NUCLEAR ENERGY: SECURING THE FUTURE

A CASE FOR VOLUNTARY CONSENSUS STANDARDS

DEBRA DECKER AND KATHRYN RAUHUT

STIMSON

JANUARY 2016

Cover image: camknows via Flickr Creative Commons

Stimson Center
1211 Connecticut Avenue, NW
8th Floor
Washington DC 20036
www.stimson.org

CONTENTS

ACKNOWLEDGMENTS

This paper is based on more than 150 confidential interviews with stakeholders from 2014 to 2015 and on research supported by the US State Department Partnership for Nuclear Security and the Stanley Foundation, with pro bono support from Pillsbury Winthrop Shaw Pittman, LLP. The Stimson Center is grateful to the MacArthur Foundation for the early support it provided to this project. The report authors would also like to thank the following people for their contributions to this effort: Brian Finlay, Gerson Sher, Roger Howsley, Roger Brunt, Dan Lipman, and Anya Loukianova. Much gratitude is also extended to the many individuals in the nuclear industry, governments and intergovernmental organizations, standards/auditing/technical support organizations, and universities who were willing to speak off the record and share their insights. Finally, this paper would not have been possible without the invaluable support of Stimson research assistant Ariella Knight and the many Stimson interns/fellows who helped on this project: Joseph Coye, Matt Ellison, Luana Macinic, Levi Maxey, James McKeon, Rose Morrissy, and Nicole Restmeyer. The recommendations in this paper are the authors' own.

About The Authors

Debra Decker is a Senior Advisor at the Stimson Center's Managing Across Boundaries Initiative. She is a strategy and risk expert with a specialization in critical infrastructure and weapons of mass destruction. She has advised public and private sector clients as an independent consultant, as a manager of planning, and under contracts with Booz Allen Hamilton. Her research areas include nuclear forensics, public preparedness, civil society engagement for international security, nuclear insurance, and terrorism risk insurance. Her work has been featured internationally, including at the World Economic Forum and UN Security Council. She has also been a research associate at Harvard University Kennedy School's Belfer Center for Science and International Affairs, and currently serves on the Board of Governors of the Washington Foreign Law Society. She holds a BA in economics and international relations from American University, an MBA from the University of Pennsylvania's Wharton School, and an MPA from Harvard University's Kennedy School.

Kathryn Rauhut is an attorney based in Vienna, Austria, specializing in international security. She works primarily on nuclear security governance, accountability, and liability issues with a focus on cybersecurity. Prior to her work with the Stimson Center's Managing Across Boundaries Initiative, she was a Strategic Advisor to the Internet Security Alliance and to the World Institute for Nuclear Security (WINS). In her role at WINS, Ms. Rauhut led international roundtables and authored policy papers on improving global governance of nuclear and cybersecurity through building the business value of security. She has lectured internationally at numerous conferences on market incentives including tort liability, cyberinsurance, and limited liability. From 1990 to 2005 she was a senior attorney and from 2005 to 2010 she was the Deputy General Counsel for Lawrence Livermore National Laboratory in California. She is a member of the California Bar Association, the American Bar Association, and the International Nuclear Lawyer's Association.

About The Stimson Center and Managing Across Boundaries Initiative

The Stimson Center is a nonprofit, nonpartisan institution devoted to enhancing international peace and security through a unique combination of rigorous analysis and outreach. Stimson's Managing Across Boundaries Initiative (MAB) develops innovative government responses at the national, regional, and international levels, and identifies pragmatic public-private partnerships to mitigate complex transnational challenges. Read more about the Stimson Center at **www.stimson.org**.

EXECUTIVE SUMMARY

The Challenge

As global energy demands grow in parallel with climate change and energy security concerns, States are looking to nuclear power to satisfy their baseload electricity needs and reduce their reliance on carbon fuels. Nuclear new builds need to have comprehensive security measures incorporated into their planning, design, construction, and operations because the consequences of nuclear incidents can be grave – as the world has witnessed in Japan, the Ukraine, and the United States. Existing nuclear power plants were not designed to meet the challenges of today's terrorist attacks. Governments, the private sector, and citizens all have an interest in incident-free facility operations that are efficient and profitable. However, current international oversight mechanisms are insufficient, and national oversight through domestic nuclear regulators is challenged by differing levels of experience and conflicting cultural norms. In addition, operators are faced with implementing complex and sometimes conflicting guidelines with limited industry input and a corresponding lack of commercial motivation.

An Opportunity

As the fourth and final Nuclear Security Summit approaches, it is time to energize nuclear security – in particular through new approaches. The summits have brought needed attention to the issue of nuclear security and have made some good progress in addressing selected risks. After the final Nuclear Security Summit in March 2016, a framework will be needed to sustain momentum. The imperatives for nuclear security and safety already exist in treaties, conventions, and UN Security Council resolutions; however, the details of how to implement the agreements often pose dilemmas. With the Amendment to the Convention on the Physical Protection of Nuclear Material likely to enter into force in 2016, and States looking for guidance on complying with its principles, the global community now has an opportunity to support a new framework of multistakeholder engagement to develop voluntary performance standards and to include industry in their development. Such standards could be used to demonstrate compliance with internationally agreed-upon principles. Financial and nonfinancial incentives could be structured to motivate voluntary compliance with these standards so that security can become a valuable commodity instead of an add-on cost.

Recommendation

Policymakers and governments need to facilitate the development of a business case for nuclear security.

Policymakers and governments need to facilitate the development of a business case for nuclear security. Voluntary consensus standards should be developed with direct input from stakeholders, starting with areas of critical interest to industry. The standards must be such that:

- Operator adoption of the standards would mean that critical areas of risk are reduced and/or better managed, and, as a result, would assure more efficient, profitable nuclear operations that continue to be safe and secure.
- Compliance with a standard would demonstrate the competence of the organization and its personnel and would reduce risks. Operators with verified standards compliance must be able to obtain commensurate external benefits in insurance terms, financings, rating-agency assessments, liability limitations, regulatory recognition, and/or public acceptance.

Advocacy is needed to drive such an effort to adapt general State-level guidance from institutions such as the International Atomic Energy Agency (IAEA) into voluntary standards for operators that can be verified by a third party. Voluntary standards could be developed in selected areas of risk that are of highest interest to industry, such as cybersecurity, human-reliability assurance (e.g., integrated safety-security culture, insider threat mitigation), and other areas including export controls.

The World Institute for Nuclear Security (WINS) should lead a a working group of industry stakeholders, including the World Nuclear Association (WNA) in this effort. Assistance could be provided via the International Framework for Nuclear Energy Cooperation (IFNEC) and/or from a consortium of regulators such as the Western European Nuclear Regulators Association and the Forum of Nuclear Regulatory Bodies in Africa and the US Nuclear Regulatory Commission (NRC).

The project could also be pursued on an "incremental" basis through actual initiatives that are currently being undertaken by private sector and governmental organizations. For example, IFNEC is taking a multinational approach to facilities for the disposition of spent power-reactor fuel. Such collaboration within IFNEC could provide an opportunity for industry and governments to seek consensus on all aspects of such a facility, including physical security, cybersecurity, and organizational culture standards.

NUCLEAR POWER FACES UNCERTAINTIES AND RISKS

> "In the 2D scenario, global installed capacity would need to more than double from current levels of 396 GW to reach 930 GW in 2050, with nuclear power representing 17% of global electricity production."
>
> INTERNATIONAL ENERGY AGENCY/ NUCLEAR ENERGY AGENCY, 2015

Global nuclear expansion comes with increased concerns

The Fukushima incident in Japan caused countries to rethink their current reliance on and future development of nuclear energy. However, many countries reaffirmed their commitment to nuclear development. Even the European Parliament's Energy Roadmap 2050 agreed on the principle that nuclear energy would continue to play a large and significant role in energy production.[1] Nuclear is a large, stable baseload power source with low carbon emissions. The 2015 joint report of the International Energy Agency and Nuclear Energy Agency notes that to meet the goal of limiting the rise in global temperature to two degrees Celsius by 2100, energy emissions need to be cut 50 percent by 2050; to achieve this, the nuclear power industry must double its capacity.[2] Indeed, 65 power reactors are currently under construction worldwide, with China accounting for the largest share of this increase. Countries from Egypt to Indonesia are considering nuclear power generation, and so-called newcomer countries with limited or no experience operating nuclear power reactors present even higher risks (see Appendix I). This expansion and the related increased commerce in nuclear materials raise the potential for future adverse incidents as well as the need for new ways to mitigate security and other risks.

Some States with existing nuclear power facilities, as well as newcomers, are challenged by an array of governance issues including regulatory capability, reputational risk, and human resource issues. Regulatory oversight is often initially placed within an atomic energy agency that promotes development, which is in potential conflict with regulatory enforcement, and safety and security oversight may reside in different State entities. Questions have also arisen about regulators' relationships to plants under the build-own-operate (BOO) model, such as Rosatom's in Turkey,[3] and which risks are increased or reduced in the BOO model.[4] Furthermore, regulators and insurers have found that even within one country, behavioral norms can differ within each facility as a result of variations in management and oversight.

Challenges are plentiful. The industry has to contend with aging infrastructure and facilities, rapidly evolving cybersecurity challenges, and new plant designs. Even with security and safety built into some new plant designs, industry is apprehensive over the likely high cost of regulator-defined security affecting the profitability of the developing small modular reactors. Furthermore, the escalating costs of new builds make nuclear facilities more costly to finance and thus to insure.

Threats, vulnerabilities, consequences pose potentially high risks

These general concerns are all in addition to rising threats from malevolent actors that could target nuclear operations. Terrorist attacks against vulnerable populations have increased, with tragedies in many countries that could easily be translated into attacks against vulnerable targets.[5] With Boko Haram and ISIL in or near countries that have or are considering nuclear facilities, and with the spreading reach of all terrorists – including through cyber – potential threats increase.

But how vulnerable are nuclear facilities to threats? One recent Harvard study finds: "There are still countries with: no on-site armed guards to protect nuclear facilities…; no required background checks be-

fore granting access to nuclear facilities and materials; and limited protections against insider theft. Few countries conduct realistic tests of their nuclear security systems' ability to defeat determined and creative adversaries; and few have targeted programs to assess and strengthen security culture in each relevant nuclear organization."[6] Nuclear security is only as good as its last successful ability to prevent, detect, and respond to a nuclear security event. The global threat, planning, and coordination of recent terrorist attacks, such as those recently in Europe, only highlight the urgency.

Vulnerabilities are compounded by simple lack of awareness. Although industry associations share information on safety, they often consider security information too sensitive to share and/or not within their purview. Considering cyber risks, a Chatham House report notes that nuclear energy executives lack sufficient awareness of cyber threats and vulnerabilities due partly to a lack of information sharing both within the nuclear industry and with other industries; developing countries are particularly at risk given their limited resources to invest in cybersecurity.[7] (See Appendix III for a sample of some incidents.) Most recently, one plant at the facility in Doel, Belgium, was sabotaged in 2014, and another plant was faced with a fire after an open-air transformer exploded in 2015.[8] Transformers and the grid can be an issue as nuclear plants not only contribute power to the electric grid but also rely on electricity for running and maintaining their plant operations.

> "The August 19, 2006, shutdown of Unit 3 at the Browns Ferry nuclear plant near Athens, Alabama, demonstrates that not just computers, but even critical reactor components, could be disrupted and disabled by a cyber attack … The failure of these controllers was not the result of a cyber attack. However, it demonstrates the effect that one component can have on an entire PCS network and every device on that network. Combined with the Davis-Besse worm infection, the Browns Ferry shutdown presents a possible attack scenario."
>
> BRENT KESSLER, "THE VULNERABILITY OF NUCLEAR FACILITIES TO CYBER ATTACK," CITED IN 2015 DHS REPORT

The electric sector and nuclear facilities have indeed been targets. Two of the most infamous attacks to date have been: the 2013 sniper attacks on transformers supporting the electric grid in California, with an insider likely involved;[9] and the 2007 attack – also with reported insider assistance – on a South African nuclear research facility that houses highly enriched uranium.[10] The defense-in-depth approach that commercial power facilities generally follow allows for multiple, independent, redundant systems to protect against hazards; thus these events were not of high consequence.

Yet, incidents happen that defy the defenses. Emergency response plans limit consequences, but major events can displace populations – temporarily as with Three Mile Island, or longer term as with Chernobyl and Fukushima. Less considered but of important consequence is the possible loss of electric output from a plant, especially any long-term outages. For countries without an integrated, well-managed grid system, heavy reliance on a nuclear plant that suffers an outage could lead to incapacitating blackouts.

Good practices need to be front and center

The potential for establishment of agreed-upon baseline good practices can help address some of these risks and reduce uncertainties associated with the expansion of nuclear power. Efforts to reduce some of the risks would be easier to undertake today than in the future. Currently there are only about 30 countries operating commercial nuclear power plants. This number is likely to increase by about 50 percent over the next 25 years, even without considering the development and potentially widespread use of small modular reactors in the future.

