International Journal of Nuclear Security

Volume 5 | Number 1 Article 2

5-3-2019

Risk-Based Approach in the Self-Assessment of Nuclear Security Culture for Users of Radioactive Sources

Igor Khripunov
Nonresident Fellow of Stimson Center, USA

Risk-Based Approach in the Self-Assessment of Nuclear Security Culture for Users of Radioactive Sources

Cover Page Footnote

International Atomic Energy Agency, “Nuclear Security Culture: Implementing Guide,” Nuclear Security Series No. 7, IAEA, 2008, p. 3. International Atomic Energy Agency, “Self-Assessment of Nuclear Security Culture in Facilities and Activities: Technical Guidance,” Nuclear Security Series No. 28-T, IAEA, 2017. International Atomic Energy Agency, “Nuclear Security Culture: Implementing Guide,” Nuclear Security Series No 7, IAEA 2008, p.19. International Atomic Energy Agency, “Nuclear Security Recommendations on Radioactive Material and Associated Facilities,” IAEA Nuclear Security Series No 14, p. 13. International Atomic Energy Agency, “Nuclear Security Recommendations on Radioactive Material and Associated Facilities,” IAEA Nuclear Security Series No 14, IAEA, p. 13. Andrew Bieniawski, Ioanna Iliopulos, Michelle Nalabandian. “Radiological Security: Progress Report,” Nuclear Threat Initiative, March 2016, p.10. Edgar Schein, “Organizational Culture and Leadership,” 3rd ed. (San Francisco, CA: Jossey-Bass, 2004), p.17. Edgar Schein, “The Corporate Culture: Survival Guide,” (San Francisco: Jossey-Bass, 1999), p.20. Edgar Schein, “The Corporate Culture: Survival Guide,” (San Francisco: Jossey-Bass, 1999), p.16. “Nuclear Security Culture,” Nuclear Security Series No.7, IAEA, 2008. “Nuclear Security Recommendations on Radioactive Material and Associated Facilities,” Nuclear Security Series No 14, IAEA, 2011, p.5. International Atomic Energy Agency, “The Interface Between Safety and Security at Nuclear Power Plants,” INSAG-24, IAEA. Steve Nibbelink, “Hospitals Meet Security Challenges with Integrated Security and Facility Solutions,” Schneider Electric, January 2012, pp.6-7. International Atomic Energy Agency, “Guidance on the Management of Disused Radioactive Sources,” 2018 Edition. IAEA.

International Journal of Nuclear Security, Vol. 5, No. 1, 2019

Risk-Based Approach in the Self-Assessment of Nuclear Security Culture for Users of Radioactive Sources

Dr. Igor Khripunov

Nonresident Fellow, Stimson Center, USA

Abstract

The current emphasis on the need to protect radioactive sources from being used for malicious purposes makes it imperative to explore and shape an appropriate culture-based response. Promoting a robust security culture is consistent with the international legal instruments and standards including the Code of Conduct for the Safety and Security of Radioactive Sources and IAEA guidance publications. This promotion would be dependent upon the successful implementation of relevant self-assessment tools and a series of culture indicators, both of which would serve as benchmarks to take a culture's measure and identify practical ways to improve security. This approach must adjust the generic IAEA model and self-assessment methodology for nuclear security culture in order to accommodate the specific requirements in operation when using radioactive sources. Though the IAEA's concept of security culture and its self-assessment recommendations are designed to be generic in order to apply to a wide range of facilities and activities, the modifications proposed in this paper are needed to make those recommendations more user friendly and consistent with the security risks and requirements. The distinct features of the proposed recommendations, to be reflected in the new design of security culture, can be summarized as: continued prevalence of safety orientation, application in diverse work environments, multiple and inter-modal transport, integration of host organizations into overall security regime, mobile and portable operation, limited security awareness and resources, and disposal challenges. These special features also justify a differentiated approach to security culture inside organizations licensed to use radioactive sources. More frequent and more concerted efforts, including training and self-assessment, are expected to focus on a select group of employees who have direct relationships with radioactive sources (e.g. management teams, security personnel, operational staff, technicians and others). For other employees, efforts would be made concurrently to engage them in the process of raising security awareness, a less proactive endeavor than the development of security culture. The proposed differentiation is a targeted approach designed to make time and resource investment in training and culture assessment commensurate with specific roles and responsibilities of individuals. This risk-based approach can facilitate a more robust and sustainable security regime for radioactive sources throughout their life cycle, i.e. from cradle to grave.

