Refresher Course-13: Consequence Management of Malevolent Use of Radioactive Material
Strategies for Enhancing Security of Radioactive Materials

Cynthia G. Jones, Ph.D.[a*]

[a]United States Nuclear Regulatory Commission, Office of Nuclear Security and Incident Response, Mail Stop T4-D22A, Washington, D.C. 20555

Abstract. This IPRA-12 refresher course on Consequence Management of Malevolent Use of Radioactive Material provides lessons learned since the events of September 11, 2001, in planning for, establishing and integrating a radioactive materials security program into an overall regulatory infrastructure initially developed for health and safety purposes. Experience in the United States has shown that risk-based approaches to enhancing the security of radioactive materials can significantly reduce the potential threat from a radiological dispersal device. Regulatory Authorities around the world have an important responsibility to continue working closely within their government and with international partners to continuously assess, integrate and improve their security programs to make risk-significant sealed radioactive sources more secure and less vulnerable to terrorists. This refresher course will describe the unique aspects and potential changes needed to existing regulatory and emergency preparedness programs, in order to ensure enhanced initiatives are in place and effective for responding to, preparing for, and responding to a terrorist event involving radioactive materials. Suggested references are provided for developing a further understanding of the many actions to take under consideration when establishing a comprehensive security program for enhancing existing security of radioactive sources and devices, thereby protecting individuals against capricious and unpredictable radiation exposure situations involving the malevolent use of radioactive materials.

KEYWORDS: Radioactive Dispersal Devices, IAEA Code of Conduct, consequence management, dirty bombs, radioactive source security.

1. Introduction

The events of September 11, 2001, heightened nations' awareness on the need to prevent intentional unauthorized access of radioactive materials that could be used in a malevolent act. Such an attack has been of particular concern because of the widespread use, and thus potential availability, of radioactive materials (often contained in doubly-encapsulated sealed sources) worldwide by industry, hospitals, academic institutions, and research and development facilities. Not all radioactive sources in these locations are viable for use as *a radiological dispersal device (RDD)*, or what the media calls a "dirty bomb." A *dirty bomb* is one type of RDD that combines a conventional explosive, such as dynamite, with radioactive material. The terms dirty bomb and RDD are often used interchangeably in media reports. Most RDDs would not release enough radiation to kill people or cause severe illness — the conventional explosive itself would be more harmful to individuals than the radioactive material. However, depending on the scenario, an RDD explosion could create fear and panic, contaminate property, disrupt commerce, and require potentially costly cleanup. Effective response and making prompt, accurate information available to the public immediately following such an event could prevent the panic sought by terrorists.

A dirty bomb is in no way similar to a nuclear weapon or nuclear bomb. A nuclear bomb creates an explosion that is millions of times more powerful than that of a dirty bomb. The cloud of radiation from a nuclear bomb could spread tens to hundreds of square miles, whereas a dirty bomb's radiation could be dispersed within a few blocks of the explosion. A dirty bomb is not a "Weapon of Mass Destruction" but a "Weapon of Mass Disruption," where contamination and anxiety are the terrorists' major objectives [1].

* Presenting author, E-mail: cynthia.jones@nrc.gov

2. IAEA Code of Conduct

Even before September 11, 2001, governments worldwide were involved in efforts to establish international guidance for the safety and security of radioactive sources [2]. In 2003, these continued efforts resulted in a major revision of the International Atomic Energy Agency (IAEA) "Code of Conduct on the Safety and Security of Radioactive Sources," hereafter called the Code or Code of Conduct [3]. The Code aims to strengthen existing security, management and control of radioactive sealed sources used in non-military applications from a global cradle-to-grave perspective, including the manufacture, distribution, licensing, export, import, recycle, disassembly, and disposal. While the Code of Conduct is a voluntary set of national guidelines for the safety and security of sealed radioactive sources, it does recommend the development and implementation of national registries and tracking systems for certain *risk-significant*[1] radioactive sealed sources. To date, 92 nations have formally made a political commitment of its support for the Code of Conduct to the Director General of the IAEA [4].

In summary, the objectives of the Code of Conduct are, through the development, harmonization and implementation of national policies, laws and regulations, and through the fostering of international co-operation, to:

(i) Achieve and maintain a high level of safety and security of radioactive sources;
(ii) Prevent unauthorized access or damage to, and loss, theft or unauthorized transfer of, radioactive sources, so as to reduce the likelihood of accidental harmful exposure to such sources or the malicious use of such sources to cause harm to individuals, society or the environment; and
(iii) Mitigate or minimize the radiological consequences of any accident or malicious act involving a radioactive source.

The Code provides some common themes for increasing source security by a Regulatory Body that include:

- Identifying a list of radioactive sources requiring security based on potential attractiveness of the source to terrorists and criminals and the extent of the threat to public health and safety;
- Establishing a national system for recovery of lost or stolen sources;
- Establishing requirements and issuing guidance for ensuring adequate security of radioactive sources;
- Establishment of a national source registry;
- Establishment of a national system (including user fees and other methods) to provide for the proper disposal of sources at end-of-life;
- Enhancing existing import and export controls on radioactive sources to ensure that recipients of sources are able and willing to assure adequate control; and
- Revising procedures for improving the security of use, transportation and storage of sources, including the inspection program; security measures; fines, background checks for individuals with access to radioactive sources; exchange of information on background checks; and physical security of facilities that store or use radioactive sources

2.1 Categorization of Sources

One of the essential features of the Code of Conduct is the categorization of certain risk-significant sealed radioactive sources, contained in Annex 1 of the Code and in IAEA's Safety Guide for *Categorization of Radioactive Sources* [5]. This categorization provides a foundation upon which

[1] For discussion purposes here, *risk-significant* sources are those Category 1 and 2 sealed sources or devices and Category 3 sealed sources that are aggregated or collocated.

countries worldwide may base their overall security framework for radioactive sources within their national regulatory infrastructure in order to prioritize actions and allocate resources. The Code's categorization scheme provides the starting basis for:

- A National Registry for Category 1 and 2 radioactive sealed sources;
- National import and export controls for Category 1 and 2 sealed sources; and
- Enhanced security requirements for risk-significant sealed source licensees.

The Code of Conduct categorization is composed of a list of 26 radionuclides and threshold activity levels that fall into three major categories. These are nuclides that have been identified as those generally used in sealed radioactive sources in common practices. The operational definition of a dangerous source is known as the *D-value*, which is that quantity of radioactive material, which, if not under control, could give rise to exposure sufficient to cause severe deterministic effects (i.e., an effect that is fatal, life threatening, or results in a permanent injury that reduces the quality of life) [5,6]. Table 1 contains the Code of Conduct list of major "risk-significant" radionuclides.

Table 1. Activities Corresponding to Thresholds of Categories[a] [3]

Radionuclide	Category 1 (TBq)	Category 2 (TBq)	Category 3 (TBq)
Am-241	60	0.6	0.06
Am-241/Be	60	0.6	0.06
Cf-252	20	0.2	0.02
Cm-244	50	0.5	0.05
Co-60	30	0.3	0.03
Cs-137	100	1	0.1
Gd-153	1000	10	1
Ir-192	80	0.8	0.08
Pm-147	40000	400	40
Pu-238	60	0.6	0.06
Pu-239/Be	60	0.6	0.06
Ra-226	40	0.4	0.04
Se-75	200	2	0.2
Sr-90 (Y-90)	1000	10	1
Tm-170	20000	200	20
Yb-169	300	3	0.3

[a] NOTE: There are 10 other radionuclides (Au-198, Cd-109, Co-57, Fe-55, Ge-68, Ni-63, Pd-103, Po-210, Ru-106/Rh-106, and Tl-204) included in Table 1 of Reference [3] which have not been reproduced here. They are very unlikely to be used in individual quantities that would place them within Categories 1-3.

The underlying methodology for the risk-based ranking of sealed radioactive sources in this categorization is detailed in IAEA Safety Guide No. RS-G-1.9 [5]. In general:

- *Category 1* sources, if not safely managed or securely protected would be likely to cause permanent injury to a person who handled them, or was otherwise in contact with them, for more than a few minutes. It would probably be fatal to be close to this amount of unshielded material for a period of a few minutes to an hour. These sources are typically used in practices such as irradiators used in sterilization or food preservation and teletherapy.

