UNIVERSITY OF GEORGIA

Center for International Trade & Security

NUCLEAR SECURITY CULTURE FOR USERS OF RADIOACTIVE SOURCES: MODEL, SELF-ASSESSMENT, ENHANCEMENT

This report was developed as Sub-Task One under the 2015 Research Agreement between the International Atomic Energy Agency and the University of Georgia Research Foundation, Inc. (IAEA Research Agreement No: 19092/RO) which extends the University of Georgia the opportunity of participating in the IAEA Coordinated Research Project "J02007" entitled "Developed of Nuclear Security Culture Enhancement Solutions."

Editor and Contributor:

Dr. Igor Khripunov

Project Coordinator:

Danielle Williams

Contributors:

James Siuzdak
Katherine Nichols
Valeriia Lozova
Haston Gerencir
Robert Mudano
Jenna White

Table of Contents

1. Introduction

Extensive efforts by the world community to place radioactive sources and material under effective control remain largely elusive and may benefit from human based innovative approaches. The International Atomic Energy Agency (IAEA) Incident and Trafficking Database (ITDB) reports a total of 2,889 confirmed incidents (as of 31 December 2015) reported by participating states, but this could be just the tip of the iceberg.[1] The database provides clear evidence of porous security, easy accessibility, human complacency, and inadequate regulatory control. The majority of thefts and losses reported to the ITDB involve radioactive sources that are used in industrial or medical applications. Industrial sources are mostly used for non-destructive testing and for applications in construction and mining. Most devices use relatively long-lived isotopes such as Iridium-192, Caesium-137, Cobalt-60, and Americium-241, which constitute an attractive target for groups and individuals with malicious intent. A significant proportion of incidents reported at medical facilities were related to the loss of sources used in diagnostic and radiotherapy applications.

Millions of sources have been distributed worldwide over the past 50 years, with hundreds of thousands currently being used, stored, and produced in over 100 countries. The IAEA has tabulated over 20,000 operators of significant radioactive sources globally. In many countries, the inventory amounts are not well known as regulatory control of radioactive sources is weak. This increases the risk of spreading orphan sources. These "orphan sources" are sources that have been abandoned, lost, or misplaced, as well as sources that were stolen or removed without proper authorization. Exactly how many orphan sources there are in the world is not known, but the numbers are thought to be in the thousands. Moreover, orphan sources expose society to the risk of radiological accidents and terrorism.

A malicious act involving radioactive material has several serious effects on society, some are clearly understood while others are still underexplored. For example, insured losses from a medium-sized radiological attack on Washington, D.C., are estimated at over US $100 billion.[2] This estimate factors in automobile, commercial property, residential property, worker compensation, general liability, and group life insurance. What remains obscure and poorly understood is "indirect damage," the category into which most psychological traumas and disorders would fall. Many such ailments will remain undiagnosed, untreated, and ignored, possibly leading to serious psychological dysfunctions, failed professional careers, broken families, and diminished educational performance.

Radiophobia is a major reason why the social and psychological impact of radiological terrorism is so difficult to assess and deal with in each individual situation. The irrational belief that any level of ionizing radiation is highly dangerous, if not immediately deadly, creates a psychological vulnerability within the community that the government is unable to address. Few if any reliable criteria are available to help government planners draw up standard scenarios because each affected community will react to unknown and fearsome threats differently.

[1] The ITDB system was established in 1995 to record and analyze incidents of illicit trafficking in nuclear and other radioactive material and incorporates all reported incidents in which nuclear and other radioactive material is out of regulatory control; http://www-us.iaea.org/security/itdb.

[2] ''President's Working Group on Financial Markets: Terrorism Risk Insurance Analysis," American Academy of Actuaries, Washington, DC, April 21, 2006, p. 30.

While terror attacks involving chemical or biological agents or attacks on associated production and research facilities could claim a higher casualty toll than radiological attacks, they would not give rise to the same psychological traumas or require special assistance. Chemical substances, including highly toxic ones, are an everyday part of our households; and pharmaceuticals and other substances help us combat dangerous diseases and pandemics. Radioactive substances have no such offsetting benefits in the public mind, notwithstanding their widespread use in diagnosing and treating cancer and other diseases. Indeed, terrorists covet radiological weapons precisely because of their resemblance to nuclear weapons. Thus, radiological terrorism can be an awesome and destabilizing weapon for terrorists who are intent on intimidating and coercing citizens and their government.

This report provides a roadmap for improving security management of radioactive sources with an emphasis on a culture model, including self-assessment tools and a series of indicators as benchmarks to help convey a culture's measure and identify practical ways for enhancement. The purpose of assessment is to provide a clear picture on how the human factor influences security-related functional areas at the organization level. To this end, the report adjusts the existing IAEA methodology for nuclear security culture to meet specific requirements for the operation of radioactive sources. Though the IAEA security culture model in Nuclear Series Report No.7 is designed as generic in an effort to be applicable to a wide range of operations involving nuclear and radiological materials, its modifications proposed in this report are needed to make it user friendly and more focused on the security requirements of radioactive sources.[3] Their special security features include continued predominance of safety on the management priority list; diverse applications and categorization; mobile mode of operation for some sources; limitations to the use of traditional approaches in physical protection; different disposal options; and others. This toolset can facilitate a more robust and sustainable security regime for radioactive sources throughout their life cycle, i.e. from cradle to grave. Furthermore, it proposes a set of interrelated elements that establish policies and objectives by striking the right balance between safety, security, and efficiency.

2. Benefits and Risks

Radioactive sources are used throughout the world in many widespread applications for a variety of peaceful, productive, and beneficial purposes. These applications can include industrial radiography, oil well logging, medicine, research and education, and military. Such beneficial uses include:

- Killing bacteria in food, medical supplies, and equipment;
- Treating cancer and other diseases;
- Mapping underground sources of water and prospecting for oil and gas reserves;
- Non-destructive testing for integrity of pipe welds, pressure vessels, and other mechanical structures;
- Checking liquid levels in vessels during manufacturing operations; and
- Measuring the density of soil for construction projects.

Typically, these sources use radioactive materials that are contained or bound within a suitable capsule, (sometimes referred to as "housing") also known as sealed radioactive sources, but occasionally sources include

[3] "Nuclear Security Culture," Nuclear Security Series No7, IAEA, 2008: http://www-pub.iaea.org/books/IAEABooks/7977/Nuclear-Security-Culture.

radioactive materials in an unsealed form. These sources vary considerably in a number of ways such as physical size and properties, the amount of radiation they emit, and the type of encasing. They can comprise portable instruments (e.g. gauges for taking measurements), and pieces of equipment (e.g. a radiotherapy machine for cancer treatment).

It is important to note that when radioactive sources are safely managed and securely protected, the risks to workers and the public are minimal. However, if a radioactive source becomes out of control and unshielded or its radioactive material is dispersed as the result of either an accident or a malicious act, the danger of radiation exposure becomes very real. There have been many instances all over the world in which radioactive sources have been smuggled, lost, stolen, abandoned, or even used for malevolent actions—samples of which are illustrated in Appendix C. Such incidents stimulate worst-case fantasies and scenarios amongst the public. In addition, radiation exposure may not manifest itself immediately, leaving those in affected—or potentially affected—areas in anxiety and fear.

The IAEA reports that, until the 1950s, only radionuclides of natural origin—particularly Radium-266—were generally available for use. Since then, radionuclides produced artificially in nuclear facilities and accelerators have become widely available, including Cobalt-60, Strontium-90, Caesium-137, and Iridium-192. The IAEA has categorized radioactive sources to identify the types that require particular attention for safety and security reasons. Certain industrial and medical radioactive sources, including Cobalt-60, Caesium-137, Strontium-90, and Iridium-90 are most significant given that they emit high levels of radiation. These categories range from Category 1 (most dangerous to human health if not managed safely and securely, with exposure from a few minutes to an hour) to Category 5 (least dangerous, but would still require appropriate regulatory control) and are displayed below:

Table 1: IAEA Categorization, Conceptualization, and Examples of Radioactive Sources[4]

Category	Conceptualization		Examples
	Risk	**Dispersal Scenarios**	**Devices**
1 – Extremely dangerous to the person	• Likely to cause permanent injury to a person who handled the source, or were otherwise in contact with it, for more than a few minutes • Could be fatal to be close to this amount of unshielded material for a period of a few minutes to an hour	• Little or no risk of immediate health effects to persons beyond a few hundred meters away • For large sources, the infected area could be a square km or more	• Radioisotope thermoelectric generators • Irradiators (research and blood) • Teletherapy sources (including, fixed multibeam teletherapy)
2 – Very dangerous to the person	• Could cause permanent injury to a person who handled the source or who was otherwise in contact with it for a short time (minutes to hours) • Could be fatal to be close to this amount of unshielded radioactive material for a period of hours to days	• Little or no risk of immediate health effects to persons beyond a few hundred meters away • For large sources, the infected area would not exceed a square km	• Industrial gamma radiography sources • High/medium dose rate brachytherapy sources
3 – Dangerous to the person	• Could cause permanent injury to a person who handled it or who was otherwise in contact with it for multiple hours • Could be fatal to be close to this amount of unshielded radioactive material for a period of days to weeks	• Little or no risk of immediate health effects to persons beyond a few meters away • The infected area would not exceed a small fraction of a square km	• Fixed industrial gauges that incorporate high activity sources • Well logging gauges
4 – Unlikely to be dangerous to the person	• Very unlikely that anyone would be permanently injured by this source • Could temporarily injure someone who handled it or who was otherwise in contact or in close proximity with the source for many hours, days, or weeks	• Could not permanently injure persons	• Low dose rate brachytherapy (except eye plaques and permanent implants) • Industrial gauges that do not incorporate high activity sources • Bone densitometers • Static eliminators
5 – Most unlikely to be dangerous to the person	• No one could be permanently injured by this source	• Could not permanently injure persons	• Smoke detectors • Medical diagnostic sources

[4] "Categorization of Radioactive Sources," International Atomic Energy Agency, IAEA-TECDOC-1344, July 2003: http://www-pub.iaea.org/MTCD/publications/pdf/te_1344_web.pdf.

Radiological Dispersal Device

Radiological sources have the potential to be used as weapons as either radiological dispersal devices (RDDs), known as "dirty bombs", or as radiation exposure/emitting devices (REDs), known as a "hidden sealed sources". RDDs disperse radioactive material into the environment while REDs use a stationary radioactive source to expose victims to high levels of radiation. RDDs and REDs of any kind present a potent and effective terrorist weapon because they threaten to expose civilian populations to radiation, engendering anxiety, stress, and panic with the potential for casualties resulting from excess doses of radiation. Experts believe that from a public health perspective, the psychological effects may be equally harmful, if not more prevalent, than their physical health consequences.[5]

Almost any radioactive material can be used to construct an RDD and RED, including fission products, spent fuel from nuclear reactors, commercial radioactive sources, and relatively low-level materials such as medical, industrial, or research waste. Weapons-grade materials—plutonium or highly enriched uranium—are not required, although they could be used. Even if a plutonium-containing device fails to produce a nuclear explosion, it could still widely disperse the material leading to radioactive contamination, exposure, and psychological scarring. Large fractions of the particles are likely to be smaller than three micrometers in diameter and could, therefore, enter into the lungs and potentially cause cancer. Once dispersed over a vast territory, by wind and crowds of people, plutonium dioxide will remain insoluble in the vegetation, dust, and soil for a prolonged period of time.

Few, if any, deaths will result from radiation exposure in a small-scale RDD attack. Spreading small amounts of radiological material has no immediate substantial effect other than to instill public fear, panic, and alter behavior. The major challenge for governments will be long-term disaster mitigation, involving cleanup, the relocation of residents away from heavily contaminated areas, psychological care, and public education to ensure that areas struck by terrorists are not abandoned out of inflated fears of radiation.

3. Physical Protection and the Human Factor

A facility that stores and uses a radioactive source should have a sufficient level of security to address the risk of someone committing a malicious act. Financially, it makes sense that a facility would not reduce the risk to society to lower than what is required by the regulator, as the facility would then be overspending on security. Facilities often review security systems as a means of reducing overhead costs. To a limited degree, developing a robust security culture can compensate for cost-saving reductions in physical security measures.

A key step toward establishing required security measures depends on the determination of the threat-holder in utilizing the radioactive material in use, storage, and transport.[6] The threat assessment serves as a common basis for regulatory authorities and users of radioactive sources in performing their respective functions.

[5] Bromer, Evelyn, (1998), "Psychological Effects of Radiation Catastrophes" in Leif Peterson and Seymour Abrahamson eds., "Effects of Ionizing Radiation: Atomic Bomb Survivors and Their Children (1945-1995)", Joseph Henry Press, p.283.

[6] "Nuclear Security Recommendations on Radioactive Material and Associated Facilities," IAEA Nuclear Security Series No 14, p. 13.

With the threat assessment established and the graded approach applied to security arrangements, the organization starts designing a physical protection system that incorporates all the vital elements: deterrence, detection, delay, and response. This graded approach is based on the principles of risk management, which factors in the level of threat with the relative attractiveness of the material for malicious actors. In other words, the graded approach is shaped by such factors, as is the established categorization system for radioactive sources including their quality, physical and chemical properties, mobility, availability, and accessibility.

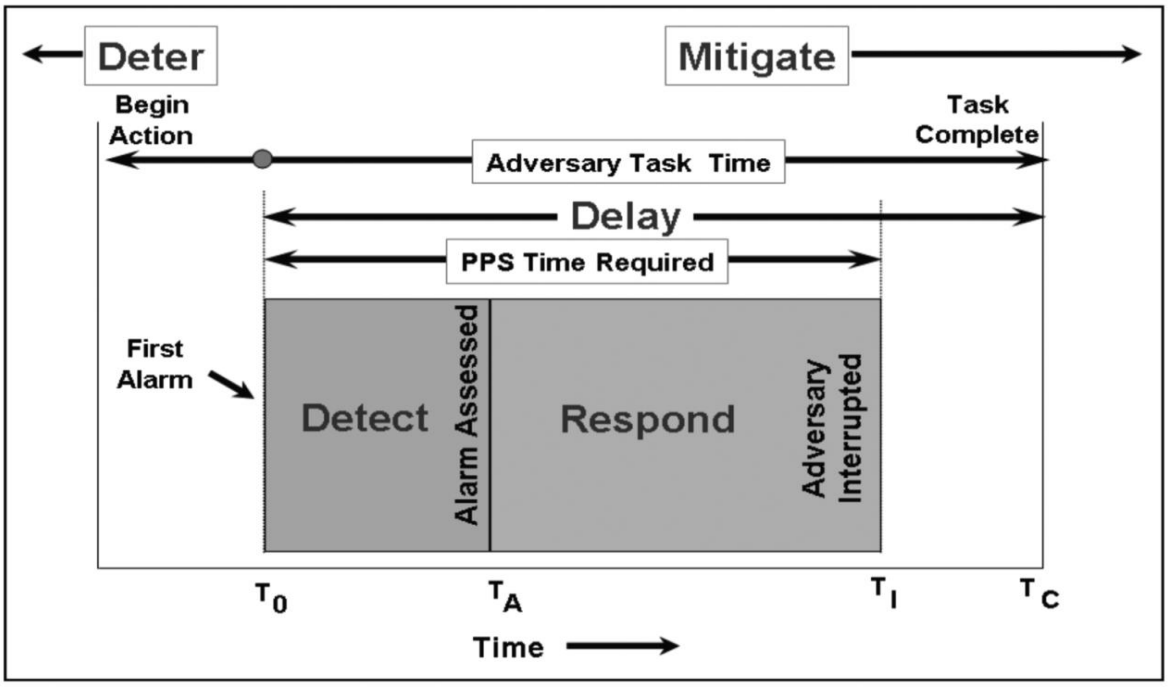

Figure 1: Deterrence, Detection, Delay, and Response

- ***Deterrence*** occurs when an adversary, otherwise motivated to perform a malicious act, is dissuaded from undertaking the attempt. Deterrent measures have the effect of convincing the adversary that the malicious act would be too difficult, the success of the act too uncertain, or the consequence of the act too unpleasant to justify undertaking.