I. Introduction

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."**[*1*]** As a supporting and enhancing tool, the role of culture may be understood in light of the definition of nuclear security, which is "the prevention and detection of, and response to, theft, sabotage, unauthorized access, illegal transfer or other malicious acts involving nuclear material, other radioactive substances or their associated facilities."**[*2*]** 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. In 2008, the IAEA published the Implementing Guide on Nuclear Security Culture in its Nuclear Security Series, which defined the concept and characteristics of nuclear security culture while delineating the roles and responsibilities of institutions and individuals entrusted with this function. The Implementing Guide described its objective (p.2) as intended for regulatory bodies and other organizations, institutions and individuals involved in activities that utilize nuclear, or other radioactive material, who would be called upon to respond to an incident involving radioactive material or its associated facilities, including its transport. In this publication, the IAEA explicitly focused on a generic approach applicable to the entire nuclear infrastructure without providing clear distinctions for the needs of diverse facilities and activities.

The next IAEA publication, the Technical Guidance on Self-Assessment of Nuclear Security Culture in Facilities and Activities, was released by the agency in November 2017**[*3*]**. Its scope covered nuclear security culture in organizations and facilities using or storing radioactive material, particularly those using or storing nuclear material. In addition, the IAEA stated that its "generic approach" could also be used for assessing nuclear security culture in other organizations relating to nuclear security, such as law enforcement and border control agencies (p.2). From 2012, when the drafting of the Technical Guidance started, to 2018, self-assessments were conducted in Indonesia (research reactors), Bulgaria (nuclear power plant), and Malaysia (radioactive sources at two medical institutions).

Obviously, both IAEA publications in the Nuclear Security Series were intended to serve as an introduction to the subject for their 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 transport. Their 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 to each type of nuclear and radiological facility, and therefore requires 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**[*1*]**. Accordingly, given the lack of expertise and experience, for example, among some users of radioactive sources, the purpose of this paper is to demonstrate in a user friendly and efficient manner how to adjust the IAEA generic approach and meet the specific needs of their facilities for assessing security culture.

II. 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, from the perspective of those facilities, it would make sense not to reduce the risk to society to lower than what a regulator requires, as the facility would then be overspending its scarce resources on security. Such facilities, often with little practical experience in security, tend to view security systems as a means of reducing their overhead costs. To a limited degree, developing a robust security culture can be a way to be assured of a facility's capacity to successfully respond to emergency situations. 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**[*4*]**. The threat assessment serves as a common basis for regulatory authorities and users of radioactive sources when performing their respective functions.

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 covers:

- 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 national practices.

Once the security system is designed, the influence of human factors must be considered and built into the security calculation in order for it to be successful. This means looking at each of the factors that are considered risk factors as the result of human error, inconsistencies, complacency, and other reasons. A major IAEA security recommendation 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."**[*4*]**

Indeed, an effective security 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 the recognition by those who have a role in regulating, managing, or operating facilities or activities involving radioactive sources—or even those that could be affected by such activities—that a credible threat exists and that security is important. Security culture is an effective tool in addressing insider threats because—due to the work environment and ease of accessibility—motivated and vigilant personnel, in combination with adequate physical protection, are then recognized as indispensable players in safeguarding radioactive sources. 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**[*5*]**. 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 that the security regime will be effective, sustainable, and function at its optimal level.

III. The IAEA Concept of Nuclear Security Culture

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 the consequences of human failure. The synergies between safety and security culture, and their overlaps as part of overall organizational culture, provide 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."**[*6*]**

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, these dispositions 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"**[*7*]**.

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**[*7*]**. Using Edgar Schein's three layers of culture, the reproduced IAEA model for nuclear security culture divides the visible segments (artifacts) of the culture into three parts, giving a total of five elements (see Figure 1). 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 (the specific actions and patterns of behavior which are designed to foster more effective nuclear security); 4) management systems (the processes, procedures and programs in the organization which prioritize security and have an important impact on security functions); and 5) personnel behavior (the desired outcome of successful leadership behavior and operation of the management systems, when practices consistent with culture requirements are internalized).

