THE DEVELOPMENT OF THE SUPPORTING INFRASTRUCTURE FOR IMPROVED NUCLEAR AND RADIOLOGICAL MATERIAL SECURITY

A REPORT BY THE WORLD INSTITUTE FOR NUCLEAR SECURITY (WINS)

Presented to:	Nuclear Security Governance Experts Group Workshop on Improving Nuclear Security Regime Cohesion ASAN Institute, Seoul, Republic of Korea
Presented by:	WORLD INSTITUTE FOR NUCLEAR SECURITY – WINS Mr. Steven Lee Graben 19, 1010 Vienna, Austria
Date of the report:	18 July 2012

Steven Lee
Head of International Affairs

18 July 2012

OUR VISION

To help improve security of nuclear and high hazard radioactive materials so that they are secure from unauthorised access, theft, sabotage and diversion and cannot be utilised for terrorist or other nefarious purposes.

OUR MISSION

To provide an international forum for those accountable for nuclear security to share and promote the implementation of best security practices.

INTRODUCTION

Certain infrastructures are needed for the development and improvement of the nuclear security regime. To identify what they are, we have to first identify key issues surrounding the current nuclear security regime, how it can be improved to strengthen regulation and innovate improvement among those accountable for nuclear security, and propose a form of accreditation to improve and sustain the necessary improvements for the achievement of an effective nuclear security. A large part of this is also about addressing the underlying barriers and issues that influence attitudes towards security. These factors are important both at the level of the State and in nuclear organisations within the State. The most important factors are considered to be, whether:

1. adequate international guidance exists on the *practical implementation of effective nuclear security*

2. States and nuclear organisations *perceive the threat from nuclear terrorism as credible* (security culture) and are motivated/obliged to *implement a minimum design basis threat*

3. *accountability for nuclear security*, between the State authorities, Regulators, Police and Operators (security governance) has been *clearly defined and implemented*

4. *the State encourages peer review, the sharing of best practices and the establishment of security metrics* as methods to help benchmark and improve their nuclear security

5. market mechanisms and *incentives are available to encourage effective nuclear security*, including a linkage between security effectiveness and insurance cover for acts of terrorism

6. *unnecessary secrecy* surrounds nuclear security which *inhibits adequate communication, cooperation and shared learning* (a lack of communication and public accountability)

7. *personnel with accountabilities* for nuclear security (including senior management roles) have access to properly designed and *accredited professional development for security management, and know what questions to ask.*

These issues are interlinked and share mutual dependencies; if people in authority are not aware of the issues, are confused about accountabilities and believe that security performance should not be discussed outside the organisation, they are not likely to believe in peer review, benchmarking and communicating with external stakeholders, preferring instead to avoid discussion of security issues in the hope that "nothing happens." In short, Nuclear Security Governance will be weak or non-existent at the level of the Board and amongst senior executive managers.

The inter-linkages between these factors can be depicted in many ways, but they need to be addressed simultaneously to have the desired effect of improving the effectiveness of nuclear security, worldwide. As such, they provide the framework for this paper. (Appendix A contains a diagram that illustrates these seven areas.) There are many stakeholders that can contribute to these efforts including governments, international organisations such as the IAEA, Institutes such as WINS, and other organisations, including those operators that understand the need for effective security and are prepared to set an example for others to follow.

IMPLEMENTATION OF, AND BARRIERS TO, APPROPRIATE AND EFFECTIVE NUCLEAR SECURITY ARRAGNEMENTS

Since 2001, the International Atomic Energy Agency (IAEA) began to mirror their well-established safety guidance and recommendations with a suite of documents that address nuclear security implementation, as part of their nuclear security programme. However, long before 2001, the IAEA had established overarching nuclear security recommendations through a number of mechanisms including the Convention on the Physical Protection of Nuclear Material (CPPNM), which is the only internationally legally binding undertaking in the area of physical protection of nuclear material. Underpinning the Convention is the IAEA's guidance document The Physical Protection of Nuclear Material and Nuclear Facilities (INFCIRC/225) which has long been considered the internationally accepted "standard" for nuclear physical protection and the practical complement to the Convention on the Physical Protection of Nuclear Material. It is important to note that it is not a legally binding instrument, but it is given legally binding effect in some bilateral nuclear safeguards agreements that prescribe INFCIRC/225 as the "standard" to be applied to nuclear material supplied under such agreements.