- ***Detection*** involves monitoring both outside and inside the facility, determining the entry control effectiveness, and assessing intrusions. It is important that the detection features be complete with no "loopholes." Detection can be achieved through increased methods of surveillance, such as visual observation, video surveillance, electronic sensors, accountancy records, seals and other tamper-indicating devices, and process monitoring systems. In implementing the graded approach, the objectives of detection measures include not only detection but also assessment and communication of unauthorized access to radioactive sources.

- ***Delay*** measures should be implemented to impede an adversary's attempt to gain unauthorized access, remove radioactive material, or commit an act of sabotage generally through multiple barriers or

physical means, such as locked doors, cages, tie-downs or the like. A measure of delay is the time after detection that an adversary takes to remove the radioactive material or sabotage the associated facility. In implementing a graded approach, the objectives of delay measures could range from providing a sufficient delay after detection to allowing response personnel to interrupt malicious acts, or providing a delay to allow for a timely pursuit following unauthorized removal.

- ***Response*** measures should be implemented following detection and assessment. The operator should be required to make appropriate arrangements to communicate with law enforcement personnel so that they may appropriately perform the response. In implementing a graded approach, the objectives of response measures could range from providing an immediate response with sufficient resources to interrupt a malicious act, to providing alarm notification alerting the appropriate authority to investigate the event. The prospect of a successful response can also serve as a deterrent.

The core element of the security system is a security plan that is designed to protect the radioactive material while also implementing measures to address an increased threat level, respond to security events, and protect sensitive information. The scope of security plans cover:

- A description of the radioactive material and the environment of its use and storage;
- An agreed-upon level of threat;
- A description of the specific security concerns to be addressed;
- A description of the current security system and its objectives;
- Security procedures that provide guidance to operator personnel for operating and maintaining security measures, and the security procedures that are to be followed before and after maintenance;
- Administrative aspects, including defining the roles and responsibilities of individuals with security responsibilities, access authorization processes, trustworthiness determination processes, information protection processes, inventories and records, event reporting, and review and revision of the security plan;
- How procedural and administrative security measures will be scaled to meet increased levels of threat, as assessed by the state; and
- Response to actions including cooperation with relevant competent authorities in the location and recovery of radioactive material consistent with the national practice.

Once the security system is designed, the influence of human factors must be considered and built into the calculation in order for its success. This means looking at each of the factors that are considered at risk due to human error, inconsistencies, complacency, and other reasons. One of the IAEA security recommendations for radioactive sources emphasizes the importance of promoting a security culture:

> "All organizations and individuals involved in implementing nuclear security should give due priority to the nuclear security culture with regard to radioactive material, to

its development and maintenance necessary to ensure its effective implementation in the entire organization." [7]

Indeed, an effective security culture for radioactive sources depends not only on proper planning, training, operations, and maintenance, but also on the thoughts and actions of people who plan, operate, and maintain security systems. The foundation of security culture is recognition by those that have a role in regulating, managing, or operating facilities or activities involving radioactive sources, or even those that could be affected by such activities in which a credible threat exists and that security is important.[8] Security culture is an effective tool in addressing insider threats because due to the work environment and ease of accessibility it is motivated and vigilant personnel, in combination with adequate physical protection, who is recognized as an indispensable player in safeguarding radioactive sources. In many states, the physical protection, accounting, and control systems for radioactive sources are insufficient. Radioactive sources are used, stored, and transported by private entities often to a large quantity of consumers who are viewed as soft targets by potential adversaries.[9] Radioactive source users may be technically competent, but are still vulnerable if they discount the role of the human factor. The entire security regime stands or falls based on the people involved. Thus, the human factor plus the upper tier of managers and leaders must be addressed continuously and meticulously to ensure the security regime will be effective, sustainable, and optimal.

4. Security Management of Radioactive Sources

Given the evolving security threat environment, the current emphasis on the need to protect radioactive sources from being used for malicious purposes is generally perceived as inevitable. To identify an optimal relationship between traditional and new risk-based approaches for creating an operational procedure for radioactive sources, management is increasingly viewed as a multi-dimensional comprehensive system. In other words, this system must be a set of interrelated elements that establishes policies and objectives that achieve the right balance between safety, security, efficiency, and risk to society.

Such a management system binds all elements of an organization into one coherent system including resources, processes, personnel, equipment, and documented policies. The entirety of these essential security management requirements is addressed by international legal instruments, national regulations, IAEA standards and recommendations, and by professional codes and mission commitments.

The Code of Conduct for the Safety and Security of Radioactive Sources, originally produced in 2000 by a group of technical and legal experts, and later approved by the IAEA's Board of Governors, occupies the top position in this hierarchy.[10] The Code of Conduct stipulates "every state should, in order to protect individuals, society, and the environment, take the appropriate measures necessary to ensure…the promotion of safety culture and of

[7] "Nuclear Security Recommendations on Radioactive Material and Associated Facilities," IAEA Nuclear Security Series No 14, p. 13.
[8] "Security for Radioactive sources," Implementing Guide, IAEA Nuclear Security Series No. 11, p. 6.
[9] Andrew Bieniawski, Ioanna Iliopulos, Michelle Nalabandian. "Radiological Security: Progress Report," Nuclear Threat Initiative, March 2016, p.10.
[10] Experts are split as to whether UNSCR 1540 (2004) covers radioactive sources. The resolution refers in a footnote to weapons of mass destruction (WMD) and their means of delivery. For information on the ongoing debate see http://cits.uga.edu/publications/compass/.

security culture with respect to radioactive sources."[11] Addressed to states and national regulators, the Code remains non-binding. Its range of provisions specifies the need for maintaining control over sources. However, in reality the focus was still very much on incidents, such as people stealing sources for scrap value, and with little consideration given to the possibility of using sources for malicious purposes. Following the 11 September 2001 events, the Code of Conduct was revised to strengthen several security-related provisions and to address malicious and/or intentional misuse of radioactive sources. At the same time, member states agreed to develop an additional guidance on the import and export of radioactive sources. As a result, the Supplementary Guidance on the Import and Export of Radioactive Sources was drafted by experts and endorsed by the IAEA General Conference, in 2004, for inclusion in the Code. In response to the invitation from the IAEA Director General, member states made political commitments in which they indicated their intention to implement this non-binding Code with the Supplementary Guidance. As of late August 2016, 133 of 168 member states have made such commitments in writing.[12]

The Code of Conduct and the Supplementary Guidance complement the existing IAEA Safety Standards Series. Specifically, the Basic Safety Standards, which were first published in 1962, and continues to be regularly updated. Since 2004, due to the growing awareness of the need for security, the IAEA has established the Nuclear Security Series (NSS) and has published numerous documents: The Nuclear Security Fundamentals, Nuclear Security Recommendations - including NSS No. 14 (Nuclear Security Recommendations on Radioactive Material and Associated Facilities) and NSS No. 15 (Nuclear Security Recommendations on Nuclear and Other Radioactive Material out of Regulatory Control) - as well as several guides. [13] These guides include two documents exclusively related to radioactive sources: NSS No. 11 (Implementing Guide on Security of Radioactive Sources) and NSS No. 5 (Reference Manual on Identification of Radioactive Sources and Devices). Other NSS publications are applicable to the security of radioactive sources and provide additional input regarding physical protection, computer security, forensics, and other topics of study. As demonstrated by Table 2, most of the documents on radioactive sources explicitly reference security culture as a vital element for attaining desired goals, but provide very few details, if any, on how to accomplish this task in practical terms.

Table 2: IAEA Publications for Management of Radioactive Sources [14]

Series No.	Date	Title	Security Culture Reference
		Fundamentals (F)	
No.20	2013	**"Objective and Essential Elements of a State's Nuclear Security Regime"**	"Sustaining A Nuclear Security Regime: (C) Developing, fostering and maintaining a robust nuclear security culture."

[11] International Atomic Energy Agency, Code of Conduct on the Safety and Security of Radioactive Sources, IAEA/CODEOC/2004, IAEA, Vienna

[12] The International Conference on the Safety and Security of Radioactive Sources held in Abu Dhabi, United Arab Emirates (October 2013) discussed an option of developing on the basis of the Code of Conduct and Supplementary Guidance a legally binding international instrument. It recommended that the IAEA should convene a working group to assess the merits of developing such convention and make recommendations to member states; http://www-pub.iaea.org/iaeameetings/43047/International-Conference-on-the-Safety-and-Security-of-Radioactive-Sources.

[13] IAEA Nuclear Security Series Reports: http://www-ns.iaea.org/security/nss-publications.asp?s=5.

[14] IAEA Nuclear Security Series Reports: http://www-ns.iaea.org/security/nss-publications.asp?s=5.

		Recommendations (R)	
No.13	2011	**"Nuclear Security Recommendations on Physical Protection of Nuclear Material and Nuclear Facilities" (INFCIRC/225/Revision 5)**	"All organizations involved in implementing physical protection should give due priority to the security culture, to its development and maintenance necessary to ensure its effective implementation in the entire organization."
No.14	2011	**"Nuclear Security Recommendations on Radioactive Materials and Associated Facilities"**	"All organizations and individuals involved in implementing security should give due priority to the nuclear security culture with regard to radioactive material."
No.15	2011	**"Nuclear Security Recommendations on Nuclear and Other Radioactive Material Out of Regulatory Control"**	"The State should implement relevant elements of the nuclear security culture for the trustworthiness program."
		Implementing Guide (G)	
No.7	2008	**"Nuclear Security Culture"**	"Nuclear security culture: The assembly of characteristics, attitudes and behaviours of individuals, organizations and institutions which serve as a means to support, enhance, and sustain nuclear security."
No.8	2008	**"Preventive and Protective Measures Against Insider Threats"**	"Security awareness programmes should be developed in a coordinated manner with safety awareness programmes in order to establish effective and complementary safety and security cultures."
No.9	2008	**"Security in the Transport of Radioactive Material"**	"The State takes appropriate measures to ensure the promotion of a security culture for all involved in the transport of radioactive material."
No.10	2009	**"Development, Use and Maintenance of the Design Basis Threat"**	"Include assessing the operator's efforts to develop detailed adversary scenarios on the basis of the DBT, to identify vital areas, develop strategies for physical protection, and to create a security culture."
No.11	2009	**"Implementing Guide on Security of Radioactive Sources"**	"A dynamic and effective security culture should exist at all levels of operator staff and management."
		Technical Guide (T)	
No.12	2010	**"Educational Programme in Nuclear Security"**	"Educational programmes in nuclear security should aim at establishing in-depth and sustainable knowledge and skills, and foster nuclear security culture in a country or region."
No.17	2011	**"Computer Security at Nuclear Facilities"**	"The characteristics of nuclear security culture are the beliefs, attitudes, behavior and management systems, the assembly of which lead to a more

effective nuclear security programme. The foundation of nuclear security culture is recognition — by those that have a role to play in regulating, managing, or operating nuclear facilities or activities or even those that could be affected by these activities — that a credible threat exists and that nuclear security is important."

In addition, there are several professional codes and ethical standards which mention culture in the context of radioactive sources management. For example, the International Source Suppliers and Producers Association (ISSPA) has introduced for its members a Code of Good Practice designed to contribute to enhance safety and security of sources throughout their life cycle. Their objective is to be achieved through "the implementation of robust safety and security cultures, and strong regulatory compliance practices" for producers and suppliers of radioactive sources. The Code's "user support" section speaks of the need to offer training and technical support to the users regarding safe and secure operations, and to provide technical competence, when requested, in response to events regarding safety and security.[15] Another example is the U.S. Health Physics Society's (2012) Position Statement on Radiation Safety Culture, which implies there is a functional interface between safety culture and security culture.[16]

There is a clear recognition of the pivotal role the human factor plays in maintaining control of radioactive sources at the lowest possible risk level. The challenge is to identify key fundamental traits and frame them into a model of security culture that is applicable to diverse users of radioactive sources. A recent illustration of these trends can be found in the proceedings of the International Conference on the Safety and Security of Radioactive Sources held on 27-31 October 2013 in Abu Dhabi, UAE. Conference participants, for example, identified the lack of guidance on insider threat and trustworthiness and recommended that the IAEA address these issues as a priority. The special focus on education and training as sustainability tools is also noteworthy. Conference findings stress the need for "formal recognition" of experts for radiation safety and nuclear security, and those who are involved in managing radioactive sources. One of the human resource development initiatives outlined by the Conference Chair was the "establishment of national professional associations, recognized by the State, for radiation safety and nuclear security."[17]

The next logical step is to reinforce the role of security in this domain by formulizing existing IAEA security culture concepts and practices to meet specific requirements needed for the security of radioactive sources. This step would be consistent with the original concept of the Code of Conduct, which stipulates that every state should take appropriate measures necessary to ensure the promotion of safety and security culture, with respect to radioactive sources.

[15] International Source Suppliers and Producers Association, Code of Good Practices, http://isspa.com/about-isspa/.

[16] Health Physics Society, Position Statement on Radiation Safety Culture, February 2012, http://www.hps.org. The Health Physics Society has 5,000 members who are scientists, physicians, engineers, lawyers, and other professionals.

[17] International Conference on the Safety and Security of Radioactive Sources: Maintaining Continuous Control of Sources throughout their Life Cycle, Findings of the President of the Conference, 27-31 October 2013, Abu Dhabi, United Arab Emirates; http://www-pub.iaea.org/iaeapublications/43047/International-Conference--on-the-Safety-and-Security-of-Radioactive-Sources.

5. Nuclear Security Summits: Protection of Radioactive Sources

Nuclear Security Summits

The first Nuclear Security Summit (NSS) in Washington D.C. (2010) brought together three international organizations and world leaders from 47 countries to work on securing nuclear materials and preventing nuclear terrorism. Following its success, the summits re-convened every two years with the participation of the most important countries in the nuclear domain. Summits concluded with a communique—an official statement adopted by the attending states, summarizing the core themes of discussion and political pledges to address specific facets of nuclear security. Table 3 illustrates an increased awareness of radiological threats and adequate security measures discussed throughout multiple NSS.

Within each of the four published communiques, security culture emerged as a consistent factor. However, its radiological subset was not a major item until the 2016 Washington Summit. The importance of establishing a robust nuclear security culture to combat threats of nuclear terrorism emerged as an important take-away to radiological and nuclear security culture. The Summits were comprehensive in addressing nuclear security concerns but many of the participating countries lacked adequate infrastructure to mitigate radiological threats, and excluded precautions for states that rely on radiological materials for economic and industrial benefit. Communiques and Gift Baskets can provide guidance to states suffering from inadequate infrastructure, but additional support may be necessary to properly address threats.