CURRENT OVERSIGHT MUST BE AUGMENTED BY INDUSTRY SELF-REGULATION

Despite these efforts, the lack of confidence in some regulators continues to challenge the reputation of the overall nuclear industry.

Some guidance exists toward good practices — in principle

International conventions, UN resolutions, and many initiatives call for good nuclear safety and security. However, these provide very high-level guidance and few specifics. For example, UN Security Council resolution 1540 (2004) requires States to prevent proliferation through "appropriate effective" measures to account for and secure WMD, their means of delivery, and related materials.[11] The Amendment to the Convention on the Physical Protection of Nuclear Material, which applies to nuclear materials and facilities used for peaceful purposes, requires States to apply certain "fundamental principles" that include "due priority" to a security culture in all organizations responsible for physical protection of nuclear facilities, and calls for "quality assurance" programs.[12]

Such high-level principles get translated into general support for the development of good practices. This general support starts with helping the State fulfill its responsibilities through the development of its laws and regulatory structure, and cascades down to some guidance for facilities themselves. However, the broad, general support means that States and operators may not know how to prioritize efforts or how to implement the requirements.

For example, a sound regulatory regime requires an independent, competent, and capable regulator with the requisite oversight and enforcement authority. The International Atomic Energy Agency (IAEA) helps develop and strengthen national regulatory regimes by providing support for cooperative regulatory networks[13] and self-assessment tools of regulatory infrastructure for safety and regulator training.[14] The IAEA also reviews the regulatory regimes in countries upon their request,[15] while other organizations provide additional support. NEA, part of the Organization for Economic Cooperation and Development (OECD), has recently developed guidance on "The Characteristics of an Effective Nuclear Regulator," and has produced many regulatory guidance documents.[16] Despite these efforts, the lack of confidence in some regulators continues to challenge the reputation of the overall nuclear industry. The lack of transparency to stakeholders of IAEA assessments limits the pressure to truly change regulator structures/behaviors. Regulations and regulatory structures and facility operations tend to improve only after an incident occurs. Indeed, it took the Fukushima disaster for Japan to reform its regulatory structure to better ensure independence and to integrate safety, security, and safeguards oversight[17] – yet some still question the ability of the new regulator to be independent.[18]

Self-regulation can give traction to nuclear security guidance

Such regulatory assistance is part of a larger framework of support for nuclear safety and security that includes IAEA-developed safety standards and security principles as well as industry association guidelines and peer reviews. For safety, the IAEA further developed specific standards that address the "what" for general safety requirements, and are supported by technical documents to address the "how" for achieving those safety outcomes. The IAEA-developed security series is a similar series of

documents that include "fundamentals" and "recommendations" as well as "implementing guides" and "technical guidance" – notably omitting the term "standards."

Most IAEA guidelines are documents reflecting the consensus of States. While industry input to guidance documents is valued, the IAEA's mission is to work with its member countries. The responsibility of sharing the draft principles and obtaining feedback from industry lies with each member country. Some states have a systematic approach for obtaining industry input, but many do not. While the IAEA is making draft guidance more available,[19] private sector input is generally still lacking. Thus operator considerations do not weigh as heavily in the documents.

The IAEA's guidelines are nonbinding, and are not enforceable unless a State adopts specific legislative authority implementing the guidance — and then the State has to actually exercise enforcement. Because the guidance can be general, States' actual implementation and enforcement varies.

The IAEA's guidelines are nonbinding, and are not enforceable unless a State adopts specific legislative authority implementing the guidance – and then the State has to actually exercise enforcement. Because the guidance can be general, States' actual implementation and enforcement varies. In addition, recent letters from the chairman of the International Nuclear Safety Advisory Group note that countries themselves are not taking seriously enough their obligations to fortify their safety regimes, and that the risks and uncertainties to a facility involving externally initiated events need to be better considered.[20] This raises the question of where the responsibility for high-quality performance should be placed if a State is not able to sufficiently execute its regulatory responsibilities and if operators are not motivated by IAEA guidelines they have had little input in developing. If troubling issues exist in the safety regime, issues for the security regime – a newer framework – certainly exist.

Independent of a regulator's ability to represent the public's interest in ensuring good nuclear operations, the operator has strict liability for facility operations per the international treaty regimes, and thus has an interest in ensuring high-quality plant operations. Although some may say operators are responsible for safety and the government is responsible for security, inevitably both safety and security are the day-to-day responsibility of the operator.[21] A State will often define the level of security in terms of the maximum threat against which an operator has to defend, with the "design-basis threat" defining some of the physical security requirements for a facility[22] along with some IAEA best practices for managing them,[23] but ultimately, maintaining a plant culture that values professional operations, including for security, is a responsibility of management. Self-regulation thus becomes of high importance.

In addition to the operator and the owner of the plant, the insurer and financer of the plant all have an interest in ensuring plant performance without losses. As some treaty revisions increase liability limits, operators have to look for additional insurance. And as costs of new nuclear power plants rise, owners and financers of the plants also have increased amounts at stake simply in property and business continuity.

Nuclear operators are justifiably concerned about their return on additional security investments that may not translate into immediately measurable benefits. Effective incentives can help the private sector justify the costs of improved security, including cybersecurity, by balancing the short-term costs of additional investment with commercial benefits.

PEER REVIEWS AND TRAINING HELP IMPROVE PERFORMANCE

Some peer-review processes exist to educate operators and to evaluate performance at nuclear power facilities. Some drive change but some have less impact.

IAEA and industry support good practices

To be confident of a secure nuclear future, good operator performance must be built and sustained. The operators, those responsible for good plant performance, range from private companies to public utilities.[24] In newcomer countries, the State government typically is the majority owner of the plant,[25] with operations originally the responsibility of the initial contractor, overseen by a newly empowered regulatory authority.[26]

Some peer-review processes exist to educate operators and to evaluate performance at nuclear power facilities. Some drive change but some have less impact.

- The IAEA offers a multitude of review and support services,[27] including to operating licensees.[28] However, these safety and security reviews are done only upon country request. These are unlike the International Civil Aviation Organization (ICAO) activities in which state contracting parties have to submit to mandatory audits on a regular basis.[29] Nonetheless, the IAEA has tried to establish a de facto norm of State reviews with scheduled follow-up missions to assess progress and with State publication of review results, in summary if not in full. Such a norm is an excellent aspiration but may be hard to achieve unless States and facilities can be convinced of the benefits of doing this, beyond simple reputational ones. In addition, many more States have to be convinced to subject themselves and/or their facilities to time-consuming reviews.
- Nuclear industry self-regulation began when the Institute of Nuclear Power Operations (INPO)[30] was established by the US nuclear industry after the Three Mile Island accident in 1979. Promoting excellence, rather than simply complying with regulations, is fundamental to INPO's role in raising nuclear power's safety performance. Other key factors in effective self-regulation include gaining CEO and senior management personal support and engagement, and gaining industry-wide support for safe and secure operations. INPO considers peer pressure to be one of its most effective tools for improving safety and performance. INPO conducts on-site plant evaluations approximately every two years, and requires a safety culture self-assessment in the years between the external reviews. INPO findings and ratings are confidential and are communicated only to the operator and the industry's collective insurance company, Nuclear Electric Insurance Limited (NEIL). NEIL is not actually an insurance company, but an operator risk-sharing mutual insurer. NEIL requires INPO membership as a condition of insurability, and it uses plant insurance evaluation ratings as a factor in setting insurance premiums. Operator training is independently accredited through the National Nuclear Accrediting Board, part of INPO's oversight function. Because of the independence and influence of INPO reviews on insurers as well as on some plant manager and employee benefits tied to good INPO ratings, INPO can greatly incentivize improvements in operator performance.[31]
- The World Association of Nuclear Operators (WANO), established in 1989 after the Chernobyl nuclear plant disaster in 1986, promotes nuclear safety and reliability among nuclear power plant

operators around the world.[32] Since the Fukushima nuclear disaster, peer inspections went from being voluntary every six years to being mandatory every four years as a condition of membership. WANO also requires an internal assessment between reviews, as INPO does. Operators can be affiliated with different regional centers of WANO, not necessarily their local regional office. WANO is looking to have its regional offices be more consistent in their approaches.

The IAEA traditionally has separated its safety and security functions and reviews. WANO only focuses on safety but recognizes that some areas, such as human reliability and cybersecurity, affect the safe performance of operators. INPO includes cybersecurity in its assessments.

WINS security training also helps performance

In addition to making good use of the review services, operators can improve performance through engagement with WINS. Established in 2008, WINS is a nongovernmental organization whose mission is to improve the security of nuclear and radioactive materials.[33] In 2014, it launched an Academy to begin to train and certify nuclear security professionals. The program is partly based on the obligations made by 35 States at a Nuclear Security Summit to ensure that all personnel with accountabilities for nuclear security are demonstrably competent. The WINS certification program is in its early stages (in the first year 600 people registered for the program from over 70 countries), and it is beginning to gather and analyze data to measure impact on participation through key performance indicators. As WINS rolls out its training programs, it hopes to be able to demonstrate measurable increases in organizational performance and reductions in risk.

The ability to demonstrate a return on security investment associated with WINS certifications will enable insurers, financiers, and regulators to consider giving preferential terms to operators that have more staff who are security certified. Ideally, certification of security personnel will become an industry norm. Indeed, that is the hope.

Broader benefits are harder to assess

With all the support for good practices and security trainings, what are the issues?

The problem is multi-faceted. Much IAEA guidance exists in safety and security, but operators must sometimes make unclear trade-offs between safety and security. The IAEA performs reviews only upon State invitation. The WANO and INPO reviews look to develop overall good plant operations but do not place security as a priority within their mandates. All the reviews do not necessarily compel change. Transparency is lacking, thereby reducing confidence: an assessment is not generally shared unless the reviewed party decides to release it. Investments in security and in security training in particular are often considered costly investments – with potential gains not clearly evident.

If those who could provide benefits to operators were involved in developing and validating the good practices, a more secure nuclear future could be developed and sustained.

If those who could provide benefits to operators were involved in developing and validating the good practices, a more secure nuclear future could be developed and sustained.

MULTISTAKEHOLDER-DEVELOPED STANDARDS CAN DRIVE COMMERCIAL BENEFITS

This interconnectedness of risk creates an important mutuality of concern and motivation to reduce risk among insurers internationally.

Insurers can help develop standards

Security is expensive and operators face difficult trade-offs between profitability, safety and security. Insurance, if properly tailored, can be an important component of a security strategy. However, only in the case of a mutual insurer, such as the US-based NEIL, does the insurer perform a true risk-control function with clear benefits.[34] In the US case, the interrelationship of INPO peer reviews and accredited training, strong regulatory oversight,[35] and a mutual system for property and business continuity insurance make for a strong system that supports high-quality management and performance.[36] This mutual risk-sharing program illustrates the advantages of self-regulation. Mutual monitoring is incentivized because an operator with a substandard plant increases the financial exposure of all other operators.

Internationally, insurers – more than operators – are interested in the performance of each other's plants. With the longest history of insuring nuclear power, the US has the most well-developed nuclear insurance scheme – but even US insurers share risks with their overseas counterparts. Under the US Price-Anderson Act, the nuclear industry is required to maintain liability insurance to compensate the public in the event of a nuclear incident when there is a release of radiation above a threshold amount. While the cost of this insurance is borne by the industry, Price-Anderson sets a limit on liability, with any additional liability the responsibility of the government. Even with limited liability, nuclear insurers take on significant concentrated risk. The United States, with the most nuclear power plants, has the largest capacity by far at $13.6 billion in liability insurance coverage. To manage this risk, insurers form a domestic nuclear pool and also reinsure their domestic risks with foreign nuclear pools. Internationally, many pools reinsure each other.[37] Typically an insurer looks at the specific risks being insured at a foreign facility before deciding to provide reinsurance, but this may also be evaluated on a percent-of-coverage basis if the insurer and the foreign insurer have previously agreed to terms and limits. This interconnectedness of risk creates an important mutuality of concern and motivation to reduce risk among insurers internationally.

Insurers and reinsurers said they typically conduct a three- to five-day plant survey, and, depending on the facility, may be allowed read-only access to the WANO peer-review recommendations to assist in their assessment. Insurance terms for nuclear facilities do reflect risk to some extent. As one insurance industry executive explained, premiums follow a "U curve": higher premiums for new entrants and/or new plants; lower premiums for stable, operating plants; and then higher premiums again for plants facing the end of their licensing period when maintenance investments may not yield economic benefits to the operator. While some insurers have denied or qualified coverage based on subpar plant surveys or concerns over WANO recommendations, insurers say that the market is competitive and that other less risk-averse insurers or reinsurers will take up the risk. As insurance premiums are a fraction of operating costs and do not generally rise to the director level to drive change, a better option for reducing risk would be to have operators adopt specified minimum standards as a precondition of insurance coverage.

