

Improving the Security of Radioactive Sources in Industrial Radiography in South East Asia

Andrew Popp and Allan Murray ^f

Paper presented to the 36th annual conference of the Australasian Radiation Protection Society, 16 to 19 October, 2011.

Abstract

This paper describes the need and new requirements to ensure the security of radioactive sources used in the practice of industrial radiography. We describe the discussions and issues arising during the September 2010 South East Asia regional workshop held in Sydney on the application of security measures to industrial radiography practices. The workshop provided the perspectives of both radiation regulators and industry practitioners from some countries in South East Asia. We describe the outputs of the workshop, how they were developed, and make suggestions for further consideration and application of security measures in the practice of industrial radiography. Examples of uptake of the outcomes of the workshop by the Philippines Society for Non-Destructive Testing and the World Institute for Nuclear Security are provided.

Introduction

The requirements and methods to ensure radiation protection and safety of radioactive sources used in industrial radiography are long- and well-established [1] - [3]. However, in recent years there has been recognition of the threat posed by the potential malicious misuse of radioactive material by terrorists [4], [5]. The dispersal of radioactive material using conventional explosives, referred to as a 'dirty bomb', could create considerable panic, disruption and area access denial in an urban environment. As such, radioactive source security is now a priority matter being addressed by the international community. However, as it is still a relatively new topic among regulators, users, and transport and storage operators worldwide, international assistance and cooperation in developing the necessary regulatory and security infrastructure is required.

For several years international cooperation programs have been enhancing the security of highly radioactive (Category 1) sources, primarily located at medical and industrial facilities. From a foundational viewpoint, these programs support States in satisfying the elements of the International Atomic Energy Agency (IAEA) *Code of Conduct on the Safety and Security of Radioactive Sources* [6]. Since 2005, the Regional Security of Radioactive Sources (RSRS) Project of the Australian Nuclear Science and Technology Organisation (ANSTO), working with partners from the United States Global Threat Reduction Initiative (GTRI), has assisted many South East Asia countries in the development of national requirements and measures for the physical protection and security management of radioactive sources. The RSRS and GTRI programs have worked with their national partners throughout South East

^f Regional Security of Radioactive Sources Project, Australian Nuclear Science and Technology Organisation, Sydney. Email: amu@ansto.gov.au and aop@ansto.gov.au.

Asia in raising awareness, implementing physical protection upgrades, building knowledge and expertise at the local and national levels, and working with host countries to develop and implement relevant, applicable and sustainable systems that ensure the secure management, use and storage of radioactive sources. In South East Asia, the international cooperation includes working group meetings with the national regulators that have developed regulations on the Security of Radioactive Sources. For example, the Philippines Nuclear Research Institute (PNRI) developed Part 26 of the Code of Philippine Regulations (CPR) on the Security of Category 1 Radioactive Sources [7] and associated activities such as training courses and support for the development of Facility Security Plans. These regulatory requirements are based on 2003 technical guidance of the IAEA [8] and the 2005 IAEA publication “Categorization of Radioactive Sources” [9], and apply to facilities that use Category 1 sources in medical radiotherapy and industrial, blood and research irradiators. This system of categorisation was also adopted by the Australian Radiation Protection and Nuclear Safety Agency (ARPANSA) in 2007 and resulted in the publication of its Code of Practice for the Security of Radioactive Sources, Radiation Protection Series No. 11 (RPS 11) [10].

Since the incorporation of this IAEA guidance into regulations in South East Asia and Australia, updated international best practice guidance on the security of radioactive sources has been developed by the IAEA, including:

- IAEA Nuclear Security Series No. 9 (NSS 9), Security in the Transport of Radioactive Material Implementing Guide, September 2008 [11], and
- IAEA Nuclear Security Series No. 11 (NSS 11), Security of Radioactive Sources Implementing Guide, May 2009 [12].

IAEA NSS 11 includes systematic guidance on measures for the prevention and detection of, and response to, malicious acts involving radioactive sources, and replaces the earlier 2003 IAEA technical guidance [8]. The NSS 11 measures are aimed at preventing the loss of control of high-risk radioactive sources under circumstances of attempts of theft or sabotage. The security measures are intended to complement regulatory and safety requirements, and not to be in conflict with existing requirements.

A fundamental feature of the guidance is that the measures should be applied on a graded basis to ensure adequate security without imposing unnecessarily restrictive arrangements. This graded approach takes into account the current evaluation of the threat, the relative attractiveness for misuse of the source, and the potential consequences resulting from malicious use. Three security levels of A, B, and C have been developed to allow specification of security goals and performance measures in a graded manner. Using the international guidance and considering the level of radioactivity of the sources, their portable nature and the potential for them to be aggregated in storage, the practice of industrial radiography represents a Category 2 practice in terms of level of dangerous consequences [13]. This in turn requires the application of security measures which meet the security objectives of Security Level B [12]. The overall Security Level B goal is to minimize the

likelihood of unauthorized removal of a source. For comparison, the Security Level A goal (which applies to Category 1 sources) is to prevent unauthorized removal of a source.

ARPANSA has developed a series of best practice guidelines for specific industries to assist organisations which are responsible for security enhanced sources to meet the requirements of RPS 11 [10]. These guidelines provide strategies to manage risk and recommend options to secure security enhanced sources consistent with the performance based requirements of RPS 11. On request to the relevant State regulator, the practice specific security guide (PSSG) 05 - *Security Guidelines for Industrial Radiography* [14] is available to those responsible for preparing security plans [15].

At a review meeting of the South East Asia Regional Radiological Security Partnership (RRSP) in Vietnam in March 2010, it was recommended that specific, detailed provisions for the security of Category 2 industrial radiography sources be developed at the national level and implemented at the user or facility level [16]. As a result, the ANSTO RSRS Project in partnership with the US GTRI, the IAEA and the New Zealand Ministry for Foreign Affairs and Trade (MFAT) conducted a South East Asia Regional Workshop on Radioactive Source Security Level B (Industrial Radiography Practices) in Sydney from 6 to 10 September 2010. Sponsorship was provided for all regional country representatives to participate in this workshop.

The Radioactive Source Security Level B Workshop

The purpose of the workshop was to:

- a) review the IAEA and other relevant security guidance or requirements, such as specific national regulatory requirements, that apply to Security Level B radioactive sources generally and to industrial radiography sources specifically;
- b) apply these recommendations or requirements to the development of more detailed security provisions, taking account of all the conditions involved in the practice of industrial radiography;
- c) prepare a guidance document and associated training material for use by participating organizations; and
- d) make recommendations for additional workshops to further develop guidance, training programs or activities as needed, with the aim of implementing Security Level B guidance or requirements for other practices.