Table 3: Increased Cultural Awareness of Radiological Threats through Nuclear Security Summits

Nuclear Security Summit	Communique	Other Documents (Gift Baskets and Joint Statements)
Nuclear Security Summit, Washington (2010)	"Recognize that measures contributing to nuclear material security have value in relation to the security of radioactive substances and encourage efforts to secure those materials as well."	Washington (2010) Work Plan: "Participating States will consider how to best address the security of radioactive sources, as well as consider further steps as appropriate."
Nuclear Security Summit, Seoul (2012)	- Discussion pertaining to radioactive sources and their use for malicious acts - Securing radioactive sources in the following sections: Security and Safety, Transportation Security, Combating Illicit Trafficking, and Nuclear Forensics -No explicit reference to radiological terrorism	Four statements referring to radioactive material: - Germany Presents: Gift Basket: Security of Radioactive Sources - Joint Statement on Transportation Security - Statement of Activity and Cooperation to Counter Nuclear Smuggling - Joint Statement on the Contributions of the Global Initiative to Combat Nuclear Terrorism (GICNT) to Enhancing Nuclear Security
Nuclear Security Summit, The Hague (2014)	-Use of radioactive sources for malicious acts plus information regarding the safety of radioactive waste	Seven statements referring to radioactive material: - Joint Statement on Forensics in Nuclear Security - Joint Statement on Strengthening Nuclear Security

	- Securing Radioactive Sources in following sections: Fundamental Responsibility of States, Nuclear Material, Nuclear Transportation, Illicit Trafficking, and Nuclear Forensics - One direct reference of radiological terrorism	Implementation - Joint Statement on Enhancing the Security of the Maritime Supply Chain - Joint Statement on Enhancing Radiological Security - Joint Statement on the Contributions of the Global Initiative to Combat Nuclear Terrorism (GICNT) to Enhancing Nuclear Security - Joint Statement on Transport Security - Statement of Activity and Cooperation to Counter Nuclear Smuggling
Nuclear Security Summit, Washington (2016)	References to radiological terrorism: - "...radiological terrorism remains one of the greatest challenges to international security, and the threat is constantly evolving." - Recognizes that there remains work to be done to address the issue	Nine statements referring to radioactive material: - Gift Basket on Mitigating Insider Threats - Joint Statement on Certified Training for Nuclear Security Management - Joint Statement on Forensics in Nuclear Security - Joint Statement on Maritime Supply Chain Security - Joint Statement Strengthening the Security of High Activity Sealed Radioactive Sources (HAAS) - Joint Statement on Nuclear Terrorism Preparedness and Response - Joint Statement on Countering Nuclear Smuggling - Joint Statement on Transport Security - Joint Statement on National Nuclear Detection Architecture
Nuclear Industry Summits **-2012 Seoul, South Korea** **-2014 The Hague, Netherlands** **-2016 Washington, DC**	- Commitments by industrial leaders to cooperate with state authorities to better secure radiological materials - Priority given to increase role of technology in reducing enrichment levels for industrial use - Emphasis on enhancing radiological security globally while moving towards the use of alternative materials - Need for new security methods within the private sector to meet the demand of elevated roles for radiological materials worldwide	2016 Nuclear Industry Summit: - Working Group Paper Two: Securing the Use, Storage, and Transport of Strategic and Radiological Materials - Working Group Paper Three: The Role of Nuclear Industry Globally

In September 2016, Germany's Federal Office for Radiation Protection organized a three-day international workshop titled "Safety and Security of radioactive sources – Are the provisions for security in the Code of Conduct on the Safety and Security of Radioactive Sources (COC) sufficient and effective?", that focused on the efficacy and implementation of international standards and regulations concerning the security of sealed radioactive sources. The workshop was a follow-up of the discussion held on this subject at the 2016 Nuclear

Security Summit. The conclusion of the workshop called for raised awareness on the importance of security culture for users of radioactive sources, the increased information exchange between operators and manufacturers, and the establishment of new arrangements to consider threat assessments—all while reinforcing the role of the IAEA.[18]

Nuclear Industry Summits

In 2012, state leaders called for a biannual summit to facilitate communication among industrial experts. The call for cooperative efforts led to the emergence of Nuclear Industry Summits (NIS)—a convention which brings together expert leaders to discuss the pivotal role held by corporations to adequately identify, address, and prevent threats stemming from nuclear terrorism.[19] Concerns for radiological security became increasingly important among the convening leadership—as it became clear that issues surrounding the safety and security of these materials required significant attention across the industry.

In the 2012 NIS, radiological security became an underlying concern for the private sector, and a new priority was given to technological advancements to reduce the uranium enrichment level in the production of radioisotopes for medical and research purposes.[20] Similarly, the 2014 NIS focused on the security of radiological materials arising from widespread advancements in nuclear technology within modern society—particularly from extensive applications in the medical field. By the final NIS in 2016, radiological security emerged as the key theme for discussion and emphasized the growing demand to enhance radiological security worldwide while stressing the need to transition away from dangerous radioactive sources to that of safer alternative materials. Throughout all summits, the need for increased cooperation of the private industrial sector with state authorities was heavily reinforced, as well as new methods to address security and safety issues relating to evolving nuclear technology to account for the elevated role of radiological materials worldwide.

6. IAEA Concept and Model of Nuclear Security Culture

The IAEA defines nuclear security culture as "the assembly of characteristics, attitudes and behavior of individuals, organizations and institutions which serve as a means to support and enhance nuclear security."[21] In 2008, the IAEA published the Implementing Guide on Nuclear Security Culture in its Nuclear Security Series, which defines the concept and characteristics of nuclear security culture while delineating the roles and responsibilities of institutions and individuals entrusted with this function. Since 2007, the IAEA has conducted numerous international, regional, and national workshops to promote security culture and to train nuclear security personnel at all levels.

The IAEA security culture design is based on the organizational culture model developed by Professor Edgar Schein of the Massachusetts Institute of Technology (MIT). Schein's model was successfully used in the 1990's to develop nuclear safety culture following the Chernobyl accident (1986), which amply demonstrated serious gaps in safety compliance and a failure of the human factor. The synergies between safety and security and their

[18] Federal Office for Radiation Protection (2016) "Safety and Security of radioactive sources - Are the provisions for security in the Code of Conduct sufficient and effective?" International Workshop 13 – 15 September 2016, Berlin Germany.
[19] Nuclear Industry Summit, "Joint Statement of the 2012 Seoul Nuclear Industry Summit" Nuclear Industry Summit 2016.
[20] Nuclear Industry Summit, "Joint Statement of the 2014 Nuclear Industry Summit" Nuclear Industry Summit 2014.
[21] "Nuclear Security Culture: Implementing Guide," Nuclear Security Series No. 7, IAEA, 2008, p.3.

overlaps as part of overall organizational culture provides a ready-made analytical framework for exploring and modeling security culture and making it compatible with safety culture. Schein defined culture as a "pattern of shared basic assumptions that the group learned as it solved its problems of external adaptation and internal integration that has worked well enough to be considered valid and, therefore, to be taught to new members as the correct way to perceive, think, and feel in relation to those problems."[22]

Jointly learned values, beliefs, and assumptions become shared and taken for granted as a nuclear facility continues to successfully operate at an acceptable risk and compliance level. To paraphrase Edgar Schein, they become shared, sustainable, and taken for granted as the new members of the organization realize that the beliefs, values, and assumptions prevailing among the leaders and the staff lead to organizational success and, therefore, must be "right".[23]

Schein proposes that culture in organizations exists in layers comprised of underlying assumptions, espoused values, and artifacts. Some of the layers are directly observable while others are invisible and must be deduced from what can be observed in the organization.[24]

Cultures are formed by ***underlying assumptions*** about reality. In practical terms, this means that an organization will display observable artifacts and behavior that relates to what it assumes about a variety of phenomena, such as vulnerability to an inside or outside threat. All of these assumptions or beliefs ultimately manifest themselves in observable forms such as documents, practices, and behaviors. The senior managers influence these patterns of assumptions and beliefs, but are often ignored by staff members, are never discussed, and are taken for granted.

The next layer of culture within organizations is ***espoused values***; the principles by which leadership claims to believe in and wants the organization to display in their actions. The culture predominantly manifests itself through behavior defined by Schein as ***artifacts***—the third and most observable layer. Thus, the maintenance of physical protection hardware, people's behavior in response to alarms, written documents, and work processes are all artifacts of the culture.

Using Edgar Schein's three layers of culture, the reproduced IAEA model for nuclear security culture divides the artifacts of the culture into three parts, giving a total of five elements (see Figure 2). They are: 1) beliefs and attitudes (what Schein calls "underlying assumptions"); 2) principles for guiding decisions and behavior (what Schein calls "espoused values"); 3) leadership behavior (these are specific patterns of behavior and actions which are designed to foster more effective nuclear security); 4) management systems (these are the processes, procedures and programs in the organization which prioritize security and have an important impact on security functions); and 5) personnel behavior (these are the desired outcomes of the leadership efforts and the operation of the management systems).

[22] Edgar Schein, "Organizational Culture and Leadership," 3rd ed. (San Francisco, CA: Jossey-Bass, 2004), p.17.
[23] Edgar Schein, "The Corporate Culture: Survival Guide," (San Francisco: Jossey-Bass, 1999), p.20.
[24] Edgar Schein, "The Corporate Culture: Survival Guide," (San Francisco: Jossey-Bass, 1999), p.16.

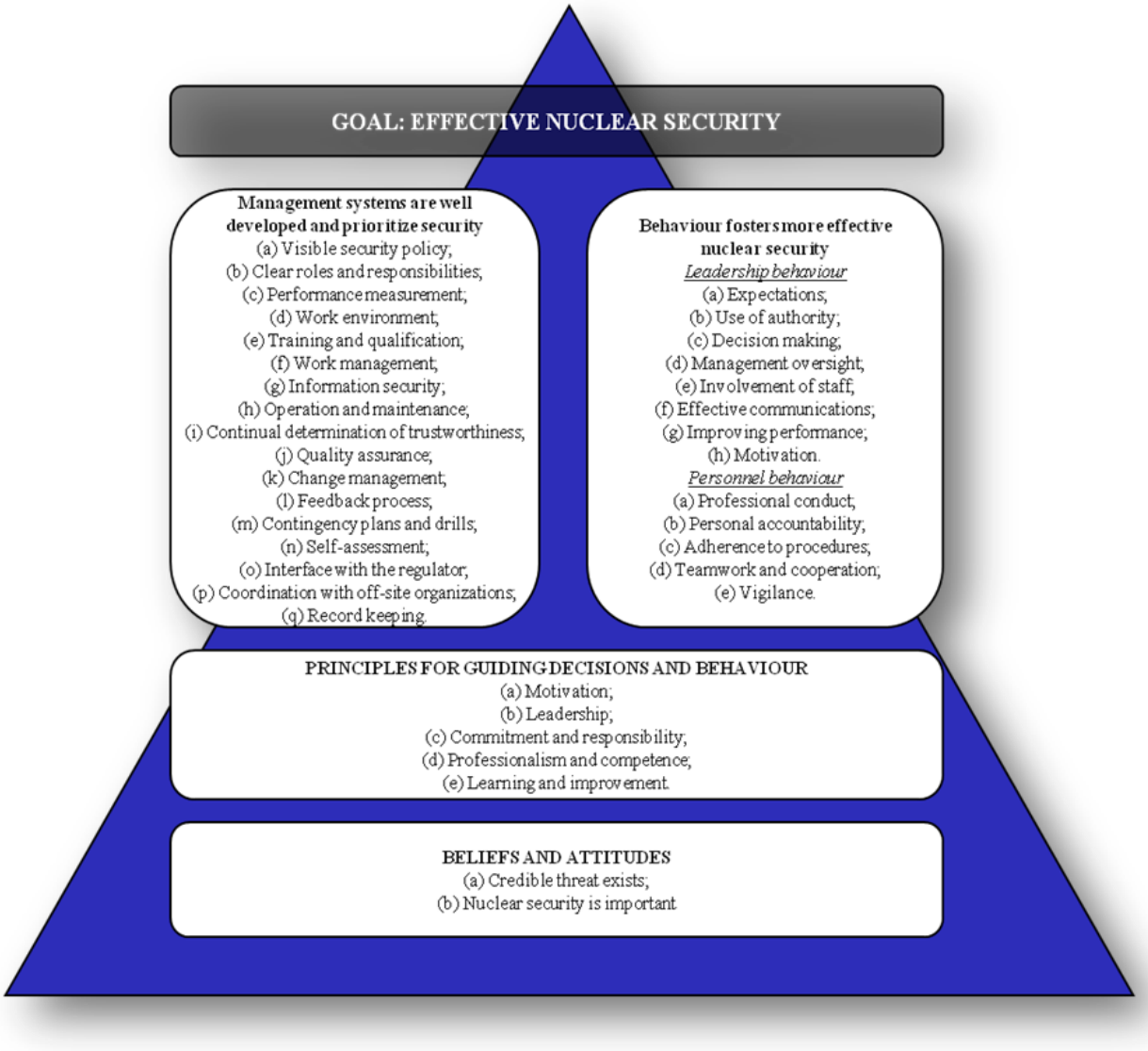

Figure 2: IAEA Model of Nuclear Security Culture[25]

Beliefs and attitudes that affect nuclear security are ingrained in people's minds over time and become causal factors in both the precursors and the response to security events. Without a strong substructure of beliefs and attitudes about threats, an effective nuclear security culture cannot exist. Accordingly, the most important assumption for nuclear security in an organization is that there is a credible insider and outsider threat. In other words, there must be an underlying assumption of vulnerability, which spreads and permeates throughout the entire workforce and not merely the organization's security specialists.

The process of building nuclear security culture is driven by a set of indicators assigned to each of its characteristics. Indicators help measure culture within these characteristics and identify practical ways for

[25] "Nuclear Security Culture," Nuclear Security Series No.7, IAEA, 2008.

improvement. These indicators constitute a framework under which to facilitate change and development, while promoting wanted and discouraging unwanted behavior. Hence, culture indicators perform four main functions: a) monitor security awareness in the organization; b) determine tools and procedures for mapping improvement; c) provide guidance for making an improvement strategy; and d) motivate the management and staff to take all necessary actions.

Before starting to build nuclear security culture, it is useful to look at some of its general properties:

- Cultures are a product of social learning. Therefore, they cannot be shifted without determined efforts from both national and facility leaders. Orientation sessions provide an outlet for explanation and discussion, and can help leaders modify the organizational culture, provided they back up these sessions with daily reinforcement and participate in leadership by example.

- Since there is always security culture within an organization, the question is whether the culture is what the management needs it to be, and whether it is improving, decaying, or remaining static.

- It is often easier to change patterns of thinking in an organization than to change patterns of behavior. New managers can come in brimming with bold new ideas yet fail to get people to change their old behaviors.

- Leaders are most influential in changing security culture, as they are able to intervene at all levels. With sustained effort, and by deploying incentives and disincentives at their disposal they can mold new patterns of thinking, establish new patterns of behavior, and even change the physical environment.

- Culture reduces anxiety for their members by establishing shared patterns of thinking, speaking, and acting. Consequently, cultural change will always increase anxiety within the organization until the new patterns are learned. Leaders must reduce the anxiety of learning a new culture and increase the anxiety of staying in the old culture.

The Implementing Guide is the only IAEA publication released thus far on nuclear security culture, and is intended to serve as an introduction to the subject for its potential users. The model, its characteristics, and its indicators are generic enough to be used by regulatory bodies and other organizations involved in activities utilizing nuclear and other radioactive material, including transportation. Its generic nature has both advantages and disadvantages. On one hand, the model can be utilized throughout the entire nuclear industry and lay the groundwork for shared values and practices. On the other hand, the model lacks specificity and comprehensiveness when applied in each type of nuclear radiological facility, therefore requiring adjustments and additions to gauge the status of security culture. The Implementing Guide recognizes these limitations and explains that the objective is to encourage self-examination by organizations and individuals, i.e. to stimulate further thought rather than to be prescriptive.[26] Accordingly, given the lack of expertise and experience among some users of radioactive sources, the purpose of this report is to assist them in appropriately utilizing the IAEA model by adjusting its generic approach to meet the specific needs of their facilities and making self-examination more productive.

[26] "Nuclear Security Culture: Implementing Guide," Nuclear Security Series No 7, IAEA 2008, p.19.

7. Safety-Security Interface in Preventing the Loss of Control of Radioactive Sources

Safety and security have a common objective—the protection of people, society, and the environment from a release of radioactive material. However, while both focus on the risk of inadvertent human error, security places additional emphasis on deliberate acts that are intended to cause harm. Because security deals with deliberate acts, security culture requires different attitudes and behavior, such as maintaining the confidentiality of information and enforcing efforts to deter malicious acts, as compared with safety culture, which is characterized by transparency.

