AN INDUSTRY-LED GOVERNANCE FRAMEWORK FOR DEMONSTRATING STRONG SECURITY

M.L.UMAYAM
Stimson Center
Washington, DC, United States
lumayam@stimson.org

K. RAUHUT
Stimson Center
Washington, DC, United States
krauhut@stimson.org

R.HOWSLEY
World Institute for Nuclear Security
Vienna, Austria
roger.howsley@wins.org

J.BARRETT
Canadian Nuclear Association
Ontario, Canada
barrettj@cna.ca

Abstract

With the entry into force of the Amendment to the Convention on the Physical Protection of Nuclear Material (CPPNM/A), the legal bedrock for physical protection has been extended to cover civilian nuclear material in domestic use, storage and transport as well as civilian nuclear facilities. The newly-added Fundamental Principles of Physical Protection (Fundamental Principles) not only include concrete actions like establishing national legislation and a competent regulatory authority, but also concepts that depend on the State's specific requirements. For instance, the Fundamental Principles call for States to ensure that all organizations involved in physical protection give "due priority" to a strong and enduring nuclear security culture. Although the responsibility to implement and maintain the physical protection regime remains under national responsibility, the Fundamental Principles also recognize the important role of the licensee who ultimately is responsible for physical protection at the facility level or during transport. While it is laudable to invoke such concepts as nuclear security culture in a legally binding international instrument, it raises questions about its effective implementation: how would industry operationalize and demonstrate to the relevant competent authority that this has been met? The paper presents a case for the development of a *nuclear security governance template* that could serve as a framework to demonstrate commitment to and implementation of the Fundamental Principles by licensees. The paper argues that good corporate governance supports key elements of physical protection including security culture. It also emphasizes that good corporate governance cannot be solely externally imposed by a State through the regulatory framework. Rather, it must be internalized and prioritized within an organization as an essential element of operations.

1. INTRODUCTION

After 11 years, the Amendment to the Convention on the Physical Protection of Nuclear Material (CPPNM/A) finally entered into force in 2016. It expands the scope of the Convention on the Physical Protection of Nuclear Material to protect civilian nuclear facilities, as well as civil nuclear material in domestic use, storage, and transport. The entry into force of the Amendment occurred right after the close of the Nuclear Security Summit (NSS) series, reinforcing the gains made at a time when international attention to threats to the civilian nuclear sector, especially concerns regarding theft of nuclear material and sabotage of nuclear facilities, was at an all-time high. Beyond the one-year mark of entry into force of the CPPNM/A, there are still outstanding issues to address: how would State Parties to the CPPNM that have ratified the Amendment encourage universal adherence? And given that there is no definitive set of nuclear security standards that all countries must meet and maintain, is it possible to achieve a level of uniformity so that countries can hold each other accountable to an agreed baseline standard of nuclear security?

Of interest is the use of the terms *reasonable* and *practicable* in the CPPNM/A. This provides States with the flexibility to determine the appropriate level of physical protection for their facilities, and affirms the longstanding view that nuclear security remains under national responsibility [1]. While such broad language poses challenges to effective and consistent implementation of national physical protection regimes across all States, it presents opportunities. Allowing for diverse approaches to meet CPPNM/A obligations could encourage dialogue among countries who are State Parties on what works best for distinct types of facilities and circumstances, insofar as these information exchanges do not compromise sensitive information [2]. A less prescriptive approach also lends greater flexibility, allowing States to adapt as their existing nuclear security concerns evolve and new threats emerge. Most importantly, *reasonable* and *practicable* allows a State to adopt the graded approach to the implementation of its obligations and to take a risk-informed approach– considering factors such as what constitutes credible threats, as well as other operational and financial-related risks – to identify the appropriate nuclear security posture for a given facility without compromising performance of inter alia the physical protection system [3]. Thus, fulfilling the obligations under the CPPNM/A requires a strong working relationship among stakeholders, including policy makers, regulators and the nuclear industry.

