

POLICY ANALYSIS BRIEF

THE STANLEY FOUNDATION | FEBRUARY 2016



The Quest for Nuclear Security Standards

Growing nuclear energy demands along with the rising tide of violence and extremism call for new and innovative measures to strengthen the largely voluntary nuclear security regime. Both the Nuclear Security Summit and the Nuclear Industry Summit in 2014 looked to the development of international harmonized nuclear security standards as part of an enduring nuclear security strategy.¹ Nongovernmental groups have likewise recommended mandatory nuclear security standards as well as incentives to motivate and reward compliance in the current voluntary regime.² International consensus on binding standards is a worthy goal but will be difficult to attain and could take years to achieve.

This policy brief explores the question of what drives successful standards development and application. First, we give a high-level overview of nuclear standards development, compliance assessments, and their historical drivers, followed by a look at other industries where standards efforts have been successful or not. We then note areas of current nuclear industry concern ripe for multistakeholder engagement for standards development and suggest pilot mechanisms where such engagement could be better leveraged to pursue standards development on a voluntary basis, given that initiatives to develop binding standards may be slow to develop, if they do at all.

Our analysis of other industries where standards development has worked or not worked suggests the following lessons:

- **The big buyer can require, but executive accountability is key.** Those with sufficient purchasing power can define contract terms, including standards of performance, but verification of compliance with those terms still has its flaws. Ultimately, executive personal and corporate accountability could have the greatest impact in assuring compliance.
- **With many in a market, differentiating performance can matter.** When there are many suppliers, buyers, or transactions in a market, differentiation becomes important, and compliance with a standard becomes a way to differentiate among them. It can be the supplier that wants or needs to stand out to the buyer, or even the insurer or government that wants or needs assistance in risk management. In areas where there are many suppliers, contractors, or other service providers involved in the marketplace, such as transporting nuclear/radiological materials or contracting for new builds or maintenance, the industry could prompt further development of standards with formal rating systems.



Debra Decker



Kathryn Rauhut

Authors

Debra Decker is a senior adviser at the Managing Across Boundaries initiative. She has more than 20 years of experience developing policies and managing processes in the private and public sectors and is an subject matter expert in the field of risk management. She has advised private- and public-sector clients on strategy and risk and has specialized in the threats stemming from weapons of mass destruction and in the vulnerabilities of critical infrastructure. Decker also has been a research associate at Harvard University's Belfer Center for Science and International Affairs specializing in nuclear issues and terrorism risks.

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 adviser to the Internet Security Alliance and to the World Institute for Nuclear Security. At the institute, Rauhut led international roundtables on improving global governance of nuclear- and cyber-security through building the business value of security. Prior to that, she was the deputy general counsel of Lawrence Livermore National Laboratory in California.

Policy Analysis Briefs are thought-provoking contributions to the public debate over peace and security issues. The views expressed in this brief are those of the authors and not necessarily those of the Stanley Foundation. The authors' affiliations are listed for identification purposes only.

- **Interdependency drives standards development but has limitations.** If the international community wants to reinforce good practices in the nuclear industry more immediately, it will have to be clear about the benefits of risk mitigation to those who comply with good practices, such as reducing liabilities and protecting or avoiding some negative attention from the general public or peers. Thus, some transparency in conformance ratings makes a difference.
- **Best practices, standards, rating, and audits are not foolproof.** Fraud regularly occurs in many industries. However, stakeholder-driven, agreed-on good practices, clearly defined benefits from compliance, and truly independent assessments are all important to ensuring safety and security.

To advance in the quest for nuclear security standards and certification, we recommend the following:

- **Industry must take responsibility for leadership.** The current reliance on states and intergovernmental organizations for responsibility over nuclear security is insufficient. Industry should take ownership and lead a multistakeholder engagement effort to develop minimum nuclear security standards and a compliance assessment process to reduce risks. Such an effort could be led by the World Institute for Nuclear Security (WINS) in partnership with a working group from the World Nuclear Association (WNA). The pools of nuclear insurers and others have expressed interest in participating in a forum for standards development.
- **Critical areas where certification schemes could reduce risk must be evaluated.** Over an 18-month period, we held more than 150 interviews in which many stakeholders identified areas of concern where consensus standards would be most useful: cybersecurity; integrated safety and security culture; human factors such as insider threats; supply chain/contracting security; export controls; and small reactor security.³
- **Incentives for adoption of agreed-on good practices in these areas must be firmly identified.** Lenders, credit-rating agencies, insurers, regulators, and other stakeholders must have input to the process with an emphasis on a suite of incentives that could motivate compliance. A review of other standards efforts shows the benefits of multistakeholder engagement, independent audits, and transparency in order to ensure compliance and achieve benefits.
- **A pilot process must be initiated.** The standards effort could be piloted on a regional basis and include an integrated safety-security culture standard, a cybersecurity standard, and an export-compliance standard being proposed for endorsement. The leaders attending the 2016 Nuclear Security Summit in Washington, DC should support this effort to develop incentives for a stronger industry-based security regime.

As the world approaches this fourth and final summit, we have a rare opportunity to focus ministerial and industry attention

on the need for a harmonized regime and the possibility of developing incentive-based voluntary standards as a more achievable interim goal. Underutilized financial and other incentives must be developed to motivate voluntary adoption of expensive security measures with a return on security investment. It is time to critically evaluate the ability to reach consensus on the development of standards and to identify a post-summit path forward.