Many of the principles inherent in both cultures are common (e.g. questionable attitude, rigorous and prudent approaches, and effective two-way communication to name a few) although their implementation may differ. There are also circumstances in which actions to serve our objective can be antagonistic to the achievement of the other. For example, under some storage arrangements, radioactive sources may be safe but not secure. In addition, in the absence high consequence security breaches, security culture is seldom homogenous. Hence, while it is reasonable to assume that most employees take ownership of safety and accept its importance, security may give rise to divergent attitudes among personnel.

As two overlapping subsets of organizational culture, both safety and security must operate in a mutually supportive way. Preventing the loss of control of radioactive sources is an important collaborative mission as it serves to protect human lives, society, and the environment.

There is a multitude of causes for the loss of control of a source. In the past, most causes were inadvertent and largely due to negligence and noncompliance. Under current conditions of growing terrorist threats, there is an increased likelihood of sources getting out of regulatory control for deliberate financial or malicious reasons. Among such motivations is avoidance of disposal costs, illegal sale for profit, and terrorism. Factors that can increase the potential for sources to be orphaned or become vulnerable include bankruptcy of users, armed conflict in the area, failure to use authorized vendors for servicing, scrap metal scavenging, restructuring of users' institutions, transfers for inappropriate disposal, and inadequately trained personnel.

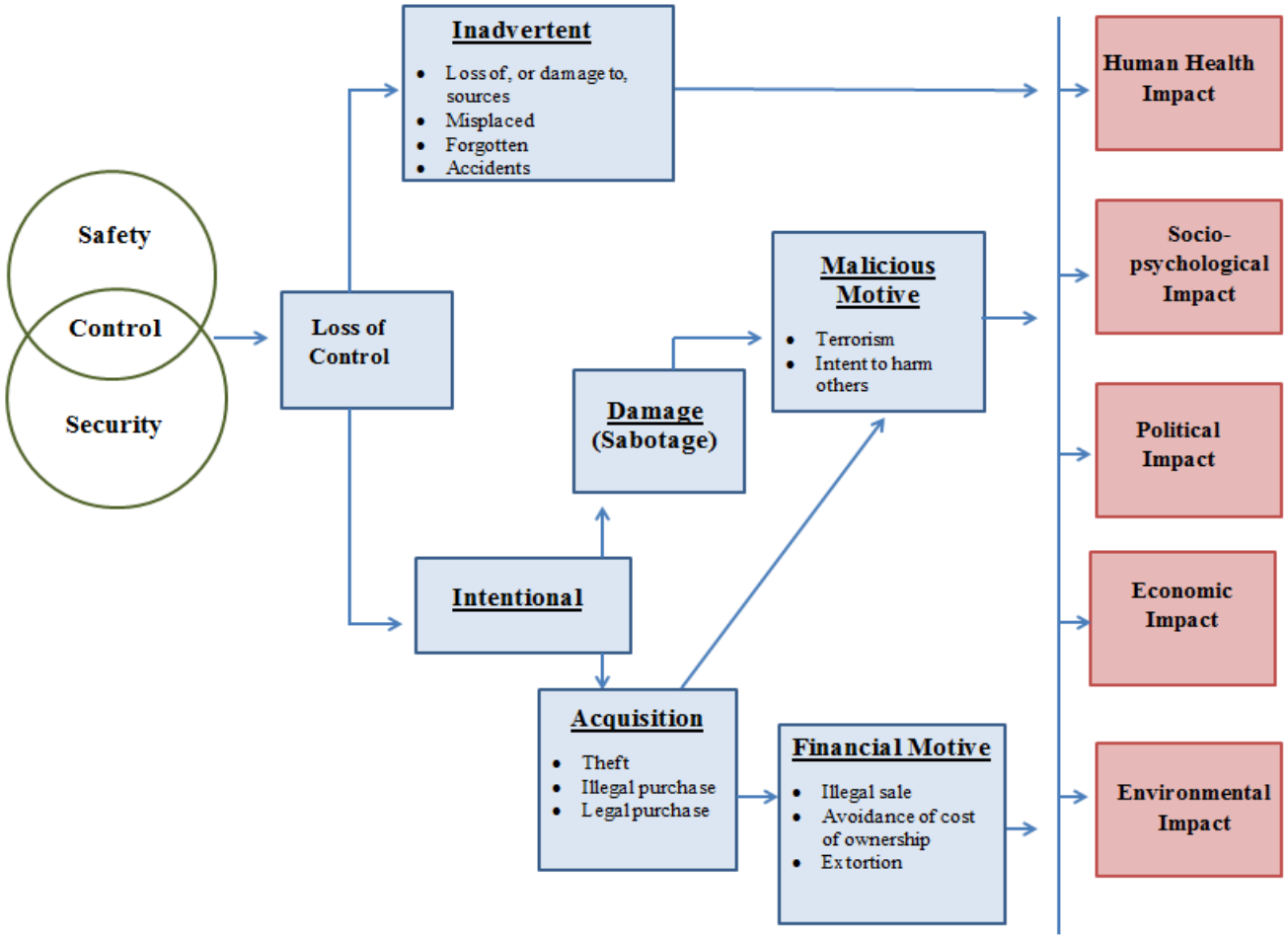

Figure 3: Loss of Control of Radioactive Sources and Possible Consequences[27]

Close interaction of safety and security culture is key to successfully accomplish this mission and to avoid the five main adverse impacts outlined on the right side of Figure 3, i.e. human health impact, socio-psychological impact, political impact, economic impact, and environmental impact. To this end, relevant safety and security personnel need to develop a teamwork mentality, understand each other's language, viewpoints, thinking, objectives and objections as well as stay committed to the common goal of keeping their facilities operational, safe, secure, compliant, and profitable.

8. Radioactive Sources: Special Considerations for Security Culture

As an assembly of characteristics, attitudes, and behavior, security culture is a supporting and enhancing tool of the security regime of radioactive sources. As defined by the IAEA, the objectives of the regime are to:

- Protect against unauthorized removal of radioactive material;

[27] Based on IAEA, "Strengthening Control over Radioactive Sources in Authorized Source use and Regaining Control over Orphan Sources", IAEA-TECDOC-1388, February 2004, pg.9.

- Protect against sabotage of material, facilities and activities, i.e. production, processing, use, storage, disposal, transport, etc.;

- Ensure the implementation of rapid and comprehensive measures to locate and recover radioactive material that is lost, missing or stolen and to re-establish regulatory control.[28]

Several features of radioactive source security make it distinctly different from nuclear security and have a substantive effect on its culture design. These distinct features can be summarized as follows:

1. Continued prevalence of safety orientation

As described in Section 4, the Code of Conduct was originally tailored to safety and radiation protection rather than security. Many organizations with limited use of radioactive sources have large operational units, where no radioactive sources are utilized, and where security mentality is not well developed or popular. As a result, managers tend to delegate security to their lower-tiered staff and are less involved personally. For those in charge of operating sources, the priority remains to protect people from radioactive sources rather than to protect sources from people. Such prevalence of safety orientation makes it necessary to design and implement both safety and security measures in an integrated manner so that security measures do not compromise safety and safety measures do not compromise security.[29] Moreover, they must complement each other and be mutually supportive. (See Section 7).

2. Multiple and intermodal transport

In view of the potential vulnerability of radioactive material in transport, the design of an adequate transport security system incorporates the concept of defense, and uses a graded approach to achieve the objective of preventing the material from becoming susceptible to malicious acts. Accordingly, it is important to factor in effective security transport schedules, routing, security of passage, information security and other relevant procedures.

Security measures taken during transport of radioactive sources to protect against malicious acts should be based on evaluating the threat to the material and its potential to generate consequences. The transport of radioactive sources is usually an interim phase between production, use, storage, and disposal. The potential radiological consequences of the loss of control due to theft of radioactive sources during use, storage, or transport do not differ in principle, although the potential consequences of an act of sabotage might differ very much depending on the location of radioactive sources. The nature of radioactive source transport poses serious challenges to the implementation of physical protection systems due to the source's increased vulnerability. Each stage of a source's life cycle may require some sort of transportation either from manufacturer to user, or while being used in field operations, or from user to disposal sites. A potential adversary, especially an insider, can choose a point along transportation routes where the sources would be most vulnerable and procedures for physical protection are least effective.

[28] "Nuclear Security Recommendations on Radioactive Material and Associated Facilities," Nuclear Security Series Nº 14, IAEA, 2011, p.5.
[29] "Security of Radioactive Sources," Nuclear Security Series No.11, IAEA, 2009, p.10.

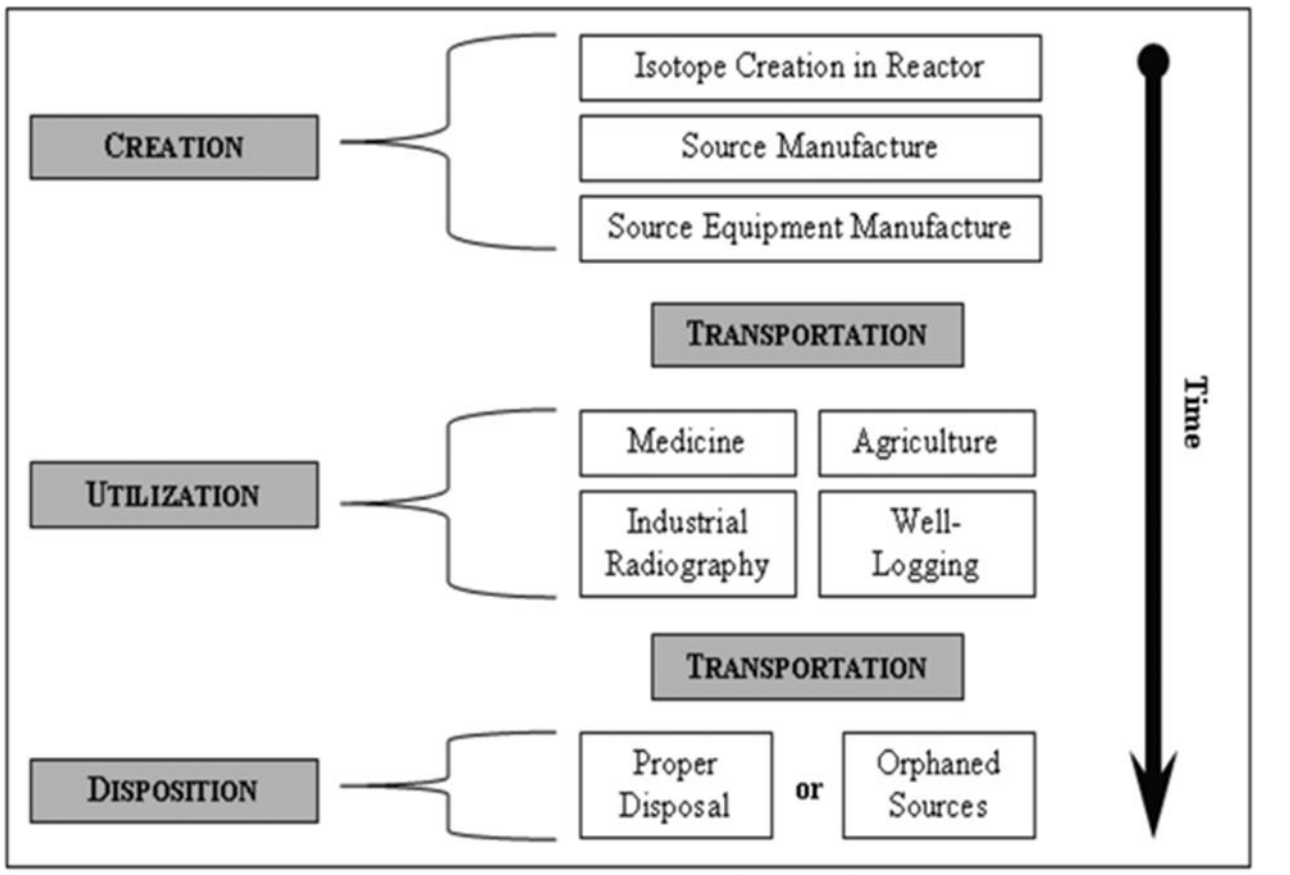

Figure 4: Radioactive Sources Life Cycle[30]

For international transport, operators should ensure in advance that any state-by-state variations in security measures are applied as the radioactive material progresses on its journey; in addition to clearly determining the point at which the responsibility for security is transferred.

3. Integration into overall security regime of host organizations

At large and diversified institutions, radiological security and culture should be blended into an overall security regime of the host organization. For example, hospitals with radiology wards have their own set of unique security and safety risks, depending on demographics, service offerings, and administrative strategy. The security of a hospital is a collaborative effort, as the security service may not be exclusively responsible for all the components of the protection program and security management plan. For example, the basic elements and environment of a hospital create many risks and challenges including:

- Healthcare is usually provided twenty-four hours per day and hospitals are easily accessible;
- Healthcare staff are predominately female and are most likely targets of violence;

[30] Fernandez, Nicolas, High-Risk Radioactive Sources: Cradle-to-Grave Physical Protection, *Journal of Nuclear Material Management*, Spring 2008, Volume XXXVI, No. 3, p. 20.

- Workplace violence is an increasing problem;
- Drugs are used and stored at the facility;
- Money is handled throughout the facility;
- Hospitals are soft targets for terrorists.[31]

4. Diverse applications

Radioactive sources are utilized across a wide range of industrial production, construction, research, medical, and other applications. The diversity of security regimes and its impact on organizational culture is much more extensive than throughout the more uniformly structured nuclear sector. For example, common users of sources include non-destructive testing, radiation sterilization of health care products, modification of polymeric materials, online process control systems, mineral resource evaluation, food irradiation and many others (See Table 4). Dispersed throughout numerous industrial units and medical institutions, security culture poses a serious challenge in efforts of formulating a uniform approach.

Table 4: Irradiation Equipment and their Application Fields[32]

	Use
Scanning	X-ray equipment is used in carrying out security checks on luggage at airports and also in verifying the quality of welds in pipelines. Other kinds of irradiation equipment are used in gauging the thickness of paper, plastic films, and metal sheets.
Agriculture	Irradiation equipment is used with the sterile insect technique, whereby male insects are irradiated and made sterile. They are then released, but have no offspring when they mate. The technique has been used successfully against the tsetse fly in Zanzibar, the Mediterranean fruit fly in Mexico, and the screwworm in North Africa and the Southern United States.
Medicine	X-ray equipment is used in, for example, dentistry, mammography, and the diagnosis of fractures. More powerful radiation is used for therapeutic purposes, such as the treatment of cancer, in which the radiation is directed at the cancerous cells to minimize the damage to healthy cells.
Sterilization and Food Preservation	Very strong radiation is used in sterilizing surgical instruments and surgical gloves, which would not withstand the temperatures involved in conventional sterilization. Certain drugs are also sterilized by means of radiation. The same technique is used in the preservation of food.

[31] Steve Nibbelink, "Hospitals Meet Security Challenges with Integrated Security and Facility Solutions," Schneider Electric, January 2012, pp.6-7.
[32] Carlton Stoiber, Alec Baer, Norbert Pelzer, WolframTonhauser. Handbook on Nuclear Law, IAEA, Vienna, 2003. pp. 60-61.

Equipment used in the above fields may have different safety and security features, as well as different safety-security interface as demonstrated by the following examples:

- *Panoramic and underwater irradiators* are generally used for commercial sterilization purposes. The two types of panoramic irradiators are dry source storage and wet source storage irradiators. The panoramic irradiator's radioactive sources are generally stored in a container constructed of solid material (e.g. concrete and lead) or in a water pool for shielding and are then brought out of the container during normal operation to sterilize products. Underwater irradiators remain in the water at all times; the product that will be irradiated is lowered into the pool to begin the sterilization process. Panoramic and underwater irradiators are self-protected during operation because the dose rate from the sources would cause incapacitation in a very short amount of time (e.g. seconds to minutes). Physical protection is required to prevent the unauthorized removal of individual pencil sources when the irradiator is not in operation.

