STIMSON
Innovative Ideas Changing The World

Security Economics - How Voluntary Standards Can Help[1]

Debra Decker and Kathryn Rauhut
Stimson Center, 1211 Connecticut Ave NW, 8th Floor, Washington, DC 20036

Abstract

The potential benefits from the development of consensus standards in nuclear safety and security and then in voluntarily compliance with those standards could be significant. Those benefits can offset the cost of compliance. This paper describes how independently-certified compliance with such standards, based on existing international guidelines and agreed-on good practices, can help operators and other entities that manage nuclear materials and technologies prioritize their risk management decisions in areas of critical concern. Voluntary standards can also harmonize disparate international practices which are costly to industry. This paper summarizes our findings on ways to incentivize appropriate security measures based on two years of research, more than 200 interviews with nuclear industry stakeholders, and our analysis of other industries where voluntary standards stimulated the adoption of good practices. This Stimson Center research has been supported by the MacArthur Foundation, the US State Department Partnership for Nuclear Security and the Stanley Foundation.

Nuclear Expansion Faces New Challenges and Requires New Responses

As global energy demands grow in parallel with climate change and energy security concerns, countries are looking to nuclear power to satisfy their baseload electricity needs and reduce their reliance on carbon fuels. Currently, 31 countries operate commercial nuclear power plants, but that number of plants will likely increase by about 50 percent in the next 25 years and the number of new countries will also expand. All managers of nuclear materials – including in power reactors, research reactors, fuel facilities and transport are facing new and evolving threats, from terrorists such as ISIL and from sophisticated cybersecurity challenges. These operations need to have comprehensive security measures incorporated into their management, including in planning, design, construction, and operations. Benefits from voluntary standards could elevate nuclear governance, responsible leadership, and security culture by offsetting the additional cost to industry of security measures. This is especially needed where host government willingness or capability to enforce legal standards may be lacking. All facilities that own, operate or manage nuclear materials should be concerned about the performance of those facilities that are the least safe and secure. The consequences of nuclear incidents can be grave – as the world witnessed in Japan, the Ukraine, and the United States. Public perceptions of the nuclear industry are not restrained by borders.

Existing nuclear facilities were designed and built to prevent and avoid accidents through safety regulations and standards which evolved over many years. Safety is closely linked with security; however, security regulations and standards have been slower to develop. Currently there

are no binding international standards for nuclear security. Although the responsibility for nuclear security lies with each State, domestic nuclear regulators are challenged by differing levels of experience and capacity as well as by conflicting cultural norms. In an increasingly globalized and digitized world, the slow, static pace of regulations is unable to keep up with the risks.

Licensees, through their Boards of Directors and senior management, own the ultimate responsibility for the design, implementation and monitoring of the security and oversight of nuclear materials. They are faced with implementing complex and sometimes conflicting guidelines, developed with limited industry input. The inefficiencies of disparate and isolated systems have become increasingly apparent, as international guidelines and domestic regulations multiply. Security risks are only one element of organizational governance efforts towards operational excellence. Security, safety, safeguards and emergency response should be approached not as separate elements but as part of a larger integrated management effort.

Another significant finding and common concern is the growing need to prioritize against terrorist and cyber threats, especially in the higher areas of risk associated with nuclear transport and research and test reactors (RTRs). The majority of RTRs are located in universities or other publicly accessible centers that were not built with physical security and terrorist threats in mind, and many still have highly enriched uranium.

With power reactors, research reactors and other facilities that store or transport nuclear materials, the inefficiencies of additional security costs currently far outweigh the incentives. There are built-in market asymmetries with security in nuclear and other critical infrastructure areas. A key objective of this project is to rebalance the security economics by providing incentives through industry development of and voluntary compliance with consensus standards in selected high-risk areas. Industry stakeholders including insurance and financiers are willing to take part in the formulation of such standards.

