Key Steps for Continuing Nuclear Security Progress

M. Bunn[1], M. Malin[1], N. Roth[1], W. Tobey[2]

[1]Project on Managing the Atom, Belfer Center for Science and International Affairs, Harvard Kennedy School, Cambridge, Mass., USA

[2]Belfer Center for Science and International Affairs, Harvard Kennedy School, Cambridge, Mass., USA; Chairman of the Board, World Institute for Nuclear Security

matthew_bunn@harvard.edu

Abstract. The work of improving nuclear security is not done, though leaders are no longer meeting at the summit level. The threats of nuclear theft and terrorism remain very real. States, nuclear operating organizations, and institutions and initiatives supporting nuclear security must strive for continuous improvement in nuclear security. The alternative is dangerous decline. Achieving genuinely effective implementation of existing recommendations and commitments in five key areas could dramatically strengthen nuclear security around the world.

First, states and operators must protect nuclear weapons, weapons-usable nuclear materials, and major nuclear facilities against the full range of plausible adversary capabilities and tactics. The focus must be on continuous improvement in the face of ever-evolving adversary threats.

Second, all operators managing nuclear weapons, weapons-usable nuclear materials, and high-consequence nuclear facilities should put in place comprehensive programs to protect against insider threats – the most important and challenging nuclear security threats. Insider protection programs are particularly important at facilities that handle weapons-usable nuclear material in bulk.

Third, states should ensure that each relevant nuclear operator has a targeted program in place to assess and strengthen security culture, and all nuclear managers and security-relevant staff receive regular information, appropriate to their role, on evolving threats. At the same time, interested countries should launch a number of initiatives designed to build understanding of the threat and combat complacency.

Fourth, states should ensure that all nuclear operators establish in-depth vulnerability assessment and performance testing programs to ensure that nuclear security systems really are able to protect against intelligent adversaries. These should include regular, realistic force-on-force exercises.

Fifth, interested countries should take a broader approach to consolidating nuclear material at fewer locations, encompassing more categories of material and additional policy tools.

These five areas are largely already included in International Atomic Energy Agency (IAEA) nuclear security recommendations, and are therefore covered in the commitment to meet the "intent" of such initiatives incorporated in the Strengthening Nuclear Security Implementation Initiative (INFCIRC/869). But achieving genuinely effective implementation will remain a challenge, particularly with national leaders no longer meeting at the summit level. As nuclear security must continue to evolve in the face of changing threats, it is essential to continue an effective ongoing international dialogue on nuclear security, both about implementation of existing recommendations and commitments and about new steps. This should include the IAEA, the "contact group" established at the 2016 Nuclear Security Summit, and other groupings. States should revitalize bilateral nuclear security cooperation efforts, including between the United States and Russia. Both industry and civil society also have essential roles to play. With champions from all these sectors around the world working together, and a focus on genuinely effective implementation, nuclear security can be dramatically strengthened, reducing risks to all countries.

Key Words: Nuclear security, adversary threat, security culture, insider threat, performance testing.

1. Introduction

The work of improving nuclear security is not done, though leaders are no longer meeting at the summit level. The threats of nuclear theft and terrorism remain very real.[1] States, nuclear operating organizations, and institutions and initiatives supporting nuclear security must strive for continuous improvement in nuclear security. The alternative is a dangerous decline. Just as with safety, the goal must be a never-ending quest for excellence in nuclear security performance.

With national leaders no longer regularly meeting to push forward additional action, sustaining momentum is likely to be difficult. Major new nuclear security initiatives may not come to fruition in the near term. But efforts focused on genuinely effective implementation of Nuclear Security Summit commitments and International Atomic Energy Agency (IAEA) recommendations that already exist could lead to dramatic improvements in nuclear security around the world. The key is *genuinely effective* implementation: existing commitments and recommendations could be implemented in ways that would do little to reduce nuclear terrorism risks, or, with an appropriate focus on the goal of nuclear security excellence, they could be implemented in a way that would transform nuclear security performance.

The IAEA and its member states have already laid out fundamental principles and objectives of nuclear security, as well as a broad range of nuclear security recommendations. Those countries that participated in the nuclear security summits have committed to additional steps – both in the consensus communiqués and action plans and in the group commitments or "gift baskets."