- *Category 2* sources, if not safely managed or securely protected, could cause permanent injury to a person who handled them, or was otherwise in contact with them, for a short time (minutes to hours). It could possibly be fatal to be close to this amount of unshielded radioactive material for a period of hours to days. These sources are typically used in practices such as industrial gamma radiography, high dose rate brachytherapy and some irradiators used for calibration purposes.

- *Category 3* sources, if not safely managed or securely protected, could cause permanent injury to a person who handled them, or were otherwise in contact with them, for some hours. It could possibly – although unlikely – be fatal to be close to this amount of unshielded radioactive material for a period of days to weeks. These sources are typically used in practices such as fixed industrial gauges involving high activity sources and some well logging devices.

The Code also encourages countries to give appropriate attention to radioactive sources considered by them to have the potential to cause unacceptable consequences if used for malicious purposes, and lower activity (e.g., Catgeory 3) sources in aggregate which may exist at some facilities, and which may also require enhanced security under the principles of the Code.

3. Developing Increased Security Requirements

Radioactive sealed sources provide critical capabilities in the oil and gas, electrical power, construction, and food industries; are used to treat millions of patients each year in diagnostic and therapeutic procedures; and are used in technology research and development by academic, government, and private institutions. These materials are as diverse in geographical location as they are in functional use.

In the United States (U.S.) alone, there are millions of radioactive sources and more than 23,000 authorized licensees [7]. While the amount of radioactive material authorized for use by these licensees varies from several kilobequerel (kBq) to petabequerel (PBq), on average only a small fraction (<10%) of these radioactive sources are considered risk-significant (e.g., Category 1 or 2); therefore the majority of licensed sources are not useful as an RDD [7,8].

3.1 A National Source Registry

As a first step in ensuring the security of sources, it is important to identify the location, type, quantity and specific uses of radioactive materials used in a country. Many countries have developed categorized lists of radionuclides (and associated thresholds) for various purposes in order to implement security enhancements to their regulatory programs. Some of these sources lists identify the sources that are required to be secured based on the potential attractiveness of the sources to a criminal or terrorist, and the extent of the threat to public health and safety. The Code of Conduct recommends that every country establish a national registry of sources that should, as a minimum, track Category 1 and 2 sealed sources by the pertinent Regulatory Authority [3].

In the U.S., the responsible Regulatory Authority, the U.S. Nuclear Regulatory Commission (NRC), developed an interim inventory of Category 1 and 2 sealed sources. Although reporting was initially voluntary, reporting process enhancements in 2006 produced a response rate of 99.7 percent from licensees [7]. This inventory was useful in supporting government efforts to respond to national emergencies (such as Hurricanes Katrina and Rita) and nationally significant security events. The NRC also used the inventory in further enhancing the safety, security, and control of radioactive sources, including issuance of security requirement (termed increased control orders), that imposed additional security measures on licensees that possess Category 1 and 2 sources. Although use of the interim inventory continues, activities have been completed for a final rule that establishes the regulatory foundation for NRC's National Source Tracking System (NSTS), which will be a database for tracking risk-significant radioactive sources. This rule will require licensees to report transactions

involving the manufacture, transfer, receipt, disassembly and disposal of nationally tracked sealed sources (Category 1 and 2 sources).

Because the information typically contained in a national registry provides sensitive information about the locations, sources and quantities of radioactive material authorized for use and storage within a country, the database should be appropriately protected to restrict the information contained in this source registry to only those individuals that have a "need to know."

3.2 Assessing the National Threat

As described in the open literature, terrorists have been interested in acquiring radioactive and nuclear material for use in malicious acts [1]. For example, in 1995, Chechen extremists threatened to bundle radioactive material with explosives to use against Russia in order to force the Russian military to withdraw from Chechnya. While no explosives were used, officials later retrieved a package of cesium-137 that the rebels had buried in a Moscow, Russia park.

Since September 11, 2001, terrorist arrests and prosecutions overseas have revealed that individuals associated with al-Qaeda planned to acquire materials for a RDD [8]. In 2004, British authorities arrested a British national, Dhiren Barot, and several associates on various charges, including conspiring to commit public nuisance by the use of radioactive materials [8]. In 2006, Barot was found guilty and sentenced to life in prison. British authorities disclosed that Barot developed a document known as the "Final Presentation." The document outlined his research on the production of "dirty bombs," which he characterized as designed to "cause injury, fear, terror and chaos," rather than to kill [8]. U.S. federal prosecutors indicted Barot and two associates for conspiracy to use weapons of mass destruction against persons within the U.S., in conjunction with the alleged surveillance of several landmarks and office complexes in Washington, D.C., New York City, and Newark, N.J.

In a separate British police operation in 2004, authorities arrested British national, Salahuddin Amin, and six others on terrorism-related charges. Amin is accused of making inquiries about buying a "radioisotope bomb" from the Russian mafia in Belgium; and the group is alleged to have linkages to al-Qaeda [8]. Nothing appeared to have come from his inquiries, according to British prosecutors. While neither Barot nor Amin had the opportunity to carry their plans forward to an operational stage, these arrests demonstrate the continued interest of terrorists in acquiring and using radioactive material for malicious purposes.

As recommended by the Code of Conduct, each country's pertinent regulatory and law enforcement agencies should define its domestic threat and assess its vulnerability with respect to this threat for a variety of sources used within its territory, based on the potential for loss of control and malicious acts involving one or more radioactive sources [3]. A comprehensive re-evaluation of the regulator's safeguards and security program should be undertaken before enhancing or developing new security requirements for Category 1 and 2 sealed radioactive sources. Factors that should be considered to determine if new sources should be included or others excluded into a security program are the radiation source activity levels, radioactive half-life, potential dispersability (if the encapsulation of the sources is broken or tampered with) and location(s) of use. Several examples of how to implement an effective, enhanced security program, based on recent U.S. experience, will be identified in the next several sections.

3.3 Establishing Security Requirements for Category 1 and 2 Sources

After an evaluation of its domestic threat, Regulatory Authorities, in cooperation with other agencies (such as law enforcement and other State regulators) as necessary, should consider establishing requirements and implementation guidance for security of Category 1 and 2 sealed radioactive sources. The purpose of these increased security requirements would be to enhance control of

radioactive material in quantities greater than or equal to values described in Table 1 for Category 1 and 2 sources, as well as for Category 3 sources that are considered to be aggregated or collocated.[2]

Enhanced security for risk-significant sealed radioactive sources should ensure that security and control of such sources is maintained by the licensee, thereby preventing such materials from being diverted for use in a malevolent act. Regulatory authorities typically require owners licensed to use or store radioactive material to secure it from theft and unauthorized access. In the U.S., for example, licensees are also required to promptly report lost or stolen risk-significant radioactive material to the regulator or designated authority. Local authorities, such as local law enforcement authorities (LLEA) may also assist the regulator in making a determined effort to find and retrieve such sources. In the U.S., most reports of lost or stolen material involve small or short-lived radioactive sources not useful for an RDD.

Past experience suggests there has not been a pattern of collecting such sources for the purpose of assembling an RDD. As an example, it is important to note that the radioactivity of the combined total of all unrecovered sources in the U.S. over the past 5 years (when corrected for radioactive decay) would not reach the threshold for one high-risk radioactive source [9]. Unfortunately, the same cannot be said world-wide. It is for this reason that each country should review their existing controls for securing radioactive sources and continue to strengthen these requirements on risk-significant Category 1 and 2 radioactive sources both at home and abroad (i.e., exports).

Enhanced requirements to existing regulatory safety programs would reduce the risk of unauthorized use of radioactive materials, through access controls to aid prevention, and prompt detection, assessment, and response to mitigate potentially high consequences that would be detrimental to public health and safety. Increased security and controls for radioactive sources are established to define licensee responsibility to maintain control of licensed material and secure it from unauthorized removal or access. As provided in the next six sections, the following suggested increased security controls are recommendations for consideration by the Regulatory Authority, based on U.S. experience, and are intended to apply to licensees whom, at any given time, possess radioactive sources greater than or equal to the quantities of risk-significant radioactive material as defined in Table 1.