Some Guidance Exists Toward Good Practices—In Principle

Ministerial-level guidance in international conventions, UN Resolutions, and other initiatives provide much needed and valuable high-level direction on security, although without many specific details. UN Security Council Resolution 1540 and the Amendment to the Convention on the Physical Protection of Nuclear Material (CPPNM) require States to emphasize various security protocols and procedures, but are vague on how to go about doing so. With the CPPNM taking effect this year, the actual operationalization of its high-level principles such as on security culture have yet to be defined.

The International Atomic Energy Agency (IAEA) provides valuable guidance documents, self-assessment tools and voluntary IAEA inspections of regulatory regimes, physical security, etc., upon State request. However, as the inspections are only on a voluntary basis and the results are only shared with the permission of the member State, the value of the potential assurances that could be provided to stakeholders are limited. Other organizations also provide support developing and improving regulatory regimes, such as the guidance documents of the Nuclear Energy Agency (NEA). Entities such as the IAEA and the European Union are limited because they have not been given oversight or enforcement authority by their sovereign States to ensure compliance. This is unlike the maritime and aviation sectors, where such international oversight mechanisms exist to some extent. The International Civil Aviation Organization, for example, mandates member States submit to routine and follow-up audits. The IAEA has tried to establish a norm of State reviews

such as for International Physical Protection Advisory Service (IPPAS) missions with publication and follow-up, but States and industry have not, as yet, subscribed to this.

How guidance documents are developed also presents limitations. As an international organization, the IAEA represents the consensus of States on these guidance documents, with States responsible for soliciting their industries' input for all except the technical documents. Consensus often takes many years to develop. Enforcement of these standards and guidelines is left to the individual States. This, of course, leads to variability in State's actual implementation of IAEA guidance. States who have little experience with the nuclear industry may not know how to prioritize or implement the guidelines. Even in States with mature operations, operators face challenges as regulatory requirements can increase without prioritization tools.

The lack of binding international standards provides industry with an ideal opportunity to proactively guide the development of standards and good practices that will demonstrate compliance with the high-level protocols in a harmonized way that can make good business sense.

Industry Has Given Some Important Support to Implementation of Good Practices

Catastrophic events like Three Mile Island and Chernobyl mobilized industry efforts towards taking increased, joint responsibility for good performance. The Institute of Nuclear Power Operations (INPO), established by the US nuclear industry after the Three Mile Island incident in 1979, has made its goal promoting excellence in operation rather than simple compliance with national regulations. The key to INPO's effectiveness has been its ability to gain support for initiatives at the senior management and CEO level, routine plant evaluations and facilitated self-assessments, and access to Nuclear Electric Insurance Limited (NEIL) mutual insurance coverage. INPO's independence as well as the influence its ratings have on the financial outcomes for facility operation incentivizes improvements in performance. The World Association of Nuclear Operators (WANO), formed in 1989 in response to the Chernobyl incident in 1986, works towards implementing similar functions as INPO on an international scale. However, its evaluations are only shared with other operators or insurers in a limited way and on a voluntary basis. Since Fukushima, WANO is targeting more frequent facility assessments, i.e., every four instead of six years, and is trying to bring more standardization to the offices' assessments. These assessments are safety based, even though the effects of a terrorist incident can be the same as a safety incident.[2]

The World Institute for Nuclear Security (WINS) assists in increasing the consistency of security approaches through its training program for nuclear security professionals, established in 2014. This program has the potential to provide standardized security resources across all States, regardless of nuclear operational history. It also has the potential to provide nuclear facilities with yet another indicator they can use to obtain better financing and insurance coverage terms.

The historic silo-ing of safety and security and the exclusion of important industry stakeholders from the development of guidelines and standards stands between the current and a more consistent and effective nuclear safety-security regime. Industry stakeholders have expressed their own concerns about certain areas of risk that need to be addressed. These risks include:

- Overall risk governance, with security not being seen as a responsibility of the broader workforce including senior managers
- Human reliability, including insider threat and safety-security culture[3]
- Cybersecurity

Some other areas that industry stakeholders noted included: supply chain security, consistent approaches in export controls, and security requirements for small modular reactors.