The Need for Nuclear Security Standards

Despite setbacks to nuclear energy after the 2011 Fukushima nuclear disaster, demand for nuclear energy is strong, both as a base-load source of power in the electricity-starved developing world and as a way to limit climate change. Currently, 66 power reactors are under construction to replace older plants and expand capacity, while countries from Jordan to Vietnam plan for their longer term energy needs and possible nuclear new builds. Many countries with limited or no experience are also making plans to develop research reactors.⁴ This expansion, and a related increase in commerce in nuclear materials, raises the potential for incidents and highlights the need for nuclear security. Concerns are heightened because countries that are geographically and politically vulnerable to terrorist sabotage and attack such as Pakistan and Turkey are building new reactors. Indeed, recent terrorist attacks in Europe and the United States remind us of the vulnerability of all countries to terrorist threats, including the possibility that a terrorist might obtain radioactive materials for malicious use.

The system of international security and safety to avoid or manage such incidents relies on a complex set of international instruments framed by states and enforced by domestic regulators.⁵ Valuable assistance is provided to states and operators through training and support from WINS, the World Association of Nuclear Operators (WANO), the International Atomic Energy Agency (IAEA), and others.⁶ The IAEA develops voluntary security guidelines with input from member states and invited experts, but much is left up to state regulatory authorities who have varying levels of experience and are constrained by varying economic resources as well as differing cultural norms. This is in contrast to the aviation and maritime areas, in which states as contracting parties to treaties must comply with standards and have regular, mandatory audits.

In nuclear safety, there are some independent assessments against good practices beyond regulators and the IAEA. Good nuclear operator safety practices have been effectively promulgated in the United States, which, after the 1979 Three Mile Island accident, established the Institute of Nuclear Power Operations (INPO) with peer reviews of agreed-on good practices. Reputation and financial incentives are associated with good INPO ratings—that is, a rating indicating the quality of a plant's operations. It took the 1986 Chernobyl disaster for the industry to establish WANO with similar although less-compelling audits against good practices at nuclear facilities worldwide. This brings up the interesting sociological and behavioral question

of why we wait for a disaster to do the right thing when we know that better practices reduce risk. Can industry deliberately get ahead of the curve and proactively improve self-governance over security instead of responding to disaster? Those responsible for developing WINS hope that it will be able to stop a security disaster before it happens.

Unlike safety, where the risks have long been analyzed, nuclear security risks are less well explored. A consensus on nuclear security threats is slow to materialize because of resistance to information sharing, partly due to history. The limits to political and diplomatic solutions to the internationalization of nuclear security have their roots in the initial development of nuclear energy for weapons. The pursuit of peaceful uses for nuclear energy was deferred until after World War II. The viability of nuclear technology as a safe, secure, and peaceful source of energy requires balancing its simultaneous potential for civilian and military applications. States have historically been resistant to cede control by agreeing to binding nuclear standards. Limited treaty support is found, for example, in UN Security Council Resolution 1540 (2004), which requires states to prevent proliferation through “appropriate effective” measures.⁷ More specifically, the 2005 Amendment to the Convention on the Physical Protection of Nuclear Material, when it comes into force, will require states to protect their nuclear facilities and materials and establishes “fundamental principles” such as, “All organizations involved in implementing physical protection should give due priority to the security culture, to its development and maintenance necessary to ensure its effective implementation in the entire organization.”⁸ This and other principles detailed in the amendment, such as on quality assurance, will make security more of a management imperative.

Seeking more than such general requirements, some have called for various solutions, including the Nuclear Security Governance Experts Group’s call for an international convention on nuclear security that would clearly define standards and assess compliance.⁹ Additionally, an amendment to the IAEA statute or its broader interpretation might allow some broader IAEA authorities. However, the likelihood of this or of the development of another convention with specific binding nuclear standards appears small. Thus, in the short term, voluntary consensus standards appear the most promising avenue for development. If standards are agreed on by multiple stakeholders, then accompanying incentives could be developed that motivate their voluntary adoption. The benefits would justify the costs of compliance with the standardized security measures.

What drives standards development? Standards develop to serve a specific need or, perhaps more often, to respond to a realized harm, such as boiler explosions after the invention of steam engines. Recognizing this, each country has a process for developing standards that are of use to the general population or segments of it, such as industry, and for interacting internationally in standards development and conformity assessment. De facto standards and industry norms can also develop into standards.

Standards conformance can be measured in varying gradations. The most formal would be certification by an independent third party, which may be an accredited auditor performing audits in compliance with agreed-on standards. The least formal is an organization’s self-assessment. Between these two extremes are management or board-directed audits, peer reviews, and independent reviews by a governmental organization. A review by a governmental body can be mandatory, such as in the aviation and maritime industries, or voluntary and by invitation of the member state, as in the nuclear area with the IAEA. Compliance takes time and can be costly, especially if outside auditors are used, but its goal is to reduce risks, improve performance, and assure stakeholders of quality conformance.

Catastrophic events spur the development of agreed-on norms and standards. In the nuclear field, the formation of INPO and WANO exemplify this. Further, it took the Fukushima disaster to spur international stress tests on nuclear plants and the Japanese to confront important issues related to safety culture.¹⁰ Fukushima led the private nuclear insurance pools to reissue their assessment guidelines in 2015 with an increased emphasis on the evaluation of organizational culture and led WANO members to increase their required peer reviews.¹¹ The emphasis on organizational culture and executive accountability is a fundamental risk-management issue.