In other words, the lack of prescription associated with obligations contained in the CPPNM/A can be one of its strong suits: the absence of a rigid, top-down approach can open opportunities for all invested stakeholders to be involved in the policy discussions as to the parameters of what is *reasonable* and *practicable* under the circumstances.

The paper explores ways in which nuclear industry – the "licensee" – can take on a proactive role in fulfilling the obligations under the CPPNM/A. Specifically, it looks at the licensee's responsibility to implement the requirements that will be set out in the regulatory framework through the Fundamental Principles, especially Principle F on security culture -- arguably the most difficult to assess. Given that security culture depends on many factors including the specific conditions of the work environment and the relationship dynamics in the workforce, how would licensees operationalize and demonstrate due priority to security culture? And is it feasible to develop an industry-led framework on security culture that could help set expectations and best practice across all organizations? The paper proposes a framework that industry stakeholders can adopt to show how a licensee's *corporate governance* model creates the right conditions to foster a strong security culture. This also involves Fundamental Principle J Quality Assurance that encourages the licensee to ensure that a quality assurance policy and programs are established and implemented with a view to providing confidence that specified requirements for all activities important to physical protection are satisfied. Voluntarily offering such information not only encourages knowledge sharing at the operational level, but also could also help establish a foundation for standards and norms for security culture that does not impinge on the additional requirement to protect sensitive information (Principle L Confidentiality).

2. OPPORTUNITIES WITHIN THE CPPNM/A FUNDAMENTAL PRINCIPLES

After the September 11 terrorist attack, countries heavily scrutinized security measures in various critical infrastructures, realizing that non-state adversaries were devising new insidious ways to achieve their objectives. The incident prompted review of Design Basis Threats in several countries to ensure that nuclear facilities could withstand a similar attack by adding force-on-force exercises and other requirements [4]. At the international level, the international community pressed the importance of expanding the scope of the CPPNM; while the drafting process for the Amendment was already underway, the shift in the threat environment since 2001 compelled various countries to promote amendment ratification as soon as possible [5]. But any international-led initiative to strengthen nuclear security will inevitably run into the underlying challenge of determining what can be shared with the international community. Nuclear security is one aspect that makes up the intricate web of national security; oversharing could compromise sensitive information. Thus, the Amendment had to strike a balance in delineating what States should do to strengthen their physical protection regimes while recognizing that they ultimately hold the final determination

since the responsibility for security "rests entirely with the State" [6]. A prescriptive approach to nuclear security could be perceived as a challenge to national authority and potentially discourage countries in supporting the Convention altogether.

Thus, the CPPNM/A's Fundamental Principles were drafted using INFCIRC/225/Rev. 4 (Corrected) to ensure consistency with existing IAEA guidance at the time, and so as not to run contrary to legal agreements States have already implemented that follow INFCIRC/225/ Rev. 4 (Corrected) recommendations [7]. This was further improved with the completion of INFCIRC/225/Rev. 5 (Corrected), which explicitly calls out the Fundamental Principles; the revised recommendations clearly outline the essential cast of characters – the State (Principle A), the Competent Authority (Principle D), and the licensee (Principle E) – and the foundational tasks they must undertake to maintain a strong physical security regime. While the Fundamental Principles and INFCIRC/225/Rev. 5 (Corrected) neatly explain the appropriate relationship among the State, the Competent Authority, and the Licensee, it stops short in describing exactly how each actor should fulfill their respective tasks so as not to infringe upon State's rights to determine their own security requirements. Indeed, certain fundamental principles such as assessing the threat (Principle G) and developing a graded approach (Principle I) must be determined at the State level, which is in turn incorporated into the licensee's security plan and verified by the competent authority. But there are fundamental principles that do not follow a clean progression, and instead should permeate all aspects of the physical protection regime. Security culture (Principle F) fits into this category; the CPPNM/A and INFCIRC/225/Rev.5 (Corrected) note that all organizations at all levels should work together to establish an effective nuclear security culture [8]. The same can be argued for Principle J Quality Assurance, which states that all stakeholders should establish policies and programs to achieve consistent and efficient, high-quality processes to maintain security in all nuclear facilities. For this to be fully realized, each organization must foster values that uphold security such that all personnel internalize the importance of security practices in their work. Thus, security culture and quality assurance cannot be simply imposed externally, but produced organically and shared willingly across the nuclear enterprise. As such, a solely structural approach would not be effective since it would lead only to minimal levels of compliance as opposed to values building and sharing. But how would the international community gauge effective security culture in those State Parties to the CPPNM that have ratified the CPPNM/A? For licensees, this could be achieved by committing to share information about how security policies are incorporated in their corporate governance model.