INFCIRC/225 (Revision 5) identifies those responsibilities placed on Operators for nuclear security, by providing a list of "what" Operators should do, but it omits the "how." Generally, the "how" is much more complicated and will be the determining factor in whether attempted attacks are successful. In some respects the "how" is being partially addressed by the IAEA in a series of Implementing Guides, but the majority of them are written for the benefit of States or State-agencies such as regulators, police, border guards or postal workers and are narrative rather than performance based. Generally, they do not identify Best Practices or Metrics that can be easily applied to operators, and do not raise the issue of beliefs and culture in a way that is likely to generate changed attitudes amongst senior management.

Conversely, the WINS Best Practice Guides take on the perspective of the Operator/Licensee and focus on the "how" and address issues that have been raised by the nuclear security community. From WINS' experience, we have learned that any guides that are expected to be used by practitioners need to be clear, concise and add value. They should also be specifically designed to begin to introduce the concept of self-assessment, benchmarking and performance standards amongst the nuclear security community. This stands in contrast to the IAEA documents which provide a mixture of generalised recommendations to Operators and State entities.

A top analysis of the subject matter overall concludes that the IAEA and WINS provide comprehensive guidance on a broad range of security related issues that are "requirements" under INFCIRC/225 Rev5. Having said that, WINS is conscious of the fact that much of the guidance is based on a Western approach to management and control and that regional culture and associated management styles are generally absent from international guidance. For example, in Western countries, optimum security arrangements almost certainly use a mixture of human and technical means; e.g. manned guarding supported by high technology intruder detection systems, sensors, cameras, etc. In countries where labour is cheap, it may be more cost effective and realistic to deploy much larger numbers of guards rather than making investments in technology. Another example could be the way that decisions are taken and whether learning from experience and the reporting of security failures or weaknesses is culturally acceptable. Rather than continue to believe that the Western style guidance is "always applicable" it would be interesting to conduct a gap analysis between what is considered best practice and the cultural obstacles to it working in different regions of the world; this could both identify improved ways to help implement "best practice" or identify equally valid and effective systems that are more acceptable to local cultures.

This issue raises the important question of beliefs and culture; what do different societies and countries believe is the risk of terrorism involving nuclear and radioactive materials? Some would argue that the threat

of terrorism is closely correlated to whether a country's foreign policies align with those of the US and others that are engaged with global anti-terrorism programmes and who are perceived as the target for terrorist action. Others would argue that some countries fail to understand potential threats from domestic terrorism, and some fail to see any linkage between domestic corruption and the scope for the misuse of nuclear and radioactive materials. Whatever the cases may be, this is a relevant factor affecting security investment and performance, since a key issue affecting worldwide implementation of effective security measures is the difference in the perception of risk and threat assessment.

DESIGN BASIS THREAT TO ENCOURAGE EFFECTIVE IMPLEMENTATION OF NUCLEAR SECURITY

It would seem as though there are structural and legal problems with government officials unilaterally defining the threat when they are generally free from prosecution in the event of an incident and for the main part do not own the assets or the liabilities in the event of an underestimated threat. For these reasons, governments officials with these accountabilities need to educate Boards and related oversight organisations that the Boards (in private companies) and oversight committees (in government owned organisations) need to take a proactive attitude to threat assessment in order to protect their assets. They need to make clear that the State assessment is imprecise but that a minimum DBT should be implemented by the Boards.

The DBT should be thought about as the "residual" threat after the efficacy of border controls and State intelligence systems are taken into account. Moreover, States and Licensees should agree on the credible, residual, national DBT and agree that it should be legally binding between them; i.e. the Licensee must be able to defend against the threat for a defined period of time, until reinforcements arrive, but if the threat which materialises is larger than agreed, the Licensee should be indemnified against legal actions stemming from the attack. This would seem equitable and a positive way forward. Most "advanced" States might assess that the residual threat might comprise a number of individuals operating in 2 groups, armed and with explosives, etc, and this should become the international minimum DBT to be applied to all relevant facilities. Clearly, in dysfunctional States, the size of the attacking force and its ability to go undetected would be larger.