Proactive Security Standards Development: Small Steps in the Nuclear World

IAEA Efforts

The IAEA has a long history of work in the safety area, but only more recently has the threat of terrorists—in the aftermath of the September 11 attacks—drawn the IAEA more fully into the security area. While the IAEA has inspection authority under its negotiated safeguards agreement to monitor for diversions of nuclear material/technology,¹² it must be invited into states to review their safety and security oversight systems and/or their facilities’ practices, and it is up to each state to make all or part of these reviews public. Under IAEA safeguards, states can be referred to the IAEA Board of Governors for possible referral to the UN Security Council for sanctions when the IAEA sees possible wrongful (i.e., suspicious) practices; while in safety and security reviews, the IAEA can only make recommendations and suggest corrective action for follow-up reviews. The IAEA lacks the clear mandate and authority over nuclear security to issue binding rules, and that authority does not reside with any other international agency.

At the 2010 Nuclear Security Summit, states reaffirmed the essential role of the IAEA in the international security framework.¹³ The summits’ efforts to strengthen and enhance the IAEA’s authority are ongoing, and, if appropriately authorized and funded, the IAEA could perform the functions of assessment and verification that are needed. This, however, could be years away, and voluntary consensus standards would augment and complement the IAEA’s mission.

Nuclear security is a relatively new area that is still developing. In 2012, a Nuclear Security Guidance Committee open to all IAEA member states was established in order to advise on publications prepared in the IAEA Nuclear Security Series, while a coordination committee was also established to consider areas where safety and security overlap.¹⁴ These fairly new mechanisms still need some sorting out, as safety and security personnel have not always interacted well in guidance preparation.¹⁵ Draft guidance is distributed for member state comment, and it is generally up to each state to reach out to specialists and industry to solicit their input. These documents require state consensus and can take up to eight years to produce.

The nonserialized security publications called TecDocs provide technical descriptions of best practices and do not require comments or consensus by all member states. In the cyber area, for example, the Technical Guidance Document, Nuclear Security Series 17, *Computer Security at Nuclear Facilities* is being further developed, with IAEA personnel working with specialist advisers and actively inviting industry to assist. Since 1977, the IAEA has had a cooperation agreement with the International Electrotechnical Commission (IEC) to specifically work on instrumentation and control at nuclear facilities. The agreement expanded to the security area, and in 2014, the IEC published IEC 62645:2014. This document “establishes requirements and provides guidance for the development and management of effective security programmes for I&C [instrumentation and control] computer-based systems for NPPs [nuclear power plants].”¹⁶ The IAEA notes that its security series can serve to inform standards such as these. However, no compliance-assessment process exists for this standard, as it has not yet been requested.

The IAEA also has agreements with the International Telecommunication Union and the International Organization for Standardization (ISO). However, they and the IEC have states as voting members; individuals, industry, and other stakeholders do not directly participate as they do in other technical standards-development organizations (SDOs). It is only through active participation in technical and policy meetings that stakeholders can influence the standards.

WINS Efforts

As no international forum for sharing specific security practices existed, the Nuclear Threat Initiative, the US Department of Energy, and the Institute of Nuclear Materials Management together developed the World Institute for Nuclear Security (WINS), using WANO as a model. The nonprofit organization, started in 2008, works in cooperation with the IAEA. Unlike the IAEA, which works primarily with governments, WINS works directly with security practitioners from a wide range of stakeholders, with industry as a primary participant.

The work by WINS to develop and support best practices and interactions with security personnel and industry highlighted the need for nuclear security professional development. The 2014 Nuclear Security Summit recognized such efforts: 35 states signed a Joint Statement on Nuclear Security Implementation that explicitly commits them to “ensure that

management and personnel with accountability for nuclear security are demonstrably competent.”¹⁷ WINS addressed this need by establishing a mechanism for promoting certified professional development in the nuclear security field, the WINS Academy. The WINS Academy Nuclear Security Management Certification Program began in 2014. It is the first of its kind and also has ISO 29990 certification, international standards for nonformal learning, to improve and standardize the quality of its education and training.¹⁸ Currently over 500 people worldwide have registered for the program, and over 100 have completed their certification. As the certification scheme develops, it may be able to become a de facto industry standard that draws additional stakeholder benefits. WINS is also addressing other governance concerns, including accountability and liability issues.

Suppliers/Nongovernmental Organization Efforts: Nuclear Power Plant Exporters’ Principles of Conduct

The Carnegie Endowment for International Peace launched an initiative in 2008 to develop guiding principles for nuclear power plant exporters. The underlying rationale behind the effort was to raise the bar globally by establishing common standards of nuclear conduct. At the time, nuclear power appeared to be going through a renaissance, with some new and less-experienced players entering the field. The Carnegie initiative took three years, engaged major nuclear exporters, and resulted in establishing principles of conduct of self-management in the exportation of nuclear power plants.¹⁹

The principles are a voluntary industry guideline for conduct intended to complement, or exceed, national regulations. Exporters are required to establish and incorporate physical security and cybersecurity designs, establish best practices for training security staff, and improve coordination among law enforcement and plant security staff, if requested by the customer. Perhaps one of the highest-impact aspects of the principles is the requirement that membership in most of the major treaties is a condition of participation. Though the Exporters’ Principles of Conduct were founded on the belief that nuclear power plant exporters share a common interest in responsible nuclear energy, one of their implementation challenges has been the disparity in the cultures of corporate social responsibility. Participation in the process is voluntary, and participating vendors conduct their own periodic review of implementation processes.

Suppliers/Industry Efforts: The Botticelli Project

Focusing on dual-use goods, the Botticelli Project is a new effort among industry and other stakeholders to respond to the challenge from governments and international organizations to help prevent proliferation of weapons of mass destruction. A group of major dual-use exporters—from AIRBUS Helicopters and Boeing to Rolls Royce and Siemens—is working with the WNA, the UN 1540 Committee and others. It hopes to develop reference guidelines for industry to follow to control dual-use exports and then will promote related self-assessments and peer reviews. Similar efforts have been tried in the past.²⁰ This

project is in its earliest stages and is working toward broader multistakeholder buy-in. Critical support is needed from export-control authorities so they can help develop agreed-on principles and then recognize them as a means for compliance with the authorities' regulations.