3.3.1 Security Control 1: Controlling Access

In order to ensure the safe handling, use, and control of licensed radioactive material, the Regulatory Authority should consider establishing requirements to ensure that each licensee controls access at all times to radioactive material for risk-significant quantities as defined by the Regulatory Authority. In developing the security program, the following security controls should be considered:

a. The licensee should allow only *trustworthy and reliable* individuals, approved in writing by the licensee, to have unescorted access to risk-significant sources and devices. Licensees should only approve unescorted access to those individuals with job duties that require access to such radioactive material and devices. Other personnel who require access to such radioactive material to perform a job duty, but who are not approved by the licensee for unescorted access, must be escorted by an approved individual.

b. For individuals employed by the licensee for 3 years or less, and for non-licensee personnel,

---

[2] Radioactive materials are considered to be aggregated or collocated if breaching a common physical barrier (e.g., a locked door at the entrance to a storage room) that would allow access to the radioactive source or device. For a combination of radionuclides, the unity rule is used to determine if the activity of aggregated sources of different radionuclides is greater than the Table 1 threshold quantities. For example, if several radionuclides are aggregated, the sum of the ratios of the activity of each source, i of radionuclide, n, A(i,n), to the quantity for radionuclide n, Q(n), listed for that radionuclide equals or exceeds one. [(aggregated source activity for radionuclide A) ÷ (Category threshold value for radionuclide A)] + [(aggregated source activity for radionuclide B) ÷ (Category threshold value for radionuclide B)] + etc..... ≥1.

such as physicians, physicists, house-keeping personnel, and security personnel under contract, trustworthiness and reliability should be determined, at a minimum, by verifying employment history, education, and personal references. For individuals employed by the licensee for longer than three years, trustworthiness and reliability could be determined by a review of the employees' employment history with the licensee.

c. Service providers should be escorted unless determined to be trustworthy and reliable by a Regulatory Authority-required background investigation as an employee of a manufacturing and distribution licensee. Written verification attesting to or certifying the person's trustworthiness and reliability should be obtained from the manufacturing and distribution licensee providing the service.

d. Licensees should document the basis for concluding that there is reasonable assurance that an individual granted unescorted access is trustworthy and reliable, and does not constitute an unreasonable risk for unauthorized use of radioactive material quantities of concern. The licensee should also maintain a list of persons approved for unescorted access to such radioactive material and devices by the licensee.

3.3.2 Security Control 2: A Documented Security Program

In order to ensure the safe handling, use, and control of licensed material in use and in storage, the Regulatory Authority should consider a requirement for each licensee to have a *documented program* to monitor and immediately detect, assess, and respond to unauthorized access to radioactive material quantities of concern and devices. As an example, in the U.S., enhanced monitoring is provided during periods of source delivery or shipment, where the delivery or shipment exceeds 100 times the Table 1 values. Specific issues addressed by this security control should include:

a. Immediate response by the licensee to any actual or attempted theft, sabotage, or diversion of such radioactive material or of the devices. The response should include requesting assistance from a Local Law Enforcement Agency (LLEA).

b. In order to reinforce this coordination, the licensee should have a pre-arranged plan with LLEA for assistance in response to an actual or attempted theft, sabotage, or diversion of such radioactive material or of the device(s) which is consistent in scope and timing with a realistic potential vulnerability of the sources containing such radioactive material. The pre-arranged plan should be updated when changes to the facility design or operation affect the potential vulnerability of the sources. For temporary job sites, prearranged LLEA coordination would not be required.

c. The licensee should also have a dependable means to transmit information between, and among, the various instruments used to detect and identify an unauthorized intrusion, to inform the assessor, and to summon the appropriate responder.

d. After initiating appropriate response to any actual or attempted theft, sabotage, or diversion of radioactive material or of the devices, the licensee should, as promptly as possible, notify the Regulatory Authority.

e. The licensee should maintain written documentation describing each instance of unauthorized access and any necessary corrective actions to prevent future instances of unauthorized access.

3.3.3 Security Control 3: Enhanced Security During Transport

In order to ensure the safe handling, use, and control of licensed material during transportation for domestic highway and rail shipments by a carrier other than the licensee, the Regulatory Authority should consider a requirement for enhanced security for each licensee that transport quantities that equal or exceed those for Table 1, Category 2 sources, but are less than Table 1, Category 1 quantities, per consignment. For these shipments, the Regulatory Authority should consider requiring the following elements in a security program for transport companies and carriers:

a. Use real-time package tracking (e.g., global positioning) systems;

b. Implement similar licensee methods to assure trustworthiness and reliability of its drivers;

c. Maintain constant control and/or surveillance of the consignment during transit; and

d. Have the capability for immediate communication to summon appropriate response or assistance.

During typical radioactive material shipments of the Category 1 and 2 sources, the Regulatory Authority should establish guidance and/or requirements for licensees to coordinate with the originator to establish an expected time of delivery; and confirm receipt of transferred radioactive material. If the material is not received at the expected time of delivery, notify the originator and assist in any investigation.

Prior to transporting domestic highway and rail shipments that exceed the quantities established by the Regulatory Authority (e.g., Category 1, Table 1 quantities, per consignment), it is recommended that the licensee notify the Regulatory Authority (preferably in writing), at least 90 days prior to the anticipated date of shipment when the shipment will occur. This enables the Regulatory Authority to issue additional Orders or immediately effective requirements to implement additional security measures for the transportation of large quantities of risk-significant radioactive material.

If, through the course of the consignment, it is determined the shipment has become lost, stolen, or missing, the Regulatory Authority should have a notification requirement in place so that the licensee is responsible for immediately notifying the appropriate authorities of the status of the source.

3.3.4 Security Control 4: Special Considerations for Mobile and Portable Devices

In order to ensure the safe handling, use, and security of radioactive material in storage and use, the Regulatory Authority should consider establishing the following requirement for licensees that possesses *portable or mobile devices* containing radioactive material in quantities greater than or equal to Table 1 values:

a. For *portable devices*[3]*,* have two independent physical controls that form tangible barriers to secure the material from unauthorized removal when the device is not under direct control and constant surveillance by the licensee.

b. For *mobile devices*[4]*:*
   1. that are only moved *outside* of the facility (e.g., on a trailer), have two independent physical controls that form tangible barriers to secure the material from unauthorized removal when the device is not under direct control and constant surveillance by the licensee.
   2. that are only moved *inside* a facility, have a physical control that form a tangible barrier to secure the material from unauthorized movement or removal when the device is not under direct control and constant surveillance by the licensee.

c. For devices *in or on a vehicle or trailer*, licensees should also utilize a method to disable the vehicle or trailer when not under direct control and constant surveillance by the licensee

3.3.5 Security Control 5: Document the Security Program

In order to effectively document the security program requirements for enhanced security of sources, the Regulatory Authority should consider establishing a minimum set of recordkeeping and retention requirements (e.g., 3 years) for licensees for the following items:

---

[3] As described in Reference [10], a *portable* device is designed to be carried by one person alone. The mass of such a device should not exceed 35 kg.

[4] As described in Reference [10], a *mobile* device is not a portable device, but is designed to be moved easily by a suitable means provided for the purpose.

a. Documentation regarding the trustworthiness and reliability of individual employees after the individual's employment ends
b. Revised lists of approved authorized individuals
c. Documentation on each radioactive material carrier after the licensee discontinues use of that particular carrier
d. Documentation on shipment coordination, notifications, and any investigations after the shipment or investigation is completed
e. Security program documentation after the license is terminated or amended to reduce possession limits below the levels required for enhanced security controls

3.3.6 Security Control 6: Protection of Sensitive Information

Detailed information generated by the licensee that describes the physical protection of radioactive material quantities of concern, is sensitive information and the Regulatory Authority should consider establishing the following requirement for licensees in order to protect this information from unauthorized disclosure:

a. The licensee should control access to its physical protection information to those persons who have an established need to know the information, and are considered to be trustworthy and reliable
b. The licensee should develop, maintain and implement policies and procedures for controlling access to, and for proper handling and protection against unauthorized disclosure of, its physical protection information for radioactive material covered by these requirements established by the Regulatory Authority.

The policies and procedures established by the Regulatory Authority should consider requiring the following:

a. A general performance requirement that each person who produces, receives, or acquires the licensee's sensitive information, protect the information from unauthorized disclosure
b. Protection of sensitive information by the licensee during use, storage, and transit
c. Preparation, identification or marking, and transmission,
d. Access controls
e. Appropriate destruction of sensitive documents
f. Use of secure automatic data processing systems, and
g. Removal from the licensee's sensitive information category.

For further recommendations for implementing guidance for the security controls discussed in his section, please see References [11,12,13,14,15,16].