There are other components of the DBT that need to be included and which currently are frequently lacking; a gap exists. These include a DBT for cyber security, which defines the type and scale of attack and the capability and objectives of the attacker. Again, this should be discussed between State regulators, specialist technical advisers and the licensees so that there is a shared understanding of the risks and action necessary. It must also be the case that the nuclear industry sees equity in the DBTs as they are applied to the critical national infrastructure (CNI) and the potential consequences to society from an attack on any part of the CNI.

MARKET INCENTIVES AS INNOVATIVE IDEA TO ENCOURAGE EFFECTIVE IMPLEMENTATION OF NUCLEAR SECURITY

The cost of security is a key consideration in the acceptance of threat assessments, DBTs and their implementation. All too often, there is no financial consideration when threat assessments are discussed. All too often, organisations do not know how much they spend on different aspects of their security programme and which components provide the best value for money. All too often, the hidden costs of security (such as access delays) are not factored into the true costs of implementing security. This calls for a new approach to security implementation in which a better financial understanding of security is established through proper analysis. Boards and CEOs are much more likely to be able to assess the cost benefits of a security programme if it is properly costed and prioritised.

For example, in respect of the physical protection and guarding arrangements, the typical cost of an effective security regime, able to withstand a minimum DBT attack force for an appropriate time, is in the order of 2.5 –

5.0% of annual operating costs for a reactor site and rather less for category 2/3 fuel cycle facilities. Most Boards do not know this and have never thought about it. If they did, most would probably agree that the level of expenditure to provide high security assurance would be a good investment to avoid legal liability issues for the organisation and them personally. It would be more attractive still, if the agreed DBT came with a legal obligation to meet it and indemnity for the organisation if the residual threat had been mismanaged by the government.

Since the perception of risk is also about a perception of cost to put in place the necessary measures, it is important to raise the issue of how to incentivise operators to implement effective security arrangements. It is important to realise that market incentives have the power to improve nuclear security by making attractive the adoption of costly security and infrastructure improvements.

The nuclear industry is one of the most highly regulated industries in the world. Expecting nuclear organisations to voluntarily adopt additional security measures is not particularly realistic. This is especially true for privately owned organisations whose fundamental obligation is to protect shareholders' assets. In a highly competitive nuclear energy sector with volatile equity markets, businesses are under extreme pressure to cut overhead costs. In this context, additional, expensive and time-consuming voluntary security measures are difficult to justify. A possible solution to this dilemma is to use market mechanisms such as insurance as an incentive for voluntary implementation of best security practices.

Insurance increases an organisation's resilience by providing a funding mechanism for recovery from catastrophic losses; it also reduces the need for government financial assistance. It has a risk reduction effect also; since insurers are required to pay out losses in the event of an incident, they, too, have a strong interest in loss avoidance.

When insurance operates as a business incentive, it can encourage the adoption of voluntary security measures using a variety of risk coverage mechanisms. For example, it can offer discounted insurance premiums (or lower deductibles) to policy holders who reduce their risks by voluntarily adopting certain security measures. Insurance companies can also require that all policy holders adopt certain security measures as a pre-condition of insurance coverage. In addition to setting minimum standards, cognizant of regulatory requirements, insurance companies can provide a market-based monitoring and assessment function that may reduce potential government liability while assuring compliance with constantly rising standards and practices. Third party inspections, or audits, by an independent organisation can be used to verify that policy holders have adopted the required measures.

An industry-led effort to use insurance as an agent for improved nuclear security practice would augment and compliment existing government regulations and international treaties. Combining national peer review of best practices with market incentives for the adoption of voluntary nuclear security practices would combine nuclear operators' considerable hands-on working level experience with the insurance industry's intellectual capital in risk assessment and loss mitigation to the benefit of both industries.