This model was adopted by the United Kingdom in its Cyber Essentials scheme. The insurance industry and the government developed basic, cost-effective cybersecurity controls that are required in

order to do business with the UK government. Adopters are gaining market advantage by demonstrating their cybersecurity awareness. Cyber Essentials certification is used by companies as evidence of the security protection they have in place.[38] Cybersecurity is currently underinsured in nuclear industry, and thus presents a good starting point for aligning industry, insurance, and other stakeholder goals. Procurement requirements would be more difficult to implement on an international basis. In the United States, a federal government effort is underway to help develop market incentives such as insurance to offset the costs of improved cybersecurity by balancing the short-term costs of additional investment with corresponding benefits.[39]

Nuclear insurance pools have indicated interest in participating proactively with other stakeholders in the area of cyber standards development so as to become more knowledgeable before providing coverage. Whether minimum standards in cyber or other areas could become required as part of insurance and reinsurance coverage – as a norm if not by explicit inter-insurer agreement – depends on whether multiple stakeholder groups come to the table to develop agreement on specific standards.

Financiers can help develop incentives

In addition to insurers, financiers can be important influencers of nuclear facility performance. Financing is the biggest obstacle for nuclear power projects, especially in this time of financial conservatism. Plant financings typically have certain performance requirements attached.[40] Given the high cost of nuclear power plants and the outside financing provided even in the build-own-operate model, the effect of independent ratings organizations on loan costs can be significant, one industry lawyer noted. The challenge for financiers is the difficulty of pointing to specific performance assessments. The plant financers do their own audits, but, just as insurers noted, the financiers who were contacted would also be supportive of participating in a process in which certified compliance with voluntary consensus standards could reduce financial risk.[41]

Multistakeholder engagement is needed to drive commercial benefits

With insurers, financiers, regulators, the IAEA, and association peers performing various reviews, some have noted the burdensome duplication of effort with multiple and separate assessments and self-assessments. A more integrated approach with enterprise-level risk management is needed in which important quality-management functions in a plant are considered holistically rather than separately.[42] Several industry experts have noted that operators should be taking an integrated approach to overall good plant performance. One suggested, "It would be better to propose that they ensure that different functions are effectively integrated in practice and reviewed regularly to ensure that good practice is being followed by the responsible management teams." However, without integrated guidance (developed with industry input on good practices and insights on risk trade-offs), management can be hard-pressed to self-determine appropriate actions sufficient to garner insurer, financer, regulator, and others' approval and concomitant benefits.

Security is undervalued by the market politically and economically. The risk-management questions at issue are: How much security are operators willing to buy when the return on investment is so hard to demonstrate in low-probability/high-consequence markets such as nuclear?

Security is undervalued by the market politically and economically. The risk-management questions at issue are: How much security are operators willing to buy when the return on investment is so hard to demonstrate in low-probability/high-consequence markets such as nuclear? How do corporate executives and decisionmakers justify increased security spending?

Standards are developed in order to reduce risk, to reduce liabilities and losses, and to allow for more consistency in/across operations.[43] Insurers, lenders, and/or investors could require owners and operators to adopt minimum standards in specified areas as a precondition of insurance coverage or funding. Such an industry-led effort, which combines industry self-regulation with insurers and financiers as agents for improved nuclear security practices, would complement existing government efforts and international agreements.

The insurance and finance industries are powerful market players whose imprimatur can help establish a business case for good security practices. Third-party inspections to international standards can provide a dynamic assurance process that verifies that preventive measures, good corporate governance measures, and infrastructure improvements are adopted to reduce risks of future attacks and disruptions. This would help address current and emerging vulnerabilities and risks in global nuclear safety and security and level cultural norms and experience differences.

GOOD STANDARDS CAN SAVE MONEY AND REDUCE RISKS

Compliance with a standard of care can reduce potential liabilities

The essential elements for successful voluntary standards include agreement among stakeholders about the risks, including: who is liable for potential losses, the scope of the standards and their ability to constrain risks, and how compliance with the standards is assured, including the degree of transparency in independent conformity assessments.

The essential elements for successful voluntary standards include agreement among stakeholders about the risks, including: who is liable for potential losses, the scope of the standards and their ability to constrain risks, and how compliance with the standards is assured.

In the nuclear area, operators are strictly liable for third-party damages.[44] The public accepts much of the costs of incidents, as the existing limitations of liability in the international treaties are a fraction of the potential total cost of a nuclear incident, and sometimes insurance coverage does not apply. The cleanup at Three Mile Island cost about US $1 billion and took 14 years. The estimated damages associated with Chernobyl will exceed $235 billion.[45] The much more complicated Fukushima cleanup[46] will result in costs, including lost economic assets and opportunities, of up to $250 billion, according to a Japanese survey.[47]

Nuclear liability regimes are only triggered when an incident occurs that results in releases of radiation above a threshold limit. Cases that do not involve radiological consequences, such as a loss of power due to impairment of the electric grid, could leave operators vulnerable to risk and potentially serious financial exposure. The escalation of cyber threats and potential for a systematic cyber and physical attack against the electric grid that causes cascading outages holds the potential for a massive and uninsured liability for nuclear operators. In addition to the fact that such potential attacks are not covered by the special nuclear liability regimes, as noted, there is no insurance commercially widely available to cover the consequences of a catastrophic cyber attack to critical nuclear infrastructure. The losses in a worst-case scenario are too large to insure without government assistance.

Organizations that store, use, and transport nuclear materials are charged with minimizing the threat of a terrorist event and controlling access to those materials. The magnitude of the potential consequences requires clearly defined legal duties that can be communicated and understood by corporate executives and decisionmakers who make risk-management decisions. Voluntary consensus standards can be used to demonstrate due diligence that reasonable security steps were taken.

The nuclear industry has some standards in addition to IAEA guidance documents. (See Appendix II for details on standards-development bodies that affect the nuclear industry.) Some of these standards are developed with a broad group of stakeholders, often with industry in the lead, through standards development organizations such as the American Society of Mechanical Engineers (ASME). In the United States, agencies are required to look to industry voluntary consensus standards in developing regulations. However, these standards are generally related to technical performance standards and not applicable to security.

Standards can be scoped to address selected risks

The key question is: Are there specific areas where industry could look to itself to lead in the development of standards to reduce risks in areas of growing concern? In discussions with industry, regulators, associations, and other stakeholders, some areas were identified where voluntary consensus standards might be most beneficial, such as:

- Human-Reliability Assurance, broadly including:
  - ► Insider-threat mitigation
  - ► Safety and security culture[48]
  - ► Other behavioral-monitoring programs
- Cybersecurity
- Export controls
- New reactor security (especially of interest for smaller reactors)

The key question is: Are there specific areas where industry could look to itself to lead in the development of standards to reduce risks in areas of growing concern?

Standards can demonstrate compliance with general principles and/or performance objectives, and can help reduce liabilities while helping operators accrue benefits.

In one area of human reliability assurance – that is, culture – much work is already being done but not yet in a coordinated way. INPO has developed safety culture guidelines,[49] as has WANO.[50] INPO's Addendum I takes the guidelines to the next step and includes behaviors and actions that exemplify the traits.[51] Then INPO provides a crosswalk between INPO and IAEA guidelines and NRC principles in its Addendum II.[52] Meanwhile, the IAEA is updating its security culture guidelines and is publishing self-assessment and enhancement guides.[53] The approaches to both safety and security assessments require extensive surveys and in-person interviews. Could these be combined not only to be more efficient but also to increase plant safety as well as security, especially given the trade-offs that sometimes need to be made between the two?

Regarding cybersecurity, in June 2015 the IAEA held a technical conference that attracted over 700 participants.[54] The Nuclear Energy Institute and the Nuclear Security Summit 2016 have a working group on cybersecurity[55] and already have done much work in this area. Interestingly, cybersecurity is not unrelated to the other concerns mentioned above. Human reliability and security culture are the major elements driving cybersecurity,[56] given that the majority of breaches come from human failings rather than from firewall or other technical issues.[57] Aspects of regulator-required human reliability programs such as a fitness-for-duty assessment could be researched across regulators to determine where performance was potentially most positively impacted by the program, and could help define or redefine international approaches.[58]

In export controls and small modular reactor security, industry-supported development of standards could help address some public and regulatory concerns. [59]

The IAEA does indeed have memoranda of understanding with selected international standards organizations. Some have noted that these are standards organizations with a one-country, one-vote system – such as the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC) – that do generate international consensus but that also may lack

the weighted expertise of industry. In nuclear security in particular, however, where the IAEA does not set standards and other standards are few and far between, it would appear that more energetic steps are required.

Verified standards compliance is needed to gain most benefits

Once agreement is reached among stakeholders on standards and their potential benefits, the final step to achieving the benefits of following standards is to show evidence of compliance. Standards implementation can be monitored via self-assessment, via peer review, or – preferably to ensure independence and sustainability – via independent third-party certification.

Third-party audits of performance with certification of compliance would be the most robust way to validate good performance. Independent audits of performance are not new.

The simplest way to demonstrate compliance is via self-certification. The IAEA has many self-assessment guides.[60] Self-certification, while less expensive than third-party certification, carries less credibility. Without an independent third party there is no unbiased appraisal or evidence that a thorough assessment has been conducted. However, one developer of a self-assessment guide noted that, "The survey process itself can help develop culture" – simply through increased awareness. Indeed, any facility that would make the effort to go through the extended process of a security self-assessment demonstrates prima facie concern for security.

In terms of outside reviewers, as already noted, the IAEA, WANO, and INPO all perform respected in-depth reviews, and WINS has developed peer review methodology and has experience in the field. The IAEA would like reviews such as its International Physical Protection Advisory Service missions, in which a State's physical protection systems are compared to IAEA guidance and other best practices, to become the industry norm, with regularly scheduled follow-up reviews. WANO and INPO reviews are regularly scheduled. However, all three organizations do not have the mandate or authority to require compliance with the practices and norms they develop and use in their evaluation procedures. Because the reviews are not fully shared with other stakeholders, their usefulness in generating voluntary compliance is limited; some levels of transparency would be needed to those potentially bestowing benefits.

WANO is already working with INPO and others to consider where it can look to comparable third-party reviews to evidence compliance with WANO good-practice guidelines.[61] Some have suggested that different levels of information from these reviews might be able to be shared based on the stakeholders' needs and the potential benefits to the facility. However, others worry that the honesty of a peer or IAEA review could be lost if information is shared beyond the requesting party.

Third-party audits of performance with certification of compliance would be the most robust way to validate good performance. Independent audits of performance are not new. IAEA safety standards call for independent assessments and verification by those outside the reporting line being audited – not necessarily totally independent third parties.[62] Independent third-party audits provide the most robust demonstration of compliance with standards.

Compliance assessment details could be differentially shared

The benefits of standards and third-party verifications are being recognized. Independent assessments of an organization's management system would, as one industry insider noted, "[D]rive consistency, spread good practice and establish benchmarks for diligence in compliance." China and Lloyd's Register

recently agreed to develop nuclear codes and standards for China's floating nuclear reactors.[63] Bureau Veritas plays a similar role in supporting clients' conformance to existing codes and in inspecting and verifying compliance.[64] Other Technical Support Organizations (TSOs) also play a major role in supporting some nuclear regulators. However, security is often outside the realm of third-party audits because the information that in part forms the design basis threat is deemed confidential within a State.

Security standards and audits need not be so closely held. Information derived in a standards conformity assessment could be shared on a graded basis according to stakeholder requirements. Assurances by third parties could be provided very generally to the public and then more specifically to various stakeholders. The most detailed information could be provided to regulators, who could also use compliance with selected standards as demonstration of regulatory compliance and could provide some concomitant benefits themselves.

Lessons can be taken from the financial services area, where cybercrimes in the payment card industry forged the development of security standards, independent compliance audits, and liability concessions nearly a decade ago.[65] This was driven by rampant cybercrime in the financial sector. Unfortunately, in the nuclear field, as in others, risk-management actions are often taken retroactively.

SELF-INTEREST IS KEY TO NUCLEAR STANDARDS

Good Corporate citizenship is important but more is needed

If the major international organizations and associations in the areas of nuclear safety and security have neither the missions nor powers to ensure minimum good practices, then who does? Do the providers of nuclear power plants have any responsibility for good performance?

The Carnegie Endowment for International Peace, a nonprofit organization based in Washington, DC, launched the Nuclear Power Plant and Reactor Exporters' Principles of Conduct in 2008 in order to "develop norms of corporate self-management in the exportation of nuclear power plants."[66] Updated twice since their inception, in 2011 and most recently in 2014, these regulations are formed through regularly convening leading vendors of civilian nuclear power plants, along with world-class nuclear experts. The principles include robust safety and security standards for participating organizations and speak to the need for integrating safety and security concerns. For example, in the latest draft, Goal 2.11 states: "an integrated safety and security oversight organization is established with responsibility for establishing, monitoring, and continuously adjusting the balance among security, safety, emergency response, and efficient plant operation." However, with only good corporate citizenship driving compliance and without transparent third-party verifications to call noncompliant parties to account, the incentives for compliance are limited.