Workshop participants were experts with a background or relevant expertise in radiation safety, security, technical training and industrial radiography practice within their national nuclear operating organisations, regulatory authorities, training organisations, professional non-destructive testing associations and industrial radiography company operators. Regional countries represented were Indonesia, Malaysia, Philippines, Singapore and Vietnam. All of these participants, with their different points of view and concerns, contributed constructively to the discussions and in developing the workshop outputs which resulted in practical and achievable results for all concerned.

The workshop was conducted in an open and interactive manner. This was achieved through presentations and discussions on:

- a) a review of the IAEA nuclear security guidance covering radioactive source use and storage (NSS 11) and transport (NSS 9);
- b) a review of radioactive source practices that fall within Security Level B, and in particular the practice of industrial radiography. Some incidents involving radiography sources were presented, with descriptions of root causes, their consequences, implications for security and the need for better protection;
- c) reviews of the operational life cycle of an industrial radiography device from import to export by representatives of industrial non-destructive testing companies from the Philippines and Malaysia;
- d) five national presentations covering:
 - the types and numbers of sources and practices that fall within Category 2, Security Level B;
 - the scope of industrial radiography practices (such as number and size of companies, geographical distribution);
 - specific safety and regulatory requirements given in regulations, decrees or guidance;
 - description of relevant incidents and issues involving industrial radiography, including examples of theft;
 - relevant training course syllabus, delivery, schedule and participation;
 - suggestions for workshop outcomes of interest.
- e) introduction and development of a structured framework for applying Security Level B security measures to industrial radiography sources in use, storage and transport.

Workshop outputs

The discussions and issues arising during the regional workshop provided the practical perspectives of both radiation regulators and industry practitioners in developing recommended security measures for industrial radiography sources. These measures were then used to produce guidance on the structure and contents of a security plan for industrial gamma radiography. Both the recommended security measures and the security plan guidance are structured in terms of use and storage at home base and in the field, as well as transport by the licensee, see Figure 1.

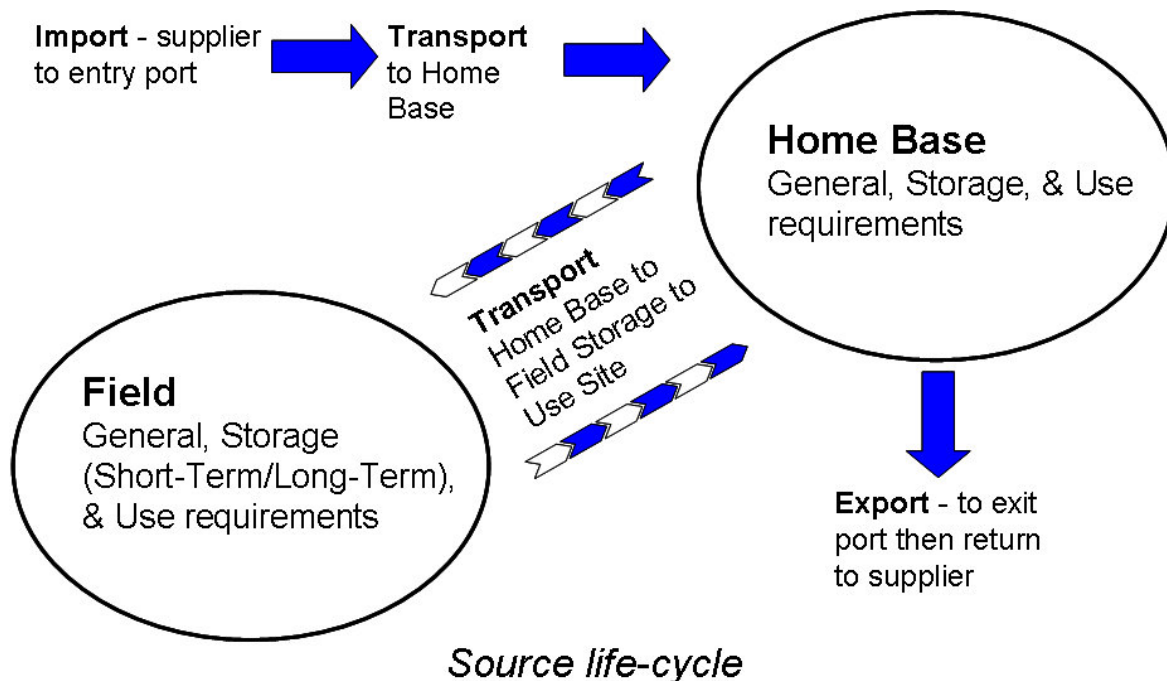


Figure 1: Source life-cycle

The recommended security measures and associated contents of security plans for industrial radiography sources in use and storage are based on IAEA NSS 11 guidance [12], utilising its table 7 structure as follows:

IAEA NSS 11 Guidance, Table 7 - Recommended Measures for Security Level B [12]		
Security function	Security objective	Security measures
Detect	Provide immediate detection of any unauthorized access to the secured area/source location	Electronic intrusion detection equipment and/or continuous surveillance by operator personnel
	Provide detection of any attempted unauthorized removal of the source	Tamper detection equipment and/ or periodic checks by operator personnel
	Provide immediate assessment of detection	Remote monitoring of CCTV or assessment by operator / response personnel
	Provide immediate communication to response personnel	Rapid, dependable means of communication such as phones, cell phones, pagers, radios
	Provide a means to detect loss through verification	Weekly checking through physical checks, tamper detection equipment, etc.
Delay	Provide delay to minimize the likelihood of unauthorized removal	System of two layers of barriers (e.g. walls, cages)
Response	Provide immediate initiation of response to interrupt unauthorized removal	Equipment and procedures to immediately initiate response

IAEA NSS 11 Guidance, Table 7 - Recommended Measures for Security Level B [12]		
Security function	Security objective	Security measures
Security management	Provide access controls to source location that effectively restrict access to authorized persons only	One identification measure
	Ensure trustworthiness of authorized individuals	Background checks for all personnel authorized for unescorted access to the source location and for access to sensitive information
	Identify and protect sensitive information	Procedures to identify sensitive information and protect it from unauthorized disclosure
	Provide a security plan	A security plan which conforms to regulatory requirements and provides for response to increased threat levels
	Ensure a capability to manage security events covered by security contingency plans	Procedures for responding to security-related scenarios
	Establish security event reporting system	Procedures for timely reporting of security events

This was further developed during the workshop with considerations of actual operational practice, recognising national regulatory and individual company differences to the extent practicable. The approach to transport security is based on IAEA NSS 9 guidance [11] and regulatory requirements using the Malaysian Atomic Energy Licensing Board (AELB) model and actual operational practice.

The recommended security measures developed by the workshop participants are given in tabular form in [Appendix A](#), and the guidance on the structure and contents of a security plan for industrial gamma radiography is in [Appendix B](#). This document provides an example of the structure, contents, and guidance in developing a security plan for the practices involved in industrial gamma radiography following international (IAEA) guidance and best practice from industry practitioners. A security plan should include all information necessary to describe the security approach and system being used for protection of the source(s). The level of detail and depth of content should be commensurate with the security level of the source(s) covered by the plan.