In spite of these potential benefits, several principles fundamental to the international nuclear liability regime could prevent the application of insurance as a risk management incentive for nuclear security. One principle is risk internalisation. To provide optimal incentives for mitigation, insurance pricing must be based on risk. This means the nuclear operator must be exposed to the countries limit a nuclear power plant operator's liability to well below the full consequences of potential damage. After the operator's liability has reached the limit, the risk is transferred either to the state or to insurance pool (or both), in effect socialising the cost of nuclear power. Consequently, the operator's limited liability is a disincentive to mitigation because it shields

corporate organisations and their executives from the real financial consequences of their safety and security decisions.

One way to avoid this effect is to audit plants in confidential reports with ratings, and link these ratings to the insurance industry. This method is what INPO currently employs as a risk sharing agreement between operators. It further illustrates the advantages of self regulation. The industry pool can provide excellent incentives for mutual monitoring because an operator with a substandard plant increases the financial exposure of all other operators. The strongest link in the chain is the weakest operator in the pool. Today INPO considers industry peer pressure to be its most effective tool for driving change and improved performance.

Although there is strong evidence from other industries (such as cyber security, maritime transportation and the US nuclear safety sector) that insurance measures could be used successfully to encourage best practice in nuclear security, one potential objection would be the issue of secrecy. Inter-operator pooling and mutual monitoring may require mandatory audits and third party verification; it has the potential to conflict with the requirement placed by states on many nuclear organisations to keep nuclear security-related information confidential.

COMMUNICATING NUCLEAR SECURITY INFORMATION

The above mentioned secrecy is only one aspect of a larger veil. Historically, the traditionalist ***"need to know"*** approach to information exchange is based upon the assumption that it is possible to know in advance who needs to have the information and that the risks of inadvertent disclosure outweigh the benefits of wider sharing. These assumptions proved to be mistaken in the aftermath of 9/11, where one of the hard lessons learned was that it is essential for the right people to have the right information at the right time in order to protect individuals and prevent adverse impacts on the environment, society and economy. In contrast, adopting a ***"need to share"*** approach achieves a much better balance between the risk of malicious or unintended disclosure and the risk of failing to share information that could help to avert a threat or event.

Achieving a fundamental change in attitude to the secrecy of nuclear-related information is a prerequisite for peer review, be it at a corporate level, or through in-depth reviews of the security programme. Effective nuclear security relies on excellent communications within an organisation and between an organisation and its regulator, government agencies, police, local community, other nuclear organisations and the media. Clearly, communicating with stakeholders does not mean providing classified information to just anyone on access arrangements to specific facilities or detailed measures to counter threats. It does mean, however, that the industry provides details about its management systems, corporate governance and oversight functions by those in the industry who are trusted with this accountability. It also means understanding the benefits of peer review and a more open attitude to learning from shared experiences.

One of the most important steps to take to overcome barriers to sharing security information is to create clear, consistent guidelines for how to communicate with each of the stakeholders. If current guidelines are complex and confusing, the process of sharing information may be so convoluted that people just give up trying. Moreover, increased transparency is based upon a presumption that information should be made available to those who have a legitimate interest in the organisation's activities. If certain types of information cannot be shared, it is important to explain why. If an incident or event occurs, well-prepared, well-practiced crisis communication plans should be set in motion immediately to manage and resolve the situation in the safest, most secure way possible for all concerned. Corporate Social Responsibility Report and Memorandum of Understanding are good tools the industry can use to establish clear understanding and communicate

effectively within an organisation and with regulators, government agencies, local communities, other nuclear organisations and the media.

Another step in overcoming barriers to communicating security information is to manage risk carefully. To do so, the industry needs to decide how to balance the risk of sharing information against the risk that an important stakeholder will fail to fully appreciate the threat. Taking this step requires that the development of a common language; secrecy and misunderstanding can be significantly reduced if consistent definitions are used.