Critical risks and standards' benefits need to be articulated

In summary, industry-driven voluntary consensus standards in selected areas could be developed where they would have the greatest potential impact for reducing risk. Indeed, the 2014 Nuclear Industry Summit had working groups in several important areas, and industry continues to work in areas such as cybersecurity in preparation for the 2016 Summit.[67] (To note the importance of work in some of these areas, Appendix III gives a few examples of security, cyber, and safety incidents that might have been averted with a better organizational culture, training, and/or personnel checks/reliability programs.[68])

In summary, industry-driven voluntary consensus standards in selected areas could be developed where they would have the greatest potential impact for reducing risk.

The key benefits to industry from possible new industry-driven standards would be many, including:

- To reduce human error, losses, and industrywide risks.
- To demonstrate compliance with national regulations, international guidance, and good practice, and to forestall additional regulation that would be shown to be unnecessary.
- To improve efficiency and effectiveness of oversight and to reduce plant-performance time lost to regulation. Industry knows its plants and what works on the ground. Standards would be designed to be efficient and effective, thereby making compliance easier.
- To identify and codify reasonable trade-offs among regulatory and best-practice imperatives.
- To obtain regulator/insurer/financer acknowledgement of operator conformance with these standards to reduce liabilities, oversight, additional performance requirements and to provide the basis for better terms.

With so many imperatives – sometimes conflicting – for nuclear industry managers, judgments need to be made from among competing priorities. Safety and security need not be separate. Unfortunately, in the government and policy communities, safety and security are considered as entirely distinct concerns with very little overlap in concept or requirements. However, at the level of the nuclear plant itself, both safety and security require awareness and compliance by the same actors – owners, management, and employees. At that level, safety and security need not be separate; in fact, they must not. The challenge for operators and their contractors lies in how to meet and demonstrate their compliance with the requirement for an integrated management system that includes many aspects of both safety and security. The IAEA recognizes this need.[69]

While financial and regulatory benefits are important, the importance also of industrywide risk reduction cannot be underestimated. As members of the 2014 Nuclear Industry Summit noted, "… [A] harmful event involving nuclear materials anywhere can be considered to be a harmful event everywhere. …"[70] Strengthening industry self-control can proactively prevent incidents, pre-empt reactive regulation, and build overall public confidence in the nuclear industry.

INTERNATIONAL SUPPORT FOR INCENTIVIZED SECURITY STANDARDS

Governments and their regulators are supportive of industry initiatives to harmonize international standards, including security. The Hague Communique of the 2014 Nuclear Security Summit states the need to "develop a nuclear security culture, with a particular focus on the coordination of safety and security" and to "share good practices and lessons learned at [the] national, regional and international level."[71] Increasingly, leaders in the international community and from governments of developing as well as developed nations are voicing this same concern and calling for the setting of international standards. (See Appendix IV for some public statements, including from industry.)

WINS raised the idea of insurance as an underutilized and understudied tool to incentivize nuclear security performance in a series of three roundtables and white papers from 2011-2013. This two-year governance project assessed the extent to which nuclear operators could be motivated by market incentives such as insurance, loan preferences and liability management to improve governance over nuclear security. Recommendations included adjusting counterterrorist insurance pricing, loans, or credit ratings for implementing voluntary security measures as a tool to elevate executive-level commitment to security spending. WINS also advocates increased board awareness of potential corporate and executive liability as a tool to influence decision making by incentivizing adoption of best security practices to avoid potential liability for risk-management decisions.[72]

In the area of security culture, in particular, countries have issued strong statements of support.

In the area of security culture, in particular, countries have issued strong statements of support. The Moroccan government stated that it is "convinced of the importance of promoting nuclear security culture" and, furthermore, acknowledged the importance of public-private sector and intergovernmental partnerships in this area, affirming that it will "spare no effort to strengthen the regional and international cooperation for the promotion of nuclear security culture between and among all stakeholders."[73] The United Arab Emirates' IAEA progress report indicates similar dedication to the "[the promotion] of a strong nuclear security culture ... at all regulated facilities."[74] Additionally, the G-8 saw cause to jointly address safety and security in the nuclear industry, and launched the Nuclear Safety and Security Group, whose inaugural meeting took place in Moscow in late February 2014.[75]

Similarly, many countries have voiced recognition for the importance of nuclear security culture and activities, including training. To meet this need, South Africa announced the launch of a Nuclear Security Support Centre in 2014, stating the need for "sustainability of expertise in the nuclear security field" in the country as well as a coordinating mechanism for all nuclear-security-related activities.[76] Countries including Indonesia and Brazil have followed suit with similar announcements.[77]

States must continue to look for innovative ways to sustain interest in nuclear security improvements and to build safety and security cultures that complement rather than conflict with each other. Industry-led oversight through the development of voluntary standards that focus on selected areas, such as an integrated safety and security culture, could be one of the driving elements of an enduring nuclear safety and security architecture.

However, many areas for multistakeholder-developed standards should be considered. In particular, the industry needs to start addressing the human element of security, not just the physical. In in-

dustry worldwide, as noted in recent cyber assessments, 95 percent of all security incidents involve human error.[78]

A 2015 Brazil-US workshop, "Strengthening the Culture of Nuclear Safety and Security," noted the importance of taking a holistic approach to human factors and technology but also recognized the need to prioritize among efforts. It noted, "The regulatory structure needs modern risk analysis techniques, which can identify unnecessary measures so that an organization can better prioritize resources."[79] Even for necessary measures, prioritization of efforts is important and should be risk-informed. Noting that the cumulative effects of regulation can potentially increase risks, the Nuclear Energy Institute. developed a safety prioritization tool to help prioritize facility activities and scheduling.[80]

One longtime industry stakeholder suggested that perhaps an overall "'leadership risk manual" be developed that would be a board-level, "principles-based" checklist of requirements outlining senior-level responsibility and including key control documents that would help leadership manage risks, including, for example, an enterprise risk management manual. That would indeed help direct management in assessing how to trade off among different actions.

With so many in agreement on the need for some form of standards, and with industry recognizing the potential benefits, the question only remains of how to operationalize such an effort so that risks are truly reduced.

CONCLUSIONS AND A PATH TO IMPLEMENTATION

The end of the Nuclear Security Summits in their current form means that new forums are needed to continue the focus on nuclear security – but not in isolation. Nuclear security is very much part of the overall quality management that covers activities from cybersecurity to human reliability assurance.

An effort is needed to develop voluntary consensus standards that can reduce risks in areas of concern to operators as well as to stakeholders who can provide benefits for compliance. This includes insurers, financiers, exporters, regulators, and the public. Independent third-party compliance with standards that have commercial advantage could be used as a tool to influence industry leaders to place a higher priority on security. Nuclear owners and operators could then better value security as an important commodity instead of as a drain on resources. Such a system of compliance with voluntary standards would not substitute for national supervision but would enhance confidence that the operators and their suppliers are implementing good practices.

Challenges to such an endeavor – especially in the sensitive security area – do exist but can be overcome, as has happened already in the cybersecurity area in some industries/countries. Information from assessment with voluntary standards could also be shared in a graded manner – for example, with some parties such as the regulators receiving the most knowledge regarding compliance with standards, with others such as the insurers and financiers receiving less confidential but sufficient information needed to provide benefits, and still others such as the public receiving general assurances.

The issue then becomes who would champion such an effort. WINS is already taking the lead in developing certified training programs for all levels of nuclear industry management that could, when more fully established, become accepted as a standard for the industry in terms of assuring quality personnel. If more fully funded and developed, the WINS certification program could be one of the leading indicators in demonstrating compliance with a quality performance standard. A broader standards effort will require cooperation among WINS, IAEA, WANO and WNA to bring in other relevant stakeholders to identify areas to target for standards development. This paper has already mentioned some areas of industry interest, for example, human-reliability assurance (insider-threat mitigation, safety and security culture), cyber security, export controls and security for small reactors. The effort could begin by leveraging and further developing some existing areas of interest and engagement.

Assistance to such an effort could be provided via the International Framework for Nuclear Energy Cooperation (IFNEC), a forum of 32 countries and additional observers established to promote cooperation in the development of efficient, secure nuclear energy. It could also be provided from a consortium of regulators such as the Western European Nuclear Regulators Association and the Forum of Nuclear Regulatory Bodies in Africa, and the US Nuclear Regulatory Commission.

Although we have explored the potential for voluntary consensus standards and stakeholder incentives for verified compliance primarily in nuclear power plants, such initiatives must also be explored in other nuclear areas – from transport to research reactors – to consider the possible benefits of independent voluntary standards leading to better, more publicly assured performance. Finally, the issue of personal accountability and liability also deserves further exploration as individuals in board and management positions are ultimately responsible for assuring insurers, financiers, regulators, international institutions, and the public that **nuclear energy can indeed be secure in and for its future.**

There has been much talk about the need for standards. It is time for action. The threats and challenges abound, the global energy demands are unabated, and the international nuclear security regime requires innovative security solutions at the operational level. Let us begin.

APPENDIX I: STATUS OF EMERGING NUCLEAR COUNTRIES

Countries developing or beginning to develop nuclear power have also been developing their regulatory capacity, including with the help from the IAEA and others.[81] The chart below represents countries that have no current power reactors but anticipate developing nuclear power. Their experience with nuclear research reactors is also noted.

Note that Past Research Reactors include those that are decommissioned or shutdown, and Present Research Reactors are operational or temporarily shut down. Note also that Lithuania for many years had operated nuclear power reactors, but these were shut down in response to concerns about their design.

Countries with Limited/No Nuclear Experience

Country	Past/Present Research Reactors	Power Reactors Under Construction	Power Reactors Planned	Power Reactors Proposed
Bangladesh	0/1	0	2	0
Belarus	1/3	2	0	2
Chile	1/1	0	0	4
Egypt	0/2	0	2	2
Indonesia	0/3	0	1	4
Israel	0/2	0	0	1
Jordan	0/1	0	2	N/A
Kazakhstan	0/4	0	2	2
Korea DPR (North)	N/A	0	0	1
Lithuania	N/A	0	1	0
Malaysia	0/1	0	0	2
Poland	4/1	0	6	0
Saudi Arabia	0/0	0	0	16
Thailand	0/1	0	0	5
Turkey	2/1	0	4	4
UAE	N/A	4	0	10
Vietnam	0/1	0	4	6

Sources: International Atomic Energy Agency (IAEA). "Research Reactor Database." Accessed November 18, 2015. http://nucleus.iaea.org/RRDB/RR/ReactorSearch.aspx?filter=0.; World Nuclear Association (WNA). "World Nuclear Power Reactors & Uranium Requirements." Last modified November 3, 2015. Accessed November 18, 2015. http://www.world-nuclear.org/info/Facts-and-Figures/World-Nuclear-Power-Reactors-and-Uranium-Requirements/; World Nuclear Association (WNA). "Nuclear Power in Lithuania." Updated September 2015. Accessed November 19, 2015.

APPENDIX II: NUCLEAR QUALITY STANDARDS-DEVELOPMENT BODIES

Consensus standards for the nuclear industry are designed to improve and standardize the technical performance, safety, and security of nuclear power plants, and are developed by government regulators and international and national nongovernmental organizations. The following is a non-exhaustive list of organizations, including some standards-development bodies, that are involved in creating standards or best practice guidelines or recommendations related to nuclear power plant operations for a multinational audience. An explanation of each body's work is included along with a link to more information on the relevant standard or organization. A separate list of selected national level standards-developments bodies is also included; many of the organizations listed are also that nation's representative member of ISO.