3. DEMONSTRATING "DUE PRIORITY" THROUGH CORPORATE GOVERNANCE

The concept of corporate governance is drawing new attention due to growing public concerns about lax corporate accountability as witnessed in recent cybersecurity incidents compromising personal data [9]. While there has not been a significant security incident in the nuclear sector that would warrant public scrutiny since STUXNET, there is general unease about how protection of critical infrastructure would hold up to evolving threats, especially an advanced coordinated physical cyber-attack [10]. Organizations across many sectors are beginning to consider ways to publicly showcase responsible behavior, particularly steps taken at the Board and Executive level to assess threats and reduce security risks [11]. The goal is to demonstrate that security is a top priority, and a willingness to exceed minimum regulatory requirements and standards to demonstrate to shareholders, clients, and the general public responsible behavior and duty of care [12]. Studies have shown that corporate governance – the system that defines expectations, controls and monitors organizational matters, and evaluates overall performance – can deeply inform workforce culture, including a sense of responsibility towards security [13]. Although governance is not explicitly called out in the IAEA Nuclear Security Series guidance on Nuclear Security Culture (NSS 7), it raises the importance of managerial leadership to reinforce the belief and attitude that a credible threat exists, and that nuclear security is an important aspect of daily work such that it is widely shared and embraced throughout the organization [14].[1] The key

[1] There are references to aspects of governance in the IAEA Nuclear Security Series guidance on *Objective and Essential Elements of a State's Nuclear Regime* [NSS 20], in other IAEA resources on how leadership affects nuclear safety (i.e., materials for the *IAEA Workshop for Senior Managers on Leadership and Culture for Safety*), as well as in the soon-to-be published

to strong governance, and by extension an effective and sustainable security culture, is that it cannot be externally imposed but must be intrinsically valued.

These observations are not particularly groundbreaking; most individuals can intuit that corporate governance and leadership have a considerable influence on individual work performance. The challenge then becomes a matter of practice: how do organizational leaders create the right conditions such that everyone — from managers to operational-level workers — internalizes the importance of nuclear security so that it automatically feeds into every task? And how would organizational leaders convey these practices to a wider audience to demonstrate that they have given "due priority" in fostering security culture?

There is an emerging interest in some States to adopt outcomes-based performance regulations to encourage strong security culture, as well as good quality assurance policies and other elements under the CPPNM/A Fundamental Principles. For instance, the UK Office for Nuclear Regulation (ONR), as part of its shift towards an "outcome-focused" approach to nuclear security such that the licensee has a sense of "ownership" to security arrangements, has developed the Framework and Fundamental Security Principles (FSyPs) that correspond to the CPPNM/A Fundamental Principles [15]. ONR also issued Nuclear Security Technical Assessment Guides for inspectors to help them ascertain whether the security plans submitted by licensees demonstrate attributes under the FSyPs, including effective leadership and management oversight [16]. These guides do not set out how ONR regulates its duty holders, but rather provide "general advice and guidance to ONR inspectors on how this aspect of security should be assessed" [17].