International Journal of Nuclear Security, Vol. 5, No. 1, 2019

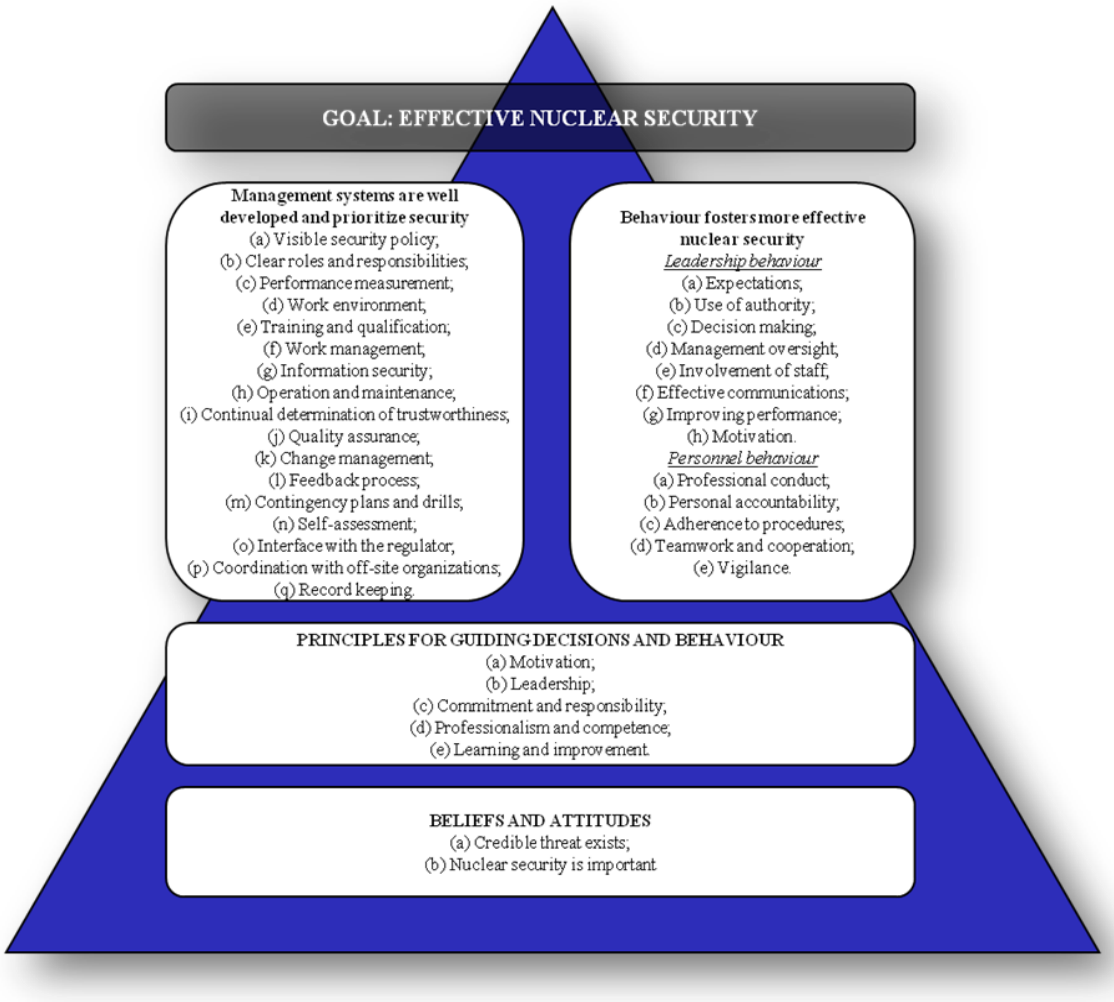

Figure 1. IAEA Model of Nuclear Security Culture **[*1*]**

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 responses 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 throughout and permeates the entire workforce, 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 (a total of 30 characteristics in the IAEA model). Indicators help measure culture within these delineated characteristics and identify practical ways to improve. 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) to monitor security awareness in the organization; b) to determine tools and procedures for mapping improvement; c) to provide guidance when making an improvement strategy; and d) to motivate the management and staff to take all necessary actions. It is important to remember that security culture self-assessment is a creative, multidisciplinary process; users of the IAEA methodology should feel welcome to review potential risks and develop new culture indicators consistent with the profile of their organizations.

IV. 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 focused on protecting radioactive sources. As defined by the IAEA, the objectives of that regime are to:

- Protect against unauthorized removal of radioactive material;
- Protect against sabotage of material, facilities and activities, i.e. production, processing, use, storage, disposal, transport, etc.;
- Ensure that implementation of rapid and comprehensive measures to locate and recover radioactive material that is lost, missing or stolen and re-establish regulatory control**[*4*]**.