The 2016 Nuclear Industry Joint Summit Statement called for nuclear safety and nuclear security measures to be "designed and managed in a coherent and coordinated manner."[4] The industry working groups recognized the importance of security governance and called that out specifically with some suggested guidance[5] and also called for the industry "to move from a culture of compliance to a culture of excellence in cyber security."[6] These are all important steps but must be more than simple corporate social responsibility aspirations. They must make economic sense to the industry and indeed can.

Industry has demonstrated it can take leadership on important issues. For example, the Nuclear Energy Institute (NEI), an organization representing the nuclear industry, developed an approach to cybersecurity that has been well received by the US Nuclear Regulatory Commission.

Some Standards Already Apply in the Nuclear Industry and More Are Developing

There have already been successful efforts at integrating standards and inspections with other market incentives. The American Society of Mechanical Engineers (ASME) is a standards development organization with members in more than 150 countries. It provides certification that an organization has a quality assurance program in place to comply with selected standards such as NQA-1. Over 100 companies internationally have nuclear component certifications, or the "N stamp." Many of the companies that provide inspections also have ties to specialty insurers. Thus, an N stamp communicates to insurers and most importantly purchasers of components that a high level of quality is assured at a facility. Increased validation for the NQA-1 and N stamp comes from official State recognition, with Chinese contractors even reportedly requiring an N stamp for components being imported for its nuclear reactors. The Nuclear Quality Standard Association, started in 2011 by the French company AREVA and Bureau Veritas, has also developed a supplier certification process for those that could not afford ASME's certification. The NSQ-100 is new, but has the backing of the French energy authority and is in an early stage of ISO development. Such quality assurances thus provide benefits in terms of valuable market differentiation.

In the United States, the Nuclear Energy Standards Coordination Collaborative met for many years in order to have stakeholders within industry, across government and from among relevant standards development organizations discuss standards that needed updating, recognition by regulators or developing.[7] A similar systematic discussion is needed of nuclear standards internationally with many stakeholders at the table – and expanded to the areas noted of concern.

The IAEA has held technical meetings open to industry to update IAEA Safety Standards Series No. GS-R-3 (2006). The IAEA approach toward safety evolved over time, going from quality control to now focus on continual improvement in a management system that "integrates safety, health, environmental, security, quality and economic elements."[8] A new version of GS-R-3 is being published whose title alone notes the senior leaders' responsibilities: Leadership and Management for Safety (IAEA Safety Standards Series No. GSR Part 2). If this could seriously integrate some of the elements of security and economics and place appropriate responsibility on leadership and if it became an auditable standard that industry adopts, then much will have been accomplished. Other industry stakeholders, including broader industry players such as financiers and insurers, need to be included in the standards development discussions.

The World Nuclear Association (WNA) has provided support through its working groups such as the Cooperation and Development of Reactor Design, Evaluation, and Licensing Working

Group (CORDEL), where industry, governments and regulators can come together and discuss standardization and approvals for new reactor design. The Multinational Design Evaluation Program (MDEP) does similar work, but with State regulatory agencies leveraging each other's review processes. The work of both CORDEL and MDEP reinforce each other. The benefits to industry are clear – as are the benefits to regulators: both save time and money through harmonization. CORDEL is currently in discussions on further industry needs for standardization in operating reactors.[9] Based on our discussions, this broader look at international standardization is what industry needs, especially in critical risk areas. WINS needs to have a major role here, too, as it provides certifications in the security area and is increasingly being looked to and accepting leadership on security issues.[10]

Multi-Stakeholder-Developed Standards can Drive Commercial Benefits

Nuclear is a high risk business and security is expensive. Those who manage nuclear materials often face hard choices between profitability, safety, and security. However, only mutual insurers like NEIL provide a true risk-control function with obvious benefits. The interaction of this aspect of mutual insurance combined with the robust industry regulation in the United States creates an environment where mutual monitoring for nuclear power plants is incentivized since substandard operations increase the exposure of all other operations. Other nuclear operations and other States are not structured like this, although insurers overall are interdependent. Given the high domestic market exposures, nuclear insurers pool their risks internationally; these reinsurance pools absorb much of the national risks.