Name	Explanation	Link
American Society for Mechanical Engineers (ASME)	NQA-1: Third-party certification of conformance with Quality Assurance Requirements for Nuclear Facility Applications	https://www.asme.org/shop/certification-accreditation/nuclear-quality-assurance-nqa1-certification
American Nuclear Society (ANS)	Standards cover topics related to nuclear power plant operations, technical specifications, safety, and security	http://www.ans.org/standards/
ASTM International	ASTM publishes a wide variety of standards on nuclear technology; see C26 Technical Committee on Nuclear Fuel Cycle and E10 Committee on Nuclear Technology and Applications	http://www.astm.org/Standards/nuclear-technology-standards.html
Electric Power Research Institute (EPRI)	Publishes research, best practices, and standards; see EPRI Materials Reliability Project (MRP) and BWR Vessel and Internals Project (BWRVIP)	http://www.epri.com/Our-Work/Pages/Nuclear.aspx Links to EPRI reports: http://www.epri.com/Our-Work/Documents/Nuclear/NEI%2003-08%20Document%20List.pdf
International Electrotechnical Commission (IEC)	TC 45: Technical Committee (TC) on nuclear instrumentation	http://www.iec.ch/dyn/www/f?p=103:30:0::::FSP_ORG_ID,FSP_LANG_ID:1244,25
	SC 45A: Subcommittee (SC) on instrumentation, control, and electrical systems of nuclear facilities	http://www.iec.ch/dyn/www/f?p=103:23:0::::FSP_ORG_ID,FSP_LANG_ID:1358,25
Institute of Electrical and Electronics Engineers (IEEE)	Nuclear Power Engineering Committee (NPEC): Technical Committee within the IEEE, works on all nuclear-power-related technical and standards-writing activities	All nuclear power standards: http://standards.ieee.org/findstds/standard/nuclear_power.html NPEC: http://grouper.ieee.org/groups/npec/index.html
International Laboratory Accreditation Cooperation (ILAC)	Develops performance and monitoring standards and practices for quality assurance of calibration and testing services; publishes guidance, policy, and rules documents	http://ilac.org/publications-and-resources/publications-list/

Institute of Nuclear Materials Management (INMM)	N14 and N15 standards committees: N14 prepares standards on packaging and transportation of radioactive materials and non-nuclear hazardous materials, N15 creates standards on methods of nuclear material control	http://www.inmm.org/N_15.htm
Institute of Nuclear Power Operations (INPO)	INPO establishes performance objectives, criteria, and guidelines promoting safety and reliability in operation of nuclear power plants	http://www.inpo.info/AboutUs.htm
International Commission on Radiological Protection (ICRP)	Provides recommendations and guidance on radiation protection	http://www.icrp.org/publications.asp
International Organization for Standardization (ISO)	ISO/TC 85: Technical Committee develops and is responsible for many standards on nuclear energy, nuclear technologies, and radiological protection	http://www.iso.org/iso/iso_technical_committee%3Fcommid%3D50266
	ISO 9001: Quality management	http://www.iso.org/iso/iso_9000
	ISO 14001: Environmental management	http://www.iso.org/iso/home/standards/management-standards/iso14000.htm
North American Electric Reliability Corporation (NERC)	NUC-001-2.1: Nuclear plant interface coordination, currently mandatory standard in US	http://www.nerc.com/pa/Stand/Reliability%20Standards/NUC-001-2.1.pdf
Nuclear Quality Standard Association (NQSA)	NSQ-100: Nuclear quality, nuclear safety, and project quality standard	http://www.nqsa.org/nsq-100-standard/nsq-100.html
World Institute for Nuclear Security (WINS)	Publishes international best practices guides on nuclear security management; WINS is certified by ISO 9001 (quality management) and ISO 29990:2010 (professional development training)	https://www.wins.org/index.php?article_id=120

Selected National-Level Standards-Development Bodies	Explanation	Link
China	Standardization Administration of the PRC (SAC)	http://www.sac.gov.cn/sacen/
France	Association Française de Normalisation (AFNOR)	http://www.afnor.org/en/core-activities/standardization/standardization-mission-overview
Germany	Nuclear Safety Standards Commission/ Kerntechnischer Ausschuss (KTA)	http://www.kta-gs.de/welcome_engl.htm
	German Institute for Standardization (DIN)	http://www.din.de/en
Russia	Federal Agency on Technical Regulating and Metrology (GOST R)	http://www.gost.ru/wps/portal/en
South Africa	South African Bureau of Standards (SABS)	https://www.sabs.co.za/
South Korea	Korean Agency for Technology and Standards (KATS)	http://www.kats.go.kr/en/main.do
UK	British Standards Institution (BSI)	http://www.bsigroup.com/en-US/Standards/
USA	American National Standards Institute (ANSI)	http://www.ansi.org/standards_activities/standards_boards_panels/nescc/overview.aspx?menuid=3
	National Institute of Standards and Technology (NIST)	http://www.nist.gov/index.html

Full diagrams explaining the national standards systems for several countries including the United States, Korea, and Canada are available from the American National Standards Institute at this site: http://www.ansi.org/standards_activities/international_programs/critical_issues.aspx?menuid=3.

APPENDIX III: SAMPLE NUCLEAR SAFETY AND SECURITY CULTURE INCIDENTS

Nuclear Power Plant Location	Insider Incidents	Result
Doel, Belgium (5 August 2014)	An insider tampered with the system used for emptying oil from the turbine and caused an oil leak and three reactors to shut down. The damaged turbine reportedly cost $37 million to repair, and the continual shutdown had an impact of about $44 million per month on net recurring income.[82]	Damaged systems, temporary shutdown
San Onofre, USA (21 October 2012)	A plant operator discovered that engine coolant had been poured into an oil reservoir on an emergency-backup diesel generator, which would have likely caused the generator to malfunction if it had been needed to help cool the reactor during a power failure. The damage to this crucial piece of safety equipment was suspected sabotage, possibly by an employee.[83]	Damaged safety systems
Juzbado, Spain (September 2007)	Guards at a fuel-element-producing facility found uranium tablets along a perimeter fence, in what authorities believe was an attempt by a member of the workforce to smuggle the goods out of the complex.[84]	Potential theft for illicit trade
New Jersey, Pennsylvania, and Maryland, US (2002-2008)	American Sharif Mobley, suspected member of terrorist group al-Qaida in the Arabian Peninsula, spoke openly of militant views while working as a contractor at six nuclear plants in three states. He reportedly had clearance for unescorted access to protected and vital areas inside of the plants, which requires background checks and psychological assessments every five years. He was arrested in Yemen in 2008 and remains imprisoned.[85]	Weak employee screening and reporting mechanisms resulted in vulnerability to malicious activity
Koeberg, South Africa (25 December 2005)	While the generator was being powered up after scheduled refueling and maintenance, a loose bolt, left inside the generator, caused severe damage and forced the plant to be shut down in a case of suspected sabotage.[86]	Damaged machinery, temporary shutdown
Bradwell, UK (January 2001)	A security guard attempted to breach a computer system at a nuclear site to alter sensitive information. Later it was discovered that the guard had never been vetted before starting at the plant, and he had two undisclosed criminal convictions.[87]	Weak employee screening resulted in vulnerability to malicious activity
Nuclear Power Plant Location	**Cyber Incidents**	**Result**
Monju, Japan (2 January 2014)	A control room computer was compromised with malware after an employee updated a free computer program application. More than 42,000 confidential emails and training reports were made available.[88]	Information theft
Gori & Wolsong, South Korea (15 December 2014)	A hacker accessed internal data such as blueprints, floor maps, radiation-exposure estimates, air-conditioning and cooling systems, manuals, and personal information on 10,000 employees through the operator's website. The hacker released five leaks on Twitter and threatened to leak further information unless the reactors were shut down. The plants subsequently conducted large-scale drills to prepare for a cyber attack.[89]	Information theft and public disclosure

NRC, US (2014)	A Nigerian money-scam email was sent to more than 5,000 NRC employees stating the need to install system updates requiring their account information. Eight employees accessed the link and provided their login information.[90]	Information theft
Nationwide, US (2012)	The US Department of Homeland Security (DHS) reported that there were six cyberattacks on nuclear companies in 2012 that compromised their enterprise networks and in some cases stole data.[91]	Information theft
Hatch, Georgia, US (8 March 2008)	After an unapproved software update was installed on a single computer and critical systems were suspected to be compromised by malware, a plant was forced into an emergency shutdown for 48 hours.[92]	Temporary shutdown
Davis Besse, Ohio,US (January 2003)	Malware, sourced from a consultant's network, infected the computer systems of the corporate network of the licensee for the plant, and from there infected the process control network. The malware clogged the corporate and control networks so that for four hours and 50 minutes plant personnel could not access the Safety Parameter Display System.[93]	Temporary shutdown of critical safety features
Nuclear Power Plant Location	**Safety Incidents**	**Result**
Hanbit, South Korea (November 2012)	More than 5,000 small components used in the five reactors had not been properly certified; eight suppliers faked 60 warranties for the parts. Two reactors were shut down for component replacement.[94]	Temporary shutdown
Fukushima, Japan (11 March 2011)	The cooling system at the reactor failed shortly after a magnitude-9.0 earthquake and resulting tsunami caused emergency generators to flood. This led to an explosion, which caused one of the buildings to collapse. Two more explosions and a fire had officials and workers at the plant struggling to regain control of four of the six reactors. The fire was eventually contained, but not before the incident released radioactivity directly into the atmosphere and contaminated the groundwater. According to the National Diet of Japan Fukushima Nuclear Accident Independent Investigation Commission's official findings report, the "root causes were the organizational and regulatory systems that supported faulty rationales for decisions and actions," and there was failure to "correctly develop the most basic safety requirements."[95]	Massive radiation leaks, shutdowns, and public displacement
Asco, Spain (November 2007)	Radiation leaked when an inexperienced worker dumped radioactive waste in a pool of cooling water. Two plant directors were fired for covering up the incident for months before it became public in early 2008.[96]	Radiation leak
Forsmark, Sweden (25 July 2006)	A short circuit in the switchyard caused severe disturbance to the electrical systems as a result of work there not being carried out in the correct manner. Forsmark reviewed its safety culture and "concluded that there had been a gradual deterioration over the last few years."[97]	Temporary shutdown
Japan (Summer 2003)	TEPCO was forced to temporarily close all 17 of its nuclear power plants across Japan after admitting it had faked safety inspection reports for more than a decade.[98]	Temporary shutdowns

APPENDIX IV: INTERNATIONAL SUPPORT FOR NUCLEAR SECURITY STANDARDS HARMONIZATION

Over the past several years, support has been growing in the international community for the development of a standards regime – voluntary or involuntary – dealing directly with issues of nuclear security. Several recent stakeholder summits, including the 2014 Nuclear Industry Summit and the 2014 Nuclear Security Summit, have called for such frameworks to be established. The 2016 Nuclear Security Summit appears to be geared toward such international standards harmonization and accountability. In addition, nongovernmental groups have expressed support for a similar plan of action regarding standardization.

Author: Document	Statement	Link
Nuclear Industry Summit 2014: "NIS 2014 Joint Statement"	"Specifically, the recommendations include: Incorporating national and international **guidance and good practices** in the implementation of nuclear security measures, including security-by-design for both physical and cyber security provisions, Acknowledging that **sharing good practices** has long been a strength of the nuclear industry and has resulted in improved safety and operations, to **extend** this spirit of **international cooperation, information exchange and review** for nuclear security to the extent possible under national laws, … Pursuing discussions in different forums, including collaboration between States and industry, on managing the dynamic and international cyber security threats and **extending the discussions to operational standards to provide a common framework for the nuclear industry.**"	https://www.nis2014.org/uploadedfiles/nis2014-jointstatement_final.pdf
Nuclear Industry Summit 2014: "Report of Working Group 2 – Managing Cyber Threat"	"IAEA recommendations, guidance and ultimately/eventually **international standards** for cyber security in the Nuclear Industry could serve as a base to improve the national regulatory environment in nuclear security, leading to a solution to balance risks and reach effective, pragmatic regulations." (Point 5.1, p. 12) "Nuclear industry participants of the Working Group are proposing the following recommendations (or good practices) to increase the level of cyber security: Pursue discussions at IAEA level with a view towards establishing common guidelines related to the cyber security of Nuclear facilities and supporting infrastructures and ultimately extend these discussions to eventually include generally accepted **standards** providing a common framework for the industry. …" (Point 6, p. 16)	https://www.nis2014.org/uploadedfiles/nis2014-wg2report_mct_final.pdf

Nuclear Security Summit 2014: "The Hague Nuclear Security Summit Communiqué"	"We encourage States, regulatory bodies, research and technical support organisations, the nuclear industry and other relevant stakeholders, within their respsective responsibilities, to build such a security culture and **share good practices and lessons** learned at [the] national, regional and international level." (Point 6) "We recognize the need for a strengthened and comprehensive international nuclear security architecture, consisting of legal instruments, international organizations and initiatives, **internationally accepted guidance** and **good practices**." (Point 8) "We reaffirm that nuclear safety measures and nuclear security measures need to be designed and managed in a **coherent and coordinated manner** in the specific areas where nuclear security and nuclear safety overlap. In these areas, efforts to further improve nuclear security might benefit from experience gained with nuclear safety. We emphasize the need to develop a nuclear security culture, with a particular focus on the coordination of safety and security. **Sharing good practices**, without detriment to the protection of sensitive information, might also be beneficial." (Point 25)	https://www.government.nl/documents/directives/2014/03/25/the-hague-nuclear-security-summit-communique
Nuclear Security Summit 2014: "Statement on Nuclear Information Security: Progress Update"	"Ahead of the 2014 Nuclear Security Summit, the supporting States have reaffirmed the importance of comprehensive action to ensure the effective protection of sensitive nuclear information, and their commitments to: Developing and strengthening national measures, arrangements and capacity for the effective management and security of such information; Enhancing their related national security culture; Engaging with national scientific, industrial and academic communities to further raise awareness, **develop and disseminate best practice, and increase professional standards**; Supporting, drawing on and collaborating with the IAEA, other key international organizations and partner countries to facilitate mutual achievement of these aims."	http://conferences.wcfia.harvard.edu/files/nuclearmatters/files/statement-on-nuclear-information-security-uk_gb_2014.pdf?m=1446142183