3.4 Interactions and Communication with Licensees

One of the key elements of success for an enhanced security program for risk-significant radioactive material is ensuring that the communication pathways to licensees and the public are direct and frequent. In addition to the health and safety mission of the Regulatory Authority, a greater emphasis may now be placed on the need for ensuring that regulatory actions are effective, realistic, and timely regarding enhanced security of radioactive materials. In rapidly transmitting information or newly established requirements to licensees on security related issues, NRC regulatory experience has shown that it is important to establish several types of communication processes for this to be successful. Several types of measures and transmittal pathways for consideration are discussed below.

3.4.1 Advisories, Orders & Interim Compensatory Measures

Advisories can be used as a term for non-public, rapid communications from the Regulatory Authority to its licensees that provide information obtained from the intelligence community or law enforcement agencies on changes to the threat environment and guidance for licensees to take specific actions

promptly to strengthen their capability against the threat [16]. As they are used by the NRC in the U.S., advisories are typically not legally binding, but they are effective in quickly conveying important information to large numbers of licensees. They are tailored to various categories of licensees such as power reactors, non-power reactors, fuel facilities, reactors undergoing decommissioning, independent spent fuel storage installations, gaseous diffusion plants, and materials licensees (e.g., irradiators, radiographers, industrial, academic and medical licensees).

An Order is a term that can be used for issuing immediately effective regulatory requirements that may modify, suspend, or revoke a license by the Regulatory Authority, or require specific actions by the licensee. As used in the U.S., Orders will typically modify the operating license for each facility and will remain in effect until the Regulatory Authority determines that the level of threat has diminished or that modifications to the issued Orders are appropriate. It is important to recognize that some requirements for increased security may not be possible or necessary at some licensee sites, or may need to be tailored to accommodate the licensee specific circumstances to achieve the intended security objectives in order to avoid any unforeseen adverse effect on the safe use and storage of the sealed sources.

As used in the U.S., *Interim Compensatory Measures (ICMs)* can be included with the Orders that are issued by the Regulatory Authority to enhance security, but are considered sensitive information and are therefore not made available to the public. Such ICMs can be used to direct licensees to take immediate action while more deliberate vulnerability studies are completed that will determine further licensing action. ICMs help to delineate specific licensee responsibilities that are outlined in an Order.

In establishing additional security requirements for Category 1 and 2 risk-significant radioactive materials, some Regulatory Authorities have found it more effective and efficient to issue immediately effective Orders to specific *groups* of licensees, issued first to those licensees with the largest quantities and the need for the highest degree of increased security for radioactive material (i.e., risk-based Orders). The specific security measures generally include increased security measures, installation of additional physical barriers, background and reliability checks of individuals that have authorized access to radioactive materials, enhanced coordination with law enforcement, and more restrictive access controls. Regulatory Authorities evaluate implementation of such security requirements through onsite inspections following receipt of the mandatory licensee compliance data or by reviewing licensee security plans while on site. Issuance of increased security requirements typically remain in effect until the Regulatory Authority incorporates similar measures into its regulations. In all the groups noted below, it is advisable to have licensees be required to verify *in writing* to the Regulatory Authority that they have received the Orders, are implementing them, and the date of when they are in full compliance.

In the U.S., the NRC found it desirable to issue Orders to four specific groups of risk-significant sealed source licensees to quickly issue immediately effective requirements to increase the security of these sources based on the quantity of radioactive materials possessed or in use by the licensee. It is advisable that Regulatory Authorities, if also issuing enhanced security requirements, consider issuing Orders in similar groups for practicality and efficiency. The specifics of each of the four groups of Orders are discussed below.

a. *Orders to Panoramic and Underwater Irradiators* were issued to those licensees authorized to possess greater than 370 TBq of Category 1 and 2 radioactive sources. The Orders provide reasonable assurance that the public health and safety and common defense and security continue to be adequately protected in the current security environment. These Orders imposed additional requirements regarding the security of and access to these radioactive sources. The actual requirements were considered to have information that must be secured and controlled (classified), and were therefore not publicly available for security purposes.

b. *Orders to Manufacturing and Distribution Licensees* were issued to those licensees authorized to manufacture or distribute significant quantities of at least Category 2 radioactive materials. The Orders imposed new requirements regarding the security of and access to these sources. Just as with

the panoramic irradiators, the actual requirements were considered to have information that must be secured and controlled (classified), and were not made publicly available for security purposes.

c. *Transportation Orders* were issued to those licensees that routinely ship Category 1 quantities of radioactive material. These Orders addressed pre-shipment notification to the Regulatory Authority, in-transit shipment communications capabilities, shipment tracking, and escorts. Just as with the previous two Orders, the actual requirements and routing specific were considered to have information that must be secured and controlled (classified), and were not therefore made publicly available for security purposes.

d. *Increased Security Control Orders to other Materials Licensees.* These remaining licensees (typically the largest group of the four) were those that are authorized to possess at least Category 2 quantities of radioactive material. The Orders for these licensees required strengthening of the measures regarding the control over use and storage of these sources. The requirements also involved enhanced measures for the transportation of Category 2 quantities of radioactive material.

3.4.2 Additional Administrative Security Upgrades

In addition to the trustworthiness, reliability and other requirements discussed in Section 3.3, the Regulatory Authority should also consider requirements for *fingerprinting* of any individual who is permitted unescorted access to radioactive material, or other property, subject to regulation that the Regulatory Authority determines to be of such significance (i.e., Category 1 and 2).

The regulator should also consider *law enforcement identification and criminal history records* requirements for individuals to have unescorted access to Category 1 and 2 quantities of sealed radioactive material. This type of fingerprinting Orders raise the level of administrative security requirements to that previously issued by the Regulatory Authority for some sources, such as those issued to panoramic irradiator or manufacturers and distributor licensees. These new requirements would provide yet another barrier to the prevention of inadvertent or unauthorized access to radioactive materials.

Depending on the variability and the number of facilities that are licensed by the Regulatory Authority, *revised inspection procedures* may also be needed to require on-site inspections or in-office meetings with all, or nearly all, new materials license applicants, to confirm their identity. Possible exceptions for a separate inspection could be applicants whose identity is known, because they already possess another license. NRC has performed a retrospective examination of its licenses to verify that the licensees are legitimate and has re-evaluated its licensing procedures to implement long-term solutions regarding the falsification of identity and unauthorized alteration of license documents. Enhanced administrative measures such as these will help to verify the identity of potential licensees and to prevent license counterfeiting which effectively improve the overall security of Category 1 and 2 sources.

In addition, consideration should be given to implement programs to recover sealed sources, including Category 1 and 2 sources that are unwanted or orphaned. In some countries, this cooperative agreement may be between several agencies or countries to allow for information exchange and related activities that assist in prioritizing, recovering, and storing radioactive sealed sources. Once the orphaned or lost sources are identified, recovered sources are moved to safe and secure storage or disposal. Owing to public health, safety, or security concerns, this activity currently includes recovering both risk-significant sealed sources lacking a disposition path and other selected sealed sources. Such a mission could include the following elements:

- Recovering radioactive sealed sources from the licensed sector that pose a threat to public health, safety, or security, prioritized on the basis of risk;
- Developing and maintaining short- and long-term secure interim storage capabilities;

- Working with manufactures to recycle and reuse sources and radioactive materials whenever appropriate; and
- Disposing of recovered sources in approved waste disposal sites, when available.

In situations where lost or abandoned radioactive material is found, the Regulatory Authority, local law enforcement, or cognizant environmental agency should take immediate actions to secure the material. For these cases, the Regulatory Authority should facilitate disposition efforts by identifying the owner. In cases in which the owner cannot be determined, the owner is not licensed to possess the material, or the owner is unable to resume possession, the Regulatory Authority should recover and dispose of the material.

3.5 Law Enforcement Coordination

Regulatory Authorities around the world have an important role in establishing working relationship both within their government and with international partners to continuously assess, integrate and improve their security programs to make risk-significant radioactive sources more secure and less vulnerable to terrorists. In the unlikely event of a terrorist action involving radioactive material however, partnerships amongst the various Regulatory Agencies, law enforcement officials, and the intelligence community will be critical in ensuring that information obtained at the scene is controlled and processed as the site will be considered a conventional crime scene and both the law and intelligence communities will have great interest in assessing the event. For the most part, the prospect of radioactive material in the hands of terrorists is different that any other law enforcement or national security threat a nation could face and places new and unusual demands on the regulator.