Insurers and reinsurers have vested interests in reducing overall nuclear risks and can be important drivers of security. However, insurance premiums are a small portion of operating costs and may not prove enough of an incentive to offset the cost of additional security. An alternative is for insurers to incentivize good practices and reduce risk by requiring specified minimum standards as a precondition for certain coverages. Having preconditions to garner benefits is a principle put into practice through the UK's Cyber Essentials scheme. In order to contract with the UK government, businesses must adopt a basic set of controls developed by the government and industry and be certified as compliant. This scheme effectively communicates that a facility's base level of cybersecurity procedures, including awareness, are in place.

Financiers should also be brought into the process of standards development. Loan agreements and other financing mechanism have some level of performance requirement attached to them. The prospects for leveraging independent ratings and standards into the financing process are significant. For example, given the high cost of new builds and the levels of debt financing required, a loan preference can have a significant benefit to the construction and operation of a facility. However, current operating standards for plants are not well discerned by financiers.[11] Some work may be developing in this area as the Japanese government has established a panel to pre-qualify countries that follow good nuclear standards in an effort to help develop good financing and insurance terms for projects in those selected countries.[12]

Both financiers and nuclear insurance pools have shown a willingness to participate in developing standards. Getting both to include consideration of these standards in their insurance and financing schemes will involve making sure all involved parties are at the table when developing the standards used to set rates and requisites for coverage. Standards are specifically developed to reduce risks and losses; those that set the market values for these need to be included.

It should be noted that market benefits can involve more than rate or premium advantages. Other economic advantages from an investment in compliance with good practices are important. These include reputational benefits, market differentiation, and waivers of liability (discussed further below). Private sector rating systems for compliance with good standards have arisen to assist in contracting suppliers and other service providers, including in transport or other service contractors where one might want to rate costs versus quality.[13] In the security area specifically, the US Customs-Trade Partnership Against Terrorism (C-TPAT) provides a general standard that makes trade both safer and more profitable. Developed originally by the US government, C-TPAT provides optional inspection certification for trade that moves with it across participating State's borders. C-TPAT certification streamlines the shipping process by submitting participants to an initial rigorous inspection process then expediting their shipments thereby reducing transportation delays and related costs for industry. C-TPAT also provides another incentive in the form of market differentiation, with certification being a factor in insurance and a requirement for some private business contracting.

Regulatory benefits can also come from industry-generated standards when regulators recognize compliance with that standard as a way an operator may demonstrate compliance with a regulatory directive, e.g., as noted earlier with some of the work of NEI. However, national governments are sometimes the ones jumpstarting a standards process that industry then finds beneficial, as in C-TPAT or the UK Cyber Essential. Another good example in the United States is the Cybersecurity Framework, initiated by a Presidential Executive Order (February 2013, EO 13636: Improving Critical Infrastructure Cybersecurity). It involved many stakeholders including industry in its development; the US government has been considering ways to promote its adoption, including potential waivers of liability.[14]

Compliance with a Standard of Care Can Reduce Potential Liabilities

Liability protections can provide important market incentives to encourage security-driven information sharing as well as standards adoption. The Cybersecurity Information Sharing Act of 2015 is a good example of the government facilitating the voluntary adoption of good cyber standards such as information sharing among companies and with the government by reducing liabilities that constrained those practices.[15] The Support Anti-Terrorism by Fostering Effective Technologies Act (SAFETY Act) of 2002 similarly provides incentives for the development and deployment of anti-terrorism technologies and services. The Green Bay Packers organization was awarded SAFETY Act-designated protections for its implementation of the National Football League's Best Practices for Stadium Security[16] – an important liability limitation for a stadium that holds over 80,000 fans.