The workshop participants acknowledged that these documented methods and measures will form a practical and effective approach for industry practitioners and regulators to ensure and verify appropriate security of Category 2 industrial radiography sources.

Note there were also “intangible” outcomes and these emerged over the course of the workshop. They cannot be formalised as deliverables but they include:

- networking;

- a consensus on future challenges and a shared sense of commitment to radioactive source security was established jointly and shared by participants from different sectors and institutions;
- a common understanding of future challenges was developed ensuring a collective awareness of them;
- the development of a security culture by participants. This could even result in new ways of working emerging in participating organisations;
- changed attitudes and mind sets: Participants sharing insights about long-term developments helped to orient people's thinking towards longer-term issues. This enriched their views of desirable and feasible options – and of futures to avoid – by interaction with each other; and
- the indirect integration of the workshop results into the projects, programmes, strategies and policies of national authorities, regional organisations or companies.

These will all have a positive impact on source security.

Workshop discussions and issues arising

During the workshop the following issues were considered of particular importance to source security from the perspectives of both radiation regulators and industry practitioners.

a) Agreement on satisfying the Security Level B goal

Participants acknowledged the value of the IAEA nuclear security series guidance as a comprehensive starting point to further develop and implement the requisite security measures from both regulatory and operator viewpoints. The meeting recognised that interpreting such guidance can be somewhat subjective and that the translation for use by the participants requires careful consideration. It was highlighted that the regulators are ultimately responsible for correct terminology and interpretation within their national regulatory contexts. A primary challenge for regulators and operators is to obtain substantial agreement on the operational or practical meaning of the Security Level B goal "to minimize the likelihood of unauthorized removal of a source" and to recognise when this goal has been satisfied.

b) The variable nature of the environment that industrial radiography is conducted in

Participants recognised that industrial gamma radiography operations routinely involve changing circumstances for storage and use at home base and in the field, with many movements of the device. The variety of scenarios highlights that any regulation or guidance produced should be broad, and may use a combination of the prescriptive and performance-based approaches [12]. For example, if a license condition or regulation requires a security plan to be submitted by a licensee, then the regulator may choose to specify the required contents of the security plan at a general level. Nevertheless, regulatory verification of the adequacy and effectiveness of a security plan requires that the regulator acquire, or have

access to, the requisite security knowledge, expertise and experience to perform an assessment.

c) *The frequent transport of industrial radiography sources*

The meeting recognised that the transport of industrial radiography sources is an integral part of the licensee's operations and should not be compartmentalised or considered separate for purposes of security (and safety). Therefore, security arrangements for transportation by the licensee in its own vehicles should form key elements of the licensee's operational plans and procedures. In this case, there would be no requirement for a separate transport security plan. This is reflected in the guidance on the security plan ([Appendix B](#)).

d) *The aggregation of sources in storage or transport*

Participants reviewed the possibility that aggregation of sources in storage or transport could result in a change to the higher Security Level A requirements. The consensus was that Category 2 and Security Level B is generally the appropriate classification for industrial radiography sources when aggregated in typical numbers. For companies represented at the workshop, and from knowledge of the industrial gamma radiography practices, including shared storage facilities, in the countries represented, it was determined to be very unlikely that an aggregation of industrial radiography sources would require Security Level A measures.

e) *Companies sharing access to storage facilities at field sites*

The issue of companies sharing access to storage facilities at field sites was discussed. It was considered that the access control and associated measures could be implemented in a manner that would complement the current storage controls without disrupting the operations. Industry practitioners currently exercise a high level of source and device accounting during all movements. This is considered a good example of where best safety practice in source and device control also satisfies security needs.

f) *Cross-border movements and off-shore operations*

Participants noted the particular issue of cross-border movements and off-shore operations involving industrial radiography sources licensed in one country but temporarily used in another country's territory, either offshore or onshore. This situation highlighted that regulatory control of sources - which is essential to security - would be enhanced by development and implementation of arrangements to ensure that national regulatory bodies are aware of all operations involving industrial radiography sources in their jurisdiction, especially those that occur on a temporary basis. The workshop noted that the Code of Conduct [6] and its associated Guidance on the Import and Export of Radioactive Sources [17] require that national regulatory bodies be notified of the international transfer of all Category 1 and 2 sources. The workshop recognised that regional regulators should share knowledge of the movement of sources between jurisdictions through a cooperative approach among regulators and operators within the region, in accordance with the procedures set out in the Guidance [17]. This networking and proactive regulatory interaction

will improve national and regional capabilities and consistency in implementing and sustaining Security Level B security measures.

g) *Operator implementation of security measures*

It was acknowledged that these recommended security measures are readily achievable for larger enterprises, but a concern was raised that small and medium enterprises (SMEs) may require additional support. It was agreed that further consideration must be given on how SMEs can adequately implement these security measures. Support for SMEs was encouraged particularly through professional bodies, such as the Philippines Society for Non-Destructive Testing (PSNT).

Workshop recommendations for next steps

The workshop discussed and identified the following activities for further consideration and possible actions:

National Regulatory Authorities

- a) Update to Codes of Practice, Regulations and/or Guidance based on Workshop products and IAEA guidance. This is underway in the Philippines, Malaysia, and Vietnam.
- b) Development of guidance for, and/or an example of, a security plan for Category 2 industrial radiography sources.
- c) Information outreach to licensees on requirements.

Operators / Licensees

- a) Large Enterprises (particularly those represented at the Sydney Workshop) - implementation and leading by example.
- b) NDT Associations, Societies or related professional/business groupings - promotion of best practice via education and outreach. An example of this in practice was the Philippines Society for Non-Destructive Testing presenting the outcomes and recommendations of the September Sydney workshop at their 25th Annual Convention in Manila on 19 November, 2010.
- c) Small and Medium Enterprises - training and awareness of requirements.
- d) Client companies - source security awareness seminars.

International cooperation

- a) Between national regulatory authorities, covering import/export, transit, and agreements or arrangements for notification of the temporary presence of sources within their respective jurisdictions, in accordance with the IAEA Guidance on the Import and Export of Radioactive Sources.
- b) Training courses and technical train-the-trainer programs.

- c) Development and peer review of Regulations, Codes of Practice and/or Guidance. An example of this being applied is the World Institute of Nuclear Security's¹ draft International Best Practice Guide on Security of Industrial Radiography Sources [19] which uses much of the consensus guidance from the September 2010 Sydney RSRS Project workshop, with WINS inserting in their IBPG the Industrial Radiography Security Plan Guidance that was developed ([Appendix B](#)).
- d) Licensee equipment needs assessments and upgrades.
- e) Security Plans Write-shops for Operators / Licensees.
- f) Development of public understanding of Category 2 industrial radiography sources via outreach material, including brochures and posters (with support from US GTRI and ANSTO RSRS programs).
- g) If required in future, conduct additional review meetings of progress of implementation of guidance and the next steps.
- h) The IAEA stands ready to support and assist, as requested, with efforts to secure radioactive sources.