- *Self-shielded irradiators* use radioactive sealed sources that are completely contained in a dry container constructed of solid materials (e.g. lead). As a result, they are inherently safe and can be stored in unshielded rooms. Self-shielded irradiators are typically located at hospitals, blood banks, universities, and research laboratories, and are routinely used to irradiate research samples, small animals, and blood products.

- *Fixed gauges* containing radioactive materials are used for measuring the thickness of paper, steel, or other products; the density of materials; the level of materials in vessels and tanks; and the volumetric flow rate of products in piping, vessels, or other equipment. The use of fixed gauges present security challenges given their size.

- *Teletherapy medical devices* that contain risk-significant radioactive material are generally used for killing cancerous tissue, reducing the size of as tumor, or reducing pain. A teletherapy device is an example of medical equipment that uses an intense beam of radiation from a powerful radioactive source, which is external to the patient and is focused on the cancerous tissue. A gamma stereotactic radiosurgery device (the Gamma Knife) is an example of a teletherapy device.

- Other forms of sealed sources used in various medical and industrial applications include *high dose rate remote afterloaders, well logging, fixed and portable nuclear gauges, and industrial radiography.* Manufactures and users should use a continuous physical barrier to limit access to the permanent security zone.

- *Well logging* involves lowering a logging tool that contains a sealed radioactive source into a borehole to obtain information about the properties of geological formation and identify any fluids (e.g. oil, gas, water) contained within the formation. Well logging operations generally involve the storage of radioactive sources at a field station or base camp from which they are transported and used at the well site.

5. <u>Mobile and portable operation</u>

Industrial radiography sources, a wide range of gauges and others, are routinely moved around and often located 'off-site' where traditional approaches of physical protection cannot be applied effectively. For this category of sources, a timely detection, delay and response are not easy to accomplish. Users of portable gauges are required to both maintain control and constant surveillance when in use, and at a minimum use two independent physical controls to secure them from unauthorized removal when not in use. The security procedures used must ensure that the two physical barriers implemented clearly increase the deterrence value over that of a single barrier. In addition, the two physical barriers would make unauthorized removal of the portable gauge more difficult. The difficulty in controlling the use of traditional methods amplifies the importance of human reliability, vigilance, and improvisation as key traits of security culture. The mobile and portable modes of operation impose a burden on users of radioactive sources to continuously improve security arrangements in coordination with local law enforcement personnel across the country. One such compensatory measure is establishing a communication link to allow response to incidents. In many countries, save large urban centers, local law enforcement is often inadequately trained to respond to radiological emergencies.

6. Limited resources and awareness

In some countries, financial, technical, and human resources are still lacking efforts to address the risk of diversion of radioactive material and its malicious use. Most of these countries do not have an established nuclear power infrastructure which, given its scale and significance for the national economy, often serves as a source of advanced security methodology and good practices to share with users of radioactive sources. The absence of factual evidence to demonstrate the risk of radioactive material being used for malicious purposes has precipitated a sense of complacency among users of radioactive sources and regulatory authorities. In addition, trained and armed professional guards who must protect the site 24 hours a day are expensive. Security equipment and hardware, including intrusion detection and assessment systems, are costly to install and maintain.

7. Disposal challenges

End-of-life source management is challenging due to a lack of uniformity in practices and regulation. Options open to users include a return to manufacturers, recycling or disposal, and storage. However, financial and other constraints frequently prevent them from following these procedures in a consistent manner. For example, the cost of returns to manufacturer or for disposal are difficult to predict into the future to a time when the sources may become disused and be either prohibitively expensive or greatly underestimated. Efforts are made to request source owners to develop plans for disposal prior to import and implement such plans when the sources become disused. However, the issue of financial provisions to support such plans continues to be poorly planned and implemented. As a result, some disused sources become vulnerable to weak regulatory control and may fall into the category of "orphan sources," meaning those not under such control after being abandoned, misplaced, lost, stolen, or transferred without appropriate authorization.

8. Security culture model for radioactive sources

The security culture model proposed in this report for radioactive sources (see Figure 5 and Appendix A) cannot be an exact replica of the IAEA model described in the 2008 Implementing Guide.[33] Based on the same organizational culture approach, the proposed model, its characteristics and indicators must reflect features specific to the operation of radioactive sources. The underlying principles promote and support the security regime by:

- Raising security awareness among staff members of the entire organization while building an effective security culture for individuals who are managing and operating radioactive sources, or are otherwise professionally associated with their use;
- Providing the organization with the means to support individuals and teams in successfully performing security related tasks, taking into account the interaction between individuals, technology, and management;
- Ensuring a common understanding of the key aspects of security culture within the organization;
- Reinforcing a learning and questioning attitude at all levels of the organization; and
- Providing the organization with the means to develop and improve its security culture as well as make it sustainable.

9. Beliefs and attitudes as drivers of people's behavior

Without a strong substructure of beliefs and attitudes about threats, an effective security culture cannot exist. Efforts to instill such beliefs and attitudes must be carefully calibrated to reach everyone working in the facility. The most important assumption for security culture is that there is a credible insider and outsider threat. Cognizance that a radiological event could have devastating health, environmental, economic, social, and psychological impacts is likely to reinforce the belief that a robust security regime is not only desirable but also necessary. Since most people within an organization will often have many shared experiences, they will also hold the same unconscious assumptions of vulnerability, which will spread and permeate throughout the entire workforce, rather than the organization's security specialists alone.

10. Leadership behavior as role models

Managerial behavior and proactive security leadership help improve awareness and culture at all levels. Leaders are vital components in dealing with malicious capabilities, unintentional personnel errors, inadequate organizational procedures, and management failures. They are in a position to integrate the security regime for radioactive sources into organization's overall security arrangements. Leaders can promote new and different assumptions and patterns of thinking, establish new patterns of behavior, and they can change the physical environment, the mentality, and the guiding principles. Culture, therefore, tends to mirror the real intentions, specific actions, and priorities of the management. Given the diversity of radioactive source users, management includes the individual or groups of people who direct, control, and appraise the organization. It can include the

[33] "Nuclear Security Culture," Nuclear Security Series No 7, IAEA, 2008.

chief executive officer (CEO), director general, executive team, plant manager, top manager, managing director, laboratory director, and supervisor.

Managers develop individual values, institutional values, and behavioral expectations for the organization to support the implementation of the security management system, and act as role models in the promulgation of these values and expectations. Characteristics of management behavior include explicitly demonstrated expectations; effective decision-making process and management oversight; involvement of staff and feedback; effective communication; and motivational tools. Each characteristic is supported and illustrated by associated culture indicators, which are listed in Appendix A.

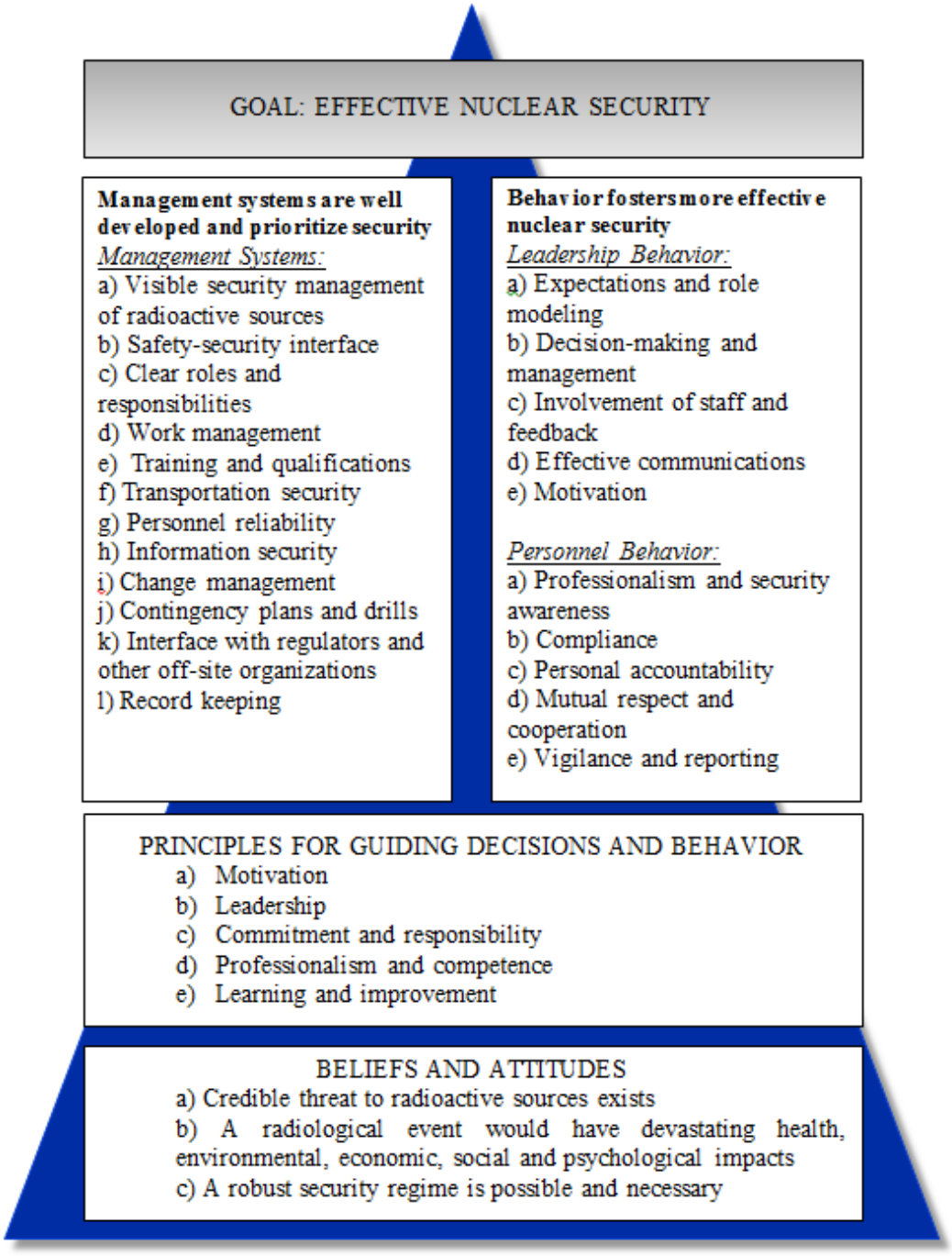

Figure 5: Security Culture Model for Radioactive Sources

11. Management systems as tools to promote desired patterns of behavior

The management systems integrate characteristics that either relate directly to the security of radioactive sources or are part of the managerial framework, without which security cannot be ensured and maintained. They are designed and shaped by senior management consistent with their vision of an effective security culture and the need for appropriate management tools to facilitate and support this process. At the same time, management systems ensure that health, environment, safety, quality and economic requirements are not considered separately from security requirements to help preclude their possible negative impact on security. Characteristics of management systems include: visible and effective security policy; the safety-security interface; clear definition of roles and responsibilities; trustworthiness determination; training and qualifications; information security; change management; contingency plans and drills; interface with regulations and other off-site organizations; and record keeping. Each characteristic is supported and illustrated by associated culture indicators, which are listed in Appendix A.

12. Personnel behavior as key to robust and sustainable security

The ultimate objective of security culture development is a set of desired standards of personnel behavior. Security awareness and culture are driven by personnel beliefs that security is necessary to avoid malicious radiological events, which may have devastating health, environmental, economic, social, and psychological effects. While security awareness is a low-tier construct applicable to the entire workforce, more rigorous efforts must concentrate on a high-tier culture construct that targets individuals who manage and operate radioactive sources as well as those professionally associated with their use. There are many overlaps between awareness and culture, and they are often used interchangeably, but the latter implies commitment and ownership rather than being aware of possible risks and vulnerabilities. Culture is a more proactive construct than awareness. The behavior of security culture conscious personnel includes the following characteristics: professionalism and security awareness, compliance, personal accountability, mutual respect and cooperation, and vigilance and reporting. Each characteristic is supported and illustrated by associated culture indicators, which are listed in Appendix A.

Though not a panacea, the Security Culture Model for Radioactive Sources can enhance the security regime and contribute to its major objectives throughout the entire life cycle of radioactive sources, i.e. from cradle-to-grave. Whilst a security regime for radioactive sources is traditionally built on existing radiation regulatory and safety measures, there are factors in the use, storage, and transport of radioactive sources that make security distinctly different and challenging. In addressing these challenges, an integrated approach is required to ensure that all responsible organizations have adequate and compatible security culture to establish, strengthen, implement, and sustain security regimes for radioactive sources from their production to disposition.

9. Differentiated Approach toward Awareness and Culture

Special security requirements for radioactive sources discussed above may justify a more differentiated approach toward security culture. More frequent and intense efforts are expected to focus on a select group, which has a direct or indirect relationship with radioactive sources (management teams, security personnel,

operations, technicians, and others). The determination of the dividing line between this group and the rest of the workforce outside radioactive source operations is up to the organization's leadership.

Security awareness development is applicable to all employees as a core value. However, given limited resources, it would be reasonable to place more emphasis on the security commitments as well as evaluation and enhancement for a more limited group. In other words, this is a targeted approach and makes time and resource investment in training and culture development commensurate with the roles and responsibilities of individuals.

Awareness raising is a common foundation for across-the-board effective security throughout organizations that handle radioactive sources. All staff members are expected to have shared beliefs and attitudes that (a) a credible threat to radioactive sources exists; (b) a radiological event would have devastating health, environmental, economic, social, and psychological impacts; and (c) a robust security regime is desirable and necessary.

The goal is to develop an awareness of possible risks, danger, or threats to the security and safety of radioactive sources that will be translated, when and if necessary, into support for actions, which would address those risks and threats. The emphasis is on performance and behavior because security awareness raising is not simply about enhancing understanding or imparting risk-based information, but preferably empowering people to act at appropriate times and in appropriate ways commensurate with their roles and responsibilities. All employees must be informed about how to recognize indicators of danger and react accordingly. Moreover, they must be guided to do the right thing, at the right time, once they recognize such situations.

In selecting models and tools for security awareness raising, it is useful to consider the following:

- budget and resource limitations often limit choices;
- Security performance objectives and the volume of expected information must be clearly formulated;
- The characteristics of the target audience (in terms of its size, educational background, and familiarity with radioactive sources) should be taken into account.

Topics covered during security awareness sessions should explain (1) why radioactive sources may be targeted and by whom; (2) how adversaries including insiders can endanger them; (3) their motivation and possible consequences of their actions; (4) the limitations of security regimes and concurrent vulnerabilities; and (5) what can be done to prevent their loss or damage. Emergency drills and exercises would complement, if possible, these sessions.

The proposed Security Culture Model with its characteristics and culture indicators provides guidance for the differentiated process of security awareness and culture enhancement through several stages until reaching the security commitment, i.e. ownership stage. The model outlines the elements of an effective security culture as the ultimate goal based on proactive skills and practices enabling personnel to address threats by taking appropriate actions and setting an example for others to follow. Ideally, all personnel must reach the commitment stage, but this may often be a challenge given special operational and structural features of radioactive source users. Hence, while applying these principles as much as possible to the entire workforce,

emphasis and priority is accorded to a group of managers and staff with roles and responsibilities associated with the operation, transport, and storage of radioactive sources.

As Figure 6 below shows, there are four stages to raising security awareness on the way to an effective security culture:

- ***Education*** provides staff members with an understanding of the rationale, basic principles, and mechanisms of the security regime for radioactive sources.
- ***Training*** produces skills, knowledge, and information enabling staff to perform their security-related roles and responsibilities.
- ***Awareness*** allows staff members to recognize threats, their resultant implications, and their capacity to address them.
- ***Commitment*** when staff members (a) understand why security is necessary and what it means (*education*), (b) know how to perform their security-related roles (*training*) and (c) are able to combine, if necessary, their knowledge and skills to address both specified and unexpected threats. Security-conscious people are motivated to contribute to an effective security. This is the stage when the organization can claim to have an effective security culture among its relevant personnel.