Suppliers/National Lab Efforts: Supply Chain Security Culture Code of Conduct

Approximately ten years ago, Pacific Northwest National Laboratory (PNNL) launched an effort to promote industry self-regulation to control sensitive dual-use technologies. PNNL developed seven principles that companies could follow to go "beyond compliance" to reduce proliferation risks and promote such efforts as part of corporate social responsibility reporting.²¹ These principles are similar to those the Nuclear Suppliers Group cites as good corporate practices for ensuring nonproliferation.²² However, in promoting good corporate compliance, PNNL has changed the term *nonproliferation* to *supply chain security*, referring to measures a company can take to secure its goods and technical know-how all along its supply chain, with a focus not just on export compliance but also on the security followed by those supplying a company. It is a fresh way of thinking about internal compliance programs.

PNNL is targeting specific areas. Of primary importance have been large integrators: companies that combine numerous components from other suppliers into more complex goods. PNNL asks them to preferentially source from suppliers who adopt higher compliance standards—and thus, tighter security protocols—than their competitors. In addition, PNNL is developing a methodology for financial institutions to identify proliferation risks in their lending to ensure due diligence.²³ As a national laboratory and market participant, PNNL is trying to demonstrate its commitment to going beyond compliance and encourages semigovernmental organizations to do likewise in developing their own supply chain security cultures.

Suppliers/American Society of Mechanical Engineers Efforts: N Stamp and NQA-1 Quality Assurance

The American Society of Mechanical Engineers (ASME) is an SDO with 140,000 members in more than 150 countries. It has had a long history of working to certify nuclear components, beginning with its early Boiler and Pressure Vessel code; ASME provides certification that an organization has a quality assurance program in place, including NQA-1, that complies with a section of that standard.²⁴ ASME has a very structured process for developing consensus standards with balanced representation on its committees.

Well over 100 companies internationally have active nuclear component certifications (the N stamp).²⁵ Companies may need to invest heavily in improving quality controls to prepare for such certifications. ASME reviews a company for compliance, but then an authorized inspection agency (e.g., Lloyds Register, Bureau Veritas, or Hartford Steam Boiler) makes sure the company continues to be compliant. It is

not insignificant that some of the inspection agencies are affiliated with specialty insurers. This standard also works because buyers require high safety standards. Companies that obtain ASME nuclear certification expect to gain new revenue streams, and some contracts state that N stamps are required. Reports are that China requires the N stamp for any component it is importing for construction of its AP1000 nuclear power plants. ASME states that the US Nuclear Regulatory Commission also recognizes ASME's formal standards development consensus process, and the Department of Energy promotes it on its Web site.²⁶ With insurers, purchasers, and regulators all giving credit for third-party audited compliance with a standard, the standard gets more validation.

Suppliers/Nuclear Quality Standard Association Efforts: NSQ-100

Areva with Bureau Veritas started the Nuclear Quality Standard Association (NQSA) in 2011. Their goal was to develop a simpler but broader standard than ASME's that could appeal to lower volume suppliers who could not easily afford ASME's certification. Areva also worked with Rosatom, the WNA, Rolls Royce, Mitsubishi, and others to develop NSQ-100—a standard for supplier quality with an independent certification and qualification requirements for certification bodies and auditors. The standard is based on the ISO 9001:2008 quality management standard but adds in ASME NQA-1-2008 criteria and the IAEA's GS-R-3, which defines "requirements for management systems that integrate safety, health, security, quality assurance and environmental objectives."²⁷ The NQSA is working with ISO/TC 85, the ISO technical committee that considers nuclear energy and technologies, to bring this specific quality management system into the ISO system. (Note that we were told that ISO quality standards are adopted more by nuclear power operators outside the United States.)

This standard is new and has been driven by some in industry who have yet to fully commit to requiring the standard of their own suppliers. Unlike with other standards organizations that assess fees for standards downloads, this standard is free and is based on the most widely used ISO standard on quality management. As NSQ-100 was not developed following the traditional structured format of an SDO with broad stakeholder representation and a strict review process, some have questioned the developers' qualifications to put forth a standard. Nonetheless, the French energy authority is encouraging the French nuclear safety regulator to consider NSQ-100 support.²⁸

Analysis: Learning From Where Standards Development Has Worked or Not Worked

Efforts to drive higher quality and more consistent performance through standards or certified good practices have met with varying amounts of success. Following is a look at several efforts and how they worked—well or otherwise.

The Big Buyer Can Require, but Executive Accountability Is Key

A basic economic principle is that government procurers, such as the US Department of Defense, or large companies, such as Walmart, have enormous power in compelling compliance with their specifications.

The US government contracted directly with ASIS International to develop a standard for private security company operations that the Defense Department now requires as a condition of contracting. ASIS facilitated the standard development with input from about 200 stakeholders, based the standard on the Montreux Document²⁹ and other international guidelines, and most importantly, developed a companion auditing standard detailing requirements for third-party certification.³⁰

A similar example is the 2014 UK Cyber Essentials scheme, a government-backed, industry-supported standard to help organizations protect themselves against common cyberattacks. This core set of security controls is a requirement for doing business with the UK government.³¹ Also on the cyber front, US President Barack Obama issued Executive Order 13636 in 2013 for the development of a voluntary cybersecurity framework motivated by incentives to improve critical infrastructure security. The US Department of Homeland Security (DHS) has looked at, but so far not adopted, procurement requirements as a condition of contracting with the government. It is currently working with insurers and others to look for other effective incentive mechanisms.