But overall, the nuclear community has yet to seize the opportunity in highlighting the intimate link between corporate governance and security culture, and the role it plays in operational performance. For instance, the World Institute for Nuclear Security (WINS) found that competent authorities and licensees in the nuclear sector do not raise "security" in annual reporting as often as they do with "safety" [18]. Analyzing annual reports issued between 2014 - 2015, WINS observed that regulators used the word "safety" six times more often than "security," while facility operator reports used "safety" three times as much [19]. But even reports that include "security" are often referencing concepts other than nuclear/plant security, such as financial and energy security [20]**.** Out of the 44 operator annual reports that WINS analyzed, about 80% addressed corporate governance, but only 9% mentioned nuclear security policy. Given public demand for corporate accountability and transparency, and trends towards performance- or outcomes-based regulatory systems to encourage a proactive rather than a compliant mindset among licensees, it is worthwhile to explore what licensees can report to help build confidence in their security practices.

4. A CASE FOR AN INDUSTRY-LED NUCLEAR SECURITY GOVERNANCE FRAMEWORK

Per Fundamental Principle F and the recommendations under INFCIRC/225/Rev.5 (Corrected), all organizations have the responsibility to establish the optimal conditions within their respective environments to forge a strong and pervasive security culture. As mentioned above, these open-ended guidelines lend flexibility to what organizations can use to demonstrate their contributions. The licensees can take initiative to demonstrate their own approaches to security culture, particularly how corporate governance and leadership encourage adoption of characteristics, beliefs, and attitudes necessary to achieve security best practices.

Strong corporate governance also builds a business case for security. There are reputational gains to be made from independently demonstrating a proactive approach to security. Other sectors including shipping, civil aviation, and chemical industries have pursued self-initiated programs to improve security and spur general responsible behavior among industry actors, recognizing that a security incident at one facility could harm an entire industry [21].

guidance document on Sustainability. But as it stands, the linkage between strong governance and strong security culture have not been explicitly called out or explored.

These initiatives have experienced some success in improving public image, and in facilitating better relationships with their respective regulatory bodies. Various institutions within the nuclear community are exploring how some of these models could apply to both nuclear energy and research sectors.[2] There also are potential market and legal incentives for adopting security practices and "standards" beyond minimum compliance [22]. One of the most promising incentive mechanisms stems from a potential gray area in nuclear liability: that the nuclear industry must be ready to demonstrate its *duty of care*, or the duty to protect the public from a reasonably foreseeable security incident, in the court of law. This is especially important in the event of a security breach that does not result in a release of radiation, and therefore existing international nuclear liability regimes would not be triggered [23]. Thus, demonstrating *duty of care* via documentation that an organization – a nuclear facility operator, for example – has done everything reasonable under the circumstances to protect a nuclear facility against a foreseeable attack could help the organization defend itself from negligent security claims.

4.1. A potential framework – a nuclear security governance template

One way for licensees to demonstrate a proactive approach to security is to voluntarily offer information about how their respective governance models manage security risks for a given facility, i.e., how security risks are communicated and assessed by Board Members, Directors and other high-level leadership. Decision-making at the top affects the rest of the workforce by encouraging operational-level workers to hold *everyone* accountable, including managers. Sharing this information would not necessarily divulge sensitive information since it is an insight into managerial processes, and not details of sensitive security measures or information. Thus, the focus is on organizational decision-making and how this affects the beliefs and attitudes of the individuals tasked as the responsible custodians of nuclear material and technologies.

Licensees can offer such information through a *nuclear security governance* template, a document that presents key questions organizational leadership, including Boards of Directors and Executive Managers, should be able to address in their reporting to competent authorities and in regularly published annual reports. The first iteration of the template was developed and included in the WINS Corporate Governance Arrangement for Nuclear Security report released prior to the 2016 NSS [24]. Building off this version, participants in the 2016 Nuclear Industry Summit (Working Group III - The Role of Nuclear Industry in the World and How it Manages the Security of its Materials and Technologies) discussed the utility of the template and offered adjustments so that the questions align with industry experience [25]. Since then, WINS and the Stimson Center have shared the early iterations of the template in a series of industry roundtables to test its viability and to receive critical feedback. The process of prototyping, iterating, and obtaining criticism is key to designing a final template that provides maximum utility to all users, i.e., the licensees who will provide the answers, as well as the competent authorities and the general public who will review its contents.