Nuclear Security Summit 2014: "Strengthening Nuclear Security Implementation"	"The current and previous Summit hosts (NL, ROK, US) have launched a concrete initiative that allows States (hereafter referred to as "Subscribing States"), at their own discretion, to subscribe explicitly to the essential elements of a nuclear security regime and to commit to the effective and sustainable implementation of the principles therein. Such commitment does not alter the non-binding status of the Nuclear Security Summit documents. States may commit themselves voluntarily to implement the intent of the individual recommendations. The proposed joint statement … contains a **commitment to embed the objectives of the nuclear security fundamentals and the IAEA recommendations in national rules and regulations** and to host peer reviews to ensure effective implementation. … … The aim of this initiative is to demonstrate progress made in improving nuclear security worldwide following the Nuclear Security Summit in The Hague in 2014. Public commitment to subscribe to the fundamentals of the nuclear security and to commit to meet the intent of the recommendations contained in the IAEA Nuclear Security Series and the Code of Conduct should result in improved nuclear security. Such a commitment could also serve as a role model worldwide of excellent and transparent behaviour." (1-2)	http://nuclearsecuritymatters.belfercenter.org/files/nuclearmatters/files/strengthening-nuclear-security-implementation_gb_2014.pdf?m=1446142276
European Commission Delegation to the Nuclear Security Summit 2014: "EU Efforts to Strengthen Nuclear Security: Joint Staff Working Document"	"TOWARDS EU CBRN STANDARDISATION In May 2011, the European Commission and the EFTA (European Free Trade Association) states launched Mandate M/487 to the European Standardisation Organisations: CEN, CENELEC and ETSI. The scope of the Mandate is the analysis of the current security standards landscape in Europe, taking into account the legislative background, issuing recommendations on the **full range of standards** needed and drawing a roadmap for **standardization in security**. On this basis, a work programme for the definition of **European standards** and other standardization deliverables in the area of security will be developed. The programme will take into account all aspects linked to the different specific products, systems, procedures and protocols that should be covered by security standards, to assist the EU in ensuring that security is consistently addressed in the relevant areas. This Mandate is exclusively focused in civilian applications. The Objectives of the Mandate are: Increasing the **harmonization** of the European security market and reducing fragmentation, with the establishment of a set of **comprehensive European standards**. … " (p. 18-19)	https://ec.europa.eu/jrc/sites/default/files/swd-2014-107-nuclear-security-final.pdf
White House: "Statement by the Press Secretary on the 2016 Nuclear Security Summit, August 10, 2015"	"The United States seeks a strengthened global nuclear security architecture that is comprehensive, is **based on international standards**, builds confidence in nations' nuclear security implementation, and results in declining global stocks of nuclear weapons-usable materials. We cannot afford to wait for an act of nuclear terrorism before **working together to collectively raise our standards for nuclear security**."	https://www.whitehouse.gov/the-press-office/2015/08/10/statement-press-secretary-2016-nuclear-security-summit

Nuclear Security Governance Experts Group: "Preventing Weak Links in Nuclear Security: A Strategy for Soft and Hard Governance"	"Over the long-term, 'phase-in' measures could be pursued to significantly strengthen and modernize the international nuclear governance framework, such as: **Establishment of international nuclear standards** to cover nuclear safety, nuclear security, accounting and control …" (p. 3) "For nuclear security, **financial and reputational incentives** are likely to be the most important elements driving additional self-regulation." (p. 8) "Support has been growing for the pursuit of new actions to eliminate weak links in the nuclear security regime, including greater **international harmonization of nuclear security standards**, confidence-building through non-sensitive information sharing, the concept of continuous improvement, and culturally-sensitive peer review." (p. 13)	http://www.stanleyfoundation.org/publications/report/NSGEG_SPC_Rpt314.pdf
Fissile Materials Working Group: "The Results We Need in 2016: Policy Recommen-dations for the Nuclear Security Summit"	"The international nuclear security regime has significant gaps: There are **no binding standards**, no built-in peer review process, and no mechanism to assess and improve the system as a whole … much more attention to the universal **implementation of standards** and best practices is needed" (p. 22) "**International standards** that are applicable for security arrangements are relatively young, and the culture of applying them shows wide implementation differences … the desired potential to **strengthen standards** and build confidence, both regionally and with the public, has not been realized. Other **international standards and review systems** for aviation safety and security with more mandatory and universal arrangements (e.g., the International Civil Aviation Association) offer **useful precedents** for the nuclear sector." (p. 24-25) Recommendation D: "**Incentives**. Identify mechanisms to demonstrate and reward good performance and practices." (p. 25)	http://www.fmwg.org/FMWG_Results_We_Need_in_2016.pdf
US-Korea Institute at SAIS: "Nuclear Security: Seoul, the Netherlands, and Beyond"	"*Use **voluntary regimes** to improve performance*. NSS participants should be considering alternative structures that create **strong incentives** for better regime-wide performance. Financial, reputational, and accreditation incentives have been used in other industries to raise performance above legal mandates." (p. 15) "Assessing the current nuclear security architecture has left many with the impression that the current patchwork of instruments does not provide coverage commensurate with the threat. A more comprehensive approach is needed that includes greater transparence, accountability, and cohesion. Support in the NGO community is growing for **baseline security standards**, universalization of the existing regimes structures, and HEU and plutonium guidelines" (p. 31)	http://uskoreainstitute.org/research/special-reports/nssreport100313/

ENDNOTES

1. Schumacher, Ingmar. "The True Cost of Disaster Insurance Makes Nuclear Power Uncompetitive." *The Ecologist*. February 6, 2014. Accessed November 20, 2015. http://www.theecologist.org/blogs_and_comments/commentators/2265605/the_true_cost_of_disaster_insurance_makes_nuclear_power_uncompetitive.html. See also: European Parliament. *Resolution of 14 March 2013 on the Energy Roadmap 2050: A Future with Energy (2012/2103(INI)).* Last updated December 10, 2014. Accessed December 4, 2015. http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+P7-TA-2013-0088+0+DOC+XML+V0//EN

2. International Energy Agency (IEA), Nuclear Energy Agency (NEA). *Technology Roadmap: Nuclear Energy*. 2015. Accessed December 3, 2015. https://www.iea.org/publications/freepublications/publication/TechnologyRoadmapNuclearEnergy.pdf. The IAE is an autonomous organization with 29 member States. The NEA has 31 member States and is an agency within the Organization for Economic Co-operation and Development (OECD).

3. World Nuclear Association (WNA). "Nuclear Power in Turkey." Country Profiles. Last modified October 2015. Accessed November 19, 2015. http://www.world-nuclear.org/info/Country-Profiles/Countries-T-Z/Turkey/.

4. For a comparison of BOO in nuclear to other industries: Starz, Anne. "Alternative Contracting and Ownership of NPPs: Build-Own-Operate/Transfer." Slideshow presented at the 2nd Regional Conference on Energy and Nuclear Power in Africa, Cape Town, South Africa, May 30-June 1, 2011. Accessed November 19, 2015. http://www.iaea.org/NuclearPower/Downloadable/Meetings/2011/2011-May-Africa/AlternativeContracting-A.Starz-IAEA.pdf.

5. Vision of Humanity. "2015 Global Terrorism Index." November 17, 2015. Accessed November 20, 2015. http://www.visionofhumanity.org/#/page/news/1283.

6. Bunn, Matthew, Martin B. Malin, Nickolas Roth, and William H. Tobey. "Advancing Nuclear Security: Evaluating Progress and Setting New Goals." Belfer Center for Science and International Affairs, Harvard University. March 2014. Accessed November 20, 2015.

7. Baylon, Caroline, Roger Brunt, and David Livingstone. "Cyber Security at Civil Nuclear Facilities Understanding the Risks." (London: Chatham House. September 2015. Accessed November 20, 2015. https://www.chathamhouse.org/sites/files/chathamhouse/field/field_document/20151005CyberSecurityNuclearBaylonBruntLivingstone.pdf. See also: US Department of Homeland Security. "Nuclear Reactor, Materials and Waste Sector Cyberdependencies."October 6, 2015. Accessed November 20, 2015.

8. Williams, Diarmaid. "Electralabel confirms Doel 4 nuclear plant sabotage." Power Engineering International. August 15, 2014. Accessed November 20, 2015. http://www.powerengineeringint.com/articles/2014/08/electrabel-confirms-doel-4-nuclear-power-plant-sabotage.html.; Hope, Alan. "Explosion and fire at Doel nuclear plant over weekend." Flanders Today. November 2, 2015. Accessed November 20, 2015. http://www.flanderstoday.eu/current-affairs/explosion-and-fire-doel-nuclear-plant-over-weekend.

9. Pagliery, Jose. "Sniper attack on California power grid may have been 'an insider,' DHS says." CNN Money. October 17, 2015. Accessed November 20, 2015. http://money.cnn.com/2015/10/16/technology/sniper-power-grid/.

10. Birch, Douglas, and R. Jeffrey Smith. "How armed intruders stormed their way into a South African nuclear plant." The Washington Post. March 13, 2015. Accessed November 20, 2015. https://www.washingtonpost.com/world/how-armed-intruders-stormed-their-way-into-a-south-african-nuclear-plant/2015/03/13/470fc8ba-579d-4dba-a0c0-f0a1ed332503_story.html.

11. Few details are generally provided for fulfilling the mandate, however, the 1540 Committee believes that the "reliability check of personnel" handling nuclear-related materials is important and that States should work with industry. United Nations 1540 Committee. "Matrix Template." United Nations. Accessed November 20, 2015. http://www.un.org/en/sc/1540/national-implementation/1540-matrix/matrix-template.shtml.

12. International Atomic Energy Agency (IAEA). "Nuclear Security - Measures to Protect Against Nuclear Terrorism." Board of Governors General Conference. September 6, 2005. Accessed December 4, 2015. https://www.iaea.org/About/Policy/GC/GC49/Documents/gc49inf-6.pdf.

13. International Atomic Energy Agency (IAEA). "Welcome to the Regulatory Cooperation Forum." RegNet: International Regulatory Network. Accessed November 15, 2015. http://gnssn.iaea.org/regnet/embarking/rcf/Pages/default.aspx.

14. International Atomic Energy Agency (IAEA). "Self-Assessment of Regulatory Infrastructure for Safety (SARIS)." Nuclear Safety & Security. Last modified May 29, 2015. Accessed November 15, 2015. http://www-ns.iaea.org/tech-areas/regulatory-infrastructure/sat-tool.asp; International Atomic Energy Agency (IAEA). "Foreword," Regulatory Control of Nuclear Power Plants: NS Tutorial. Accessed November 19, 2015. http://www.iaea.org/ns/tutorials/regcontrol/intro/default.htm.

15. International Atomic Energy Agency (IAEA). "Integrated Regulatory Review Service." Nuclear Safety & Security. Last modified December 9, 2014. Accessed November 19, 2015. http://www-ns.iaea.org/reviews/rs-reviews.asp?s=7&l=47.

16. OECD Nuclear Energy Agency (NEA). "Publications." Last modified March 30, 2015. Accessed November 20, 2015. http://www.oecd-nea.org/pub/policypapers/.

17. Paton, James, and Amit Prakash. "IAEA Says Japan Nuclear Regulators Need More Oversight Power." Bloomberg Business. June 1, 2011. Accessed November 19, 2015. http://www.bloomberg.com/news/articles/2011-06-01/iaea-says-japan-underestimated-risk-to-nuclear-plants-from-tsunami-quakes; "New Japanese regulator takes over." World Nuclear News. September 19, 2012. Accessed November 19, 2015. http://www.world-nuclear-news.org/RS-New_Japanese_regulator_takes_over-1909125.html; Yamada, Tomoho. "Regulatory Changes for Nuclear Power Plants in Japan." Slideshow presented at the Technical Meeting on Technology Assessment of Embarking Countries, June 28, 2013. Accessed November 19, 2015. http://www.iaea.org/NuclearPower/Downloadable/Meetings/2013/2013-06-24-06-28-TM-NPTD/21-nra-regulatorychanges.pdf.

18. Sheldrick, Aaron, Kentaro Hamada, and Nick Macfie. "Japan nuclear regulator advisers fear loss of its 'essential' independence." Reuters. February 18, 2015. Accessed November 19, 2015. http://www.reuters.com/article/2015/02/18/us-japan-nuclear-concerns-idUSKBN0LM0I420150218; and Stimson Center interviews.