In almost all situations, the classification of information should not be seen as a valid reason for isolating the security function from the rest of an organisation's activities; some information will have to be protected but the vast majority needs to be written and/or produced in a declassified manner to aid communications, cooperation and effective implementation of the security programme. Moreover, sharing information openly, honestly, appropriately and effectively will give stakeholders the confidence that the people managing the nuclear business are trustworthy, highly-trained and competent. The result is that nuclear organisations will be seen as effective, well governed and well respected by its employees, local community, regulator, and national and international bodies.

NUCLEAR SECURITY LEADERSHIP

The recently released report of the Fukushima incident by the NAIIC (Fukushima Nuclear Accident Investigation Commission) of the National Diet of Japan highlights and reinforces the fact that nuclear safety relies greatly on human factors. The report addresses lack of governance and communication among different entities; lack of competencies for those accountable for nuclear security; and lack of a clear understanding of accountability and liability among licensees and regulators. Calling the incident a result of "willful negligence" by the top management and of "serious deficiencies" in their response, the report concludes that the fundamental cause of the "man-made" incident is the complacent mindset of those accountable for nuclear safety. What this report indicates is the lack of nuclear safety awareness, which fundamentally inhibits implementation of an effective nuclear safety regime.

There are parallels for nuclear security; an effective nuclear security regime would have the following list of items that distinguish an organisation with outstanding nuclear security management.

- **Leadership**

The board and executive management have clear expectations, communicate them effectively, listen carefully, welcome feedback (both positive and negative) and require regular evidence that the goals they set are being carried out.

- **Commitment to Excellence**

Commitment begins with strong, proactive leadership from the board and radiates throughout the entire organisation. They know that regulations cannot regulate excellence; at best, they can only regulate adequacy to reasonable levels. Because nuclear material always entails risk, they understand the danger of complacency and constantly strive to remain vigilant.

- **Nuclear Acumen**

They understand that security is both a legal and a moral issue. As a licensee, they have taken an oath to protect the health, safety and security of the public, and they take this oath seriously. They know that failure

to do so would not only make themselves and their organisation liable, but could also have serious local and worldwide consequences. For this reason, they incorporate *loss prevention* into everything they do.

- **Excellent Communication Skills**

They are excellent communicators and have the capacity to seek out and listen to the voices of people throughout the entire organisation. They are able to receive information, distil it, and take effective action. They also welcome feedback—from the bottom up as well as from the top down—and they reward people for their honesty. And they communicate externally to inform stakeholders about their oversight processes and performance.

- **Commitment to Collaboration**

They are willing to share their insights, experiences, tools and talents with others in the industry because they understand that the failure of just one nuclear facility has the potential to destroy the credibility of all others. They also understand that security does not compete with safety; on the contrary, maintaining the safety and security of nuclear organisations and materials requires close cooperation between both functions.

- **Accountability**

They make decisions about what needs to be done, prioritise actions for implementation, and follow through on what they agree to do. They put systems in place that review, monitor and audit performance, and they take corrective action when performance slips.

- **Commitment to Integration**

They understand that maintaining safety and security is a complex, challenging task that requires the knowledge, skills and input of numerous stakeholders. Consequently, they put policies and programmes in place that bring operations, safety, security, engineering, accounting, vendors and other professionals together to learn from each other, provide input and find joint solutions.

- **Commitment to Being a Learning Organisation**

They understand that maintaining excellence in a competitive, perpetually changing industry requires commitment to continuous improvement and learning. They recognise that improvement is a process, not a destination, so they continually review, test, refine and benchmark what they do and how they do it.

Overall, these underlying factors make up the composition of an effective nuclear security regime. From the Fukushima incident to other small-scale incidents around the world, it is evident that such high standards of awareness and culture are still not implemented or institutionalised. This calls for an urgent need for a framework that would be able to aid in the implementation of effective nuclear security management in organisations.

WINS is currently engaged in a project, the WINS Academy (for more information, see www.wins.org/content.aspx?id=133), that would establish a global nuclear security framework for professional development and accreditation to create an environment that leads to the recognition of the Nuclear Security Manager as a recognised and regulated profession. Our reasoning behind this is that our work on Best Practice Guides and interaction with industry and other nuclear security practitioners has highlighted a stark fact: security managers need no formal training and there is no such thing as a Nuclear Security Professional. There are no accredited courses and no structure of required competencies for the "profession." In most cases, the work is performed by a mixture of ex-police, ex military and/or general

managers. And as far as we are aware, none of the Nuclear Regulators have specified any requirement for nuclear security professional at management level to hold any nuclear security accreditation.