Conclusions

This was a first of a kind workshop that addresses Security Level B in industrial practices and the workshop agreed the following outcomes from the discussions and outputs:

- a) The application of international (IAEA) guidance on the security of radioactive sources for the widespread practice of industrial gamma radiography can be readily achieved. This has implications for other practices, such as well logging.
- b) Regulatory authorities can appropriately set requirements and use a licensee's or licence applicant's Security Plan to ensure adequate and effective implementation and compliance.
- c) The draft Recommended Security Measures and the draft Guidance on the Contents of a Security Plan for Industrial Radiography developed at the Sydney Workshop form a practical and effective approach for industry practitioners and regulators to ensure and verify appropriate radioactive source security.

¹ **Role of the World Institute of Nuclear Security**

The World Institute of Nuclear Security (WINS) [18] was established to improve security of nuclear and high hazard radioactive materials from unauthorised access, theft, sabotage, diversion and being utilised for terrorist or other malicious purposes. Its mission is to provide an international forum for those accountable for nuclear security to share and promote the implementation of best security practices, primarily from an industry or user perspective. WINS produces International Best Practice Guides (IBPG) to assist radioactive source users and security practitioners to reduce the vulnerability to theft or sabotage of radioactive sources.

References

- [1] International Atomic Energy Agency, Safety Reports Series No. 13, *Radiation Protection and Safety in Industrial Radiography*, Vienna, 1999.
- [2] Philippines Nuclear Research Institute, Code of Philippines Regulations Part 11, *Licenses for Industrial Radiography and Radiation Safety Requirements for Radiographic Operations*, 2009.
- [3] Australian Radiation Protection and Nuclear Safety Agency (ARPANSA), Radiation Protection Series Publication No. 6, *National Directory for Radiation Protection*, 2011.
- [4] International Atomic Energy Agency, Proceedings of an international conference on *Security of Radioactive Sources*, Vienna, 2003.
- [5] International Atomic Energy Agency, Proceedings of an international conference on *Safety and Security of Radioactive Sources: Towards a Global System for the Continuous Control of Sources throughout Their Life Cycle*, Bordeaux, 2005.
- [6] International Atomic Energy Agency, IAEA/CODEOC/2004, *Code of Conduct on the Safety and Security of Radioactive Sources*, Vienna, 2004.
- [7] Philippines Nuclear Research Institute, Code of Philippines Regulations Part 26, *Security of Category 1 Radioactive Sources*, 2007.
- [8] International Atomic Energy Agency, IAEA-TECDOC-1355, *Security of Radioactive Sources (Interim Guidance for Comment)*, Vienna, 2003.
- [9] International Atomic Energy Agency, IAEA Safety Standards Series No. RS-G-1.9, *Categorization of Radioactive Sources*, Vienna, 2005.
- [10] Australian Radiation Protection and Nuclear Safety Agency (ARPANSA), Radiation Protection Series No. 11, *Code of Practice for Security of Radioactive Sources*, 2007.
- [11] International Atomic Energy Agency, Nuclear Security Series No. 9, *Security in the Transport of Radioactive Material*, Vienna, 2009.
- [12] International Atomic Energy Agency, Nuclear Security Series No. 11, *Security of Radioactive Sources*, Vienna, 2009.
- [13] International Atomic Energy Agency, Safety Standards Series No. RS-G-1.9, *Categorization of Radioactive Sources*, Vienna, 2005.
- [14] Australian Radiation Protection and Nuclear Safety Agency (ARPANSA), Practice Specific Security Guide 05, *Security Guidelines for Industrial Radiography*, 2008.
- [15] New South Wales Department of Premier and Cabinet, Office of Environment and Heritage (OEH), <http://www.environment.nsw.gov.au/hazmat/measures.htm>.
- [16] *Report of the South East Asia Regional Review Meeting on Radioactive Source Security*, March, 2010. Available for download from the Australian Nuclear Science and Technology Organisation website, http://www.ansto.gov.au/business_services/specialised_services/regional_security_of_radioactive_sources_project
- [17] International Atomic Energy Agency, *Guidance on the Import and Export of Radioactive Sources*, Vienna, 2005.
- [18] World Institute of Nuclear Security (WINS), www.wins.org.
- [19] World Institute of Nuclear Security (WINS), draft *Best Practice Guide on Security of Industrial Radiography Sources*, 2011.

Appendix A – Workshop Output 1 Recommended Security Measures

Appendix A - Recommended Security Measures

These recommended security measures for industrial radiography sources are based on the security objectives from IAEA NSS 11 and 9 and in the case of transport, incorporating recommendations provided by representatives of Malaysia's AELB. They are structured on

- a) use - home base and field,
- b) storage - home base and field, and
- c) transport - to and from field site.

		Home Base – Storage	Home Base - Use	Field – Storage (Short-Term < 1 week)	Field – Storage (Long-Term)	Field - Use
Security function	Security objective	Security measures and associated procedures				
Detect	Provide immediate detection of any unauthorized access to the secured area/source location	Electronic intrusion device - Balanced Magnetic Switch (BMS) and Infrared motion detector.	Enclosed: Motion detector. Operator personnel. Open/semi-enclosed: Operator personnel. Portable and/or fixed duress buttons.	Regular monitoring via personnel and/or guards. Sensor with local audio and visual alarm. In some cases the preferred alternative may be storage in a vehicle with audible alarm, near local law enforcement to facilitate prompt alarm assessment and response. Remote location: Sensor with local audio, visual alarm and a radiofrequency alarm. <i>Where measures are not feasible prohibit use or allow with limitations, i.e. cannot store sources there or case by case justification to modify measures. Requires regulatory judgement based on operator argument.</i>	Regular monitoring via personnel and/or guards. Sensor with local audio and visual alarm. Remote location: Sensor with local audio, visual alarm and a radiofrequency alarm.	Operator personnel. Laser-beam perimeter motion detector – “trip wire”.