In particular, participants in the Strengthening Nuclear Security Implementation Initiative (agreed at the 2014 Nuclear Security Summit in The Hague, but now open to all states as Information Circular 869) commit to taking a range of important steps to strengthen nuclear security, including conducting self-assessments, hosting periodic peer reviews of their nuclear security arrangements, and ensuring that "management and personnel with accountability for nuclear security are demonstrably competent." [2] Crucially, they also pledge to "meet the intent" of the IAEA's nuclear security recommendations on physical protection of nuclear material and facilities, security for radioactive material, and radioactive material out of regulatory control.

The word "intent" was included in INFCIRC/869 because countries differ in the specifics of their nuclear security implementation while meeting similar objectives. Overall, we would argue that the intent of the IAEA recommendations is that nuclear security systems should provide effective protection against nuclear theft and sabotage, reducing the overall risk of a security breach to a very low level. Many elements must be in place for a nuclear security system to provide effective protection, ranging from independent regulatory oversight to well-designed barriers and intrusion detection systems to accurate and timely material control and accounting. These protections must be ongoing and sustainable. As suggested by the use of "intent," the specifics necessary for effective protection are likely to vary from country to country, depending on factors such as the types of nuclear facilities and materials to be protected and the level of adversary threat.

Nevertheless, five broad elements are especially central to effective nuclear security: designing nuclear security systems to protect against the full spectrum of plausible adversary capabilities and tactics; establishing comprehensive programs to protect against insider threats; implementing targeted programs to strengthen security culture; conducting realistic

performance testing and vulnerability assessment; and consolidating nuclear weapons-useable material to the minimum number of locations. The first four of these are called for (with varying degrees of specificity) in IAEA recommendations; the fifth is included in commitments from the nuclear security summits.

The remainder of this paper will address each of these five elements in turn. In the final section, we discuss what forums might contribute to progress toward such objectives.

2. Protecting Against All Plausible Adversary Capabilities and Tactics

A central nuclear security challenge is to ensure that nuclear weapons, materials, and facilities are protected against the full spectrum of plausible adversary threats and capabilities, without going too far. Underestimating threats creates vulnerabilities, while protecting against unrealistic threats wastes resources and inhibits successful operations.

Nuclear security systems able to cope with the assessed threat are already a fundamental element of the IAEA's nuclear security recommendations (and hence part of the commitment states make in joining INFCIRC/869). In the IAEA's recommendations for physical protection of nuclear material and facilities (INFCIRC/225/Rev. 5), the Agency recommends that physical protection systems be "based on the State's current evaluation of the threat."[3] This is a very broad statement, but if taken seriously, it implies that countries should commit to establishing and sustaining security systems that will protect nuclear weapons, weapons-usable material, and major nuclear facilities against the full spectrum of plausible adversaries, as assessed on a regular basis by their intelligence agencies. In an age or globalized threats, where all nuclear materials and facilities are potential targets of theft or sabotage, this should include, at a minimum, a well-placed insider; a modest group of well-trained and well-armed outsiders, capable of operating as more than one team; and both an insider and the outsiders working together. Facilities or transports in countries facing more substantial adversary threats should have more extensive protection.

Most states with such materials and facilities already have a formal process for determining the set of threats operators will be required to design their security systems to protect against, known as the design basis threat (DBT). There is no international agreement, however, on any common baseline level of threat that all such materials and facilities should at least be protected against, even at the broad level of generality described above. As a result, DBTs vary significantly from country to country – and unfortunately, nuclear security experts in several countries dismiss as implausible adversary capabilities and tactics that have already been demonstrated in thefts from and attacks on non-nuclear facilities.[4] Furthermore, sharing of DBT information, even among close allies, is too often impeded by secrecy requirements.

Tactics and capabilities demonstrated in non-nuclear thefts and attacks include:[5]

- Attack by well-armed, well-equipped teams with military-style training and tactics and vehicles such as helicopters (e.g., the 2009 Västberga cash depot heist in Sweden).
- Use of prolonged intelligence collection, planning, and specialized tools and skills to overcome many layers of security (e.g., 2003 Antwerp Diamond Center heist in Belgium).
- Insider-outsider and insider-insider conspiracies (e.g., the 2004 Swissport Heathrow heist).
- Tunneling to bypass security systems (e.g., multiple prison breaks and bank heists).

Cyber intrusions are also becoming increasingly common in non-nuclear thefts. Nuclear security planners must plan for the possibility of combined cyber and physical thefts and assaults. For example, cyber means could be used to disable key elements of physical protection systems (which are now increasingly digital); to alter nuclear material accounting and control records; to turn off key intrusion detection systems; to sabotage facilities; and more. Increasingly, cyber security is a fundamental part of effective nuclear security.[6]

All security systems for nuclear weapons, weapons-usable nuclear material, and major nuclear facilities whose sabotage could cause a major catastrophe should be designed to protect against all of these threats.