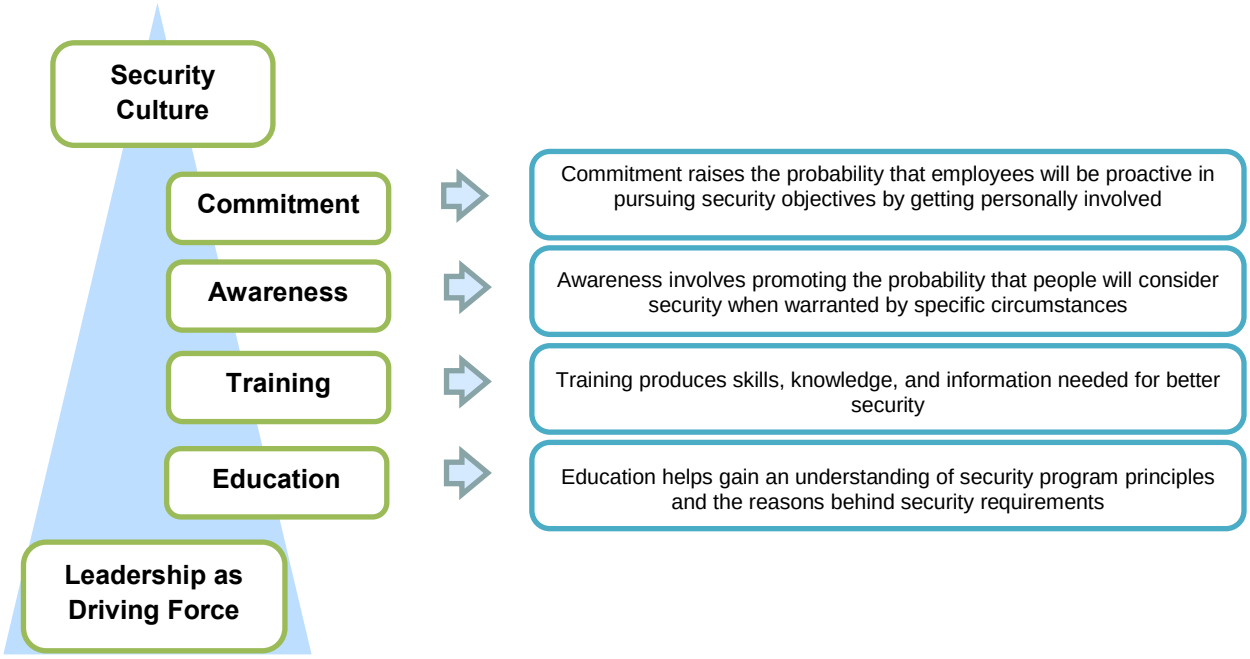

Figure 6: The Road to Security Culture

A security culture development program has the following three goals:

- Increase understanding by relevant personnel of the importance of security, the nature and immediacy of the threats, and their personal accountability for security.

- Improve manager performance, both in terms of enhancing security effectiveness and contributing to a strong security culture.

- Establish an organizational policy and structure that create the basis of a strong security culture and support sustainability of the radiological security program. Culture indicators assigned to each characteristic of the Model (see Figure 5) are designed to maintain the adequate level of security culture and ensure it sustainability.

The ability to assess the status of security culture is a prerequisite of its successful business development and maintenance. Applying assessment methodology requires a multidisciplinary approach since culture is composed of intangible human traits such as beliefs, values, and ethics, which are acquired and internalized differently by each individual.

10. Evaluating and Enhancing

Security awareness and culture assessments play a key role in developing and maintaining an awareness of the strengths and weaknesses in protective systems. The purpose of a security culture assessment is to provide a clear picture of the influence of the human factor on an organization's security regime. Charting trends over time can provide the management an early warning to investigate the causes of most problems revealed, thereby reinforcing sustainability. A prerequisite for successful assessment is ensuring confidentiality in its participants throughout its entire process.

There are at least three options for evaluating security awareness and culture: (1) basic, (2) intermediate, (3) comprehensive. Their selection depends on many factors and circumstances including risk estimates, the size of the organization and workforce, and the records of previous security incidents or near misses.

Basic This method is based on statistical methods and information derived mostly from document review, observations, and other sources. Basic indicators focus on:

1. Percentage of security incidents or near misses during previous quarter or year compared to previous periods;
2. Percentage of employees who have received security refresher training during the previous quarter or year;
3. Percentage of security improvement proposals submitted, considered, or implemented during the previous quarter or year;
4. Percentage of employee communication briefs that included security information;
5. Number of security inspections conducted by senior managers, managers, or supervisors during the previous quarter or year;

6. Number of employee suggestions relating to security improvements during the previous quarter or year; and
7. Percentage of routine organizational meetings with security as an agenda item.

While this audit-type assessment will not provide any insights into the drivers of personnel behavior, it may send a signal about potentially negative trends in the evolution of the security regime and the need to take corrective action including the launch of a more in-depth assessment.

Intermediate This type of assessment is based on managers' own "yes" or "no" judgment regarding the evolving structure and functionality of the security component of the organization's management systems. Being non-interactive, these security management indexes have limited utility but can pinpoint the functional areas where major deficiencies or gaps are most likely to exist as a result of inadequate human performance. Compared to basic, the intermediate approach can stimulate managers' further consideration of specific problems and justify a more comprehensive method. Such security management indexes requiring a "yes" or "no" response include:

1. A security policy is established and posted;
2. Processes are in place to identify the mandatory requirements relating to security;
3. Regularly held management meetings cover significant security items;
4. Professional rewards or recognition is associated with the achievement of security goals;
5. Roles and responsibilities for all security positions are clearly defined in relevant documents;
6. Security related performance results are compared to targets and regularly communicated to staff;
7. Feedback from staff is requested and analyzed;
8. Periodic evaluation of security training programs is conducted and revisions incorporated;
9. Contingency plans are established to address unforeseeable events;
10. Processes and protocols exist for handling sensitive information;
11. Checklists/detailed procedures for maintenance of security systems exist;
12. Training is provided to guide appropriate personnel in identifying high-risk behavioral symptoms;
13. An insider threat mitigation program is in place;
14. Management processes are in place for changes that could affect the security function;
15. Contingency plans are in place; and
16. Management level communication with local and national organizations involved in nuclear security is regularly performed.

An alternative to this method would be for a management team to review culture indicators in Appendix A and self-reflect on the state of security to identify human-factor-related gaps. A quick look, however, would not preclude a more labor-intensive assessment should it become necessary to check whether the original diagnosis was correct, if the measures adopted by the management really worked, and if the organization is on the right track.

Comprehensive This is a multi-stage process comprising of both non-interactive and interactive assessment tools focusing on management and behavior characteristics of the Radiological Security Culture Model. These

characteristics are evaluated by comparing where the culture is at present to their optimal parameters specified by culture indicators assigned to each characteristic as benchmarks (See Appendix A for the list of characteristics and assigned culture indicators). Due to the heavy focus on perceptions, views, and behavior, regularly held comprehensive assessments help to understand the rationale of an organization's patterns of behavior in certain circumstances, devise optimal security arrangement, and predict how the workforce may react to a wide range of risks. Due to the cost and the time required for a comprehensive assessment, it may be reasonable, however, to limit them to those individuals in the organization who are directly or indirectly associated with radioactive sources.

An important initial step is drafting an assessment plan, paying due attention to the need to minimize the cost and avoid organizational disruptions. Methods to be included in the plan are broken into two categories: 1) non-interactive methods (surveys, document review, and observations) and 2) interactive methods (individual interviews and focus-group discussions). As all of these methods have their strengths and weaknesses, a reasonable approach would be to combine a non-interactive method with an interactive method; for example, an organization can carry out a survey followed by a set of onsite interviews to fill out possible gaps and clarify ambiguities. However, other options are possible but the choice would be made at the management's discretion.

Surveys are important to self-assessment because they establish a baseline for tracking changes over time. Survey statements are derived from culture indicators but must be shortened and personalized to facilitate responses (see Appendix B for samples of survey statements). It is up to the management to determine the scoring scheme for the survey. The present report suggests a scoring system employing a 7-point scale from 1 ("Strongly Disagree") to 7 ("Strongly Agree"). This scheme indicates that a particular indicator is either fully observed or present, completely unobserved and absent, or somewhere in between. Respondents to a survey are requested to offer comments if they have something else to say.

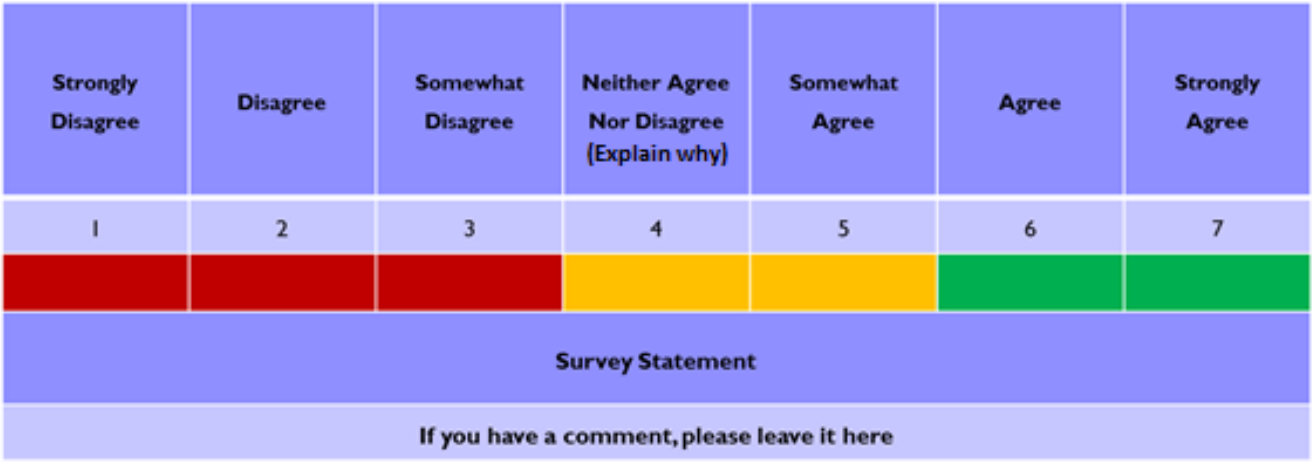

Figure 7: Example of Survey Format

To calculate the results of the survey for each statement, all scores should be summed up and divided by the number of respondents to formulate an average. A color-coded scheme based on the average score is

recommended for better visibility and follow-up analysis. If the score is in the 1 to 3-point segment (red), it is a sign of weakness. If it is within the 4 and 5-point segment (yellow), then there are grounds for concern because the status quo falls short of the standards outlined in the survey statement. The 6 and 7-point segment (green) signify strengths that should be preserved and reinforced to keep up the momentum. For example, if the total is 135 and the number of respondents is 30, the average score would be 4.5 (yellow). As a recommendation, survey results would be easier to manage, analyze, and store for future use if the averaging for each statement were graphically represented in the form of histograms.

Once red, yellow, and green ratings have been assigned, the next step is to develop subgroups within each color code, or across the color codes, based on convergent or conflicting views among respondents. Each subgroup demands special scrutiny regardless of whether they represent predominantly negative, positive, or conflicting views across the color codes. The latter sends a message that the workforce is split on an important issue of security. As evaluators identify convergent or conflicting views, through efforts such as tapping comments from respondents, they formulate themes to further explore based on the qualitative data from interviews.

Interviews play a significant role in cultural assessment because they allow for flexible questioning and follow-up clarifications from the interviewees. This eases the task of getting at the deeper tenets of an organization's culture. Interviewees who need to be carefully selected by their experience, work positions, and skills, can give specific examples of past practices that they have experienced, and even supply explanations that would provide insight into people's beliefs and attitudes.

It generally benefits interviewers to prepare an informal "interview guide" listing groupings of topics and sample questions derived from survey results and other additional sources that can ask the questions in different ways for different participants. This helps the interviewer focus on the topic at hand while tailoring questions to meet the assessment goals.

Training and briefings for interviewers should ensure that they behave respectfully while showing empathy and open-mindedness for the interviewee. A major challenge during interviews is establishing trust and providing credible assurances of anonymity. Efficient note taking is a vital skill for each interviewer to master before launching the assessment campaign.

Compared to individual face-to-face interviews, focus-group sessions create an advantage in which the interactions within the group often prompt and sustain discussions with minimal input from the interviewer. Group members share a short description of their experiences, views and attitudes about the topic in question, eliciting responses from one another. The interviewer's role is to facilitate discussion while recording key points that emerge from the discussion.

Document reviews and observations can take place prior to assessment to familiarize evaluators with past security incidents, their root causes, and corrective measures taken, or used as a tool during the process of assessment. Document review can supply insight into how management sets its priorities and how it intends for its policies, programs, and processes to operate in practice. Combined with surveys and interviews, a document review helps evaluators appraise differences between stated policies and procedures and actual behavior. A document review is, however, a labor-intensive process with administrative implications due to the sensitive nature of some documents.

The purpose of conducting observations is to record actual performance and behavior in real time and under different circumstances, especially at general meetings, training sessions and emergency drills. Observations are a well-established, time-tested, commonplace tool for managing security if they were conducted and are available. To provide relevant input into a cultural analysis, evaluators need access to records of recent observations. Previously recorded observations are often more reliable than observations conducted in the midst of a well-publicized assessment campaign when staff members are aware of the program and its purpose.

Observational information comes mainly from observational notes. The effective use of observations depends on the ability of team members to develop notes as well as analyze and store them. Following each observation event, data collectors need to expand their notes into rich descriptions of what they have observed.

The analysis stage is critical for comparing and integrating the quantitative and qualitative findings of assessment tools. Without conducting an analysis, evaluators are at risk of merely reporting what they have learned and presenting a factual summary. Assessment starts as a fact-based process but must go well beyond the facts. The significant value that evaluators can bring is their interpretation of the findings, their analysis of underlying root causes, and their informed opinion about what problems might exist and what should be done. Upon receipt of the assessment report, senior managers should expect to be able to draw upon the insight of evaluators in efforts to address identified cultural deficiencies. Assessment reports may focus on specific security culture related problems in the organization such as overconfidence and complacency, poorly organized vertical lines of communication, lack of a systemic approach toward security risks, excessive dependence on security technology while underestimating people's input, apathy or ignorance toward security, or indifference to the experience of others. Assessment reports serve as a basis for senior managers to develop and implement corrective action plans.

11. Conclusion

This report highlights the major role radioactive sources play in industry and health care. Due to their variety and numerous potential applications, they have security features distinct from generic approaches applicable to nuclear infrastructure. The importance of effective life cycle management from cradle to grave is imperative to the safety and security of radioactive sources. In this context, the human dimension of their security, i.e. radiological security culture, can provide much needed multidisciplinary cooperation in the face of expected and unexpected risks.

The use of radioactive sources is spreading globally. There are signs that more sources will soon operate in areas characterized by a lack of stability, inadequate operational experience, and low security priority. The global Radiation Therapy Equipment market is forecast to total US $8.7 billion by 2022, driven by the epidemic spread of cancer across the world, growing preference for non-surgical cancer treatment options, and increased R&D focus on cost effective cancer treatment equipment.[34] The need to expand the use of radioactive sources across continents is a matter of urgency. For example, an estimated 198 million people live in 29 African countries that lack any teletherapy treatment.

[34] "Radiation Therapy Equipment: A Research Brief." Global Industry Analysts Inc., March 2017.