Essentially, there is a stark lack of professional development opportunities for nuclear security management. There needs to be a consolidated effort on an international basis to address this deficiency and to better coordinate and support the work of the newly established Centres of Excellence (CoE). This also ties back to improving lack of security awareness that has been so fundamental in nuclear security (and safety) incidences around the world.

The programme to establish global accreditation standards for professional development and the encouragement to adopt these mechanisms by those institutes and organisations with responsibility for training and education will further enhance and strengthen the nuclear security regime. Following a capability and gap assessments for nuclear security management, the industry will be able to develop nuclear security metrics and identify the best processes and mechanisms that promote adherence to nuclear security guidelines.

PEER REVIEW: OPPORTUNITES AND BARRIERS

A variety of factors have been identified as reasons why a comparable system of peer review does not exist for nuclear security; most significantly, different perceptions about the threat, blurred accountabilities, excessive secrecy, etc remain the biggest barriers to change and need to be addressed both individually and simultaneously to generate sufficient momentum for change. Of course, a major terrorist incident at any nuclear facility would change the political and public attitudes and priorities immediately, as they have for nuclear safety, aviation safety and now for maritime security in response to piracy off the coastline of various countries around the Horn of Africa and elsewhere.

It seems to WINS that nearly all of the operational learning from nuclear safety is applicable to nuclear security if, as mentioned above, nuclear security information can be communicated in a meaningful way that does not compromise highly classified information and weaken the security regime.

Arguing for the introduction of detailed security peer reviews on an international basis will fail. A more subtle and measured approach will be necessary as outlined below:

First, there needs to be collective buy-in that nuclear safety or, call it integrated risk management, includes safety, emergency planning/response and security. This is essential to redefine the meaning and scope of nuclear safety,

Second, to recognise that there are elements of the security regime that must be protected and cannot be shared with the rest of the risk management community: these elements need to be defined and tested using a hypothetical site and management structure; by listing the types of security information and seeing what the justification and consequences are for withholding the information from the rest of the management and operations team, and under what circumstances and how this information would ever be shared. This process is essential and will be time consuming involving experienced practitioners and regulators so that the conclusions are both sound and shared

Third, there will be a range of security-related information identified that could be classified (for the purpose of the exercise) into

1. Information that can be shared easily
2. Information that can be shared with some care
3. Information that the security teams are not prepared to share yet
4. Genuinely classified information that must not be shared

We might expect that information relating to corporate oversight might fall into the "shared easily" or "with some care" category, i.e. questions about the management oversight of nuclear security, its integration with safety etc, measures to assess the security culture, etc. These are exactly the kinds of thing that INPO includes in its corporate review process and WINS has made good progress in developing such an approach.

Fourth, INPO's Principles and Objectives for Nuclear Safety is an excellent peer review scheme. These can be developed into a parallel set of questions for Nuclear Security, and ways found to conduct corporate peer reviews of the security oversight arrangements on a trial and experimental basis, at a number of power plants that would volunteer to assist the process can be arranged.

Fifth, by using a combination of WINS Guides and INPO structured questions, it should be possible to develop a set of security questions and metrics to gauge the effectiveness of the more classified security arrangements. We believe that this could not be put into practice as a peer review on anything other than a national basis.

Sixth, both the high level corporate review and the more classified Security Operations review will be assessed on the 1 - 5 point scale (with 1 being inefficient and 5 as world-class) and the respective paired scores from each of the reviews will be plotted in a simple matrix and the results examined for correlation. This type of analysis should indicate whether an unclassified corporate review provides an adequate insight into the performance of the classified part of the programme.

Seventh, on the basis that the approach works as hoped (and the logic is good), this would mean that international peer reviews of corporate (by which we mean the governing bodies, be they private or government entities) oversight and behaviours would provide a useful and meaningful measure of security performance (i.e security outcomes) without having to go through the long process of conducting international peer reviews of nuclear security.