Just as was demonstrated with the United Kingdom's response to the 2006 Litvinenko polonium-210 event, the ability of the Britain's Regulatory Authority, the Health Protection Agency (HPA), in effectively dealing with a wide range of stakeholders during the response of the radiation poisoning, was crucial in both effectively managing an on-going criminal investigation as well as successfully identifying and coordinating the radiation-related media response to the event [17]. One of the key elements of the regulator's success in dealing with this event was the ability to bring together three technical centers, along with frontline experience of its criminal divisions to work together in coordinating the government response from both the radiation and law enforcement perspectives.

While not too dissimilar to a conventional radioactive material contamination event, regulatory decisions related to information release and access to the scene of the event, Regulatory Authorities must consider the possible effects on: (1) gaining and maintaining control of the event; (2) identifying and capturing other possible participants and accomplices; (3) and much later working with its law enforcement and intelligence agencies in eventually prosecuting the case in a court of law [18].

As part of the overall assessment of an enhanced security program for risk-significant sources, the Regulatory Authority should actively work with local law enforcement authorities (LLEA) in making a determined effort to become knowledgeable in the countries inventory of radioactive sources, and of the required security controls put in place to secure such sources from malevolent use. As described in Section 3.3, it is essential that pre-arranged written plans between licensees and LLEA be established in advance for assistance in response to an actual or attempted theft, sabotage, or diversion of such radioactive material. In case of an event involving lost, stolen or missing sources, LLEA can greatly enhance the ability to find and retrieve such sources.

Although there have been numerous general threats against nuclear facilities in the U.S. since September 11, 2001, none of these threats have been considered credible [16,18]. As a matter of practice, in the U.S., the competent Regulatory Authority (NRC) receives a substantial and steady flow of information from the national intelligence community, law enforcement, and licensees that requires prompt evaluation and coordination. Early coordination and prompt cooperation between these agencies is essential in combating the threat of radiological terrorism. Additional information on this subject can be found in References [15,16,20].

3.6 Import/Export

It is important that every country involved in the import or export of risk-significant radioactive sources take appropriate steps to ensure that transfers are undertaken in a manner consistent with the Code and that transfers of Categories 1 and 2 take place only with the prior notification by the exporting country and, as appropriate, consent by the importing country in accordance with their respective laws and regulations [3]. For some countries, this means that for all imports and exports of Category 1 and 2 radioactive sources, a specific license may be needed to authorize the transaction.

In the U.S. for example, the Regulatory Authority considers: (i) whether the foreign recipient is appropriately authorized to receive and possess the material under the laws and regulations of the importing country; (ii) whether the importing country has the appropriate technical and administrative capability, resources and regulatory structure to manage the material in a safe and secure manner; (iii) for Category 1 sources, whether the government of the importing country provides consent to the U.S. Government for the import; and (iv) information available regarding the risks of diversion or malicious acts [21]. In cases where the importing country does not have the technical and administrative capability, and there is insufficient evidence of the recipient's authorization to receive and possess the material, the Regulatory Authority considers whether exceptional circumstances exist and whether the export should be authorized in light of those circumstances.

To date, specific licenses issued in the U.S. for these materials generally indicate whether the activity levels of individual export or import shipments will exceed the Category 1 or 2 thresholds specified in Table 1, but do not set total maximum activity or maximum total number of shipments authorized over the life of the license. Some Regulatory Authority's regulations include bulk material, and thus can be more encompassing than the Code (which only applies to sealed sources). Anyone using such licenses for export or import should be required to notify the appropriate Regulatory Authority and, in the case of exports, the government of the importing country in advance of each shipment. In practice, U.S. experience has shown that it is advisable that notifications be received by the Regulatory Authority at least 7 days in advance of each shipment, to the extent practical, but in no case less than 24 hours in advance of each shipment.

To facilitate international coordination and communication, some Regulatory Authorities have also developed bilateral memorandums of cooperation with neighboring countries that also import and export Category 1 and 2 risk-significant sources of radioactive material. The memorandum serves to provide an avenue to ensure that exports and imports of radioactive sources between co-located countries are consistent with the Code and guidance, and to facilitate the sharing of information related to imports and exports of radioactive sources, as well as to harmonize regulatory approaches in authorizing imports and exports of radioactive sources.

4. Incident Response & Consequence Management

In preparation for the response to an act of terror involving the malevolent use of radioactive sources, Regulatory Authorities can look to the lessons learned from previous accidents and contamination events involving dispersal and release of radioactive material. One of the most studied cases is the event that occurred in Goiânia, Brazil, in 1987. Although this incident was not malevolent in nature, it highlighted the difficulties involved with the release of a highly dispersible radioactive material, cesium-137 (Cs-137) into the environment [22]. In this event, briefly summarized here from Reference [23], Brazilian scavengers dismantled a 51 TBq Cs-137 source from an abandoned teletherapy unit. Destruction of these sources combined with accidental dispersal of the radioactive material led to the overexposure of 14 people, 4 deaths, 249 contaminated individuals, and mass monitoring and evacuation activities [23]. As a result, the Regulatory Authority initiated extensive environmental and personnel monitoring programs. Although approximately 112,000 people were surveyed for radioactive contamination, only about 249 were contaminated—the rest were "worried well." Of 159 houses monitored for contamination, 85 were found to have significant contamination, and 200 individuals were evacuated from 41 of them. In addition, topsoil and debris were removed from the area, which produced 3500 m^3 of contaminated waste stored in more than 6000 containers.

This large volume of waste was directly attributable to the restrictive action levels chosen, in both the early (emergency) and late (recovery) phases. As stated in Reference [23], the action levels for remediation "… were selected under strong political and social pressure and were set substantially lower that would have resulted from an optimization process." As reported by IAEA, there were also considerable economic consequences, resulting in a 25% decrease in agricultural produce and cotton sales [23].

The Goiânia event and that associated with the deliberate dispersal of radioactive materials, such as a dirty bomb, involves a number of common elements: radiological, psychological, medical, first response, triage, financial, waste management, and public perception of the consequences of the event. Therefore, in preparation for a potential RDD event, it is important for the Regulatory Authority and licensees to review their emergency preparedness and response programs to determine if any necessary changes should be made to anticipate the types of response that might be necessary.

4.1 Impact of an RDD

As discussed in the scientific literature, although an RDD would typically have very localized effects, it is possible that a large area, a few to several tens of city blocks or more, could be contaminated following the release of radioactive material to the environment [19, 24]. This would depend on a number of factors, including the amount of radioactive material dispersed, the means of dispersal (i.e., explosion, spraying, fire, etc.), the physical and chemical form of the radioactive material, size of the explosive, the local topography, and the local weather conditions [24]. It is unlikely that significant immediate health effects or prompt fatalities would result, other than from the explosion itself, because people would run away from the explosion and the radioactive material would disperse, reducing the potential for high radiation exposure. Over the long term, people who were contaminated or exposed to elevated radiation levels may have an increased risk of cancer.

Those closest to the RDD would be the most likely to sustain physical injuries due to the explosion. As radioactive material spreads, it becomes less concentrated and less harmful. Prompt detection of the type of radioactive material used will greatly assist local regulatory and law enforcement authorities in advising the community on protective measures, such as sheltering in place, or quickly leaving the immediate area. As shown in the Goiânia event, subsequent decontamination of the affected area may involve considerable time and expense.

Immediate health effects from exposure to the low radiation levels expected from an RDD would likely be minimal. Just as with a ruptured source in the public domain, the effects of radiation exposure would be determined by:

- the amount of radiation absorbed by the body
- the type of radiation (gamma, beta, or alpha)
- the distance from the radioactive material to an individual
- the means of exposure–external or internal (absorbed by the skin, inhaled, or ingested)
- the length of time exposed

4.2 Establishing RDD Planning Guidance

On August 1, 2008, the U.S. finalized its guidance for how to adequately prepare and respond to an RDD event. This guidance entitled, "Planning Guidance for Protection and Recovery Following Radiological Dispersal Device (RDD) and Improvised Nuclear Device (IND) Incidents," (Guidance) was developed to assist Federal agencies, State and local governments, emergency management officials, and the general public in developing plans for responding to an RDD or IND incident [25]. Just as with other previously established response guidance for nuclear power plant events [26], this Guidance recommends *protective action guides* (PAGs) to support decisions about actions that should be taken to protect the public and emergency workers when responding to or recovering from an RDD or IND incident. The Guidance, which can be useful for Regulatory Authorities worldwide, outlines a process, discusses existing operational guidelines that should be useful in the implementation of the

PAGs, and encourages Federal, State and local emergency response officials to use these guidelines to develop specific operational plans and response protocols for protection of emergency workers responding to catastrophic incidents involving high levels of radiation and/or radioactive contamination. The objective of the Guidance is to aid decision makers in protecting the public, first responders, and other emergency workers from the effects of radiation, and cleaning up the affected area, while balancing the adverse social and economic impacts following an RDD event. In addition, site cleanup and recovery guidance following such an event is also provided. The document, as it applies to RDD events in the U.S, is summarized briefly in the following sections.