There is a significant link between the expanding use of radioactive sources and global development of health care capacities. According to a recent analysis on the future needs for radiotherapy in low and middle-income countries (LMIC), more than 50 percent of patients requiring radiotherapy in LMIC do not have access to treatment. The situation is more devastating in low-income countries, where the proportion of patients needing therapy is higher than 90 percent.[35] Demand for more radiation-based technologies is expected in industry, agriculture, and research as part of the globalized economy. Such technologies are becoming widely used as state-of-the-art tools in laboratories to provide needed information without destroying the sample, improve analysis results, achieve optimal cost effectiveness, and promote rapid data acquisition.

Against the background of these developments and trends, a cultural approach to the protection of high-risk radioactive sources is becoming indispensable. In this context, however, seldom will a security culture self-assessment yield clear-cut or easily actionable results. Instead, it helps move the organization along its learning curve by determining what attitudes and beliefs need to be established in an organization, how these attitudes and beliefs manifest themselves in the behavior of assigned personnel, and how desirable attitudes and beliefs can be transcribed into formal working methods. In this sense, assessment of security culture should complement the currently used evaluation methodology for gauging vulnerability and physical protection, thus helping refine the overall security arrangements for radioactive sources.

[35] Zubizarreta EH, Fidarova E, Healy B, et al: Need for radiotherapy in low and middle-income countries—the silent crisis continues. Clin Oncol 27:107-114, 2015.

Appendix A: Security Culture Indicators for Users of Radioactive Sources

The objective of this Appendix is to illustrate the characteristics of security culture at facilities where high-risk radioactive sources are present by using culture indicators as benchmarks for actual characteristic performance. The Appendix groups indicators around the relevant characteristics of the Security Culture Model. Some of them are generic by nature and should be treated as illustrations that can help each organization tailor a self-assessment project to its own needs. Asking whether the development of additional indicators reflects the profile and activities of the organization is of particular importance. As most characteristics overlap, so do some of their indicators.

Leadership Behavior

a) Expectations and Role-Modeling

Leaders must establish performance expectations for the security of radioactive sources to guide staff in carrying out their responsibilities as well as act as the role model.

Culture Indicators:

Senior management develops individual values, institutional values, and behavioral expectations regarding the security of radioactive sources to support the implementation of management systems and act as a role model in the promulgation of these values and expectations.

Senior management ensures that resources are readily available to guarantee effective security of radioactive sources.

Management recognizes and addresses the challenges in security requirements regarding the use, storage, and transport of radioactive sources.

Senior management demonstrates a sense of urgency to correct significant security weaknesses or vulnerabilities.

Senior management personally inspects the performance in the field by conducting walk-arounds, listening to staff and observing work being conducted, and then taking action to correct deficiencies.

Senior management provides on-going reviews of performance as well as appraises roles and responsibilities to reinforce expectations and ensure that key security responsibilities are being met.

Management has a system of rewards for new, innovative ideas, to improve the security of radioactive sources.

b) Decision Making and Management Oversight

The process through which an organization makes decisions is an important part of security culture. Adherence to formal and inclusive decision-making processes demonstrate to staff the significance that management places on security decisions, and improves the quality of decisions. Management oversight is required to support security-related decisions and make them sustainable.

Culture Indicators:

Management explains, as appropriate, the necessity and significance of each decision regarding the security of radioactive sources.

Senior management develops the goals, strategies, and plans in an integrated manner so that all personnel understand their collective impact on the security of radioactive sources.

Management ensures that a security-conscious environment permeates throughout the organization, involving both security and non-security personnel.

Design Basis Threat methodology is used, where

applicable, as a method to design a security system for the protection of radioactive sources.

Management determines the cause of security breaches and near misses and takes remedial actions to prevent their recurrence.

Depending on the categorization of radioactive sources in use and the underlying potential risks, management allocates adequate resources for the security of radioactive sources.

Management takes diverse actions to avoid complacency among personnel and continuously challenges existing conditions to identify discrepancies that might endanger the security of the radioactive sources.

Management plans, executes, and evaluates periodic security exercises to ensure the security of the radioactive sources and supervises its use.

Management allocates sufficient resources to provide a secure environment for the radioactive sources.

Managers ensure that when sources are not in use they are promptly stored in an approved manner as required for the category to which they belong.

c) Involvement of Staff and Their Feedback

Management encourages staff members to raise security concerns without fear of retaliation, intimidation, harassment, or discrimination. The value of feedback and its use must be clearly demonstrated to the entire workforce.

Culture Indicators:

Staff members, contractors, and facility clients are encouraged to make suggestions for improving security and are properly recognized for their contributions.

Staff members and contractors are involved, as appropriate, in the identification, planning, and improvement of security-related work and work practices.

Senior management supports and promotes mechanisms, which staff members and contractors can use to contribute their insights and ideas on how to address security-related problems.

There is a system of rewards for new, innovative, and effective security improvement suggestions.

Plans are in place to handle labor disputes without an unacceptable impact on the security of radioactive sources.

Staff and contractors report any problem in confidence because they know that questioning attitudes is encouraged.

d) Effective Communication

An important part of an effective security culture is to encourage and maintain the flow of information, both upward and downward within the organization.

Culture Indicators:

Management welcomes input from staff members and contractors and takes action, or explains why no action was taken.

Management keeps staff members and contractors informed on policy issues and organizational changes regarding security.

The management evaluates the results of the security culture self-assessment regarding radioactive sources and reasons for them are communicated to staff members and contractors.

Senior managers communicate their vision of the status of security, consistently, and in a variety of ways.

The system of communication is regularly tested to ensure that messages are being both received and understood by the workforce at all levels.

Processes are in place to ensure that the experience of senior staff is shared with new and junior staff members and contractors at the organization.

e) Motivation

The satisfactory behavior of individuals depends upon their motivation and attitude. Both personal and group motivational systems are important in improving the effectiveness of security.

Culture Indicators:

Managers encourage, recognize, and reward commendable attitudes and behavior that lead to security improvements.

Reward and promotion systems are in place to recognize staff members and contractors' contributions toward improving security.

Rewards and sanctions relating to radioactive source security are known to the entire workforce.

The principles used to reward good performance in security mirror those used to reward good performance in safety and operations.

When applying disciplinary measures in the event of violations, the sanctions for self-reported violations are tempered to encourage the reporting of future infractions.

Senior management has taken action to make career paths in security management career enhancing.

Management Systems

a) Visible Security Management of Radioactive Sources

An organization needs a radioactive source management, which states the security commitment in managing radioactive sources. The plan should describe the overall system in place and include measures to address an increased risk level, respond to relevant events, and protect sensitive information. This document should establish the highest expectations for decision-making and conduct and be supported by an atmosphere of professionalism and teamwork.

Culture Indicators:

A security plan for radioactive sources, which describes the overall system in place, is implemented and its content is shared with staff on a need-to-know basis.

The implementation of security plans is regularly reviewed against the evolving risk environment and actions are taken where necessary to address deviations from the plans.

The management's actions to secure radioactive sources have respected status within the organization as a whole.

Procedures are in place to detect human errors, which may jeopardize security management, as well as to correct or compensate for them.

Security plans for radioactive sources define how technical and administrative measures are implemented to counter insider threat.

Effective control procedures are established for relevant categories of radioactive sources to track and document the inventory, its use, transfer and disposition.

An appropriate waste management policy for radioactive materials is established and explained to all staff.

A security plan for the transport of radioactive material is developed, adopted, implemented and periodically reviewed as necessary.

Procedures are in place for the security personnel to obtain relevant information about the sources handled in the facility and provide the necessary advice, guidance and co-operation in devising and implementing the security plan.

b) Safety-Security Interface

Safety and security culture share many common elements and both serve to protect radioactive sources with the ultimate aim of protecting people,

society, and the environment. There are also challenges in their promotion, management, and coordination related to differences in approach and risk perception. This means that an optimal decision-making process requires an integrated concept that ensures the involvement of experts in each discipline on a continuous basis. Safety and security culture issues should be promoted and evaluated on mutually supporting and reinforcing terms.

Culture Indicators:

Policies and procedures are established that identify both the safety and the security of radioactive sources as being a high priority.

Problems concerning the safety and the security of radioactive sources are promptly identified and corrected in a manner consistent with their importance and with due regard for their similarities and differences.

Organizational arrangements and communication links are established that result in an appropriate flow of information discussing the safety and the security of radioactive sources at various management and staff levels as well as between them.

Major decisions regarding safety and security are taken with the participation of experts on safety and security on a continuous basis.

Effective security measures are ensured, when appropriate, by complementing existing safety measures with additional security measures identified through a specific vulnerability assessment.

c) Clear Roles and Responsibilities

Members of all organizations need a clear understanding of "who is responsible for what" in order to achieve the desired results. A significant part of establishing an effective security management of radioactive sources is the clear definition of roles and responsibilities. It is particularly important to review and update this system when organizational change is being planned and executed.

Culture Indicators:

The organization has clearly defined and documented roles and responsibilities for all security-related positions.

Staff members and contractors understand potential security threats to radioactive sources well enough to accept their roles and responsibilities.

Staff members and contractors know why they are assigned security-related functions, how these functions fit into a broader picture, and what impact their noncompliance may have on the organization.

Staff members and contractors understand their roles and responsibilities for the security of radioactive sources and are encouraged to seek clarification when necessary.

Document users are aware of and use appropriate, correct, and updated documents.

Measurable objectives for implementing the security-related goals, strategies, and plans are established through appropriate processes throughout the organization.

The responsibilities of each individual for security are clearly identified and each individual is suitably trained, qualified and determined to be trustworthy.

The description of roles and responsibilities state who has overall responsibility for maintenance and who has the authority to conduct each particular type of maintenance.

d) Work Management

All security related work must be suitably planned and managed to ensure that radiological source management is not compromised.

Culture Indicators:

The approach to risk assessment and management is defined with respect to its scope, nature and timing so that it is proactive rather than reactive.

Management activities regarding security of radioactive sources are integrated into the overall policies and administrative procedures of the facility.

Processes are in place to identify new and changed laws, regulations, codes and other compliance obligations to ensure ongoing compliance.

Measurable objectives for implementing the radiological source management-related goals, strategies, and plans are established through appropriate processes.

Resources are allocated to establishing, developing, implementing, evaluating, maintaining and improving a robust compliance culture through awareness-raising activities and training.

Provisions describing security management also address procedures and training for visitors, contractors, and suppliers.

Maintenance programs include the capacity to rapidly repair operational or other vital systems and to rapidly replace parts that have been damaged.

An accurate and up-to-date radioactive source inventory is established and maintained.

Documented procedures to define, record, analyze and learn from accidents and incidents involving radioactive sources are established and maintained.
Periodic accounting for each radioactive source (as prescribed by the regulatory body) uses such methods as a physical check, remote video monitoring, examination of seals or other tamper-indicating devices, or radiation measurements.

e) Trustworthiness Determination

Any security barrier or procedure can be defeated with insider cooperation. Therefore, effective processes for the determination of trustworthiness and for mitigation of an insider threat must be in place, especially for users operating the radioactive sources at sites open to outside visitors and the public, e.g. hospitals' radiology units. The formal process should serve to assist in reducing the risk of authorized personnel engaging in illegal activities. Relevant elements of the security culture are important for the trustworthiness program.

Culture Indicators:

Measures are taken to determine the trustworthiness of individuals involved in the operation, maintenance and management of radioactive sources.

Trustworthiness measures are based on a graded approach and range from confirmation of identity to a comprehensive background carried out by a legitimate national authority, including the verification of references, as required by states' national practice.

Appropriate background checks and psychological examinations of staff members and contractors are regularly performed by certified or reputable institutions.

Persons whose trustworthiness has not been determined are escorted by, or kept under continuous surveillance of, a person who is authorized and qualified to perform such escort services.

Staff members and contractors are aware of and understand the importance of trustworthiness determination.
Training is provided to management and other appropriate personnel to guide them in identifying apparent high-risk behavioral symptoms and in applying other observational and analytical skills.

f) Training and Qualifications

An effective security culture depends upon staff having the necessary knowledge and skills to

perform their functions to the desired standards. International standards, i.e. the Code of Conduct for the Safety and Security of Radioactive Sources and relevant IAEA documents as well as domestic regulations must be adequately covered by the training program. A systematic approach to training and qualifications is required for an effective security culture at the user facility.

Culture Indicators:

A security-training program exists with requirements and qualification standards established, documented, and communicated to the personnel.

Participation in security training is given a high priority and is not disrupted by non-urgent activities.

Training ensures that individuals are aware of the relevance and importance of their security-related activities and of how their activities contribute to the overall security of radioactive sources.

All security personnel are appropriately trained and qualified so that they understand their security responsibilities for radioactive sources and can perform their duties with appropriate judgment according to defined procedures.

Security related training programs are routinely evaluated and updated as necessary.

Leadership skills and best practices in security are included in training programs for managers and supervisors.

Systems are in place to ensure that procedures and practices learned in training are applied in practice.

All relevant personnel are trained in procedures for information security.

Personnel outside of the security function are trained in appropriate security procedures.

Individuals engaged in the transport of radioactive material receive training including training in the elements of security awareness, commensurate with their responsibilities in implementing security plans.

g) Transportation Security

Radioactive sources are vulnerable in transport. Therefore, it is important to factor in effective security, transport schedules, routing, security of passage, information security and other relevant procedures.

Cultural Indicators:

An adequate transport security system is in place, which incorporates the concept of defense in depth and uses a graded approach.

The transport security system includes measures that are required to deter, detect, and delay unauthorized access to radiological material while in transport and during storage in transit.

Effective security in transit is achieved by considering transport schedules, routing, security of passage, information security and procedures.

The total time that radioactive material is in transport, the number of intermodal transfers and the waiting times associated with the intermodal transfer are kept to the minimum.

Procedures are in place to control the procurement of items and services used for the transport of radioactive material that may directly or indirectly affect the safety and security of such transport.

h) Personnel reliability determination

Any barrier or procedure can be defeated with insider action. Therefore, effective processes for the determination of reliability and for mitigation of insider threat must be in place at sites, particularly those open to outside visitors and the public. The formal process should serve to assist in reducing the risk of authorized personnel engaging in illegal

activities. Relevant elements of the security are important for the reliability.

Culture Indicators:

Measures are taken to determine the reliability of individuals involved in the use, storage, and management of radioactive sources.

Reliability measures are based on a graded approach and range from confirmation of identity to a comprehensive background check by the legitimate national authority, including a verification of references, as required by the states' national practice.

Appropriate background checks and psychological examinations of staff members are regularly performed by certified or reputable institutions or individuals.

Staff members are aware and understand the importance of reliability determination.

Training is provided to management and other appropriate personnel to guide them in identifying apparent high-risk behavioral symptoms and in applying other observational and analytical skills.

Measures and procedures are in place to ensue reliability of personnel is regularly validated.

i) Information Security

Controlling access to sensitive information is a vital part of the security function. Accordingly, the organization must implement classification and control measures for protecting sensitive information.

Culture Indicators:

An information and computer security function is established, funded, staffed, and visible.
Access to information assets is restricted to those who need such access to perform their duties, have the necessary authority, and have been subjected to a trustworthiness check commensurate to the sensitivity of the asset.

Staff members and contractors are aware of and understand the importance of adhering to the controls on information.

Management is fully committed to and supportive of computer-security initiatives.

Records of radioactive sources inventories and accountings are protected at a security level consistent with the sources covered.

Internet access is controlled and protected while recognizing the inherent vulnerability of this medium.

Measures are taken to ensure the security of transport information is contained in the security plan.

The "need to know" principle is adopted in the dissemination of information that has to be controlled.

j) Change Management

Many security problems arise from inadequate handling of operation change, which may involve unexpected field and off-site operations or handling disused radioactive sources. Therefore, the organization should have effective processes in place to understand, place, implement, and reinforce compensatory changes as they apply to the security function.