In the retail area, standard efforts arose after a disaster focused attention on suppliers' conditions, but competing standards and audits confound improvements. A building collapse in which more than 1,100 workers died led to the Bangladesh Accord, an agreement between the garment industry and Bangladeshi trade unions to work toward a safe working environment, including through an inspection process. Major retailers in Germany, France, and the United Kingdom pledged their support, but few of the top US retailers have.³² In 2013, 17 major North American retailers announced a rival Bangladesh Worker Safety Initiative that drew criticism for being much more lenient than the Bangladesh Accord.³³ Walmart, a safety-initiative signatory, has imposed its own separate standard on suppliers, addressing social and environmental responsibilities, although required audits focus primarily on safety.³⁴ And although Walmart uses independent accredited firms for audits, which occur as frequently as every six months depending on previous inspection results, factories can effectively bypass, bribe, or deceive auditors.³⁵ Whereas retail standards efforts have had uneven results, authorities' willingness to assign responsibility for negligence and criminal acts may prove more compelling: Bangladesh filed murder charges this year against 41 people for the 1,100 worker deaths.³⁶

The lesson here is that those with sufficient purchasing power can define contract terms, but verification of compliance with those terms still has its flaws.³⁷ Ultimately,

executive personal and corporate accountability could have the greatest impact in assuring compliance. The potential for liability for security incidents needs to be explored and may be a key factor in motivating adoption of voluntary security measures. Tragedies such as Fukushima and the Deepwater Horizon oil spill in the Gulf of Mexico in 2010 have led to increased citizen and government efforts to hold corporations and individuals accountable for both civil and criminal negligence. Compliance with a standard could provide more predictability with determinations of reasonableness and negligence; this could be especially important, as the trend is to increase liability limits for nuclear damage.

With Many in a Market, Differentiating Performance Can Matter

When there are many suppliers, buyers, or transactions in a market, differentiation becomes important. It can be the supplier that wants or needs to stand out to the buyer, or even the insurer or government that wants or needs assistance in risk management.

Maritime Industry. How does an exporter or freight forwarder choose from among the many vessels it can use to ship its goods? In 2001, an Australian firm, Rightship, established a system to analyze reams of publicly available information and to supplement that with its own ship inspections and developed a ship rating of one to five stars. It sells its risk assessments and advanced knowledge to its customers, including insurers. This allows customers to make a judgment on cost versus quality in their contracts. Because the ports visited and ship crews and other factors are always changing, the business model must provide for continual assessment. Rightship ratings have been written into insurance contracts, and the rating system has expanded to include fuel efficiency ratings.³⁸ Rightship offers an efficient risk-management tool to its customers that they could not afford to develop individually.

Contractor Management. ISN, a Texas-based company that started in the oil and gas industry, helps many capital-intensive industries manage contractor services. In industries where many contractors are needed for construction or maintenance, firms are looking for responsible service providers. ISN focuses on contractor performance in terms of lost time and injuries/fatalities so that firms can compare themselves to their industry peers. Such measures are important not only to regulatory compliance (i.e., health and safety regulations) but also to job performance. ISN recently signed Canadian Nuclear Laboratories as a client and is assisting with its prequalification program, looking at health, safety, security, and environmental performance of contractors.³⁹

Exporters/Importers. The US Customs-Trade Partnership Against Terrorism (C-TPAT) began as a way to assure enhanced security in the supply chain, initially with a focus on goods imported into the United States. It allows the US Customs and Border Patrol to differentiate risks by working with those willing to take part in the voluntary program.

The benefits to those firms signing up for the program are primarily reduced inspections and faster processing times in return for validated good supply chain security practices; the validation inspections take about ten business days. Recently, the United States also started an exporter program with defined security criteria. The US government has signed mutual recognition agreements with other countries that have similar programs so that the countries can recognize each other's benefits. Some major companies now require C-TPAT participation as a condition of a contract bid; participation signals that the company has good security practices and that it is less likely to have shipping delays in fulfilling its contract requirements. C-TPAT participation also leads to lower insurance costs.⁴⁰ Although government created the security standard, other stakeholders saw the potential for risk reductions and provided benefits also.

Laboratories. The International Laboratory Accreditation Cooperation (ILAC) organization supports lab inspections and accreditations to: ISO/IEC 17025 requirements for the competence of testing and calibration laboratories; ISO 15189 for medical lab accreditation; and ISO/IEC 17020 for the accreditation of those performing inspections. ILAC is an association of accrediting bodies that went from an idea in the late 1970s to formal cooperation in 1996 to mutual recognition agreements among 28 states in 2001, and it is still developing further harmonization of practices.⁴¹ Accreditation by the organization provides independent assurance to regulators, governments, industry, and consumers. Recognizing the difficulty some labs may have in achieving full accreditation, the World Health Organization established the Stepwise Laboratory Improvement Process Towards Accreditation in Africa, a five-tier graded approach to laboratory improvements with recognitions and certifications. This drives lab facilities to increase and maintain high quality performance and eases the path toward full ISO accreditation.⁴² The US Centers for Disease Control and Prevention is reportedly piloting a bio safety-security standards initiative.

The takeaway for the nuclear industry from these efforts is that in areas where there are many suppliers, contractors or other service providers involved in such marketplace activities as transporting nuclear/radiological materials or contracting for new builds or maintenance, the industry could prompt further development of formal rating systems. This could be something that the WNA and others such as the Botticelli Project pursue and can be graded systems rather than simple yes/no measures of standards compliance. In addition, as small nuclear reactor technologies develop, with competing firms and countries offering to supply them, purchasing states could look to the development of small reactor standards and compliance with those standards as a system for differentiating among offerings.