The latest version of the template includes new questions based on documents from the International Atomic Energy Agency, particularly NSS7 on Nuclear Security Culture [26]. The template also pulls from the WINS Best Practice Guide on Security Governance – one of the earliest analyses linking corporate governance and security culture [27]. It also incorporates insights from the World Association of Nuclear Operators (WANO) and the U.S.-based Institute of Nuclear Power Operators (INPO) industry guidance for *safety* as these leadership recommendations can help develop strong nuclear security practices [28]. Aligning the template to these various resources helps integrate all the different information on security culture in one document. Moreover, the template reworks important

[2] For more information regarding work on industry cross-collaboration to improve security, please see Stimson Center's work on nuclear security incentives (https://www.stimson.org/content/nuclear-energy-securing-future-case-voluntary-consensus-standards); the World Institute for Nuclear Security (https://www.icao.int/Meetings/AVSEC/Documents/AVSEC2017%20PROGRAMME.pdf); and the Pacific Northwest National Laboratory (http://cgs.pnnl.gov/self_regulation.stm).

recommendations from all these resources into open-ended questions such that licensees are tasked to explain exactly how they achieve a certain recommendation within their organization.

Currently, key questions in the template are divided into four categories:[3]

— Leadership and Oversight: To gain insight into decision-making processes
- How does the Board of Directors[4] ensure good governance and oversight over the organization's security program?
- How do *Executives* demonstrate commitment to security and manage and control the implementation of the nuclear security program?

— Nuclear Security Risk Assessment: To gain insight into how an organization assesses threat and adopts a risk informed approach
- Overall, how does your organization develop a definition for its acceptable risk?
- Have you taken measures to ensure proper coordination among safety, security (including cyber) and emergency response arrangements and have adopted an all-hazards approach to risk management?

— Shared Understanding of Nuclear Security: To gain insight into how leadership communicates and encourages security practices at every level of the workforce
- What is the published policy for nuclear security in your organization?
- How does management convey the rationale for significant decisions relating to security to stakeholders and reinforce good behaviors?
- What are processes / mechanisms in place for leadership and workforce to continually challenge and test basic assumptions about security (and safety)?

— Evaluation and Continuous Learning: To gain insight into how all staff members are evaluated in their security proficiency, and the opportunities provided for improvement
- Is your nuclear security program performance based? What can you say about your use of leading and lagging indicators?
- Are personnel at the facility appropriately screened and trained in security?
- Do you regularly assess the effectiveness of your nuclear security, including cyber security?
- Does the organization have the tools and resources available to assess security performance and implement improvements?

The template is under review by select industry stakeholders to ensure that the questions are not overreaching but are challenging enough such that top-level managers and boards/advisors find it a useful tool in presenting their security governance model.[5] Continued industry input is a critical element of the template design process; it is important that the template accounts for the on-the-ground realities executive leaders face when running a facility and maintaining a viable business. Nuclear industry operators serve as the front line in nuclear security and would inevitably be responsible for establishing and demonstrating some of the Principles. Engaging industry, potentially through the Nuclear Industry Steering Group for Nuclear Security, to develop such a template would allow industry

[3] Each question under the four categories has three or four sub-questions to further guide what the answers should cover. The Stimson Center and WINS are in the process of refining the latest iteration of the template; the sub-questions are not appended to this paper as they are a work in progress. See: www.stimson.org/nucleargovernance.

[4] The term Board of Directors is used to represent a senior oversight body that represents the interests of the owners of the operation, be they state, public or private entities.