Culture Indicators:

The implementation of organizational and other changes is planned, controlled, communicated, monitored, treated, and recorded to ensure that the security of radioactive sources is not compromised.

Changes in such areas as operation, safety, and security of radioactive sources are coordinated with all potentially affected personnel.

Organizational changes are evaluated and classified according to their importance to the security of

radioactive sources and each change is justified.

In cases where the required security measures cannot be fully met during field or off-site operations, alternative compensatory measures are implemented that will provide an equivalent level of security.

Radioactive source inventory is regularly reviewed to identify any sources that are not in routine use and have become disused so that their security is adequately maintained.

Disused sources are disposed within the specified period of time after determining that extended or long-term storage of disused sources pose an increased threat to the security.

Security considerations play an important role in the selection of options for managing disused sources.

All staff members and contractors whose security-related tasks are affected by changes receive the necessary training to handle such change.

k) Contingency Plans and Drills

The security system must be in a continuous state of readiness to handle security events at any time. An important element of the system is the set of contingency plans used to respond to attempted or successful malicious acts or to address a breach of protection. Appropriate and realistic drills and exercises must be conducted periodically.

Culture Indicators:

Contingency plans are in place to address the defined threats and responses.

Contingency plans are tested periodically (e.g. weekly or monthly) through drills and other means to ensure that they are effective, current, and that the individuals involved in using them are familiar with the plans and their roles.

Practicing of the security plan procedures involves more than just the staff, to include local police force and even military, if necessary.

Staff members and contractors are trained to effectively deal with novel and unexpected situations for which no procedures have been devised and when no management supervisor is available.

Provisions are in place to ensure that security readiness can be temporarily tightened during times of increased threat (e.g. introduction of additional measures or reduction of access to radioactive sources).

Procedures are in place regarding measures to recover lost or stolen sources.

Contingency plans are regularly evaluated and updated to reflect the threat level and nature of newly deployed sources.

Contingency plans are in place to respond to malicious acts in transport, including plans for the recovery of lost or stolen material and for mitigating consequences.

The response plan is regularly reviewed to ensure that there would be an adequate response to any attempts at theft, sabotage or other malicious act.

Appropriate exercises are carried out in advance of a transport of radioactive sources to ensure that contingency plans are adequate.

l) Interface with Regulators and Other Off-site Organizations

Effective security often involves several regulatory and law enforcement bodies. A constructive working relationship with each regulatory or law enforcement body is therefore important to ensure that information is exchanged regarding security matters. Security matters involve not only the relationship between the regulatory authority and the regulated organizations but also policy making and other legal bodies.

Culture Indicators:

Regulatory interface roles are clearly defined and interagency procedures are streamlined.

Procedures are established with local law enforcement regarding intelligence information and use of appropriately reliable and secure communications as well as reactions to an increased threat.

Information on abnormal conditions and events significant to radioactive source security is made available to the regulatory authority and other relevant bodies including, where appropriate, other users.

Staff members and contractors fully understand the regulatory body's role in controlling radioactive sources.

Reports to the competent authority cover any unusual events bearing on the security of the sources including, among others, loss of control, unauthorized access, unauthorized use, malicious acts and discovery of unaccounted sources.

m) Record Keeping

Efficient record keeping and protection of sensitive information are vital to the safe and secure operation of radioactive sources as well as accurate audits and inspections.

Culture Indicators:

There is a mechanism to protect confidential records.

Records are systematized and there is a procedure for obtaining relevant information from current records and logbooks as well as archives.

The person responsible for a radioactive source maintains records for that source, which include relevant information about its characteristics.

Each radioactive source is periodically inventoried and accounted for.

A record is kept of all persons who have access to, or monitor, the use of keys associated with the operation of radioactive sources.

A system is in place for keeping records of radioactive material transported.

Personnel Behavior

a) Professionalism and Security Awareness

Awareness is a key driving force for staff members and contractors to stay committed to robust security of radioactive sources. Through training programs, briefings, work experience, mass media, and other sources, they become aware that malicious attempts by outsiders and insiders pose a real threat and, hence, security is important. They understand devastating consequences of radiological terrorism and want to prevent its occurrence. It is vital to reinforce this awareness and combat complacency.

Culture Indicators:

Staff members and contractors take professional pride in security-related aspects of their work and consider them valuable.

Staff members and contractors are involved in one way or another in maintaining and enhancing security.

Staff members and contractors are familiar with the organization's security plan and adhere to it.

Staff members and contractors are prepared to face the unknown and improvise should it become necessary.

Staff members and contractors notify their co-workers and managers when these co-workers are doing something that may downgrade security.

b) Compliance

Regulations and procedures represent accumulated knowledge and experience. It is important that they are followed to avoid errors that have already been identified and corrected. It is also important that

procedures are clear, up to date, readily available, and user friendly so that personnel do not resort to departing from the approved process.

Culture Indicators:

Staff members and contractors understand the potential consequences of noncompliance with the established rules for the organization's safety and security.

When sources are not in use, designated staff stores them in an approved manner as required by appropriate procedures.

Management frequently inspects work to ensure that procedures are being used and followed in accordance with expectations.

The organization's instructions on security are easy to follow because they are readily available, clear, up to date, and user friendly.

Staff members and contractors who discover discrepancies in the implementation of security procedures promptly report them to management.

Staff members and contractors show trust in and acceptance of security procedures.

c) Personal Accountability

Accountable behavior means that all workers know their specific assigned tasks related to the security of radioactive sources (i.e. what they have to accomplish, by when, and what results should be achieved) and that they either execute these tasks as expected or report their inability to do so to their supervisor.

Culture Indicators:

Staff members and contractors understand how their specific tasks support the security system for radioactive sources.

Commitments are achieved or prior notification of their non-attainment is given to management.
Staff members and contractors take responsibility to resolve security-related issues.

Staff members and contractors consider themselves responsible for maintaining an adequate level of security at the organization.

Personal accountability is clearly defined in appropriate policies and procedures.

Staff members and contractors avoid shortcuts in implementing security procedures.

d) Mutual Respect and Cooperation

Mutual respect and teamwork is essential. An effective radioactive source security culture can best be found in an organization where there is extensive interpersonal interaction and where relationships between various groups are generally positive and professional.

Culture Indicators:

Teams are recognized and rewarded for their contribution to radioactive source security.

Staff members interact with openness and trust, and they routinely support each other.

Problems are solved by multilevel and multidisciplinary teams.

Teamwork and cooperation are encouraged at all levels and across organizational and bureaucratic boundaries.

Team members support one another through awareness of each other's actions and by supplying constructive feedback when necessary.

Professional groups appreciate each other's competence and roles when interacting on security issues.

There are ample opportunities to exchange security-relevant information within and between units.

Team members are periodically reassigned to

improve communications between teams.

Cross training among different professional areas and groups is conducted to facilitate teamwork and cooperation.

e) Vigilance and Reporting

Security depends on the attentiveness and observational skills of staff. Prompt identification of potential vulnerabilities and reporting to superiors permit proactive corrective action. An appropriate questioning attitude is encouraged throughout the organization.

Culture Indicators:

Staff members and contractors notice and question unusual indications and occurrences and report them to management, as soon as possible, using the established process.

Staff members and contractors are attentive to detail.

Staff members and contractors seek guidance when unsure of the security significance of unusual events, observations, or occurrences.

Staff members and contractors are trained in observational skills to identify irregularities in security procedure implementation.

Staff members and contractors are aware of a potential insider threat and its consequences.

Staff members and contractors avoid complacency and can recognize its manifestations.

Staff members and contractors accept and understand the requirement for a watchful and alert attitude at all times.

Staff members and contractors feel safe from reprisal when reporting errors and incidents.

A policy prohibiting harassment and retaliation for raising radioactive security concerns is enforced.

Appendix B: Examples of Survey Statements

Security Culture Indicator Multi-focused and Generic	Survey Statement Single-focused and Personal
Staff members and contractors are aware of a potential insider threat and its consequences **(III, (e) 5)**	I am aware of a potential insider threat and its consequences
Staff members and contractors understand their roles and responsibilities for security of radioactive sources and are encouraged to seek classification when necessary **(II, (c) 4)**	Management encourages me to seek, when necessary, clarification regarding my role and responsibilities for security of radioactive sources
Senior management personally inspects performance in the field by conducting walk-arounds, listening to staff and observing work being conducted, and then taking action to correct deficiencies (I,(a) 5)	I witnessed how our leaders personally inspect performance in the field by conducting walk-throughs, listening to staff, and observing work being done

Appendix C: Select Case Studies of Radioactive Source Incidents

Location	Date	Incident	Fatalities	Cause
Spain	May 1998	An unnoticed caesium-137 source was melted in an electric furnace of a stainless steel factory in Spain. The vapors were collected in a filter system, resulting in contamination of the collected dust, which was removed and sent to two factories for processing as a part of routine maintenance. One factory used the contaminated dust in a marsh stabilization process, resulting in contamination being spread throughout the marsh. The first warning of the event was from a gate monitor that detected the material on an empty truck returning from delivering the dust. Elevated levels of caesium-137 were also detected in air samples in Southern France and Northern Italy.	The radiological consequences of this event were minimal, with six people having slight levels of caesium-137 contamination. However, the economic, political and social consequences were significant. The estimated total costs for cleanup, waste storage, and interruption of business exceeded	*Negligence*

			$25 million US dollars.	
Samut Prakan Province, Thailand	January 2000	Scrap metalworkers uncovered an insecurely licensed cobalt-60 teletherapy source in a junkyard. They transported it to another junkyard, where they opened the device. People in the area immediately began to feel ill but it took 10 days for anyone to report their symptoms, and 17 days after the initial theft for authorities to realize the theft of the radioactive source.	3 fatalities total. 1,870 people were exposed, with many seeking medical attention. The Ministry of Health monitored 258 people living within 50 meters of the junkyard for long-term health effects.	*Orphan source theft*
Mayapur, India	April 2010	Delhi University sold an unused radioactive source (reportedly 25-years-old) in the form of a gamma cell irradiator. Containing colbat-60 pencils, the source was sold to scrap metal dealers. The unsuspecting scrap dealers dismantled the object dispersing 11 different pieces of material.	1 fatality and 7 radiation-related injuries. All the metalworkers required medical treatment after dispersing the device.	*Negligence*
New York City, New York	August 2013	In a sting operation, the US Department of Homeland Security place an ad stating an interest in purchasing yellowcake online. A man from Sierra Leone responded offering 1,000 tons of yellowcake for sale. The man flew to New York and was apprehended on site. Authorities found small quantities of yellowcake in the soles of his shoes.	None	*Trafficking*
Assam, India	August 2013	The ULFA, a rebel group in northern India, issued a series of threats to carry out bombings on Republic Day. An army patrol discovered an improvised explosive device and 1.5 kilograms of uranium under a police station. The form of the uranium is unknown; however, the region is home to a uranium mining operation and the ULFA is known to target businesses and industries in the region.	None	*Theft*
Mexico City, Mexico	December 2013	A cancer therapy clinic in Tijuana, Mexico shipped a highly radioactive radiation therapy source to Mexico's radioactive waste disposal facility. The truck driver claimed he was sleeping in the truck on the side of the road when armed thieves ordered him out of the truck and stole the source. At the time of the theft, the source consisted of over 2500 curies of cobalt-60. The container holding the cobalt-60 was found about a kilometer from the truck and had been opened.	None	*Negligence and theft*

Poznan, Poland	March 2015	22 containers containing a category 5 source (Co-60) were stolen from a Poznan storage unit. The thieves dismantled the shielding containers in order to produce scrap for money. The sources caused spot-damage inside the storage unit and local soil. Only 8 of the 22 containers have been secured.	None	*Theft*
Georgia	January 2016	Georgia's security agency reportedly arrested three men for attempting to sell an unknown quantity of cesium-137 for $100 million.	None	*Theft*
Iraq	February 2016	A category 2 radioactive source was stolen from a US oilfield service company, located near Basra Iraq. The material was found undamaged three months later in a ditch near a gas station.	None	*Theft*
Ukraine	March 2016	Ukrainian authorities seized a create from a warehouse containing several radioactive materials. IAEA Reports indicate the owner of the warehouse planned to illegally sell the material.	None	*Theft*
Georgia	April 2016	Georgia's security agency reported the arrest of six men of Georgia and Armenian origin who were attempting to sell depleted uranium for $200 million. The authorities also located specially designed containers intended for transportation of significant quantities of uranium at one of the arrested individual's residence	None	*Theft*
Georgia	April 2016	Georgian authorities arrested five men who were attempting to illegally sale 1.665 kilograms of depleted uranium for $3 million. Georgian authorities believe the two April 2016 cases were related.	None	*Theft*

Appendix D: Glossary

Assessment. The process, and the result, of analyzing systematically and evaluating the hazards associated with facilities and activities, and associated protection and safety measures.

Cradle to grave management. Ensuring the security of a radioactive source from the beginning of its life cycle to the end of its disposal.

Delay. The time, after detection, that is required by an adversary to remove the radioactive material or sabotage the associated facilities.

Design Basis Threat. Defined by the U.S. Nuclear Regulatory Commission as the "profile of the type, composition, and capabilities of an adversary." Used by nuclear facilities as a basis for designing security systems to prevent radiological theft and sabotage.

Detection. Monitoring both outside and inside the facility, determining the entry control effectiveness, and assessing intrusions

Dirty bomb. Common name for a radiological dispersal device (RDD). An improvised weapon encasing radioactive material with conventional explosives, designed to produce a large amount of radioactive debris

Document review. A labor-intensive process that helps evaluators appraise stated policies, procedures, and actual behavior. Can be used prior to assessment to evaluate root causes and previous corrective measures taken, or used as a tool during the process of assessment.

Focus-group discussions. An interview session amongst a group of employees in which the members engage in discussion about their experiences, views and attitudes toward the topic in question, facilitated by an interviewer.

Insider. An individual with access to facilities, activities, or information associated with radioactive materials that could facilitate or commit a malicious act.

Interview guide. An informal list of topics and questions derived from survey results that help interviewers focus on the topic at hand while tailoring questions to meet assessment goals.

Irradiation. To be exposed to some form of radiation whether intentional or accidental; irradiation is not always harmful – the damage is dependent on the dose received.

Observations. Recordings of actual performance and behavior in real time and under different circumstances, including general meetings, training sessions, and emergency drills.

Orphan source. Radioactive sources that have been abandoned, lost, or misplaced as well as sources that were stolen or removed without proper authorization.

Radioactive material. A substance that contains unstable, radioactive atoms that give off radiation as they decay. For legal and regulatory purposes, radioactive material is limited to any substance designated by law, regulation, or regulatory body to be subject to regulatory control.

Radioactive source. A high concentration of radioactive material in a small volume that is sealed in a capsule or bonded in solid form in such a way designed to prevent the escape of material during normal usage or probable mishaps; radioactive sources include any material released due to leakage or breaking, but does not include material bonded for disposal; radioactive sources are subject to regulatory control.

Radiophobia. The irrational belief that any level of ionizing radiation is highly dangerous, if not immediately deadly.

Regulatory Body. A public authority or government agency legally responsible for regulating nuclear, radiation, and radioactive waste transportation, safety, and security by imposing requirements, restrictions, and compliance.

Survey. A self-assessment tool used to establish a baseline for tracking changes over time. Management provides personnel with security statements, derived from culture indicators, and a scoring scheme to indicate level of observance.

Threat. An individual or group with motivation, intent, and capabilities to commit a malicious act.

Threat assessment. An analysis, based on available intelligence, of the motivations, intents, and capabilities of existing hazards threatening the facilities, activities, or sources, in addition to the actions that would be useful in mitigating the potential consequences of these threats.

Teletherapy. Treatment in which the source of the therapeutic agent, usually radiation, is at a distance from the body; often used for treating cancer.