**Appendix A – Workshop Output 1
Recommended Security Measures**

		Home Base – Storage	Home Base - Use	Field – Storage (Short-Term < 1 week)	Field – Storage (Long-Term)	Field - Use
Security function	Security objective	Security measures and associated procedures				
	Provide detection of any attempted unauthorized removal of the source	Tamper indicative device on the: - transport container. - storage area access door. Assessed via verification.	Operator personnel.	Tamper indicative device on the: - transport container. - storage area access door. Assessed via verification.	Tamper indicative device on the: - transport container. - storage area access door. Assessed via verification.	Continuous monitoring by operator personnel.
	Provide immediate assessment of detection	Continuous monitoring of CCTV.	Operator personnel physically attend.	Client company guards and/or operator personnel (for small projects).	Client company guards and/or operator personnel (for small projects).	Client company guards and/or operator personnel.
	Provide immediate communication to response personnel	Radio, landline and mobile phone.	Radio, landline and mobile phone.	Mobile phone, radio and satellite phone.	Mobile phone, radio and satellite phone.	Mobile phone, radio and satellite phone.
	Provide a means to detect loss through verification	Daily monitoring via dose rate survey on device. Completion of home log book for source use (in & out).	Daily monitoring via dose rate survey on device. Completion of home log book for source use (in & out).	Daily monitoring via dose rate survey on device. Completion of field log book for source use (in & out). Liaison with home base.	Daily monitoring via dose rate survey on device. Completion of field log book for source use (in & out). Liaison with home base.	Conduct background dose rate survey before and after source is present. Dose rate survey on device before and after conducting task.

**Appendix A – Workshop Output 1
Recommended Security Measures**

		Home Base – Storage	Home Base - Use	Field – Storage (Short-Term < 1 week)	Field – Storage (Long-Term)	Field - Use
Security function	Security objective	Security measures and associated procedures				
Delay	Provide delay to minimize the likelihood of unauthorized removal	Storage room with at least two independent barriers. Security locks. *Exposure room might be used as Storage room.	Exposure room* with at least two independent barriers. Security locks. Open/semi-enclosed: operator intervention. *Exposure room might be used as Storage room.	Storage room (large projects), an improvised container - “bolt down” - or a vehicle (small projects). Each may have shared access. Security locks.	Permanent storage area provided by client, typically shared access. Security locks.	Retract source to a shielded position (<10s). Operator intervention.
Response	Provide immediate initiation of response to interrupt unauthorized removal	Arrangements with police or “designated response agency”.	Arrangements with police or “designated response agency”.	Arrangements with police or “designated response agency”.	Arrangements with police or “designated response agency”.	Arrangements with police or “designated response agency”. On-site project management team. Additionally for remote areas local administration.

**Appendix A – Workshop Output 1
Recommended Security Measures**

		Home Base – Storage	Home Base - Use	Field – Storage (Short-Term < 1 week)	Field – Storage (Long-Term)	Field - Use
Security function	Security objective	Security measures and associated procedures				
Security management	Provide access controls to source location that effectively restrict access to authorized persons only	Electronic keypad with code to storage room. Site-pass.	Dedicated exposure room: Operator surveillance, if possible with key control via log book. Site-pass with permission to access keys. Open/semi-enclosed: operator intervention.	Key control via log book to authorized persons. Separate storage areas & keys when in shared access.	Key control via log book to authorized persons. Separate storage areas & keys when in shared access.	Operator intervention. Work Permit. ID card. Large project: Client company security.
	Ensure trustworthiness of authorized individuals	Regulatory requirements implemented by Company. Process included in the Security Plan. - Check CV. - Interview. - ID card. - Background check with Police clearance. - On job training and supervision.	Regulatory requirements implemented by Company. Process included in the Security Plan. - Check CV. - Interview. - ID card. - Background check with Police clearance. - On job training and supervision.	Regulatory requirements implemented by Company. Process included in the Security Plan. - Check CV. - Interview. - ID card. - Background check with Police clearance. - On job training and supervision.	Regulatory requirements implemented by Company. Process included in the Security Plan. - Check CV. - Interview. - ID card. - Background check with Police clearance. - On job training and supervision.	Regulatory requirements implemented by Company. Process included in the Security Plan. - Check CV. - Interview. - ID card. - Background check with Police clearance. - On job training and supervision.

**Appendix A – Workshop Output 1
Recommended Security Measures**

		Home Base – Storage	Home Base - Use	Field – Storage (Short-Term < 1 week)	Field – Storage (Long-Term)	Field - Use
Security function	Security objective	Security measures and associated procedures				
	Identify and protect sensitive information	Sensitive information defined in the Security Plan. - source protection measures - access controls	Location of devices – types of isotopes, amount present. Security plan. Response plan.		Transportation route	Location of devices – types of isotopes, amount present. Security plan. Response plan.
	Provide a security plan		Making radioactive source security programs and evaluation programs.			Field operator has working procedure and work permit at job. Security briefing. Assessment and incorporation of local threat.
	Ensure a capability to manage security events covered by security contingency plans					
	Establish security event reporting system					

**Appendix A – Workshop Output 1
Recommended Security Measures**

Destination	Import (origin to arrival destination)	Arrival to Home Base	Home Base to Field Storage to Use Site	Export (end user to origin)
Elements	Transport Security Measures			
Procedure	Follow Import Guideline Base on Source Category Permit Authorization Record (training & emergency)	Approval/Notification provided to Regulatory Body Record (training & emergency)	Approval/Notification provided to Regulatory Body (Movement)	Follow Export Guideline Permit Authorization Record (training & emergency)
Vehicle	Follow Transport Safety Guideline Legally Registered Log Book Transportation Handbook with emergency contacts Closed vehicle Security Lock Break In Sensor – Local Alarm Vehicle Tracking System (If applicable) – “GPS”	Follow Transport Safety Guideline Legally Registered Log Book Transportation Handbook with emergency contacts Closed vehicle Security Lock Break In Sensor – Local Alarm Vehicle Tracking System (If applicable) – “GPS”	Follow Transport Safety Guideline Legally Registered Log Book Transportation Handbook with emergency contacts Closed vehicle Security Lock Break In sensor – Local Alarm Vehicle Tracking System (If applicable) – “GPS”	Follow Transport Safety Guideline Legally Registered Log Book Transportation Handbook with emergency contacts Closed vehicle Security Lock Break In Sensor – Local Alarm Vehicle Tracking System (If applicable) – “GPS”
Sources	Manufacturers Certified Packaging	Manufacturers Certified Packaging	Manufacturers Certified Packaging	Manufacturers Certified Packaging
Personnel present	RPO Driver Background Check. Vehicle has continuous personnel. Security Awareness training. All personnel must carry positive ID.	RPO/Authorized Worker Driver Background Check Vehicle has continuous personnel Security Awareness training All personnel must carry positive ID.	RPO/Authorized Worker Background Check Vehicle has continuous personnel Security Awareness training All personnel must carry positive ID.	RPO Driver Background Check Vehicle has continuous personnel Security Awareness training All personnel must carry positive ID.
Communication	Fax/E-mail Point of Contact Regular reporting as specified in travel plan.	Sufficient Mobile Phone/Walkie- talkie Point of Contact Regular reporting as specified in travel plan.	Sufficient Mobile Phone/Walkie- talkie Point of Contact Regular reporting as specified in travel plan.	Fax/e-mail Point of Contact Regular reporting as specified in travel plan.