[5] The Stimson Center is also exploring whether such a governance template could have the same functionality and value in a state-owned enterprise. Based on preliminary assessments, such a governance template may be applicable; while state-owned enterprises select the executive-level leadership to manage companies, the expectations and responsibilities of these managers are essentially the same as those expected from the public sector. Work on this issue is ongoing.

stakeholders to weigh in on what is reasonable and practicable given their unique risk situations. Ideally nuclear industry, alongside regulatory bodies, would eventually preside over the template design process so that it is driven by both sides and can be incorporated into formal regulatory security culture assessments. Eventually, the template could be used as a factor that demonstrates implementation of CPPNM/A Fundamental Principle F.

5. CONCLUSION

The proposed template is not an exhaustive list and does not claim to be the determining factor of what constitutes "good" or "strong" governance. Rather, it is a resource to help licensees illustrate how security considerations are decided, implemented, and internalized by their organization. Reporting this information could lead to two constructive outcomes: (1) to develop a confidence-building mechanism that demonstrates strong security without relying on top-down regulatory structures, and (2) to informally establish new norms for industry around the world by setting expectations for transparency, particularly how top-level managers should engage their workforce on security issues. For existing facilities, the governance template should be an easy exercise – if a strong security culture already exists in the workplace, it is a matter of recording the narrative to showcase operational excellence. For licensees that have yet to achieve a strong security culture or are in initial phases of doing so, seeing other industry responses could be a motivating factor to step up to the plate. While the template itself is in the nascent stages of development, the idea of creating and implementing this type of informal instrument poses a grand proposition to those committed to nuclear security: leverage the flexibility that surrounds implementation of a State's obligations under the CPPNM/A to establish innovative mechanisms that encourage nuclear security at the operational level, which could eventually contribute to the most effective implementation of the obligations under the Convention. In this case, the template – if adopted by a critical mass of licensees and integrated into regulatory reporting to demonstrate strong security culture – could become a mechanism to demonstrate compliance under the CPPNM/A, and build mutual confidence among States Parties.

ACKNOWLEDGEMENTS

The authors are grateful to Rhonda Evans at the World Institute for Nuclear Security (WINS), and Debra Decker, Jackie Kempfer, and Endi Mato at the Stimson Center for their valuable feedback on this paper and the process of developing a nuclear security governance template. Their encouragement, as well as persistent questioning of our ideas and assumptions, has led us to strengthen this concept further. The Stimson Center would like to acknowledge the MacArthur Foundation and the U.S. State Department – Partnership for Nuclear Security for their continued support, which has made Stimson research in this area possible.

REFERENCES

[1] Amendment to the Convention on the Physical Protection of Nuclear Material, INFIRC/274/Rev.1/Mod.1, IAEA, Vienna (2016).

[2] DECKER, D., HOWSLEY, R., RAUHUT, K., "Industry's potential role in implementing the CPPNM amendment and improving nuclear security", paper presented at the IAEA International Conference on Nuclear Security: Commitment and Actions, Vienna, 2016.

[3] Ibid.

[4] HOLD, M., ANDREWS, A., Nuclear Power Plant Security and Vulnerabilities, Congress report, Congressional Research Service, Washington D.C., 2014. ; IKASSON, S., RITCHEY, T., "Protection against sabotage of nuclear facilities: using morphological analysis in revising the design basis threat", adaptation of a paper presented at the 44th Annual Meeting of the Institute of Nuclear Materials Management, Phoenix, 2003. ; KOVCHEGIN, D., "Approaches to design basis threat in Russia in the context of significant increase of terrorist activity", paper presented at the Institute of Nuclear Materials Management 44th Annual Meeting, Phoenix, 2003.

[5] The International Legal Framework for Nuclear Security, IAEA International Law Series No.4, IAEA, Vienna (2011).

