of radiological security:

1) Custodial – protecting materials in the places where they are used.
2) Transport – monitoring the flow of goods and people to stop unwanted movement of illicit materials

3) Ingress – protecting potential target locations from a dirty bomb, or possibly the arrival of patients to a medical facility after a nuclear event.

For the purposes of this hearing on Radiological Source Protection, I have highlighted the application of these systems to Custodial activities. It should be noted that IP security tools could also be applied to Transport and Ingress applications. The waste management industry is one additional sector that can also use IPRS tools to help eliminate radioactive materials from transfer stations and landfills; again, not the focus of this Statement of Record.

The IAEA recently released publication number 1387, entitled **Security of Radioactive Sources**. It is an implementation guide for the security of facilities housing radiological sources that provides a comprehensive tool for legislators and regulators, physical protection specialists and facility and transport operators, as well as for law enforcement officers. (STI/PUB/1387, 66 pp.; 2009, ISBN 978-92-0-102609-5, English. Date of Issue: 6 July 2009.)

Below, I have enclosed Table 2 from IAEA's Security of Radioactive Sources publication, which outlines the specific objectives of a radiological security program, based on the prerequisite threat assessment that drives the prescribed security functions. This table identifies the many ways a fully integrated systems approach to radiation security can help to achieve the program recommended by the IAEA.

IPRS systems can be designed for a stand-alone facility, or to be incorporated into an enterprise security management software environment to maximize the scope of response capabilities. Systems can even enable communications that span across organizational boundaries. In all cases a threat assessment is conducted, and a security plan is developed, prior to systems design.

Below the IAEA's Table, I have taken the recommended security functions and measures presented in the IAEA guide and provided a lower level of detail to show how a range of commercial IP security systems, configured to work together with IP-enabled radiation instrumentation, can increase the likelihood of achieving the IAEA's stated security objectives.

TABLE 2. SECURITY LEVELS AND SECURITY OBJECTIVES

Security functions	Security objectives		
	Security Level A Goal: Prevent unauthorized removal[a]	Security Level B Goal: Minimize likelihood of unauthorized removal[a]	Security Level C Goal: Reduce likelihood of unauthorized removal[a]
Detect	Provide immediate detection of any unauthorized access to the secured area/source location		
	Provide immediate detection of any attempted unauthorized removal of the source, including by an insider	Provide detection of any attempted unauthorized removal of the source	Provide detection of unauthorized removal of the source
	Provide immediate assessment of detection		
	Provide immediate communication to response personnel		
	Provide a means to detect loss of source through verification		
Delay	Provide delay after detection sufficient for response personnel to interrupt the unauthorized removal	Provide delay to minimize the likelihood of unauthorized removal	Provide delay to reduce the likelihood of unauthorized removal
Response	Provide immediate response to assessed alarm with sufficient resources to interrupt and prevent the unauthorized removal	Provide immediate initiation of response to interrupt the unauthorized removal	Implement appropriate action in the event of unauthorized removal of a source
Security management	Provide access controls to source location that effectively restrict access to authorized persons only		
	Ensure trustworthiness of authorized individuals		
	Identify and protect sensitive information		
	Provide a security plan		
	Ensure a capability to manage security events covered by security contingency plan (see the Definitions)		
	Establish security event reporting system		

[a] Achievement of these goals will also reduce the likelihood of a successful act of sabotage.

Systems and their Capabilities

- Radiation Detection: Alerts from "stand-off" IP sensors that sit on the security network and are strategically placed in a facility. These sensors can transmit the "activity" levels in terms of dose rate to first responders. These sensors give an indication of the strength of the source and "energy level," which helps to provide an indication of the isotope that has been detected. Software from Defentect in Norwalk, CT can gather specialized radiological data from many types of detectors from manufacturers like Ludlum Measurements, located in Sweetwater, TX, and transmit "intelligent" alerts to the other components of the security framework to help radiation safety personnel, security professionals and public safety officials better understand the situation to which they are responding.

- Video Surveillance: Video from cameras in the area that would capture a person's image and for storage in Digital Video Recorders. Robust video surveillance software addresses many other functions. Systems, like those from OnSSI of Pearl River, NY, enable customized viewing of many cameras, pushing of video to specified personnel on preset events, storage and archival management of thousands of hours of recorded video, easy search interfaces to help security and radiation safety personnel investigate incidents and saving of video in tamper-proof court-admissible format. These systems offer "analytics," such as license plate recognition and specific detection rules for identifying suspicious activities.

- Access Control: Authorized persons requiring access to a facility are required to provide information for use in conjunction with a magnetic swipe, or RFID card. Identity confirmation is made whenever the card (with PIN if required) is used to access a door in the facility. The database record created in the system can include the person's name, the door accessed and date/time of the attempt to access a doorway. This information can be combined with other elements of a comprehensive security management system.

- Interaction with a "tamper strap" device used to monitor the containment receptacles in which radiological materials are stored can trigger video surveillance, text messaging and calls for personnel to investigate the incident.

- Motion detection, a common feature of IP video surveillance management systems from companies such as OnSSI, triggers alerts to be generated to the system. Infrared sensors can also identify motion in a facility.