4.2.1 Phases of Response

For the early and intermediate phases of response, guidance established by the Regulatory Authority should present levels of projected radiation dose at which it recommends that actions be considered to avoid or reduce adverse public health consequences from an RDD event. As described later in this section, for the late phase of the response, the guidance should establish appropriate exposure levels, as determined by the Regulatory Authority, based on site-specific circumstances. This guidance should address key radiological protection questions at each stage of an RDD event (early, intermediate, and late phases). Restoring the normal operation of critical infrastructure, services, industries, business, and public activities as soon as possible can minimize adverse social and economic impacts.

One very importance aspect of this Guidance is that it does not present a set of absolute standards. The Guidance is not intended to define “safe” or “unsafe” levels of exposure or contamination; rather they represent the approximate levels at which the associated protective actions are justified. In this manner, the Guidance provides Federal, State and local decision makers the flexibility to be more or less restrictive, as deemed appropriate based on the unique characteristics of the event and local considerations.

When developing similar guidance in other countries, it is important to select actions to prepare for, respond to, and recover from the adverse effects that may exist during any phase of a terrorist incident—the early (emergency) phase, the intermediate phase, or the late phase. As shown in large-scale simulated RDD exercises, there may be an urgent need to evacuate people; there may also be an urgent need to restore the services of critical infrastructure (e.g., roads, rail lines, airports, electric power, water, sewage, medical facilities, and businesses) in the hours and days following the incident—thus, some response decisions must be made quickly. If the decisions affecting the recovery of critical infrastructure are not made quickly, the disruption and harm caused by the event could be inadvertently and unnecessarily increased. Failure to restore important services rapidly could result in additional adverse public health and welfare impacts that could be more significant than the direct radiological impacts itself.

The ***Early Phase***, sometimes called the emergency phase, is the period at the beginning of the incident when immediate decisions for effective protective actions are required, and when actual field measurement data generally are not available. Exposure to the radioactive plume, short-term exposure to deposited radioactive materials, and inhalation of radioactive material are generally taken into account when considering protective actions for the early phase. The response during the early phase includes initial emergency response actions to protect public health and welfare in the short term, considering a time period for protective actions of hours to a few days [25]. Priority should be given to lifesaving and first-aid actions. In general, early phase protective actions should be taken very quickly, and the protective action decisions can be modified later as more information becomes available. If an explosive RDD is deployed without warning, however, there may be no time to take protective actions to significantly reduce plume exposure. Also, in the event of a covert dispersal, discovery or detection may not occur for days or weeks, allowing contamination to be dispersed broadly by foot, vehicular traffic, wind, rain, or other forces.

The ***Intermediate Phase*** of the response is usually assumed to begin after the incident source and releases have been brought under control and protective action decisions can be made based on actual measurements of exposure. Decisions must be made on the initial actions needed to recover from the

incident, reopen critical infrastructure, and return to a state of relatively normal activity. Just as with the early phase, some intermediate phase decisions will need to be made quickly (i.e., within hours) and should not be delayed by discussions on what the more desirable permanent decisions will be. Local officials must weigh public health and welfare concerns, potential economic effects, and many other factors when making decisions. For example, it can be expected that hospitals and their access roads will need to remain open or be reopened quickly. These interim decisions can often be made with the acknowledgement that further work may be needed as time progresses.

The ***Late Phase*** is the period when recovery and cleanup actions designed to reduce radiation levels in the environment to acceptable levels have begun. This phase ends when all the remediation actions have been completed. With additional time and increased understanding of the scope of the contamination event, there will be opportunities to involve key stakeholders in providing sound, cost-effective cleanup recommendations that are protective of human health and the environment. Generally, early (or emergency) phase decisions will be made directly by elected public officials, or their designees, with limited stakeholder involvement due to the need to act within a short timeframe. Long-term decisions, however, should be made with stakeholder involvement, and can also include incident-specific technical working groups to provide expert advice to decision makers on alternatives, costs, and impacts. Ideally, this stakeholder involvement, consisting of multidisciplinary teams of professionals, should be initiated during the development of preparedness actions for such events. The relationship between typical protective actions and the phases of the incident response are outlined in Figure 1. There is overlap between the phases; this framework should be used to inform planning and decision-making.

4.3 Protective Actions & Guides

Protective actions are activities that should be conducted in response to an RDD event in order to reduce or eliminate exposure of the public to radiation or other hazards. The principal protective action decisions for consideration in the early and intermediate phases of an emergency are whether to shelter-in-place, evacuate, or relocate affected or potentially affected populations. Secondary actions include administration of medical countermeasures, decontamination (including decontamination of persons evacuated from the affected area), use of access restrictions, and use of restrictions on food and water. In some situations, only one protective action needs to be implemented, while in others, numerous protective actions should be implemented. During such events, it may be necessary to determine whether or not to order a protective action based on the projected dose to a population. For example, evacuation of a population is much more difficult and costly as the size of the population increases.

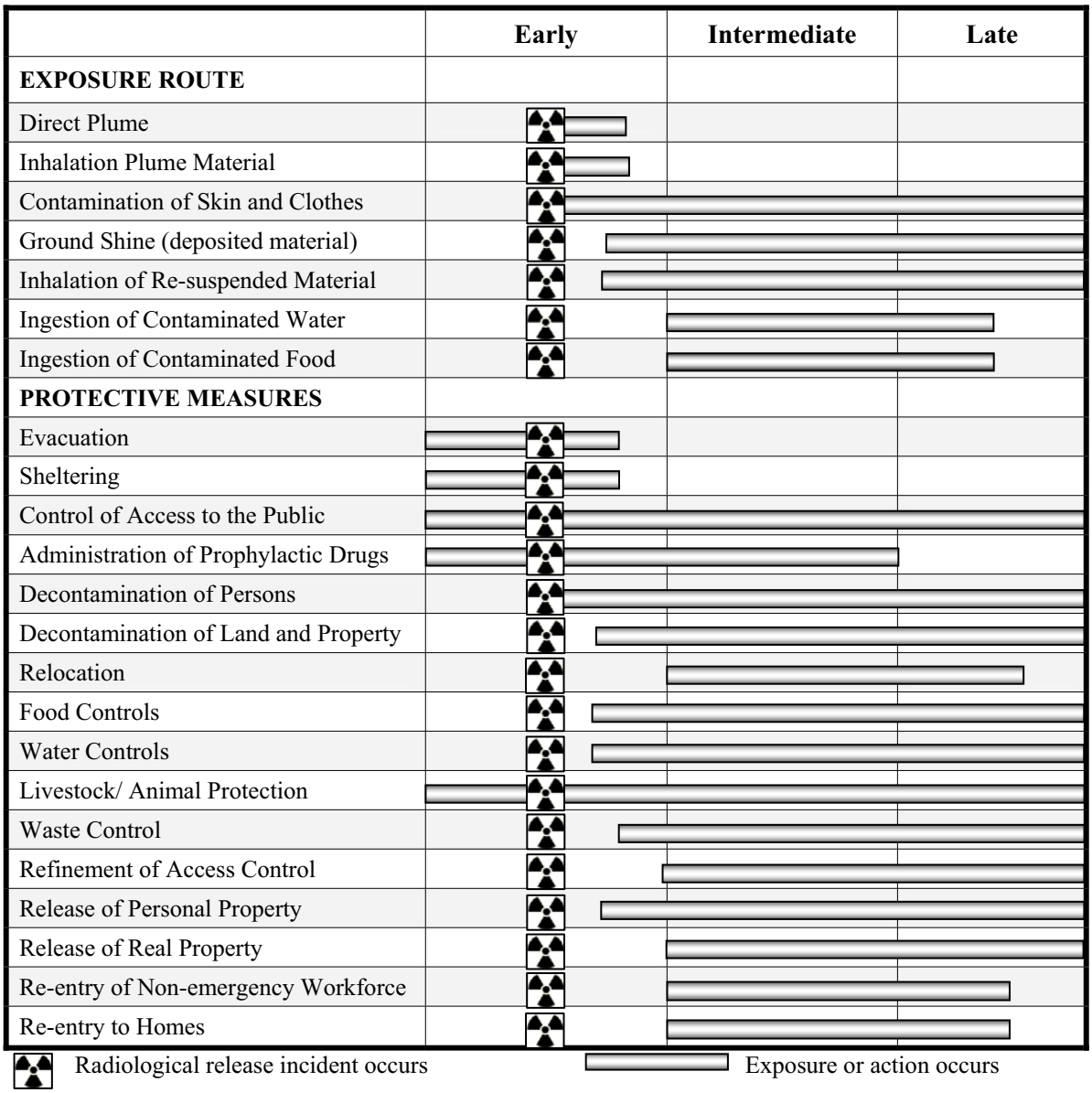
A ***Protective Action Guide (PAG)*** is the projected dose to a reference individual, from an accidental or deliberate release of radioactive material, at which a specific protective action to reduce or avoid that dose is recommended [25]. Thus, protective actions are designed to be taken before the anticipated dose is realized.