19. International Atomic Energy Agency (IAEA). "IAEA Safety Standards awaiting comment." Nuclear Safety & Security. Last modified December 9, 2014. Accessed November 19, 2015. http://www-ns.iaea.org/standards/documents/draft-ms-posted.asp; International Atomic Energy Agency (IAEA). "Safety Standards under development." Nuclear Safety & Security. Last modified December 9, 2014. Accessed November 19, 2015. http://www-ns.iaea.org/standards/documents/dsnumber-list.asp?s=11&l=86.

20. International Atomic Energy Agency (IAEA). *Annual Letter of Assessment*. International Nuclear Safety Group. August 20, 2014. Accessed December 4, 2015. http://www-ns.iaea.org/committees/files/insag/743/2014AnnualAssessmentLetterFinal.pdf.; International Atomic Energy Agency (IAEA). *Annual Letter of Assessment*. International Nuclear Safety Group. August 21, 2015. Accessed December 4, 2015. http://www-ns.iaea.org/committees/files/insag/743/INSAGLetter2015.pdf.

21. Note that the 2014 Nuclear Industry Summit produced a Working Group Statement On Strengthening Self Control that detailed Principles of Conduct. The Principles pointedly included, among other statements: "Recognizing the importance of Security systems in protecting nuclear materials and technology, industry participants will ensure high level corporate governance is established which: ….Ensures the Board of Directors includes nuclear security operations in their oversight activities." Nuclear Industry Summit 2014 Working Group 1. *Report of Working Group 1: Strengthening Self Control*. Accessed November 19, 2015. https://www.nis2014.org/uploadedfiles/nis2014-wg1report_ssc_finaltemplate.pdf.

22. International Atomic Energy Agency (IAEA). "Design Basis Threat (DBT)." Nuclear Safety & Security. Last modified December 9, 2014. Accessed November 19, 2015. http://www-ns.iaea.org/security/dbt.asp?s=4.

23. International Atomic Energy Agency (IAEA). *Nuclear Security Recommendations on Physical Protection of Nuclear Material and Nuclear Facilities*. IAEA Nuclear Security Series No. 13 Recommendations (INFCIRC/225/Revision 5). January 2011. Accessed November 19, 2015. http://www-pub.iaea.org/MTCD/Publications/PDF/Pub1481_web.pdf.

24. International Atomic Energy Agency (IAEA). *Nuclear Power Reactors in the World*. Reference Data Series No. 2. May 2014. Accessed November 19, 2015. http://www-pub.iaea.org/books/IAEABooks/10756/Nuclear-Power-Reactors-in-the-World-2014-Edition.

25. Although Russia has been offering a build/own/operate model, as noted earlier.

26. Countries may already have a regulator for radiological material or a nuclear research reactor, which may be given additional authorities over nuclear power operations.

27. Links to IAEA support can be found at: http://www-ns.iaea.org/reviews/default.asp?s=7&l=57.

28. For a listing of IAEA review services by stakeholder, see: https://gnssn.iaea.org/Pages/PeerReviewsandAdvisoryServicesByAudienceAndTheme.aspx.

29. International Civil Aviation Organization (ICAO). "ICAO Universal Safety Oversight Audit: 51 Additional Safety Officials Formed by ICAO to Assist their States throughout the Organization's Safety Audit Process." January 16, 2009. Accessed November 21, 2015. http://www.icao.int/EURNAT/News%20Archives/2009/20090116-ICAO%20Universal%20Safety%20Oversight%20Audit.pdf.

30. Institute of Nuclear Power Operations (INPO). Accessed November 19, 2015. http://www.inpo.info/Index.html.

31. Ellis, James. "The Role of the Institute of Nuclear Power Operations in Self-Regulation of the Commercial Nuclear Power Industry." Testimony presented at the National Commission on the BP Deepwater Horizon Oil Spill and Offshore Drilling, Washington, DC, August 25, 2010. Accessed November 19, 2015. http://www.nei.org/Issues-Policy/Policy-Resources/Testimony/August-25-2010.

32. World Association of Nuclear Operators (WANO). Accessed November 19, 2015. http://www.wano.info/en-gb/aboutus/centres.

33. World Institute for Nuclear Security (WINS). Accessed November 19, 2015. https://www.wins.org/.

34. As a result, mutual rates can be half as much as commercial rates. We explored the possibility of expanding the mutual model. However, plants generally do not want to take responsibility beyond their borders. NEIL has expanded to ONEIL and it's not clear where it may grow further. In countries where there are a large number of plants, such as China, there is the opportunity to start a captive/mutual-type entity to manage risks and reduce insurance costs through a nuclear service organization similar to NEILs – as one broker suggested.

35. Every operating plant in the United States has at least two NRC inspectors on site: U.S. Nuclear Regulatory Commission (NRC). "Reactor Inspection Basics." Operating Reactor Oversight. Last modified June 12, 2015. Accessed November 19, 2015. http://www.nrc.gov/reactors/operating/oversight/inspection-basics.html.

36. Note that NEIL also extends its mutual insurance to selected plants overseas. European mutuals also exists that provide some mutual capacity in property and liability markets independent of the national nuclear pools.

37. See, Nuclear Pools webpage at http://nuclearpools.com/.

38. UK Cybersecurity. The Role of Insurance in Managing and Mitigating the Risk, March 2015 https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/415354/UK_Cyber_Security_Report_Final.pdf.

39. Department of Homeland Security (DHS). "Cybersecurity Insurance." Last modified December 2, 2015. Accessed December 4, 2015. http://www.dhs.gov/cybersecurity-insurance.

41. Note the term financiers is used to designate the collective entities providing financing to the industry, whereas the term financer is used when discussing individual entities providing funding to a single facility.

42. Some have suggested that safeguards and export controls be added as part of a quality-management integrated approach. Note that the integration of safety and security is not new: U.S. Nuclear Regulatory Commission (NRC). "TH36 The Safety/Security Interface at Nuclear Power Plants—an International Interest." Public Meetings & Involvement. Last modified August 7, 2012. Accessed November 19, 2015. http://www.nrc.gov/public-involve/conference-symposia/ric/past/2012/docs/abstracts/sessionabstract-59.html.

43. For a short history of standards: Olson, Nate. *Partners in Prevention: Making Public-Private Security Cooperation More Efficient, Effective and Sustainable*. Stimson Center Staff Report, 106-107. December 2014. Accessed November 19, 2015. http://www.stimson.org/images/uploads/research-pdfs/PIP_Staff_Report_FINAL.pdf.

44. India is not totally aligned with this norm, which is causing some suppliers – fearing liability - to not enter into contracts in this market.

45. United Nations. "The Republic of Belarus." The United Nations and Chernobyl. 2004. Accessed November 20, 2015. http://www.un.org/ha/chernobyl/belarus.html.

46. Associated Press in Tokyo. "Fukushima clean-up 'more difficult than Three Mile Island.'" South China Morning Post. September 13, 2013. Updated June 11, 2015. Accessed November 20, 2015. http://www.scmp.com/news/asia/article/1309067/fukushima-clean-more-difficult-three-mile-island.

47. Zorpette, Glenn. "From Three Mile Island to Fukushima Daiichi: How IEEE Spectrum covered two of the biggest nuclear disasters in history." IEEE. February 28, 2014. Accessed November 20, 2015. http://spectrum.ieee.org/energy/nuclear/from-three-mile-island-to-fukushima-daiichi.

48. Certified training could be part of ensuring the safety and security culture. Some have suggested that compliance via a culture supporting export controls and safeguards might also be included as part of quality-assurance programs.

49. Institute of Nuclear Power Operations (INPO). *Traits of a Healthy Nuclear Safety Culture*. INPO 12-012, Revision 1. April 2013. Accessed November 19, 2015. http://nuclearsafety.info/wp-content/uploads/2010/07/Traits-of-a-Healthy-Nuclear-Safety-Culture-INPO-12-012-rev.1-Apr2013.pdf.

50. World Association of Nuclear Operators (WANO). *Principles: Traits of a Healthy Nuclear Safety Culture*. WANO PL 2013-1. May 2013. Accessed November 19, 2015. http://www.wano.info/Documents/PL%202013-01%20Traits%20of%20a%20Healthy%20Safety%20Culture.pdf.

51. Institute of Nuclear Power Operations (INPO). *Traits of a Healthy Nuclear Safety Culture: Behaviors and Actions That Support a Healthy Nuclear Safety Culture, by Organizational Level*. INPO 12-012, Addendum I, Revision 0. April 2013. Accessed November 19, 2015. http://nuclearsafety.info/wp-content/uploads/2010/07/Traits-of-a-Healthy-Nuclear-Safety-Culture-INPO-12-012-AddendumI-rev.0-Apr2013.pdf.

52. Institute of Nuclear Power Operations (INPO). *Traits of a Healthy Nuclear Safety Culture: Cross-References*. INPO 12-012, Addendum II, Revision 1. April 2013. Accessed November 19, 2015. http://nuclearsafety.info/wp-content/uploads/2010/07/Traits-of-a-Healthy-Nuclear-Safety-Culture-INPO-12-012-AddendumII-rev.1-Apr2013.pdf.

53. International Atomic Energy Agency (IAEA). *Nuclear Security Culture: Implementing Guide*. IAEA Nuclear Security Series No. 7. September 2008. Accessed November 19, 2015. http://www-pub.iaea.org/books/IAEABooks/7977/Nuclear-Security-Culture.

54. In cooperation with the International Criminal Police Organization (INTERPOL), International Telecommunication Union (ITU), United Nations Interregional Crime and Justice Research Institute (UNICRI), and the International Electrotechnical Commission (IEC); International Atomic Energy Agency (IAEA). "International Conference on Computer Security in a Nuclear World: Expert Discussion and Exchange." June 1-5, 2015. Accessed November 19, 2015. http://www-pub.iaea.org/iaeameetings/46530/International-Conference-on-Computer-Security-in-a-Nuclear-World-Expert-Discussion-and-Exchange.

55. U.S. Department of Homeland Security (DHS). *Nuclear Sector Coordinating Council*. Revision 1, August 27, 2014. Accessed November 19, 2015. http://www.dhs.gov/sites/default/files/publications/CIPAC-Nuclear-SCC-Charter-508.pdf.

56. Georgetown University School of Foreign Service. "International Conference on Cyber Engagement 2015." April 27, 2015. Accessed November 19, 2015. https://msfs.georgetown.edu/cyberproject/international-conference-on-cyber-engagement-2015.

57. "Leading Cause of Data Security Breaches Are Due to Insiders, Not Outsiders." PR Newswire. February 8, 2005. Accessed November 19, 2015. http://www.prnewswire.com/news-releases/leading-cause-of-data-security-breaches-are-due-to-insiders-not-outsiders-54002222.html.

58. For some US-reported outcomes: U.S. Nuclear Regulatory Commission (NRC). *Summary of Fitness for Duty Program Performance Reports for Calendar Year 2013*. Accessed November 19, 2015. http://pbadupws.nrc.gov/docs/ML1424/ML14246A440.pdf.

59. Lyman, Edwin. *Small Isn't Always Beautiful: Safety, Security, and Cost Concerns about Small Modular Reactors*. Union of Concerned Scientists, September 2013. Accessed November 19, 2015. http://www.ucsusa.org/sites/default/files/legacy/assets/documents/nuclear_power/small-isnt-always-beautiful.pdf.

60. International Atomic Energy Agency (IAEA). *Safety culture in nuclear installations: Guidance for use in the enhancement of safety culture*. IAEA-TECDOC-1329 (December 2002). Accessed November 19, 2015. http://www-pub.iaea.org/MTCD/publications/PDF/te_1329_web.pdf.

61. World Association of Nuclear Operators (WANO). "Peer Reviews: The heart of WANO's many programmes." Accessed November 19, 2015. http://www.wano.info/en-gb/programmes/peerreviews.

62. IAEA Safety Standards, Safety Requirements, No. GS-R-3: The Management System for Facilities and Activities calls for an independent assessment; see: International Atomic Energy Agency (IAEA). *IAEA Safety Standards for protecting people and the environment: The Management System for Facilities and Activities*. Safety Requirements, No.

GS-R-3, 15-16. July 2006. Accessed November 19, 2015. http://www-pub.iaea.org/MTCD/publications/PDF/Pub1252_web.pdf. Furthermore, the independent verification of assessment is called for in IAEA Safety Standards, General Safety Requirements Part 4, No. GSR Part 4. International Atomic Energy Agency (IAEA). *IAEA Safety Standards for protecting people and the environment: Safety Assessment for Facilities and Activities*. General Safety Requirements Part 4, No. GSR Part 4, 28-29. May 2009. Accessed November 19, 2015. http://www-pub.iaea.org/MTCD/publications/PDF/Pub1375_web.pdf. In some countries such as Spain, GS-R-3 reportedly has become a legal requirement.

63. Lloyd's Register Energy. "Lloyd's Register Energy signs major co-operation framework agreement with Nuclear Power Institute of China." October 20, 2015. Accessed November 20, 2015. http://www.lr.org/en/energy/news/framework-agreement-nuclear-power-institute-china.aspx.