**Appendix A – Workshop Output 1
Recommended Security Measures**

Destination	Import (origin to arrival destination)	Arrival to Home Base	Home Base to Field Storage to Use Site	Export (end user to origin)
Elements	Transport Security Measures			
Routing	Airway bill/Bill of Laden Transit/Transshipment ETA	Distance Routing Details (street/highway/alternative way) – a Travel Plan Cross border considerations.	Distance Routing Details (street/highway/alternative way) – a Travel Plan Cross border considerations.	Airway bill/Bill of Laden Transit/Transshipment ETD
Contingency Plan	Relevant Authorities Port/Airport Authorities Airliner Shipping Line Include specific security incident instructions.	Identifies - Regulatory Body - Police - Fire & Rescue Dept - National Security Council Include specific security incident instructions.	Identifies - Regulatory Body - Police - Fire & Rescue Dept - National Security Council - Local Administration Include specific security incident instructions.	Relevant Authorities Port/Airport Authorities Airliner Shipping Line Include specific security incident instructions.

**Appendix B – Workshop Output 2
Industrial Radiography Security Plan Guidance**

Appendix B - Industrial Radiography Security Plan Guidance

Guidance on the Contents of a Security Plan for Industrial Radiography (Security Level B) Practices

SUMMARY

This document provides an example of the structure, contents, and guidance in developing a security plan for the practices involved in industrial gamma radiography following international (IAEA) guidance and best practice from industry practitioners.

A security plan should include all information necessary to describe the security approach and system being used for protection of the source(s). The level of detail and depth of content should be commensurate with the security level of the source(s) covered by the plan.

This guidance document has been produced as part of the Security Level B (industrial radiography practices) workshop held for several South East Asia countries in Sydney, 6-10 September 2010. A full report of the workshop is available^f.

CONTENTS

1. Purpose and scope
2. Operations
3. Security Management
4. Home Base - General
5. Home Base - Storage
6. Home Base - Use
7. Field - General
8. Field - Storage (Short-Term < 1 week)
9. Field - Storage (Long-Term)
10. Field - Use
11. Transport

^f for a copy of the Workshop report, e-mail Allan Murray at amu@ansto.gov.au

Appendix B – Workshop Output 2
Industrial Radiography Security Plan Guidance

**GUIDANCE ON THE CONTENTS OF A SECURITY PLAN FOR INDUSTRIAL
RADIOGRAPHY (SECURITY LEVEL B) PRACTICES**

The security plan should include all information necessary to document the licensee's security approach and system for protection of the source(s), in compliance with applicable regulatory requirements.

The following topics should typically be included:

1. Purpose and scope

- 1.1. Cover the security of radioactive sources throughout their lifecycle under the control of the licensee, including in use and storage at home base and field base, as well as transport by the licensee.

2. Operations

- 2.1. Describe the nature of the licensee's specific operations, including the geographic extent of the business, the uses to which industrial radiography sources are put, the types and numbers of industrial radiography devices employed, overall business volume, and in general terms the locations where the company uses, stores, or transports industrial radiography devices.

3. Security Management

- 3.1. The overall objectives of the security plan for the company, including:
- a) the specific concern to be addressed: unauthorized removal, destruction, or malevolent use;
 - b) the kind of control needed to prevent undesired consequences, including the auxiliary equipment that might be needed;
 - c) the practices that require security measures.
- 3.2. The security management measures to be used, including:
- a) the security roles and responsibilities of management, staff and others;
 - b) methods for access authorization;
 - c) key (fundamental) control procedures;
 - d) determination of the trustworthiness of personnel;
 - e) information security;
 - f) accounting procedures for the source(s);
 - g) maintenance and testing of equipment;
 - h) Quality Assurance Program and Quality Control;
 - i) integration with radiation protection;
 - j) security-related aspects of the emergency plan;
 - k) contingency planning;
 - l) event reporting;
 - m) training; and
 - n) procedures for regular review and updating of the security plan, including conducting tests and exercises of the effectiveness of the security.
- 3.3. Relevant threat information provided by regulatory authorities.
- 3.4. The procedure to address increased threat level.

Appendix B – Workshop Output 2
Industrial Radiography Security Plan Guidance

- 3.5. Any compensatory measures that may need to be used.
- 3.6. References to existing regulations or standards. The security plan should be in conformance with national regulations and document compliance.

4. Home Base - General

- 4.1. Note: the guidance below assumes a separate exposure and storage room is employed. This may be changed if it does not represent the company circumstances.
- 4.2. The objectives of the security plan for the company home base, including:
 - a) the equipment or premises that will be secured;
 - b) site specific security considerations; and
 - c) site threat environment.
- 4.3. A description of license parameters, with a reference to an inventory document which includes a description of each source, categorization, and operations.
- 4.4. A description of the environment, building and/or facility where each source is used or stored, and if appropriate a diagram of the facility layout and security system.
- 4.5. The location of the building or facility relative to areas accessible to the public.

5. Home Base - Storage

- 5.1. State how sources are stored at the specific building or facility.
- 5.2. The objectives of the security plan for the specific building or facility, including:
 - a) the specific concern to be addressed: unauthorized removal, destruction, or malevolent use;
 - b) the kind of control needed to prevent undesired consequences, including the auxiliary equipment that might be needed; and
 - c) the equipment or premises that will be secured.
- 5.3. The security measures and associated procedures to be used, including:
 - a) the measures – people, equipment and procedures - to secure, provide surveillance, provide access control, detect, delay, respond and communicate; and
 - b) the design features to evaluate the quality of the measures against the assumed threat.
- 5.4. The summary table below is included as an example. It should reference security management arrangements (people, equipment and procedures) described in the security management section of the plan (section 3).

Security function	Security objective	Security measures and associated procedures Home Base - Storage
Detect	Provide immediate detection of any unauthorized access to the secured area/source location	Electronic intrusion device - Balanced Magnetic Switch (BMS) and Infrared motion detector.

**Appendix B – Workshop Output 2
Industrial Radiography Security Plan Guidance**

Security function	Security objective	Security measures and associated procedures Home Base - Storage
	Provide detection of any attempted unauthorized removal of the source	Tamper indicative device on the: - transport container. - storage area access door. Assessed via verification.
	Provide immediate assessment of detection	Continuous monitoring of CCTV.
	Provide immediate communication to response personnel	Radio, landline and mobile phone.
	Provide a means to detect loss through verification	Daily monitoring via dose rate survey on device. Completion of home log book for source use (in & out).
Delay	Provide delay to minimize the likelihood of unauthorized removal	Storage room with at least two independent barriers. Security locks. *Exposure room might be used as Storage room.
Response	Provide immediate initiation of response to interrupt unauthorized removal	Arrangements with police or “designated response agency”.