3. Establishing Comprehensive Programs to Protect Against Insider Threats

Nearly all of the nuclear theft and sabotage incidents that have occurred in which the circumstances are known were perpetrated by insiders in the nuclear organizations, or with the help of insiders.[9] Most recently, in 2014, an insider at the Doel-4 nuclear power plant in Belgium (as yet unidentified) drained all the lubricant for the turbine, shutting the plant for months and causing hundreds of millions of dollars in economic damage. Investigations revealed that almost two years earlier, an insider named Ilyass Boughalab, cleared for access to the plant's vital areas, had left to fight for the Islamic State.[1, p. 29] In short, insiders pose one of the greatest challenges to nuclear security, and nuclear organizations must establish comprehensive programs to address the insider threat.

Protecting against the insider threat is already the subject of IAEA recommendations (and hence part of the INFCIRC/869 commitment). INFCIRC/225/Rev. 5 calls for physical protection systems to protect against both insider and external adversaries, and warns that insiders pose special challenges because they "could take advantage of their access rights, complemented by their authority and knowledge, to bypass dedicated physical protection elements or other provisions, such as safety procedures."[3] The IAEA also offers technical guidance on steps to protect against insider threats, as does the World Institute for Nuclear Security (WINS) [10, 11].

Truly effective protection against insiders is difficult to achieve – particularly if the possibility of multiple insiders conspiring together is considered (something that occurs regularly in non-nuclear thefts). In some organizations, even the most alarming "red flags" can go unreported and unaddressed. [9]

Because of the difficulty of coping with the potential for insider adversaries, it is a mistake to assume that any particular measure (such as background checks) will be sufficient. Instead, operators dealing with nuclear weapons, weapons-useable materials, and major nuclear facilities, should have comprehensive insider protection programs in place providing defense in depth, including, including:

- Background checks before granting access and ongoing monitoring after access is permitted;
- Strong incentives for staff to report any concerning behavior, or any potential vulnerabilities they observe;
- Effective programs to address employee disgruntlement (which is a remarkably important driver of insider incidents across a range of industries);
- Regular training programs focused on protecting against insider threats, including real stories of insider incidents, to give management and staff a feel for the reality of the problem;

- Nuclear material accounting that is accurate and timely enough to detect either a rapid or a protracted theft, identify when and where it happened, and establish who had access then;
- Constant surveillance of nuclear material, and of vital areas that might be sabotaged;
- Two-person or three-person rules whenever people have access to weapons-usable nuclear materials or vital areas, so that nobody is ever alone with weapons-usable nuclear material or in a vital area;
- Portal monitors capable of detecting nuclear material at all potential entrances and exits to set off an alarm if any material is being removed;
- Physical protection systems consciously designed to handle both insider and outsider threats (including insiders and outsiders working together); and
- Regular tests, assessments, and inspections to ensure the effectiveness of the insider protection program in place.

4. Insider protections are particularly important at HEU or plutonium bulk-processing facilities, which appear to have been the source of nearly all of the known cases of seizure of stolen weapons-usable nuclear material. When material is being handled regularly and is in the form of powders or liquids, it is significantly easier for insiders to remove small amounts without being detected.Implementing Targeted Programs to Strengthen Security Culture

Nuclear security systems are only as effective as the people implementing them. If staff are ignoring security rules, security doors are propped open for convenience, guards are turning off intrusion detectors because of annoyance with false alarms, or guards are sleeping on the job, even extensive technological systems will not provide effective nuclear security. Hence the culture of the organization, and the priority it convinces its staff to place on security, is critical to success.

Security culture, too, is already a major focus of IAEA recommendations (and therefore included in the commitments states make in joining INFCIRC/869). INFCIRC 225 Rev. 5 recommends that "[a]ll organizations involved in implementing physical protection should give due priority to the security culture, to its development and maintenance necessary to ensure its effective implementation in the entire organization."[3] To achieve this "due priority," every organization handling nuclear weapons or weapons-usable nuclear material, or managing a major nuclear facility, should have in place a targeted program to (a) assess their security culture regularly; and (b) seek to strengthen their security culture over time.

Unfortunately, achieving a strong security culture can be quite difficult, as success – in the form of lack of incidents – breeds complacency. Most nuclear facilities have never experienced even an attempted major theft or sabotage. In an average guard's career, all the alarms he or she experiences will either be false alarms or tests. In this environment, it is difficult to develop and sustain an organizational culture where people believe there are realistic adversary threats to their organization that could strike at any time, and hence that they must be constantly to find and fix potential vulnerabilities.