PAGs should be developed as generic criteria based on balancing public health and welfare with the risk of various protective actions applied in each of the phases of an RDD event. Though the early and intermediate PAGs as described in Reference [25] are values of dose to be avoided, published dose conversion factors and derived response levels may also be used in estimating doses, and for choosing and implementing protective actions. Other quantitative measures and derived concentration values may be useful in emergency situations; for example, for the release of goods and property from contaminated zones, and to control access into and out of contaminated areas.

In order to use the early and intermediate phase PAGs to make decisions about appropriate protective actions, Regulatory Authorities and decision makers will need information on suspected radionuclides; projected plume movement, and radioactive depositions; and/or actual measurement data or, during the period initially following the release, expert advice in the absence of good information. Sources of such information include on-scene responders, as well as monitoring, assessment, and modelling centers. In general, it should be emphasized that realistic assumptions, based on incident-specific

information, should be used when making radiation dose projections so that the final results are representative of actual conditions rather than overly conservative exposures. It is very important that local officials responsible for carrying out emergency response actions conduct advance planning to ensure that they are adequately prepared if such an incident were to occur.

Figure 1: Relationship between Exposure Routes, Protective Measures, & Timeframes for Effects[a, b]



[a]Adapted from Reference [25]. For some activities, the figure indicates that protective actions may be taken before a release occurs. This would be the case if authorities have advance warning about a potential RDD event.

[b]In certain circumstances, food and water interdiction may occur in early phases. In addition, some exposure routes (e.g., ingestion of contaminated food) may occur earlier than depicted in the figure, depending on the unique characteristics of the event.

4.4 Risk Management Framework

As part of the consequence management of an RDD event, Regulatory Authorities should also consider the development of a risk management framework in their RDD preparedness and planning initiatives. A U.S. report, "Framework for Environmental Health Risk Management," provides a

guidance that could be used by Regulatory Authorities worldwide in addressing the long-term cleanup issues for RDDs and assist in the development of preparedness initiatives in this area [27]. Given the time frames following an RDD event, there is generally not sufficient time in the early phase to conduct a full risk assessment and get stakeholder involvement. In order for the framework to be most useful, it must be used in the planning and preparations stages for a radiological event.

Risk management is the process of identifying, evaluating, selecting, and implementing actions to reduce risk to public health and the environment. The goal of risk management is to make scientifically sound, cost-effective, integrated actions that reduce or prevent public health impacts while taking into account social, cultural, ethical, public policy, and legal considerations [27]. In order to accomplish this goal, information will be needed on the nature and magnitude of the hazard present as a result of the incident, the options for reducing risks, and the effectiveness and costs of those options. Decision makers also compare the economic, social, cultural, ethical, legal, and public policy implications associated with each option, as well as the unique safety and health hazards facing emergency responders and ecological hazards the cleanup actions themselves may cause.

The risk management framework is designed to help decision makers make good risk management decisions. The level of effort and resources invested in using the framework should be commensurate with the significance of the problem, the potential severity and economic impact, the level of controversy surrounding the problem, and resource constraints [27]. In addition to the health and environmental hazards that must be considered, other factors include the continued disruption in normal activities, loss of, or limited access to critical infrastructure and health care and general economic damage.

The framework [27] relies on the three key principles of: (1) broad context; (2) stakeholder participation; and (3) iteration. *Broad context* refers to placing all of the health and environmental issues into the full range of impacts and recovery factors following an RDD event, and is intended to assure that all aspects of public welfare are taken into account. The second key principle, *stakeholder participation*, is critical to making and successfully implementing sound, cost-effective, and risk-informed decisions. *Iteration* is the process of continuing to refine the analysis based on information available, and improve the decisions and actions that can be taken at any point in time. Together these principles outline a fair, responsive approach to making the decisions necessary to effectively respond to the impacts of an RDD event.

As experience has shown, stakeholders can provide valuable input to decision makers during the long-term cleanup effort, and the key decision makers should establish a process that provides for appropriate stakeholder involvement. Identifying which stakeholders need to be involved in the process depends on the situation. In the case of a site contaminated as a result of an RDD event, stakeholders may include individuals whose health, economic well-being, and quality of life are currently affected or would be affected by the cleanup and the site's subsequent use, or non-profit organizations representing such individuals. They may also include those who have regulatory responsibility, and those who may speak on behalf of the environment generally, business and economics, or future generations.

Stakeholder input should be considered throughout all stages of the framework as appropriate, including analyzing the risks, identifying potential cleanup options, evaluating options, selecting an approach, and evaluating the effectiveness of the action afterwards. Their input will assist decision makers in providing a reasoned basis for actions to be taken. Further information on the importance and selection of stakeholders can be found References [25, 27].

5. The Role of Communication

A terrorism event involving risk-significant sources of radioactive materials could have substantial psychological and socioeconomic consequences. In order to maintain and re-establish public confidence after such an event, it imperative that the Regulatory Authority has a communication plan pre-established that effectively and efficiently conveys the information needed to protect public health

and safety and restore confidence. The emerging threat of bioterrorism over the past decade has reemphasized the need for public officials to communicate effectively with the public and the media to deliver messages that inform without frightening, and educate without provoking alarm. Public outrage, concern and terror resulting from the use of an RDD rely on an individual's lack of knowledge about radiation and understanding regarding its significance [28]. Disabling wide-spread panic will depend on a large number of factors such as quick, clear, communication, a common understanding of radiation limits and potential health effects, and on an individuals' ability to make their own informed decisions based on perceived risk and reality. Informing the public of the problem and specific dangers, providing guidance on appropriate responses and easing concerns are achievable goals.

Sound and thoughtful risk communication in developing the Regulatory Authority's and licensee's emergency response programs can assist public officials in preventing ineffective, fear-driven, and potentially damaging public responses to a serious crisis, such as an RDD event. Moreover, appropriate risk communication procedures foster the trust and confidence that are vital in a crisis situation [29, 30].

Plan for communicating to the public and the news media by asking yourself the following questions [31]:

- ✓ What information is crucial to convey in initial messages in order to prompt appropriate public responses after a crisis situation?
- ✓ What are the messages to be delivered prior to (training and awareness of radiation basics), during, and after an incident?
- ✓ What are the opportunities for effective communications and how can they be optimized?
- ✓ What questions can we anticipate from the public and how can we minimize panic for these risk situations?
- ✓ Is the spokesperson deemed credible (as a trusted individual) by the public?
- ✓ What are the news media's responsibilities and how can you help reporters meet them?

Success in the communications arena is greatly assisted by striving to conduct as much of its work as possible in an open arena. As part of this process, effective and continued two-way dialog with stakeholders will help the Regulatory Authority in understanding concerns of citizens as well as State and local officials.

6. Conclusion

While strengthening the security of radioactive sources is not a new issue, recent world events have motivated many Regulatory Authorities around the world to undertake a comprehensive review of its security regime for its licensed facilities. As part of this approach, regulatory agencies, in cooperation with local law enforcement agencies, have assessed their national threat and imposed new or additional requirements to enhance physical security of risk-significant (Category 1 and 2) radioactive sources. In addition, simulated RDD exercises have lead to refined emergency response plans for such events. From these activities, Regulatory Authorities are using results achieved in identifying and targeting effective preventive and mitigative security strategies that result in long-term revisions to its existing regulatory framework.