**Appendix B – Workshop Output 2
Industrial Radiography Security Plan Guidance**

6. Home Base - Use

- 6.1. Note: the guidance below assumes that home base use occurs. This section may be removed if it does not represent the company circumstances.
- 6.2. State how sources are used at the specific building or facility, including a description of each source, categorization, and operations.
- 6.3. The objectives of the security plan for the specific building or facility, including:
- a) the specific concern to be addressed: unauthorized removal, destruction, or malevolent use;
 - b) the kind of control needed to prevent undesired consequences including the auxiliary equipment that might be needed; and
 - c) the equipment or premises that will be secured.
- 6.4. The security measures and associated procedures to be used, including:
- a) the measures – people, equipment and procedures - to secure, provide surveillance, provide access control, detect, delay, respond and communicate; and
 - b) the design features to evaluate the quality of the measures against the assumed threat.
- 6.5. The summary table below is included as an example. It should reference security management arrangements (people, equipment and procedures) described in the security management section of the plan (section 3).

Security function	Security objective	Security measures and associated procedures Home Base - Use
Detect	Provide immediate detection of any unauthorized access to the secured area/source location	Enclosed: Motion detector. Operator personnel. Open/semi-enclosed: operator personnel. Portable and/or fixed duress buttons.
	Provide detection of any attempted unauthorized removal of the source	Operator personnel.
	Provide immediate assessment of detection	Operator personnel physically attend.
	Provide immediate communication to response personnel	Radio, landline and mobile phone.
	Provide a means to detect loss through verification	Daily monitoring via dose rate survey on device. Completion of home log book for source use (in & out).
Delay	Provide delay to minimize the likelihood of unauthorized removal	Exposure room* with at least two independent barriers. Security locks. Open/semi-enclosed: operator intervention. *Exposure room might be used as Storage room.

Appendix B – Workshop Output 2
Industrial Radiography Security Plan Guidance

Security function	Security objective	Security measures and associated procedures Home Base - Use
Response	Provide immediate initiation of response to interrupt unauthorized removal	Arrangements with police or “designated response agency”.

Appendix B – Workshop Output 2
Industrial Radiography Security Plan Guidance

7. Field - General

- 7.1. Note: the guidance below assumes a separate storage facility for short term (less than 1 week) storage and long term storage. This may be changed if it does not represent the company circumstances.
- 7.2. The objectives of the security plan for source use and storage in the field, including:
- a) the equipment or premises that will be secured;
 - b) site specific security considerations; and
 - c) site threat environment.
- 7.3. A description of license parameters, with a reference to inventory document which includes a description of each source, categorization, and operations.
- 7.4. A basic description of the types of sites at which operations are conducted.
- 7.5. A description of the environment, building, facility, and/or work area where each source is used or stored, and if appropriate a diagram of the facility/work area layout and security system.
- 7.6. The location of the building, facility or work area relative to areas accessible to the public.

8. Field - Storage (Short-Term < 1 week)

- 8.1. The objectives of the security plan for the specific building, facility, work area or vehicle, including:
- a) the specific concern to be addressed: unauthorized removal, destruction, or malevolent use;
 - b) the kind of control needed to prevent undesired consequences including the auxiliary equipment that might be needed; and
 - c) the equipment or premises that will be secured.
- 8.2. The security measures and associated procedures to be used, including:
- a) the measures – people, equipment and procedures - to secure, provide surveillance, provide access control, detect, delay, respond and communicate; and
 - b) the design features to evaluate the quality of the measures against the assumed threat.
- 8.3. The summary table below is included as an example. It should reference security management arrangements (people, equipment and procedures) described in the security management section of the plan (section 3).

Appendix B – Workshop Output 2
Industrial Radiography Security Plan Guidance

Security function	Security objective	Security measures and associated procedures Field – Storage (Short-Term < 1 week)
Detect	Provide immediate detection of any unauthorized access to the secured area/source location	Regular monitoring via personnel and/or guards. Sensor with local audio and visual alarm. In some cases the preferred alternative may be storage in a vehicle with audible alarm, near local law enforcement to facilitate prompt alarm assessment and response. Remote location: Sensor with local audio, visual alarm and a radiofrequency alarm. <i>Where measures are not feasible prohibit use or allow with limitations, i.e. cannot store sources there or case by case justification to modify measures.</i> <i>Requires regulatory judgement based on operator argument.</i>
	Provide detection of any attempted unauthorized removal of the source	Tamper indicative device on the: - transport container. - storage area access door. Assessed via verification.
	Provide immediate assessment of detection	Client company guards and/or operator personnel (for small projects).
	Provide immediate communication to response personnel	Mobile phone, radio and satellite phone.
	Provide a means to detect loss through verification	Daily monitoring via dose rate survey on device. Completion of field log book for source use (in & out). Liaison with home base.
Delay	Provide delay to minimize the likelihood of unauthorized removal	Storage room (large projects), an improvised container - "bolt down" - or a vehicle (small projects). Each may have shared access. Security locks.
Response	Provide immediate initiation of response to interrupt unauthorized removal	Arrangements with police or "designated response agency".

Appendix B – Workshop Output 2
Industrial Radiography Security Plan Guidance

9. Field - Storage (Long-Term)

- 9.1. The objectives of the security plan for the specific building or facility, including:
- a) the specific concern to be addressed: unauthorized removal, destruction, or malevolent use;
 - b) the kind of control needed to prevent undesired consequences including the auxiliary equipment that might be needed; and
 - c) the equipment or premises that will be secured.
- 9.2. The security measures and associated procedures to be used, including:
- a) the measures – people, equipment and procedures - to secure, provide surveillance, provide access control, detect, delay, respond and communicate; and
 - b) the design features to evaluate the quality of the measures against the assumed threat.
- 9.3. The summary table below is included as an example. It should reference security management arrangements (people, equipment and procedures) described in the security management section of the plan (section 3).

Security function	Security objective	Security measures and associated procedures Field – Storage (Long-Term)
Detect	Provide immediate detection of any unauthorized access to the secured area/source location	Regular monitoring via personnel and/or guards. Sensor with local audio and visual alarm. Remote location: Sensor with local audio, visual alarm and a radiofrequency alarm.
	Provide detection of any attempted unauthorized removal of the source	Tamper indicative device on the: - transport container. - storage area access door. Assessed via verification.
	Provide immediate assessment of detection	Client company guards and/or operator personnel (for small projects).
	Provide immediate communication to response personnel	Mobile phone, radio and satellite phone.
	Provide a means to detect loss through verification	Daily monitoring via dose rate survey on device. Completion of field log book for source use (in & out). Liaison with home base.
Delay	Provide delay to minimize the likelihood of unauthorized removal	Permanent storage area provided by client, typically shared access. Security locks.
Response	Provide immediate initiation of response to interrupt unauthorized removal	Arrangements with police or “designated response agency”.