The now-famous July 2012 break-in at the Y-12 nuclear facility in the United States, involving an 82-year-old nun and two other protesters in their 60s, provides a good example of the vulnerabilities that can be created by a weak organizational security culture. The facility had recently installed a new security system, but had tried to save money by leaving some of the old system in place. The result was a tenfold increase in false alarms. Normally the compensatory measure would have been to use cameras to check whether the

alarms were false or real – but the cameras in some areas had been broken for months without being placed on the priority list to be fixed. Instead, guards were supposed to go out and check each alarm – but it appears they had gotten tired of doing so. The intruders set off alarm after alarm, but were able to proceed directly to the building where most U.S. highly enriched uranium is stored, pour blood on it, pound on it with sledgehammers, and sing protest songs before finally being accosted by a single guard. (The heavily armed guards inside the building heard the pounding but assumed it was pre-dawn construction and did not bother to check.) [1, pp. 87-90]

States should ensure that all organizations managing high-consequence nuclear materials or facilities have targeted nuclear security culture improvement programs that include: [1, pp. 112-119]:

- Implementing security culture recommendations of the IAEA and WINS;[7, 8]
- Conducting regular security culture self-assessments;
- Providing regularly updated information to all security-relevant managers and staff at such organizations on nuclear security threats, at levels of detail appropriate to their particular roles;
- Establishing programs of incentives for strong nuclear security performance (for individuals, teams, and organizations, as appropriate); and
- Developing mechanisms for sharing good practices and lessons learned in strengthening security culture among nuclear organizations (including, as appropriate, through the IAEA and WINS).

The goal must be a strong focus on continuous improvement in security throughout the organization, especially from the organization's leadership. An essential element of such a focus is a willingness to devote resources to improving security – including both money and capable, trained personnel.

The INFCIRC/869 commitment to ensure that all management and staff with responsibilities relevant to nuclear security are "demonstrably competent" is thus crucial not only to ensure that each individual is trained for his or her job, but for building an overall organizational culture that values nuclear security and understands that doing it well requires specialized knowledge and skills. States should ensure that organizations take part in relevant training programs, and that managers and staff demonstrate their competence through testing and certification programs (such as those offered, for example, by the WINS Academy).

5. Conducting Realistic Performance Testing and Vulnerability Assessments

Realistic performance testing and vulnerability assessments are a critical component of an effective nuclear security system. Many systems appear highly secure – with fences, barriers, armed guards, and the like – but in fact can be readily defeated by intelligent adversaries who study the system to find its weaknesses. The theft of tens of millions of dollars of jewels and other valuables from the Antwerp Diamond Center in 2003 occurred despite a security system in place that appeared to many to be impregnable.[6]

Here, too, the issue is already the subject of IAEA recommendations (and hence is part of the INFCIRC/869 commitment). INFCIRC/225/Rev. 5 recommends that nuclear operators have quality assurance programs to ensure that security systems can effectively protect against the design basis threat. Further, it recommends that these programs should include force-on-force

exercises conducted at least annually.[3] To be genuinely effective, other key elements of a quality assurance programs should include:

- Making sure that force-on-force exercises are as realistic as possible, within safe parameters, including realistic tests of the system's ability to defend against intelligent adversaries (insiders and outsiders) trying to find ways to defeat it.
- Establishing "red teams" whose job is to find security vulnerabilities and propose solutions. These teams should include individuals with a creative, "hacker" approach. They should have incentives to find vulnerabilities, and protected from potential organizational backlash.
- Conducting "tabletop" exercises, computer simulations, and brainstorming workshops to identify and assess tactics adversaries might use.

Of course, operating organizations must take action to address weaknesses identified in such vulnerability assessments and performance testing.

6. Consolidating Nuclear Weapons-Useable Material to Fewer Locations

States can achieve stronger security at lower cost by protecting fewer places. Every location where nuclear weapons, HEU, or separated plutonium are located is a potential target for theft. Each location adds to the risk that adversaries will exploit a vulnerability defenders failed to notice. Hence consolidating nuclear weapons and weapons-usable material to the minimum number of locations required for ongoing military and civilian missions is a key part of nuclear security.