Several features of radioactive source security make it distinctly different from nuclear security in other facilities and activities. These differences have a significant effect on the design of relevant security cultures. The distinct features of radioactive source security can be summarized as follows:

A. Continued prevalence of safety orientation

The Code of Conduct was originally tailored to safety and radiation protection rather than security. Many organizations that make limited use of radioactive sources have large operational units where no radioactive sources are utilized, and where security mentality is not well developed or understood. As a result, managers tend to delegate security to their lower-tiered staff and are less personally involved. In these conditions, those in charge of operating radioactive sources can often prioritize protecting people from radioactive sources rather than protecting those 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. Moreover, they must complement each other and be mutually supportive.

Hence, a security culture model for radioactive sources must put more emphasis on harmonization with safety culture and thus avoid possible conflicts and contradictions. As stated in the IAEA document INSAG-24, culture of safety and security should be integrated in the organization's management system**[*8*]**. In practical terms, individuals have diverse backgrounds and experiences, and it is necessary to provide both safety and security staff with an appreciation of the importance of each area, while emphasizing the need for a cooperative and balanced approach with the aim of achieving reliable operation at an acceptable risk level.

New culture indicators for this model must cover issues like visible commitment to the balanced approach from all levels of management; organization wide dissemination of harmonization benefits; clearly defined responsibilities for individuals; and tracking mechanisms to measure the harmonization progress and others.

B. Multiple and intermodal transport

In view of the potential vulnerability of radioactive material in transport, the design of an adequate transport security system must incorporate the concept of defense, and must use a graded approach to achieve the objective of preventing the material from becoming vulnerable to malicious acts. Accordingly, it is important for relevant individuals under this model to meticulously comply with effective security transport schedules, routing, security of passage, information security and other 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 the potential of that threat to generate consequences. The transport of radioactive sources is usually an interim phase between production, use, storage, and disposal. The possible 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, could choose a point along transportation routes where the sources would be most vulnerable and procedures for physical protection are least effective.

This is why the new model must include—among other cultural indicators—well-defined procedures to control the procurement of items and services used for the transport and adherence to those procedures; requirements to minimize the total time of transport, the number of internal transfers and the waiting time; adequate measures to deter, detect, and delay unauthorized access while in transport.

C. 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. For example, hospitals with radiology wards have their own set of unique security and safety risks, depending on, for example, service offerings and administrative strategies. 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;
- Workplace violence is an increasing problem;
- Drugs are used and stored at the facility;
- Money is handled throughout the facility; and
- Hospitals are soft targets for terrorists**[*9*]**.

Relevant culture indicators must cover, for example, support for teamwork and cooperation at all levels and across organizational and bureaucratic boundaries; exchange of security-relevant information within and between units; and encouragement of cross-training among different groups within the workplace to facilitate teamwork and cooperation.

D. Application in diverse environments

Radioactive sources are used across a wide range of activities, including industrial production, construction, research, and medical procedures, among others. The diversity of security regimes and their impact on organizational culture is much more extensive than throughout other, more uniformly structured nuclear facilities. For example, common uses of radioactive 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. Dispersed throughout numerous industrial units and medical institutions, security culture poses a serious challenge in efforts of formulating a uniform approach. New culture indicators should cover issues like integration of security management into overall policies and administrative procedures; application of security management to visitors, contractors and suppliers; and establishment of accurate and up-to-date inventories of radioactive sources.

E. Mobile and portable operations

Industrial radiography sources and a wide range of gauges, as well as other tools, are routinely moved around and often located 'off-site,' where traditional approaches of physical protection cannot be applied effectively. For this category of sources, timely detection, delay and response are not easy to achieve. 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 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 applying 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 entails establishing a communication link with law enforcement to enable their effective response to incidents. In many countries, save large urban centers, local law enforcement is often inadequately trained to respond to radiological emergencies. When mobile and portable sources are used, the above measures can be formulated as security culture indicators. Also, indicators may address other alternative compensatory measures during field or offsite operations.

F. Limited resources and awareness

In some countries, financial, technical, and human resources are still lacking, which makes efforts to address the risk of diversion of radioactive material for malicious use less effective. Most of these countries do not have an established nuclear power infrastructure, an infrastructure which, given its scale and significance for the national economy when it is in place, can often serve 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 also precipitated a sense of complacency among regulatory authorities and users of radioactive sources. 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 also costly to install and maintain. Culture indicators must focus on policies that ensure that security procedures learned in training are applied in practice; on raising security awareness for individuals engaged in transport; and on efforts to avoid complacency and recognize its manifestations.