Since cleanup costs for modern nuclear disasters like Chernobyl and Fukushima run into the hundreds of billions of dollars, the question of liability is not moot. Compounding this is the fact that nuclear liability regimes are only triggered when radiation is released above a certain threshold due to an incident. This ignores a number of modern concerns like the serious threat of a cyberattack or a terrorist group gaining possession of nuclear material during the transportation process. This leaves facilities and related operations open to extensive liabilities of which they could be unaware.

The possibility of criminal and or civil liability for failure to adequately protect/secure against terrorist acts is a vital consideration in the setting of industry norms. Directors and managers can have personal liability for corporate fault. Such liability can be triggered by failure to follow

even a voluntary standard that has become an industry norm. Although the law ordinarily only requires that reasonable measures be taken to protect the public from those harms that can reasonably be foreseen and prevented, what is "reasonable" is a very fluid concept and can be shaped by multiple factors including norms and standards, and other events that give shape to the concept of reasonableness.

The1993 World Trade Center (WTC) bombing dramatically changed that concept when the jury found that the Port Authority should have reasonably foreseen a terrorist threat. The Port Authority ignored findings from an earlier security audit that the WTC was vulnerable to an attack. Although the findings included a recommendation that the buildings' underground parking garage be closed to the public to prevent a bombing, no action was taken on this recommendation. More than 175 civil lawsuits were filed after the bombing.

An important aspect of this case is that once a vulnerability evaluation is undertaken, the information an operator derives from the vulnerability assessment may put the operator on notice of dangerous conditions, which could give rise to other civil or criminal liabilities if those conditions are not addressed. With respect to potential criminal liability, a post-audit failure to correct an identified problem arguably can show either a knowing or deliberate indifference to a violation, either of which can be construed as criminal intent. Lesser charges may be levied also.

The 9/11 disaster forever changed the concept of reasonableness. Now terrorist events are not only reasonably foreseeable, they are to be expected. Victims of the September 11, 2001, terrorist attacks brought suit in Federal District Court against airlines, airport security companies and operators, an airplane manufacturer, and government defendants for alleged failure to secure airports, individual airlines, and commercial buildings, such as the WTC, from terrorist attack. The disaster itself and the litigation have played an important role in shaping and improving security standards.

Recent events like Fukushima and the Deepwater Horizon Oil Spill and others reflect a growing trend towards holding corporations and individuals accountable for both civil and criminal negligence in both safety and security. This is where standards can have benefits. By demonstrating compliance with good standards that manage risks, liabilities can be reduced or eliminated. Increased awareness of the potential corporate and personal liability for inadequate counter-terrorism practices should improve corporate governance by incentivizing the development and adoption of best security practices to avoid liability for risk management decisions.

Standards can be Scoped and Audited to Manage Priority Risks

There are areas where industry, regulators, associations, and other stakeholders have expressed confidence in the benefits of voluntary consensus standards. Overall management of enterprise risk and appropriate governance are overarching risk areas that demand attention. Human-reliability assurance, safety and security culture, and insider-threat mitigation are currently being addressed in a piecemeal fashion. INPO, WANO, and IAEA have all developed guidelines and practices to mitigate problems in these areas, but not in a coordinated manner; the safety-security disconnect still exists, even here.

As was mentioned, cybersecurity has been the target of some work on standards already. WNA has done good work noting the issues in instrumentation and control oversight – and this basic issue of the lack of harmonization exists even before security is added to the mix.[17] Export controls and new reactor security are also areas where many feel real benefits can be gained from standardization and harmonization. Consensus industry standards on both of these could mitigate

security risks in new facilities, especially in States without a history of running nuclear facilities, and contribute to the tracking of the movement of nuclear technology, knowledge and material.