Interdependency Drives Standards Development but Has Limitations

Aviation Safety and Security. Like the nuclear industry, aviation has multiple levels of regulation and oversight from national and international bodies. However, the

efforts to standardize security are far more developed in aviation. This is partly because of differences in the way the International Civil Aviation Organization (ICAO) was formed under the Convention on International Civil Aviation (Chicago Convention).

One of the ICAO's major duties is to adopt international standards and recommended practices (SARPs). A unique aspect of the Chicago Convention is that all member states undertake to comply with the ICAO's standards upon signing the convention and have to provide notifications, which get published, of any deviation in their regulations from the ICAO standards.⁴³ The standards—SARPs—are used as a basis for each state's own regulations and enforcement; the ICAO itself has no enforcement authority. SARPs cover all aspects of civil aviation, including security and the environment. The ICAO's role in security-related SARPs was strengthened post-9/11.

However, the ICAO's audit program against these standards is mandatory, with safety audit results made available to other member states. The program was relaunched in 1999 as the Universal Safety Oversight Audit Program. Memorandums of Understanding were executed with each state, which made participation in the audit program mandatory.⁴⁴ In terms of audits, initially, reports were only provided to the assessed states. However, increased fatalities in the late 1990s forced the ICAO to increase transparency and accountability by making the audit reports identifying noncompliant states available to all states. An additional mechanism to increase corrective actions is the identification of significant safety concerns, which states are required to immediately resolve. Those concerns are also made available to member states, which may cancel flights from low-rated states.⁴⁵

A Universal Security Audit Programme, with regular, mandatory, systematic, and harmonized universal security audits, was formed after 9/11.⁴⁶ Unlike the safety reports, security reports are strictly confidential on the part of the ICAO but may be shared by states.

Maritime Safety and Security. The International Maritime Organization (IMO) is vested with the responsibility for developing international standards relating to safety, security, and pollution prevention for ships and shipping activities. It is the sole UN agency devoted exclusively to maritime affairs, and like the ICAO, international standard setting is one of its main functions. Standards become mandatory for states when they adopt a treaty, for example, the International Safety Management Code, which made safety standards mandatory through the International Convention for the Safety of Life at Sea, 1974.⁴⁷ The International Ship and Port Facility Security Code is another agreement through which security standards become mandatory.⁴⁸

The IMO drew on the ICAO audit model and in 2002 began development of the IMO Model Audit Scheme. The voluntary audit scheme was expected to improve member state accountability to treaty obligations but proved insufficient in incentivizing compliance. A drive for greater transparency and accountability led the IMO to make its audit scheme

mandatory. This decision raised legal and practical issues with regard to the IMO's monitoring power and its member states' sovereignty. Seven years later, it entered into force in January 2016.

Although the mandatory audits are expected to generate equal pressure on states to improve their legislation, the problem remains that states with fewer resources will be challenged because of limits in legal expertise, experience, and finance, and political discrepancies and national strength. Even under the mandatory scheme, there will not be punitive action for failure to comply.

Business Preparedness and Liability Limitations. Business continuity is an issue that was brought to the world's attention after 9/11 when many firms that sadly had lost key staff found they also had lost important information and facilities in the attacks. One of the recommendations of *The 9/11 Commission Report* was the development and adoption of a National Standard for Preparedness and for the DHS to encourage rating agencies and insurers to give credit for compliance with this standard.⁴⁹ The interdependencies of businesses in the economy were of particular concern. The commission asked the American National Standards Institute for recommendations, and the institute recommended the National Fire Protection Association's NFPA 1600.⁵⁰ The subsequent 2007 act implementing the recommendations of the commission called on the DHS to "begin supporting the development and updating, as necessary, of voluntary preparedness standards through appropriate organizations" and then to "develop and promote" a program in which it would certify the preparedness of private sector entities.⁵¹ Although the DHS cited three possible standards as routes to Private Sector Preparedness designation, firms were not seeking that designation. In 2014, the DHS revised the program, and it is unclear how successful it will be.⁵²

The DHS also oversees the SAFETY Act, which provides limited liability protections for products and services that meet specified antiterrorism performance metrics. Enacted after 9/11, it was intended to motivate production of antiterrorism products and services.⁵³ The standards developer ASIS was awarded SAFETY Act certification for several of its standards; this means that security service providers that receive ASIS certification will also receive the SAFETY Act's liability protections.⁵⁴

What lessons can be learned for the nuclear sector? The Nuclear Security Governance Experts Group drafted an ambitious model convention on nuclear security, mentioned earlier. Its annexes establish binding standards for national nuclear security regimes against which states can be measured, similar to the ICAO model.⁵⁵ However, such a nuclear security treaty would be many years away. For the ICAO and the IMO, it is the continual commerce and interoperability of ships and planes among states and the potential and realized harms that have driven better standards and oversight. Even with that, the ICAO's and the IMO's evolution to mandatory audit systems took time. If the international community wants to reinforce good practices in the nuclear industry more immediately, it will have to be clear about the benefits of risk mitigation to those who

comply with good practices, such as reducing liabilities and protecting or avoiding some negative attention from the general public or peers. Thus, some transparency in conformance ratings makes a difference.

The Effect of Best Practices, Standards, Rating, and Audits

Do best practices, standards, rating, and audits make a difference? Not always. Fraud regularly occurs in many industries. However, stakeholder-driven, agreed-on good practices, clearly defined benefits from compliance, and truly independent assessments are all important to ensuring safety and security. In the nuclear industry, the scandal regarding fraudulent certifications for parts cost the Korean nuclear industry billions of dollars.⁵⁶ However, bad or fraudulent practices in the nuclear industry have the potential to cost much more—to health and the environment as well as the economy. Some efforts have to be made to develop a better oversight system that includes varying levels of transparency based on the stakeholders' needs.