64. Bureau Veritas. "Nuclear Power." Accessed November 20, 2015. http://www.bureauveritas.com/home/about-us/our-business/industry-offer/power-generation/nuclear-power/default_nuclear_power_content.

65. Mohamed, Arif. "Information security: The route to compliance." Computer Weekly. April 2007. Accessed November 20, 2015. http://www.computerweekly.com/feature/Information-security-The-route-to-compliance.

66. Carnegie Endowment for International Peace (CEIP). "Nuclear Power Plant and Reactor Exporters' Principles of Conduct." About NuPoC. Accessed November 19, 2015. http://nuclearprinciples.org/about/.

67. Nuclear Industry Summit 2014. "Nuclear Industry Summit 2016." NIS 2016. Accessed November 19, 2015. https://www.nis2014.org/nuclear-industry-summit-2016.html.

68. Nuclear Industry Summit 2014 Working Group 1. *Report of Working Group 1: Strengthening Self Control*. Accessed November 19, 2015. https://www.nis2014.org/uploadedfiles/nis2014-wg1report_ssc_finaltemplate.pdf.

69. The IAEA has engaged in an effort to review safety and security policies with the goal of integrating both where desirable; this effort is jointly led by the IAEA's Advisory Group on Nuclear Security (AdSec) and the Commission on Safety Standards (CSS) and is ongoing. International Atomic Energy Agency (IAEA). "Interface Group web page." Nuclear Safety & Security. Last modified November 18, 2015. Accessed November 19, 2015. http://www-ns.iaea.org/committees/css-adsec/default.asp?fd=1157&dt=0; International Atomic Energy Agency (IAEA). *Draft Report of the Joint AdSec-CSS Task Force*. Advisory Group on Nuclear Security and the Commission on Safety Standards. August 29, 2011. Accessed November 19, 2015. http://www-ns.iaea.org/committees/files/adsec/820/ReportoftheJointAdSecCSSTaskForcetoAdSecandCSS11-08-29.doc.

70. Ibid.

71. Nuclear Security Summit 2014. *The Hague Nuclear Security Summit Communiqué*. The Hague, March 25, 2014. Accessed April 30, 2015. http://www.nss2014.com/sites/default/files/documents/the_hague_nuclear_security_summit_communique_final.pdf.

72. World Institute for Nuclear Security. "Market and Regulatory Incentives for Increased Cyber Security at Nuclear Facilities: The Role of the Design Basis Threat." February 2013 https://www.wins.org/.

73. Nuclear Security Summit 2014. *National Progress Report: The Kingdom of Morocco*. February 24, 2014. Accessed April 30, 2015. http://www.nss2014.com/sites/default/files/documents/morocco.pdf.

74. Nuclear Security Summit 2014. *National Progress Report: United Arab Emirates*. March 10, 2013. Accessed April 30, 2015. http://www.nss2014.com/sites/default/files/documents/united_arab_emirates.pdf.

75. Federal Environmental, Industrial and Nuclear Supervision Service of Russia. "The first G8 Nuclear Safety and Security Group Meeting was held in Moscow." February 28, 2014. Accessed November 19, 2015. http://en.gosnadzor.ru/news/181/; For more details on the group's goals, see: U.S. Department of State. "G8 Nuclear Safety and Security Group Summit Report." May 19, 2012. Accessed November 19, 2015. http://www.state.gov/e/eb/rls/othr/2012g8/190401.htm.

76. Nuclear Security Summit 2014. *National Report of the Republic of South Africa*. Accessed April 30, 2015. http://www.nss2014.com/sites/default/files/documents/south_africa_progress_report.pdf.

77. Nuclear Security Summit 2014. *National Progress Report: Indonesia*. Accessed April 30, 2015. http://www.nss2014.com/sites/default/files/documents/indonesia.pdf; Nuclear Security Summit 2014. *National Progress Report: Brazil*. Accessed April 30, 2015. http://www.nss2014.com/sites/default/files/documents/brazil.pdf.

78. IBM Security Services 2014 Cyber Security Intelligence Index, Accessed November 21, 2015, http://www.slideshare.net/ibmsecurity/2014-cyber-security-intelligence-index.

79. Lowenthal, Micah, and Benjamin Rusek. *Brazil-U.S. Workshop on Strengthening the Culture of Nuclear Safety and Security: Summary of a Workshop*. National Academy of Sciences. 2015. Accessed November 20, 2015. Page 55. http://www.nap.edu/download.php?record_id=21761#.

80. Nuclear Energy Institute (NEI). "NRC Staff Urges Endorsing NEI Safety-Focused Prioritization Tool." May 15, 2015. Accessed November 20, 2015. http://www.nei.org/News-Media/News/News-Archives/NRC-Staff-Urges-Endorsing-NEI-Safety-Focused-Prior.

81. World Nuclear Association (WNA). "Emerging Nuclear Energy Countries." Country Profiles. Last modified November 2015. Accessed November 19, 2015. http://www.world-nuclear.org/info/Country-Profiles/Others/Emerging-Nuclear-Energy-Countries/.

82. De Clercq, Geert. "UPDATE 2-Belgian Doel 4 nuclear reactor closed till year-end." Reuters. August 14, 2014. Accessed November 19, 2015. http://uk.reuters.com/article/2014/08/14/belgium-nuclear-doel-idUKL6N0QK43R20140814.

83. Zeller, Tom. "San Onofre Nuclear Plant Investigating Possible Sabotage of Safety System." Huffington Post. November 29, 2012. Last modified November 30, 2012. Accessed November 19, 2015. http://www.huffingtonpost.com/2012/11/29/san-onofre-nuclear-plant-sabotage_n_2215260.html; "San Onofre nuclear plant may have been sabotaged." Russia Today. November 30, 2012. Last modified December 1, 2012. Accessed November 19, 2015. http://rt.com/usa/san-onofre-nuclear-employee-009/.

84. Embassy of the United States in Spain, "Spain Taking Steps to Safeguard Nuclear Material and Facilities (C-WP8-01022)," January 29, 2009. Accessed November 19, 2015. https://wikileaks.org/plusd/cables/09MADRID98_a.html.

85. Shane, Scott. "Worker Spoke of Jihad, Agency Says." The New York Times. October 4, 2010. Accessed November 19, 2015. http://www.nytimes.com/2010/10/05/us/05mobley.html?_r=3&; U.S. Nuclear Regulatory Commission (NRC). *Audit of NRC's Oversight of the Access Authorization Program for Nuclear Power Plants*. Audit Report, OIG-10A-21. September 30, 2010. Accessed November 19, 2015. http://www.nrc.gov/reading-rm/doc-collections/insp-gen/2010/oig-10-a-21-redacted.pdf.

86. Rodseth, KL, D Nicholis, and L. Mthombeni. *Executive report on the Koeberg "bolt-in-the-generator" incident*. Energize. September 2006. Accessed November 19, 2015. http://www.ee.co.za/wp-content/uploads/legacy/GT%20ExecutiveReport.pdf; Bamford, Helen. "Koeberg: SA's ill-starred nuclear power plant." IOL News. March 11, 2006. Accessed May 4, 2015. http://www.iol.co.za/news/politics/koeberg-sa-s-ill-starred-nuclear-power-plant-1.269096#.VUepl_lVhBd.

87. "New safety checks for nuclear staff." BBC News. January 9, 2001. Accessed November 19, 2015. http://news.bbc.co.uk/2/hi/uk_news/1107353.stm.

88. Paganini, Pierluigi. "Malware based attack hit Japanese Monju Nuclear Power Plant." Security Affairs. January 10, 2014. Accessed November 19, 2015. http://securityaffairs.co/wordpress/21109/malware/malware-based-attack-hit-japanese-monju-nuclear-power-plant.html.

89. Dearden, Lizzie. "Sony hack: South Korea conducting cyber attack drills at nuclear power plants after hack." The Independent. December 22, 2014. Accessed November 19, 2015. http://www.independent.co.uk/news/world/asia/sony-hack-south-korea-conducting-cyber-attack-drills-at-nuclear-power-plants-after-hack-9939339.html?wptouch_preview_theme=enabled; "S. Korean nuclear plants hacker leaks new data right after president orders security boost." Russia Today. December 23, 2014. Accessed November 19, 2015. http://rt.com/news/217091-south-korea-nuclear-hack/; Paganini, Pierluigi. "Nuclear plant in South Korea hacked." Security Affairs. December 24, 2014. Accessed November 19, 2015. http://securityaffairs.co/wordpress/31416/cyber-warfare-2/nuclear-plant-south-korea-hacked.html.

90. U.S. Nuclear Regulatory Commission (NRC). *Semiannual Report to Congress: April 1,2014-September 30, 2014*. NUREG-1415, Vol. 28, No. 1, p. 34. October 2014. Accessed November 19, 2015. http://pbadupws.nrc.gov/docs/ML1433/ML14339A290.pdf.

91. Goldman, David. "Hacker hits on U.S. power and nuclear targets spiked in 2012." CNN Money. January 9, 2013. Accessed November 19, 2015. http://money.cnn.com/2013/01/09/technology/security/infrastructure-cyberattacks/.

92. Krebs, Brian. "Cyber Incident Blamed for Nuclear Power Plant Shutdown." Washington Post. June 2008. Accessed November 19, 2015. http://www.waterfall-security.com/cyber-incident-blamed-for-nuclear-power-plant-shutdown-june-08/; Kesler, Brent. "The Vulnerability of Nuclear Facilities to Cyber Attack." Strategic Insights, Vol. 10, No. 1, Spring 2011. Accessed November 19, 2015. http://edocs.nps.edu/npspubs/institutional/newsletters/strategic%20insight/2011/SI-v10-I1_Kesler.pdf.

93. Ibid.

94. "Korean nuclear plants renamed." World Nuclear News. May 21, 2013. Accessed November 19, 2015. http://www.world-nuclear-news.org/C-Korean_nuclear_plants_renamed-2105134.html.

95. Sanger, David, and Matt Wald. "Radioactive Releases in Japan Could Last Months, Experts Say." The New York Times. March 13, 2011. Last modified March 23, 2011. Accessed November 19, 2015. http://www.nytimes.com/2011/03/14/world/asia/japan-fukushima-nuclear-reactor.html?_r=0; Kurokawa, Kyoshi, et al. *The Fukushima Nuclear Accident Independent Investigation Commission (NAIIC).* The National Diet of Japan. July 5, 2012. Accessed November 19, 2015. http://warp.da.ndl.go.jp/info:ndljp/pid/3856371/naiic.go.jp/en/.

96. Embassy of the United States in Spain, "Spain Taking Steps to Safeguard Nuclear Material and Facilities (C-WP8-01022)," January 29, 2009. Accessed November 19, 2015. https://wikileaks.org/plusd/cables/09MADRID98_a.html.

97. Ehdwall, Hans, et. al. "The Forsmark incident 25th July 2006." Nuclear Training and Safety Center (KSU). Vol. 20, No. 1, February 2007. Accessed November 19, 2015. http://www.analys.se/lankar/Engelsk/Publications/Bkgr1-07%20Forsmark%20Eng.pdf.

98. Brooke, James. "4 Die in Accident at Japan Nuclear Power Plant." The New York Times. August 10, 2004. Accessed November 19, 2015. http://www.nytimes.com/learning/teachers/featured_articles/20040810tuesday.html.

All research compiled as of December 4, 2015.

NUCLEAR ENERGY: SECURING THE FUTURE

A CASE FOR VOLUNTARY CONSENSUS STANDARDS

The Challenge: As global energy demands grow in parallel with concerns over climate change and energy security, States are looking to nuclear power to satisfy their baseload electricity needs and reduce their reliance on carbon fuels. Given the increasing terrorism threat and the potentially high consequences from nuclear incidents, comprehensive security measures are especially important for this critical infrastructure. However, operators are faced with implementing complex and sometimes conflicting guidelines for security and safety developed with limited industry input. In addition, international oversight mechanisms are insufficient, and national oversight through domestic nuclear regulators is challenged by differing levels of experience and conflicting cultural norms.

An Opportunity: After the 2016 Nuclear Security Summit, a framework will be needed to sustain momentum toward improved nuclear security. The imperatives for nuclear security and safety already exist in treaties, conventions, and UN Security Council resolutions; however, the details of how to implement the agreements often pose dilemmas. With the Amendment to the Convention on the Physical Protection of Nuclear Material likely to enter into force in 2016, and States looking for guidance on complying with its principles, the global community now has an opportunity to support a new framework of multistakeholder engagement to develop voluntary performance standards and to include industry in their development. Such standards could be used to demonstrate compliance with internationally agreed-upon principles. Financial and nonfinancial incentives could be structured to motivate voluntary compliance with these standards so that security can become a valuable commodity instead of an add-on cost. A real public-private partnership for nuclear security can be established.

STIMSON

www.stimson.org