Consolidation is not explicitly included in IAEA recommendations, though the Agency actively supports consolidation efforts such removal of unneeded HEU around the world. The states participating in the 2014 Nuclear Security Summit, however, agreed that it was of "great importance" that plutonium and HEU be "appropriately secured, consolidated, and accounted for." The leaders encouraged all states to minimize their use and stocks of HEU, and "to keep their stockpile of separated plutonium to the minimum level."[12]

At the 2016 Nuclear Security Summit, nearly two dozen countries joined a gift basket in which they committed to a number of steps focused on consolidating HEU and minimizing its use, with the goal of eliminating civil uses. The gift basket stated that "HEU minimization is a form of permanent threat reduction and an integral component of the global effort to combat the threat of nuclear terrorism."

Fortunately, efforts to consolidate nuclear weapons and weapons-usable nuclear material have been underway for some time, with many countries participating, and have made substantial progress. More than half of all the states that once had HEU or separated plutonium on their soil have chosen to eliminate it; all weapons-usable nuclear material has been eliminated from scores of sites around the world; and the number of locations where nuclear weapons exist has been greatly reduced. Nevertheless, the number of locations with nuclear weapons, HEU, or separated plutonium remains far larger than needed, creating unnecessary risks and costs.

All countries—especially those that have endorsed INFCIRC/869 and the 2016 HEU gift basket—should continue the effort of minimizing stocks and the number of locations with HEU and plutonium. This should include (where applicable):

- Developing national-level plans to consolidate nuclear stockpiles to the smallest attainable number of facilities.

- Reviewing each location where nuclear weapons or weapons-usable nuclear material exists, and eliminating these items from any site where their continued benefits are outweighed by their costs and risks.
- Structuring nuclear security regulations to incentivize operators to reduce costs by consolidating stocks of material.
- Supporting efforts to help facilities convert from HEU to LEU fuel, and offering incentives for unneeded HEU-fueled reactors to close (such as support for research at other nuclear facilities).

The United States should continue its critical role in this effort. The United States should have a policy that it will take back, arrange for the elimination of, or assist in providing effective and sustainable security for all plutonium and HEU anywhere in the world. This would cover both a broader set of materials and a broader range of policy tools than existing U.S. programs.

The IAEA can play a critical role in this work, supporting minimization efforts at the request of states as it has in the past. Moreover, signatories of the 2016 HEU Minimization Gift Basket assigned the IAEA a key role in managing the voluntary reporting mechanism on HEU minimization progress that they pledged to establish.

7. Forums for Nuclear Security Progress

The nuclear security summit process drastically increased high-level attention to nuclear security, and led to substantial nuclear security progress in many countries – though it was limited to a few dozen states invited to participate. With the end of the summit process, the question is how nuclear security progress – including the kinds of steps described in this paper – can be sustained. Most of the needed actions described in this paper have to be done by individual states or operators – but the summit process made clear that international discussions and cooperation can be a key driver of actions within states. With the end of the summit process, what forums and institutions will be most important in ensuring progress continues?

The IAEA, of course, will play a central role. In each of the areas discussed in this paper, the IAEA could provide new or strengthened technical guidance; training programs; and assessment services. For example, the IAEA has not yet offered technical guidance on vulnerability assessment and performance testing.

Indeed, the IAEA should make every effort to encourage all member states to join in INFCIRC/ 869, with its commitment to meet the intent of the IAEA nuclear security recommendations. The IAEA should also encourage countries to focus on achieving the kind of genuinely effective implementation of each recommendation discussed in this paper – and offer assistance to states in doing so. IAEA General Conferences could become occasions for states to report on their progress in fulfilling the nuclear security commitments they have made, whether in INFCIRC/869 or elsewhere. The annual nuclear security resolutions and the every-three-year Ministerial meetings provide additional moments for discussion of nuclear security progress, challenges, and next steps. The IAEA will also be host for the review conferences for the amended physical protection convention – which will provide another opportunity, if states choose to use them in this way, for states to report on their progress in strengthening physical protection, and to discuss additional steps that might be taken.

All of this, of course, would require resources, including predictable, regular-budget resources. All member states should support expanding the budget of the IAEA's Division of Nuclear Security, and the portion of it that comes from the regular budget.