Yet, without some sort of verification scheme, all this work would be for little. The key to realizing the benefits of voluntary consensus standards lies in access to third-party verification of compliance with the agreed-upon standards.

The benefits of standards and third-party verifications are not lost on States and industry. Lloyd's Register recently agreed to develop nuclear codes for floating nuclear reactors in China, Bureau Veritas does similar work confirming compliance with existing codes, and other technical support organizations play a role in supporting nuclear regulators. However, these efforts focus on safety, as security inspections are thought to require knowledge of a State's classified information. Such security concerns could be addressed through a sharing of information based on stakeholder requirements rather than opening all information to all stakeholders. Being proactive and taking these steps now would save the industry having to deal with implementation of costly regulations retroactively in the wake of an incident, as happens all too often in other industries.

The disconnect between safety and security and the increased effort associated with the current segregation of these risk areas can be organically resolved by bringing a wider range of industry stakeholders to the table to create standards. By having a seat at the table in prioritizing and developing standards, insurers and financiers of nuclear operations would have more of a stake in the process, making it more likely that they would consider inclusion of those standards when setting rates or even offering coverage or financing in the first place. With their support, real financial incentives could be brought to bear to adhere to agreed-upon standards, which would effectively create an enforcement mechanism where one does not currently exist. This would incentivize facilities to obtain third-party certification if they want to obtain financial or insurance preferences. Other benefits as discussed in reputation and liability limitations could be explicitly recognized by management, thereby creating further incentives and a virtuous circle.

This approach would also have a positive impact in harmonizing varying standards and inspection regimes. Today, State-centric international organizations like the IAEA have different staff dedicated to particular focus areas – from nuclear industry development to safety to security to safeguards. Industry-level organizations like INPO and WANO focus more on facility safety. Including insurers and financiers – as well as regulators and others – at the onset of the development process would likely bring various concerns regarding security and safety into balance. This could also help satisfy the public's need for some assurance of the safety and security of operations, as information from the assessments could be shared in general terms at a high level. Thus, voluntary consensus standards can make the nuclear industry safer, more effective, and more secure.

The Path Forward

The summits brought much needed attention to the issue of nuclear security and made valuable progress in addressing nuclear security risks, but the framework needed to sustain momentum is a work in progress. 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 CPPNM entry into force, States are seeking guidance on complying with its principles. The global community now has an opportunity to support a new framework of multi-stakeholder 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 as well as provide economic benefits to industry members. 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 additional cost. A transparent process that includes standards and certifications would assure the public and illustrate a sustained, uniform, international commitment to a safe, secure and efficient nuclear industry.

---

[1] Debra Decker is a Senior Advisor and Kathryn Rauhut is a Nonresident Fellow at the Stimson Center. They may be reached at ddecker@stimson.org and kathryn.rauhut@gmail.com. This paper was adapted primarily from their research done for two previous publications: Debra Decker and Kathryn Rauhut, *Nuclear Energy: Securing the Future, A Case for Voluntary Consensus Standards*, Stimson Center, Washington, D.C., 2016 http://www.stimson.org/content/nuclear-energy-securing-future-case-voluntary-consensus-standards; and Debra Decker and Kathryn Rauhut, *The Quest for Nuclear Security Standards*, The Stanley Foundation, Muscatine, IA, 2016. http://www.stanleyfoundation.org/resources.cfm?id=1591. The authors thank Chris Kruckenberg, their intern from the University of Minnesota's Humphrey School of Public Affairs, for his editorial assistance.

[2] Duyeon Kim and Jungmin Kang, "Where Nuclear Safety and Security Meet," *Bulletin of the Atomic Scientists*, January 1, 2012, http://thebulletin.org/2012/january/where-nuclear-safety-and-security-meet.