Stakeholders have differing, sometimes conflicting, requirements. Owners and financiers of facilities want payback. Operators want high-performing, safe, and secure yet efficient facilities. Insurers, regulators, and the IAEA want less risk and a better understanding of risks—in insurers' case, to provide more accurate terms and pricing as well as products, such as cyberinsurance. Suppliers want to sell products. Finally, the public and states want safe, secure, reliable, affordable, and clean energy.⁵⁷

Consistent, transparent measures of compliance with safety and security standards benefit all stakeholders. More transparency could be achieved with a graded release of information. Regulatory authorities already provide limited general, public information.⁵⁸ Auditors could provide the most general information to the public, high-level assessments of compliance with good practices to insurers and financiers, and the most detailed assessments to regulators. This would allow for each stakeholder group to receive appropriate assurances by satisfying its information needs and would provide appropriate benefits on a cost-efficient basis to those facilities verified as following high standards.

Conclusion: What's Next? Voluntary Standards With Incentives

Practically speaking, ministerial agreement is unlikely to be achieved on internationally binding nuclear security standards in the foreseeable future. In the interim, for global nuclear security, the world will have to rely on other risk-reduction mechanisms to promote security in areas that appeal to stakeholder interests. A neutral convening champion is needed to bring the disparate groups together and to identify areas of opportunity for engaging to reduce security risks as well as related risks.

In the quest for nuclear security standards, the convening stakeholder should appeal to areas of most interest to other key stakeholders and use successful engagement on

selected issues as a prototype for continued engagement in broader areas. A regional pilot should be undertaken in those areas of risk.

An organization such as WINS could lead this effort in cooperation with the WNA and other stakeholders in selected areas where standards and certification could reduce risk and offset costs. Stakeholders have mentioned several areas particularly ripe for standards development, including cybersecurity; integrated safety and security culture; human factors such as insider threats; supply chain/contracting security; export controls; and small reactor security.

Coordination with other forums could help develop prototype engagement models. In addition to some of the nuclear standards efforts already mentioned, other harmonization initiatives include the Organization for Economic Cooperation and Development's Nuclear Energy Agency's Multinational Design Evaluation Programme (MDEP) and the WNA's Cooperation in Reactor Design Evaluation and Licensing (CORDEL) Group. In addition, the Western European Nuclear Regulators Association (WENRA) has worked with the European Union to create harmonized safety "reference levels" to ensure uniformity of safety approaches at plants. These efforts generally focus on regulators' requirements. However, the efforts of MDEP, CORDEL, and WENRA might be leveraged to seek regulatory input to and recognition of industry-led standards-development efforts.

Standards efforts could also be supported by other groups, such as the International Framework for Nuclear Energy Cooperation, a forum for participating states to explore safe and secure approaches to nuclear energy expansion. Other international forums should also be interested in supporting the development of this effort.⁵⁹

Governments and industry are clearly interested in better standards coordination internationally. In a world characterized by political, economic, and sectarian challenges, the promise of nuclear power's contribution requires the full measure of assurance in nuclear security. Confidence in the security of the nuclear sector is reflected by the proficiency of operators and producers relative to objective criteria founded on standards, certifications, and reviews. This is good for business and good for security. Meeting nuclear security expectations through a transparent and documented process—to include standards and certifications—demonstrates a sustained, uniform, and international commitment to the viability of nuclear power now and in the decades to come.

Endnotes

- 1 See Appendix IV in Debra Decker and Kathryn Rauhut, *Nuclear Energy: Securing the Future, a Case for Voluntary Consensus Standards*, 2016, <http://www.stimson.org/books-reports/nuclear-energy-securing-the-future-a-case-for-voluntary-consensus-standards>.
- 2 Fissile Materials Working Group, *The Results We Need in 2016: Policy Recommendations for the Nuclear Security Summit*, 2015, <http://www.stanleyfoundation.org/publications/other/FMWGRecommendations6-15.pdf>.
- 3 Decker and Rauhut, *Nuclear Energy*.
- 4 World Nuclear Association (WNA), "World Nuclear Power Reactors & Uranium Requirements," World Nuclear Association, January 1, 2015, <http://www.world-nuclear.org/info/Facts-and-Figures/World-Nuclear-Power-Reactors-and-Uranium-Requirements/>.
- 5 Carlton Stoiber, Alec Baer, Norbert Pelzer, and Wolfram Tonhauser, *Handbook on Nuclear Law* (Vienna: International Atomic Energy Agency, 2003), http://www-pub.iaea.org/MTCD/Publications/PDF/Pub1160_web.pdf.
- 6 For examples of others' support, see the US State Department's Partnership for Nuclear Security programs, <https://www.pns-state.net/en-us/>; the Nuclear Energy Agency of the Organisation for Economic Co-operation and Development work on effective regulators, http://www.oecd-ilibrary.org/nuclear-energy/the-characteristics-of-an-effective-nuclear-regulator_9789264218741-en; and Russia's efforts to improve nuclear security as part of its investment in international projects cited in <http://www.stanleyfoundation.org/resources.cfm?id=558>.
- 7 UN Security Council, *Security Council Resolution 1540 (2004)*, S/RES/1540 (2004), April 28, 2004, http://www.un.org/en/ga/search/view_doc.asp?symbol=S/RES/1540%20%282004%29.
- 8 International Atomic Energy Agency (IAEA), "Nuclear Security—Measures to Protect Against Nuclear Terrorism," December 6, 2005, <https://www.iaea.org/About/Policy/GC/GC49/Documents/gc49inf-6.pdf>.
- 9 John Bernhard, Kenneth Brill, Anita Nilsson, and Shin Chang-Hoon, *International Convention on Nuclear Security*, Nuclear Security Governance Experts Group, March 2015, <http://www.nsegg.org/ICNSReport315.pdf>.
- 10 European Commission, "Stress Tests," last updated August 12, 2015, <http://ec.europa.eu/energy/en/topics/nuclear-energy/nuclear-safety/stress-tests>; National Diet of Japan Fukushima Nuclear Accident Independent Investigation Commission, official report, National Diet of Japan, July 5, 2012, <http://warp.da.ndl.go.jp/info:ndljp/pid/3856371/naiic.go.jp/en/>.
- 11 Nuclear Pools, "Procedures," <http://www.nuclearpools.com/procedures>.
- 12 IAEA, "Safeguards Legal Framework," last updated December 2, 2015, <https://www.iaea.org/safeguards/safeguards-legal-framework>.
- 13 IAEA, "Strengthening Nuclear Security: IAEA's 'Essential Role' in Building a Global Response to a Global Threat," April 14, 2010, <https://www.iaea.org/newscenter/news/strengthening-nuclear-security>.