G. Disposal challenges

End-of-life source management is challenging due to a lack of uniformity in practices. Hopefully, the 2018 Guidance on the Management of Disused Radioactive Sources will improve the practices and facilitate implementation**[*10*]**. Options available to users include returning sources to manufacturers, recycling or disposing of them, and storing them. However, financial and other constraints frequently prevent them from following these procedures in a consistent manner. For example, the cost to return sources to their manufacturer or to dispose of them are difficult to predict and can be either prohibitively expensive or greatly underestimated or both. Efforts are made to request that source owners develop plans for disposal prior to import and implement those plans when the sources are disused. However, financial provisions to support those plans continues to be poorly arranged and implemented. As a result, some disused sources become vulnerable to weak regulatory control and may fall into the category of "orphan sources," which are sources that are abandoned, misplaced, lost, stolen, or transferred without appropriate regulatory authorization. Depending on the selected disposal options, culture indicators must focus on the disposal plan and its implementation; on allocating sufficient resources for that plan; and the need to keep the staff informed of its implementation.

V. 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 in-depth efforts will focus on select groups that have a direct relationships with radioactive sources (e.g. management teams, security personnel, operations, technicians, and others). The determination of the dividing line between these groups and the rest of the workforce outside of 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 which invests time and resources 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 overall goal is to develop an awareness of possible risks, danger, and threats to the security and safety of radioactive sources; this awareness would 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 raising security awareness is not simply about enhancing understanding or imparting risk-based information, but preferably also about empowering people to intervene at appropriate times and in appropriate ways commensurate with their roles and responsibilities. All employees must be informed about how to recognize signs 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) the motivations of these actors and the possible consequences of their actions; (4) the limitations of security regimes and concurrent vulnerabilities; and (5) what can be done to prevent the loss or damage of radioactive sources. Emergency drills and exercises would complement, if possible, these sessions.

A security culture model adjusted to users of radioactive sources has altered or new characteristics and culture indicators. It also provides guidance for the differentiated process of security awareness and culture enhancement through several stages until reaching the security commitment, i.e. security ownership stage. The model outlines the elements of an effective security culture as the ultimate goal. This culture is based on proactive skills and practices that enable personnel to address threats by taking appropriate actions and by setting an example for others to follow through knowledge, skills based compliance, and improvisation. Ideally, all personnel should reach the commitment stage, but this may be

a challenge, given special operational and structural features of radioactive source users. Hence, while applying most of these principles as much as possible to the entire workforce, emphasis and priority are accorded to a group of managers and staff with roles and responsibilities associated with the operation, transport, and storage of radioactive sources.

As Fig. 2 below shows, there are four stages to raising security awareness on the way to achieving 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 implications, and personal 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 specific 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.