Appendix B – Workshop Output 2
Industrial Radiography Security Plan Guidance

10. Field - Use

- 10.1. The objectives of the security plan for the specific building, facility or work area, including:
- a) the specific concern to be addressed: unauthorized removal, destruction, or malevolent use;
 - b) the kind of control needed to prevent undesired consequences including the auxiliary equipment that might be needed; and
 - c) the equipment or premises that will be secured.
- 10.2. The security measures and associated procedures to be used, including:
- a) the measures – people, equipment and procedures - to secure, provide surveillance, provide access control, detect, delay, respond and communicate; and
 - b) the design features to evaluate the quality of the measures against the assumed threat.
- 10.3. The summary table below is included as an example. It should reference security management arrangements (people, equipment and procedures) described in the security management section of the plan (section 3).

Security function	Security objective	Security measures and associated procedures Field - Use
Detect	Provide immediate detection of any unauthorized access to the secured area/source location	Operator personnel. Laser-beam perimeter motion detector – “trip wire”.
	Provide detection of any attempted unauthorized removal of the source	Continuous monitoring by operator personnel.
	Provide immediate assessment of detection	Client company guards and/or operator personnel.
	Provide immediate communication to response personnel	Mobile phone, radio and satellite phone.
	Provide a means to detect loss through verification	Conduct background dose rate survey before and after source is present. Dose rate survey on device before and after conducting task.
Delay	Provide delay to minimize the likelihood of unauthorized removal	Retract source to a shielded position (<10s). Operator intervention.
Response	Provide immediate initiation of response to interrupt unauthorized removal	Arrangements with police or “designated response agency”. On-site project management team. Additionally for remote areas local administration.

Appendix B – Workshop Output 2
Industrial Radiography Security Plan Guidance

11. Transport

- 11.1. A basic description of the transport operations conducted by the licensee.
- 11.2. The objectives of the security plan for transport, including:
- a) the specific concern to be addressed: unauthorized removal, destruction, or malevolent use;
 - b) the kind of control needed to prevent undesired consequences including the auxiliary equipment that might be needed; and
 - c) the equipment, premises or vehicle that will be secured.
- 11.3. The transport security management measures to be used, including:
- a) Specific allocation of responsibilities for security to competent and qualified persons with appropriate authority to carry out their responsibilities;
 - b) Provision for keeping records of radioactive material packages or types of radioactive material transported;
 - c) Review of current operations and assessment of vulnerability, including intermodal transfer, storage in transit, handling and distribution as appropriate;
 - d) Effective procedures and equipment for timely reporting and dealing with security related threats, breaches of security or security related incidents;
 - e) Procedures for evaluating and testing security plans and procedures for periodic review and update of the plans;
 - f) Measures to ensure the security of transport information contained in the security plan;
 - g) Measures to ensure that the distribution of sensitive transport information is limited, to maintain security of the information. Such measures should not preclude the provision of transport documents and consignor's declaration as required by TS-R-1;
 - h) Measures to monitor the location of the shipment; and
 - i) Where appropriate, details concerning agreements on the point of transfer of responsibility for security.
- 11.4. The security measures and associated procedures to be used, including:
- a) the measures – people, equipment and procedures - to secure, provide surveillance, provide access control, detect, delay, respond and communicate;
 - b) the design features to evaluate the quality of the measures against the assumed threat.
- 11.5. The summary table below is included as an example. It should reference security management arrangements (people, equipment and procedures) described in the security management section of the plan (section 3).

**Appendix B – Workshop Output 2
Industrial Radiography Security Plan Guidance**

Destination	Import (origin to arrival destination)	Arrival to Home Base	Home Base to Field Storage to Use Site	Export (end user to origin)
Elements	Transport Security Measures			
Procedure	Follow Import Guideline Base on Source Category Permit Authorization Record (training & emergency)	Approval/Notification provided to Regulatory Body Record (training & emergency)	Approval/Notification provided to Regulatory Body (Movement)	Follow Export Guideline Permit Authorization Record (training & emergency)
Vehicle	Follow Transport Safety Guideline Legally Registered Log Book Transportation Handbook with emergency contacts Closed vehicle Security Lock Break In Sensor – Local Alarm Vehicle Tracking System (If applicable) – “GPS”	Follow Transport Safety Guideline Legally Registered Log Book Transportation Handbook with emergency contacts Closed vehicle Security Lock Break In Sensor – Local Alarm Vehicle Tracking System (If applicable) – “GPS”	Follow Transport Safety Guideline Legally Registered Log Book Transportation Handbook with emergency contacts Closed vehicle Security Lock Break In sensor – Local Alarm Vehicle Tracking System (If applicable) – “GPS”	Follow Transport Safety Guideline Legally Registered Log Book Transportation Handbook with emergency contacts Closed vehicle Security Lock Break In Sensor – Local Alarm Vehicle Tracking System (If applicable) – “GPS”
Sources	Manufacturers Certified Packaging	Manufacturers Certified Packaging	Manufacturers Certified Packaging	Manufacturers Certified Packaging
Personnel present	RPO Driver Background Check. Vehicle has continuous personnel. Security Awareness training. All personnel must carry positive ID.	RPO/Authorized Worker Driver Background Check Vehicle has continuous personnel Security Awareness training All personnel must carry positive ID.	RPO/Authorized Worker Background Check Vehicle has continuous personnel Security Awareness training All personnel must carry positive ID.	RPO Driver Background Check Vehicle has continuous personnel Security Awareness training All personnel must carry positive ID.
Communication	Fax/E-mail Point of Contact Regular reporting as specified in travel plan.	Sufficient Mobile Phone/Walkie- talkie Point of Contact Regular reporting as specified in travel plan.	Sufficient Mobile Phone/Walkie- talkie Point of Contact Regular reporting as specified in travel plan.	Fax/e-mail Point of Contact Regular reporting as specified in travel plan.

**Appendix B – Workshop Output 2
Industrial Radiography Security Plan Guidance**

Destination	Import (origin to arrival destination)	Arrival to Home Base	Home Base to Field Storage to Use Site	Export (end user to origin)
Elements	Transport Security Measures			
Routing	Airway bill/Bill of Laden Transit/Transshipment ETA	Distance Routing Details (street/highway/alternative way) – a Travel Plan Cross border considerations.	Distance Routing Details (street/highway/alternative way) – a Travel Plan Cross border considerations.	Airway bill/Bill of Laden Transit/Transshipment ETD
Contingency Plan	Relevant Authorities Port/Airport Authorities Airliner Shipping Line Include specific security incident instructions.	Identifies - Regulatory Body - Police - Fire & Rescue Dept - National Security Council Include specific security incident instructions.	Identifies - Regulatory Body - Police - Fire & Rescue Dept - National Security Council - Local Administration Include specific security incident instructions.	Relevant Authorities Port/Airport Authorities Airliner Shipping Line Include specific security incident instructions.