And lastly, is the issue of accreditation. There is no prospect of the IAEA accrediting nuclear security arrangements under any circumstances so any accreditation body will have to be distinct. And there are likely to be potential liability issues associated with accrediting a nuclear security programme, in the event that it was subject to a successful terrorist attack. It seems more plausible to rate the performance of the security regime (rather than give a stamp of approval) as INPO does for nuclear safety, and to accredit the training and development of security related staff.

As mentioned, WINS is engaged in the WINS Academy to pursue the advancement of professional accreditation within the nuclear security regime. Moreover, WINS is currently in the advanced stages of corporate review of nuclear security culture to support the work of accreditation and peer review.

SUMMARY

Significant barriers to the worldwide achievement of effective nuclear security implementation exist and additional mechanisms will be required to improve and sustain the necessary improvements and to introduce peer review and a form of accreditation.

There must be continued practical efforts to analyse and communicate the international threat from terrorism, so that States and Operators understand that even if the local, domestic threat from terrorism is perceived to be low, the threat from international groups with concomitant international outreach are threats that must be taken seriously. The establishment of a minimum design basis threat is an essential prerequisite to achieving this goal but will be challenging to achieve.

The industry must also clarify legal roles, responsibilities and liabilities for nuclear security between the various entities in the State. The over simplistic view that "States are accountable for security" is unhelpful and misleading given that the States frequently place legal accountability on their Nuclear Licensees (Operators) for nuclear security, and can do so without giving the Licensees sufficient legal authority to prepare for and respond to the threat. A case in point is those countries that hold Licensees accountable for security but who do not allow them to have their own armed response capability, instead requiring the Licensees to rely on off-site police and other agencies that are outside the control of the Licensee. These structural problems need to be addressed with urgency.

We should identify and implement mechanisms to improve transparency and challenge the unnecessary secrecy associated with nuclear security arrangements, particularly in respect of the performance of States, corporate governance and accountabilities. Communications could be improved in certain ways and the Peer Review of Corporate Governance arrangements may evolve over time by the identification of metrics and approaches that would provide meaningful insight into the adequacy of the implemented arrangements. Overall, the time seems right to continue to push for the introduction of peer review mechanisms using a step by step approach involving corporate oversight peer review first, supplemented by detailed security programme reviews conducted by nationals of the State to avoid security clearance issues.

Moreover, the identification of market mechanisms, including terrorism insurance arrangements, will provide incentives for implementing more effective security, and financial disincentives for poor performance. Such market mechanisms are already in place in some areas of the world for nuclear safety, maritime security, and are being increasingly considered for cyber-security as the only effective mechanism for addressing the international cyber threat. This paper partially highlights the opportunities, barriers and issues to doing the same for nuclear security and recommends the need for ground breaking work in this area.

Importantly, the root cause of many of the current problems facing nuclear security is the lack of a worldwide and accredited development programme for nuclear security professionals and others with accountability for nuclear security, including regulators. All too often there is an assumption made that an ex-military or police background constitutes sufficient experience to become an effective nuclear security professional, and is a false assumption. Nuclear security professional development and accreditation lags well behind other professional fields and action needs to be taken on an urgent basis to provide an international framework of competences and accredited training centres to provide the development opportunities.

WINS position is that the inter-linkages between these factors need to be addressed simultaneously to have the desired effect of improving the effectiveness of nuclear security, worldwide.

APPENDIX A: FACTORS INFLUENCING THE ATTAINMENT OF EFFECTIVE NUCLEAR SECURITY, WORLDWIDE

2012 © World Institute for Nuclear Security (WINS) All rights reserved. Graben 19, A-1010 Vienna (Austria)

Tel.: +43 1 23060 6081 | Fax: +43 1 23060 6089 | Email: info@wins.org | Internet: www.wins.org

International NGO under the Austrian Law BGBl. Nr.174/1992 | GZ: BMeiA-N9.8.19.12/0017-I.2/2010