Experience suggests, however, that it is difficult to generate and agree on specific new ideas in broad forums such as the IAEA General Conference or the Ministerial meetings. Other forums will have to play a role as well, including the Nuclear Security Contact Group established at the 2016 summit (now open to all states who subscribe to its principles); the Global Initiative to Combat Nuclear Terrorism; the Global Partnership Against the Spread of Weapons and Materials of Mass Destruction; United Nations processes related to nuclear security, particularly those surrounding UN Security Council Resolution 1540; Interpol; and other international initiatives. To provide a forum for in-depth, focused dialogue among interested states, the member states of the Global Initiative should establish an additional working group on security for nuclear materials and facilities [1, pp.127-129]. Such forums can help make it possible both to achieve effective implementation of existing commitments and to launch new initiatives – such as a political commitment by key states to stringent nuclear security principles, going well beyond INFCIRC/869. Each national leader of a state with nuclear materials or facilities and each Chief Executive Officer of a nuclear operating organization should acknowledge their personal, undelegatable responsibility for effective nuclear security [1, pp. 100-103].

Past experience also suggests that bilateral cooperation can be critical in strengthening nuclear security. Unfortunately, U.S.-Russian nuclear security cooperation is now almost at a standstill, and other bilateral cooperation is fairly limited. New steps are needed to revitalize nuclear security cooperation, based on principles of equality and mutual respect. [1, pp. 104-112]

The role of nuclear operators will remain absolutely fundamental to nuclear security success, so it is important that in addition to the government-level processes just described, the nuclear industry has decided to continue its nuclear industry security summits, and that WINS continues to grow and strengthen as a forum for exchange of best practices, training, and more. Civil society will also continue to play a crucial role in generating ideas, fostering dialogue, and holding states accountable. Hence, it is important that efforts such as the Nuclear Threat Initiative's Global Dialogue on nuclear security (incorporating participants from government, industry, and civil society) and the Fissile Material Working Group (incorporating the leading civil society groups on nuclear security worldwide) continue to play their roles.

The work of nuclear security is never done – it requires continuous improvement. Sustaining what has been done and making further progress is likely to be more difficult with the end of the summit process. But with sustained efforts from champions in governments, industry, and civil society around the world, and a focus on genuinely effective implementation of existing recommendations and commitment, nuclear security can be dramatically strengthened, reducing risks to us all.

REFERENCES

[1] BUNN, M., MALIN, M., ROTH, N., TOBEY, W., Preventing Nuclear Terrorism: Continuous Improvement or Dangerous Decline? Project on Managing the Atom, Belfer Center for Science and International Affairs, Harvard Kennedy School, Cambridge, Mass. (2016).

[2] INTERNATIONAL ATOMIC ENERGY AGENCY, Communication Received From the Netherlands Concerning the Strengthening of Nuclear Security Implementation, INFCIRC/869, Vienna (2014).

[3] INTERNATIONAL ATOMIC ENERGY AGENCY, Nuclear Security Recommendations on Physical Protection of Nuclear Material and Nuclear Facilities, INFCIRC/225/Rev. 5, Vienna (2011).

[4] BUNN, M., HARRELL, E., Threat Perceptions and Drivers of Change in Nuclear Security Around the World: Results of a Survey, Project on Managing the Atom, Belfer Center for Science and International Affairs, Harvard Kennedy School, Cambridge, Mass. (2014), pp. 22-23.

[5] LAFLEUR, J; PURVIS, L.; ROESLER, A., The Perfect Heist: Recipes From Around the World, SAND-2014-1790, Sandia National Laboratories, Albuquerque, N.M. (2014).

[6] International Conference on Computer Security in a Nuclear World: Expert Discussion and Exchange (Proc. Conf. Vienna, 2015), IAEA, 2016.

[7] INTERNATIONAL ATOMIC ENERGY AGENCY, Nuclear Security Culture: Implementing Guide, Vienna (2008).

[8] WORLD INSTITUTE FOR NUCLEAR SECURITY, WINS International Best Practice Guide 1.4: Nuclear Security Culture, Rev. 3.0, Vienna (2016).

[9] BUNN, M., SAGAN, S., A Worst Practices Guide to Insider Threats: Lessons From Past Mistakes, American Academy of Arts and Sciences, Cambridge, Mass. (2014).

[10] INTERNATIONAL ATOMIC ENERGY AGENCY, Preventive and Protective Measures Against Insider Threats, Vienna (2008).

[11] WORLD INSTITUTE FOR NUCLEAR SECURITY, WINS International Best Practice Guide 3.4: Managing Internal Threats, Rev. 2.0, Vienna (2015).

[12] The Hague Nuclear Security Summit Communiqué, Netherlands Ministry of Foreign Affairs, The Hague (2014).

[13] Gift Basket on Minimizing and Eliminating the Use of Highly Enriched Uranium in Civilian Applications, 2016 Nuclear Security Summit, Washington, D.C. (2016).