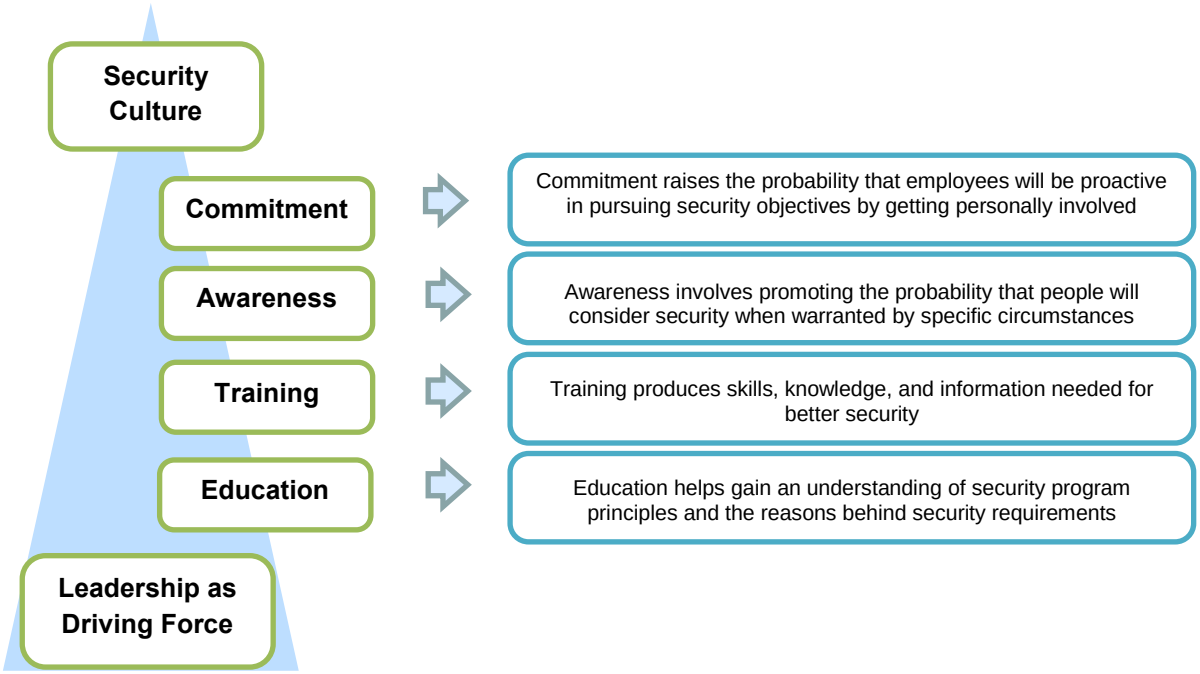

Figure 2. The Road to Security Culture

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 creates the basis of a strong security culture and supports the sustainability of the radiological security program. Culture indicators assigned to

each characteristic are designed to maintain the adequate level of security culture and ensure its sustainability. The rationale behind the indicators is consistency with the specific security considerations in a given facility and activity.

The ability to assess the status of security culture is a prerequisite for its successful development and maintenance. Adjusting the IAEA assessment methodology to the needs of radioactive sources 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.

VI. CONCLUSIONS

The two IAEA guidance documents on nuclear security culture (Implementing Guide and Technical Guidance on Self-Assessment), released in 2008 and 2017 respectively, have been widely used by the agency and member states to publicize, promote and implement its methodology. The complete set is due in 2019 when a document regarding technical guidance on security culture enhancement is expected for finalization and release. A logical next step would be to move away from the generic approach to a more specific, user-friendly methodology geared toward the needs of several distinct categories of nuclear facilities and activities. As demonstrated by this paper, the initial step in this direction is to identify special security considerations for each category (fuel cycle, waste management, radioactive sources, transport, and others), followed by a selection of relevant culture characteristics and indicators. While keeping the fundamental principles of nuclear security culture intact, this new approach will stimulate further progress in the assessment and enhancement of nuclear security culture by reducing cost, expediting the whole process, and making this activity less intellectually challenging.

VII. Works Cited

1. International Atomic Energy Agency, *Nuclear Security Culture* (INTERNATIONAL ATOMIC ENERGY AGENCY, Vienna, 2008; http://www-pub.iaea.org/books/IAEABooks/7977/Nuclear-Security-Culture), *IAEA Nuclear Security Series*.

2. International Atomic Energy Agency, *Nuclear Security Plan 2010-2013* (INTERNATIONAL ATOMIC ENERGY AGENCY, Vienna; https://www-pub.iaea.org/books/IAEABooks/8402/Nuclear-Security-Plan-2010-2013).

3. International Atomic Energy Agency, *Self-Assessment of Nuclear Security Culture in Facilities and Activities: Technical Guidance.* (IAEA, Vienna, 2017; http://public.eblib.com/choice/publicfullrecord.aspx?p=5175141), *IAEA Nuclear Security Series*.

4. International Atomic Energy Agency, *Nuclear Security Recommendations on Radioactive Material and Associated Facilities* (INTERNATIONAL ATOMIC ENERGY AGENCY, Vienna, 2011; https://www-pub.iaea.org/MTCD/Publications/PDF/Pub1487_web.pdf), *IAEA Nuclear Security Series*.

5. A. J. Bieniawski, I. Iliopulos, M. Nalabandian, Radiological Security Progress Report: Preventing Dirty Bombs - Fighting Weapons of Mass Disruption. *Nucl. Threat Initiat.*, 32 (2016).

6. E. H. Schein, *Organizational Culture and Leadership* (Wiley, Hoboken, New Jersey, 5th Edition., 2017).

7. E. H. Schein, *The Corporate Culture Survival Guide* (Jossey-Bass, San Francisco, CA, New and rev. ed., 2009).

8. J. L. Ferraz Bastos, International Nuclear Safety Group, International Atomic Energy Agency, *The Interface Between Safety and Security at Nuclear Power Plants* (International Atomic Energy Agency, Vienna, 2010), *IAEA INSAG Series*.

9. S. Nibbelink, Hospitals Meet Security Challenges with Integrated Solutions. *Schneider Electr.*, 14 (2012).

10. International Atomic Energy Agency, Guidance on the Management of Disused Radioactive Sources, 184 (2018).