Planning, establishing and integrating a radioactive materials security program into an overall regulatory infrastructure initially developed for health and safety purposes is now a key element in both licensee and regulatory control programs in establishing an effective mechanism for deterrence of radiological terrorism. Experience has shown that risk-based approaches to enhancing the security of radioactive materials can significantly reduce the potential threat against malevolent use of radioactive materials. Although results from each country are varied, national results range from completion of a national registration system for Category 1 and 2 sealed sources, and work in establishing new physical security requirements, to a robust system of licensing for export/import and pre-notification of risk-significant radioactive material shipments. Although use of the Code has become widely

accepted throughout the world, each Regulatory Authority has a shared responsibility with other countries to strive for improvement in their country's application of the Code of Conduct.

Regulatory Authorities also have an important role in continuing to work closely within their government and with international partners to continuously assess, integrate and improve their security programs to make risk-significant sealed radioactive sources more secure and less vulnerable to malevolent use by terrorists. By developing a further understanding of the actions needed in this area to ensure that a comprehensive security program is established, the Regulatory Authority is effectively enhancing the protection of individuals against capricious and unpredictable radiation exposure situations involving the malicious use of radioactive materials. Making these changes to existing emergency preparedness and response programs, and further integrating these changes into an effective public communication plan, can facilitate an effective and successful response to a potential or actual terrorist event involving radioactive materials.

REFERENCES

[1] U.S. NUCLEAR REGULATORY COMMISSION, Backgrounder: Dirty Bombs (2007) http://www.nrc.gov/reading-rm/doc-collections/fact-sheets/dirty-bombs.html.

[2] GONZALES, A. "Security of Radioactive Sources: The Evolving New International Dimensions," IAEA Bulletin 43/4 (2001) 39-48.

[3] INTERNATIONAL ATOMIC ENERGY AGENCY, "Code of Conduct on the Safety and Security of Radioactive Sources," IAEA, Vienna (2004).

[4] INTERNATIONAL ATOMIC ENERGY AGENCY, "List of States that have a made a political commitment with regard to the Code of Conduct on the Safety and Security of Radioactive Sources and the Supplementary Guidance on the Import and Export of Radioactive Sources," July (2008), http://www.iaea.org/Publications/Documents/Treaties/codeconduct_status.pdf.

[5] INTERNATIONAL ATOMIC ENERGY AGENCY, "Categorization of Radioactive Sources," Safety Guide No. RS-G-1.9, IAEA, Vienna (2005).

[6] INTERNATIONAL ATOMIC ENERGY AGENCY, "Dangerous Quantities of Radioactive Material (D-values)," EPR-D-Values, (2006), 1, http://www-pub.iaea.org/MTCD/publications/PDF/EPR_D_web.pdf.

[7] U.S. NUCLEAR REGULATORY COMMISSION, "Fiscal Year 2006 Interim Inventory of Radioactive Sources," (2006).

[8] U.S. NUCLEAR REGULATORY COMMISSION, Backgrounder: Dirty Bombs (2005) http://www.nrc.gov/reading-rm/doc-collections/fact-sheets/dirty-bombs-bg.html.

[9] U.S. NUCLEAR REGULATORY COMMISSION, "The Radiation Source Protection and Security Task Force Report; report to the President and the U.S. Congress Under Public Law 109-58, The Energy Policy Act of 2005," (2006), http://www.nrc.gov/reading-rm/doc-collections/congress-docs/correspondence/2006/president-08-15-2006.pdf.

[10] AMERICAN NATIONAL STANDARDS INSTITUTE (ANSI), "American National Standard for Gamma Radiography – Specifications for Design and Testing Apparatus, ANSI N43.9 (1991).

[11] U.S. NUCLEAR REGULATORY COMMISSION, Increased Controls for Licensees that Possess Sources Containing Radioactive Material Quantities of Concern (2005), http://www.nrc.gov/reading-rm/doc-collections/enforcement/security/2005/ml053130364.pdf

[12] U.S. NUCLEAR REGULATORY COMMISSION, Security Orders (2005), http://www.nrc.gov/reading-rm/doc-collections/enforcement/security/index.html#6.

[13] U.S. NUCLEAR REGULATORY COMMISSION, Order Imposing Increased Controls – Effective Immediately (2005), http://www.nrc.gov/reading-rm/doc-collections/enforcement/security/2005/ml053130218.pdf.

[14] U.S. NUCLEAR REGULATORY COMMISSION, Implementing Guidance for Licensees that Possess Radioactive Material Quantities of Concern (2008), http://www.nrc.gov/reading-rm/doc-collections/enforcement/security/2005/ml053130233.pdf.

[15] U.S. NUCLEAR REGULATORY COMMISSION, Supplemental Questions and Answers Regarding Increased Controls and Implementation for Licensees That Possess Radioactive

Material Quantities of Concern (2007), http://www.nrc.gov/reading-rm/doc-collections/enforcement/security/2007/supplemental.pdf.
[16] U.S. NUCLEAR REGULATORY COMMISSION, Frequently Asked Questions about NRC's Response to the 9/11/01 Events (2008), http://www.nrc.gov/security/faq-911.html.
[17] KOVAN, D., "Po-210 Poisoning in London: Radiation Protection Agencies Tested by a Real Threat," *Nuclear News*, July (2007) 29-33.
[18] MESERVE, R., Testimony provided of NRC Chairman Meserve to the U.S. House of Representatives on April 11 (2002), http://www.nrc.gov/reading-rm/doc-collections/congress-docs/congress-testimony/2002/04-11-02SecTestimony.pdf
[19] NATIONAL COUNCIL ON RADIATION PROTECTION AND MEASUREMENTS, Management of Terrorist events Involving Radioactive Material, NCRP Report No. 138, Bethesda, Maryland (2001), 7.
[20] UNITED STATES GOVERNMENT, *The 9/11 Commission Report*, Developed by the National Commission on Terrorist Acts Upon the United States [Public Law 107-306 (2002)], http://www.9-11commission.gov/report/911Report.pdf
[21] U.S. NUCLEAR REGULATORY COMMISSION, Export-Import (2008), http://www.nrc.gov/about-nrc/ip/export-import.html
[22] COLELLA, M., et. al., "An Introduction to Radiological Terrorism," The Australian Journal of Emergency Management, 20 2 (2005) 9-17.
[23] INTERNATIONAL ATOMIC ENERGY AGENCY, "The Radiological Incident in Goiânia," Publication No. 815, Vienna, (1988).
[24] NATIONAL ACADEMIES, "Radiological Attack: Dirty Bombs and other Devices," (2004) http://www.nae.edu/NAE/pubundcom.nsf/weblinks/CGOZ-646NVG/$file/radiological%20attack%2006.pdf
[25] FEDERAL EMERGENCY MANAGEMENT AGENCY, UNITED STATES DEPARTMENT OF HOMELAND SECURITY, "Planning Guidance for Protection and Recovery Following Radiological Dispersal Device (RDD) and Improvised Nuclear Device (IND) Incidents," Federal Register, Washington, D.C., Vol. 73, No. 149, (2008) 45029-45048.
[26] U.S. ENVIRONMENTAL PROTECTON AGENCY, "Manual of Protective Action Guides and Protective Actions for Nuclear Incidents," EPA 400-R-92-001, (1992).
[27] COMMISSION ON RISK ASSESSMENT AND RISK MANAGEMENT, "Framework for Environmental Health Risk Management," mandated by the 1990 Clean Air Act Amendments, (1997).
[28] HART, M., "Disabling the Terror of Radiological Dispersal," *Nuclear News*, July (2003), 40-43.
[29] Covello, V., McCallum, D., Pavlova, M., "Effective Risk Communication: The Role and Responsibility of Government and Nongovernment Organizations," New York: Plenum Press, (1989).
[30] Covello, V., et.al., "Risk communication, the West Nile virus epidemic, and Bioterrorism: Responding to the communication challenges posed by the intentional or unintentional release of a pathogen in an urban setting." Journal of Urban Health: Bulletin of the New York Academy of Medicine, 78, 382-91. (2001).
[31] U.S. DEPARTMENT OF HEALTH AND HUMAN SERVICES, "Communicating in a Crisis: Risk Communication Guidelines for Public Officials," Washington, D.C., (2002).