[6] Amendment to the Convention on the Physical Protection of Nuclear Material, INFIRC/274/Rev.1/Mod.1, IAEA, Vienna (2016).
[7] "Measures to improve the security of nuclear materials and other radioactive materials", General Conference (45/1), IAEA, Vienna (2001).
[8] Amendment to the Convention on the Physical Protection of Nuclear Material, INFIRC/274/Rev.1/Mod.1, IAEA, Vienna (2016). ; Nuclear Security Recommendations on Physical Protection, INFIRC/225/Rev.5, IAEA, Vienna (2011).
[9] TIERNEY, B., USA Today (2017), https://www.usatoday.com/story/opinion/2017/09/18/equifax-data-breach-how-do-you-fix-cataclysmic-crisis-brian-tierney-column/675183001/; WRIGHT, R., TechTarget (2017), http://searchsecurity.techtarget.com/podcast/Risk-Repeat-Equifax-data-breach-fallout-continues.
[10] PJM Interconnected, PR Newswire (2017), http://www.prnewswire.com/news-releases/pjm-conference-on-grid-resilience-explores-new-challenges-to-grid-security-300522858.html.
[11] SANTARCANGELO, M., CSO Online (2017), https://www.csoonline.com/article/3219830/leadership-management/security-leaders-need-better-visibility-of-risk-before-the-board-asks.html; Corporate Practice Group, National Law Review (2017), https://www.natlawreview.com/article/ransomware-and-corporate-governance.
[12] CENSER, M., Inside Defense (2016), https://insidedefense.com/daily-news/industry-experts-say-companies-should-go-beyond-minimum-standards-insider-threats; RAUHUT, K., UMAYAM, L., Stimson Center (2017), https://www.stimson.org/content/demonstrating-due-care-cyber-liability-considerations-nuclear-facilities.
[13] KOH, K., RUIGHAVER, A.B., MAYNARD, S., AHMAD, A., "Security governance: its impact on security culture", Proceedings of the 3rd Australian Information Security Management Conference, Perth (2005).
[14] Nuclear Security Culture: Implementing Guide, Nuclear Security Series No.7, IAEA, Vienna (2008).
[15] SAVAGE, R., "The UK nuclear renaissance: ONR delivering innovative and enabling regulation in the global nuclear environment", presented at the U.S. Nuclear Regulatory Commission 29th Annual Regulatory Information Conference, Washington D.C., 2017.
[16] Security Governance and Leadership, Nuclear Security Technical Assessment Guide, official report CNS-TAST-GD-1.1, Office for Nuclear Regulation, Bootle, 2017.
[17] Ibid.
[18] Corporate Governance Arrangements for Nuclear Security: Analysis of Annual Reports from Companies and Regulators, World Institute for Nuclear Security, Vienna, 2016.
[19] Ibid.
[20] Ibid.
[21] HUND, G., ELKHAMRI, O., Industry Self-Regulation as a Means to Promote Nonproliferation, PNNL-15355, Pacific Northwest Center for Global Security Publication, Pacific Northwest National Laboratory, Seattle (2005).
[22] DECKER, D., RAUHUT, K., Policy Analysis Brief: The Quest for Nuclear Security Standards, The Stanley Foundation, Washington D.C., 2016.
[23] RAUHUT, K., UMAYAM, L., Stimson Center (2017), https://www.stimson.org/content/demonstrating-due-care-cyber-liability-considerations-nuclear-facilities.
[24] Corporate Governance Arrangements for Nuclear Security: Analysis of Annual Reports from Companies and Regulators, World Institute for Nuclear Security, Vienna, 2016.
[25] Working Group III, "The Role of Nuclear Industry in the World and How it Manages the Security of its Materials and Technologies", Nuclear Industry Summit, Washington, DC, 2016.
[26] Nuclear Security Culture: Implementing Guide, Nuclear Security Series No.7, IAEA, Vienna (2008).
[27] Traits of a Healthy Nuclear Safety Culture, INP12-012, Institute of Nuclear Power Operators, Atlanta (2012) ; WANO: Principles – Traits of a Healthy Nuclear Safety Culture, PL 2013-1, World Association of Nuclear Operators, 2013.