- Dry contact devices, which indicate that an analog electronic circuit has either been opened or closed. These enable a wide range of capabilities from identifying open windows to taking the pulse from an analog radiation detector. Equipment from companies like Defentect now exists to "digitize" the pulse from analog radiation instrumentation, so that the signal can be included into an IP radiation security system to enhance required security procedures.

- Systems can automatically generate instructions based on predetermined events to minimize injury, or loss of life. Documented response procedures, or CONOPS can be presented to responders in a variety of formats, so that they react to an event in the best possible fashion as outlined in planning and training.

Finally, all of these components must be configured to enable a faster, more informed response by police, fire, medical, and private security -- in addition to management and regulatory officials. A security infrastructure must offer multifaceted communications and messaging between humans and machines. Examples of such communication ranked in order of response criticality include:

1) Send relevant data to other components of the security system on the IP Network using a protocol called "XML."
2) Broadcast video to guard stations, cars, handheld devices, cell phones, laptop computers.
3) Send SMS text messages with incident details to responder cell phones and pagers.
4) Send emails with incident details to personnel who need to be informed, but not necessarily respond immediately.
5) Log all data (including video) to a database for later reporting, forensic analysis, training or policy analysis and future personnel training.

With proper design and integration, mobile and wireless systems can also be supported to extend the security zone.

Conclusion

Certainly, terrorists have proven their capability to commit crimes against unsuspecting targets, making radiological security a bigger concern than ever before. While radioactive materials offer significant benefits to society and the vast majority is in well-secured environments, there are cases where responsible licensees have lost control of those sources. These cases represent only a small fraction of the total sources in use, but there have been a few cases of accidents, which have yielded serious consequences. Terrorism would make a radiation situation far worse and create serious consequences for civil society.

Vendors have begun to market COTS IPRS solutions that need broader consideration. A growing number of radiation control, physical and homeland security and information technology professionals believe additional safeguards, including the networking of radiation detectors with IP-based security systems, is needed.

By including IPRS as part of an overall program that utilizes industry standard IP security and surveillance tools, users of radiological materials – and others concerned about securing facilities from threats posed by radioactive materials – can implement radiation security and response systems on a broader and much more cost-effective basis than the proprietary systems deployed since 9/11.

IPRS is a natural extension of "digital convergence" in the disciplines of security and information technology. IPRS offers a reliable and cost-effective means to provide higher security for radiological materials. Security tools that are commercially available today can not only increase security, but also reduce start-up and operating costs in implementing large-scale source protection initiatives.

Thank you for the opportunity to submit this Statement for the Record. I am available to answer any questions you may have.

APPENDIX A:
NRC INCIDENT REPORT POST FROM IPRADIATIONSECURITY.COM BLOG:

This is a case where IP radiation security systems would improve the understanding of what happened. Networked surveillance video and IP radiation sensors that work in concert with each other should have monitored the door and strategic internal locations. The video images and any radiation information (dose rate, count rate, energy level, isotope) could have been immediately transmitted to guard stations, corporate RSOs, local and state authorities, etc. as part of the standard response procedures in a comprehensive security plan.

==

General Information or Other	Event Number: 45301
Rep Org: GEORGIA RADIOACTIVE MATERIAL PGM Licensee: KAISER PERMANENTE Region: 1 City: JONESBORO State: GA County: CLAYTON License #: GA1276-1 Agreement: Y Docket: NRC Notified By: ERIC JAMESON HQ OPS Officer: DAN LIVERMORE	Notification Date: 08/26/2009 Notification Time: 16:00 [ET] Event Date: 08/22/2009 Event Time: 07:30 [EDT] Last Update Date: 08/26/2009
Emergency Class: NON EMERGENCY 10 CFR Section: AGREEMENT STATE	Person (Organization): JOHN WHITE (R1DO) LANCE ENGLISH (ILTA) GREG SUBER (FSME)

Event Text

AGREEMENT STATE REPORT – EXTERIOR ACCESS DOOR TO RADIOLOGY LAB FOUND OPEN
While responding to an audible alarm, the Clayton County Police Department found an exterior door open to the Radiology Lab at the Kaiser Permanente Nuclear Medicine Clinic located in Jonesboro, Georgia. The Clayton County Police Department notified the Federal Bureau of Investigations and the Georgia Information Sharing and Analysis Center. The Georgia Information Sharing and Analysis Center then contacted the Georgia Radioactive Materials Program.
The licensee is authorized to possess diagnostic imaging isotopes. At this time, no information is available whether radiological material is missing, or if the open door was the cause of the alarm. The investigation is ongoing.

* * * UPDATE FROM IRENE BENNETT TO JOHN KNOKE AT 1036 EDT ON 09/04/09 * * *

The State conducted an inspection at the licensee's facility and determined that no material was missing. A complete report will follow later.

Notified FSME (Angela McIntosh), R1DO (James Dwyer), and ILTAB (via e-mail).
==
These “Event Notification Reports” are posted to the NRC Web site for public review.

==
(1) “Public Still in the Dark When it Comes to Dirty Bomb Threat” By Stew Magnuson June 2008. (2) "Testimony of Dr. Henry Kelly, President Federation of American Scientists before the Senate Committee on Foreign Relations", March 6, 2002. Online at: http://www.fas.org/ssp/docs/kelly_testimony_030602.pdf