[3] Debra Decker, "Before the Next Chernobyl," *CNN*, April 26, 2016, http://www.cnn.com/2016/04/26/opinions/chernobyl-nuclear-safety-opinion-decker/.

[4] "Joint Statement of the 2016 Nuclear Industry Summit," *Nuclear Industry Summit*, Washington, D.C., March 30, 2016, http://nis2016.org/agenda/documents/documents-nuclear-industry-summit-2016-joint-statement/.

[5] "The Role of the Nuclear Industry in the World and How it Manages the Security of its Materials and Technologies," *Nuclear Industry Summit*, Washington, D.C., March 30, 2016, http://nis2016.org/wp-content/uploads/2016/02/Working-Group-3-Report-The-Role-of-the-Nuclear-Industry-in-the-World.pdf.

[6] "Working Group 1 Report: Managing Cyber Threats," *Nuclear Industry Summit*, Washington, D.C., March 30, 2016, http://nis2016.org/wp-content/uploads/2016/02/Working-Group-1-Report-Managing-Cyber-Threats.pdf.

[7] "Nuclear Energy Standards Coordination Collaborative," *American National Standards Institute*, Accessed Jun 6, 2016, https://www.ansi.org/standards_activities/standards_boards_panels/nescc/overview.aspx?menuid=3#.

[8] "IAEA Safety Standards: The Management System for Facilities and Activities," International Atomic Energy Agency, Vienna, Austria, July 2006, http://www-pub.iaea.org/MTCD/publications/PDF/Pub1252_web.pdf.

[9] Jerry Head, "Cooperation in Reactor Design, Evaluation, and Licensing (CORDEL)," *USNRC Regulatory Information Conference*, March 2016, https://ric.nrc-gateway.gov/docs/abstracts/headj-th29-hv.pdf.

[10] "The Journey Beyond 2016: WINS Strategy and Goals," *World Institute for Nuclear Security*, Vienna, Austria, 2015, https://www.wins.org/index.php?article_id=18&file=wins_strategy_2020_l10_web_1.pdf.

[11] See comments of Paul Murphy in "Energizing Nuclear Security: A Sensible Summit Proposal," *Stimson Center*, Washington, D.C., January 28, 2016, http://www.stimson.org/content/energizing-nuclear-security-sensible-summit-proposal.

[12] Yuzo Yamaguchi, "Japan to Form Panel to Assess Nuclear Safety Standards in Overseas Markets," *Nucleonics Week* 57 no 3, January 21, 2016, p 4-5.

[13] See also the examples of Rightship and ISN in Debra Decker and Kathryn Rauhut, *The Quest for Nuclear Security Standards*, The Stanley Foundation, Muscatine, IA, 2016, ,http://www.stanleyfoundation.org/resources.cfm?id=1591.

[14] Michael Daniel, "Incentives to Support Adoption of the Cybersecurity Framework," *White House Blog*, August 6, 2013, https://www.whitehouse.gov/blog/2013/08/06/incentives-support-adoption-cybersecurity-framework.

[15] Brad S. Karp, "Federal Guidance on the Cybersecurity Information Sharing Act of 2015," *Harvard Law School Forum on Corporate Governance and Financial Regulation*, March 3, 2016, https://corpgov.law.harvard.edu/2016/03/03/federal-guidance-on-the-cybersecurity-information-sharing-act-of-2015/.

[16] "SAFETY Act: Approved Technologies," *Department of Homeland Security*, Accessed June 1, 2016, https://www.safetyact.gov/jsp/award/samsApprovedAwards.do?action=SearchApprovedAwardsPublic.

[17] "Safety Classification for I&C Systems in Nuclear Power Plants-Current Status & Difficulties," *World Nuclear Association*, 2015, http://www.world-nuclear.org/our-association/publications/online-reports/cordel-safety-classification-for-i-c-systems-in-nu.aspx.