- 14 IAEA, *Nuclear Security Plan 2014–2017*, August 2, 2013, <http://www-ns.iaea.org/downloads/security/nuclear-security-plan2014-2017.pdf>.
- 15 Author confidential interviews with representatives of industry and the IAEA and others from September 2014 to December 2015. Note, however, in emergency response, the safety and security staff reportedly do have regular collaboration.
- 16 International Electrotechnical Commission, *International Standard: Nuclear Power Plants—Instrumentation and Control Systems—Requirements for Security Programmes for Computer-Based Systems*, IEC 62645, Edition 1.0, August 2014, https://webstore.iec.ch/preview/info_iec62645%7Bed1.0%7Db.pdf. The IAEA has several publications on computer systems and recently published a new document, *Technical Challenges in the Application and Licensing of Digital Instrumentation and Control Systems in Nuclear Power Plants*, (NP-T-1.13). <http://www-pub.iaea.org/books/IAEABooks/8764/Technical-Challenges-in-the-Application-and-Licensing-of-Digital-Instrumentation-and-Control-Systems-in-Nuclear-Power-Plants>.
- 17 Acronym Institute for Disarmament Diplomacy, *Strengthening Nuclear Security Implementation* March 25, 2014, <http://www.acronym.org.uk/sites/default/files/NSS%202014%20joint%20statement.pdf>.
- 18 International Standards Organization, *Learning Services for Non-Formal Education and Training—Basic Requirements for Service Providers*, ISO 29990:2010, September 1, 2010, www.iso.org/iso/catalogue_detail.htm?csnumber=53392.
- 19 Nuclear Principles, *Nuclear Power Plant and Reactor Exporters' Principles of Conduct*, January 1, 2015, http://nuclearprinciples.org/wp-content/uploads/2015/02/PrinciplesofConduct_January20153.pdf.
- 20 Coalition for Excellence in Export Compliance, *CEEC Best Practices for Export Controls*, <http://www.ceecbestpractices.org/>.
- 21 Andrew Kurzrok and Gretchen Hund, "Beyond Compliance: Integrating Nonproliferation Into Corporate Sustainability," *Bulletin of the Atomic Scientists*, Vol. 69, No. 3, May–June 2013, pp. 31–42.
- 22 Nuclear Suppliers Group (NSG), *Good Practices for Corporate Standards to Support the Efforts of the International Community in the Non-Proliferation of Weapons of Mass Destruction*, http://www.nuclearsuppliersgroup.org/images/Files/National_Practices/NSG_Measures_for_industry_update_revised_v3.0.pdf.
- 23 Andrew Kurzrok and Gretchen Hund, "Stopping Illicit Procurement: Lessons From Global Finance," *Arms Control Today*, June 2, 2014, https://www.armscontrol.org/act/2014_06/Features/Stopping-Illicit-Procurement-Lessons-From-Global-Finance.
- 24 American Society of Mechanical Engineers (ASME), "Nuclear Component Certification," <https://www.asme.org/shop/certification-accreditation/nuclear-component-certification>.
- 25 ASME, "Locate ASME Certified Companies," <https://www.asme.org/shop/certification-accreditation/locate-asme-certified-companies>.
- 26 Nuclear Engineering International (NEI), "Sheffield Forgemasters Gets ASME NPT Stamp," February 24, 2014, <http://www.neimagazine.com/news/newssheffield-forgemasters-gets-asme-npt-stamp-4183107>; and interviews with ASME representatives and representatives of the insurance industry from September 2014 to January 2016. See also Bureau Veritas, "ASME Code," <http://www.bureauveritas.com/home/about-us/our-business/industry-offer/industrial-products-certification/onecis-asme/ASME-code/ASME-code/>; US Department of Energy, *NQA-1: An Overview for Federal Project Directors*, <http://energy.gov/projectmanagement/downloads/nqa-1-overview-federal-project-directors>.
- 27 IAEA, *The Management System for Facilities and Activities*, 2006, <http://www-pub.iaea.org/books/IAEABooks/7466/The-Management-System-for-Facilities-and-Activities-Safety-Requirements>. It has corresponding matrices with the US Nuclear Regulatory Commission's 10 CFR 50 Appendix B on quality assurance, <http://www.nrc.gov/reading-rm/doc-collections/cfr/part050/part050-appb.html>.
- 28 Nuclear Quality Standard Association, "A New Support: Chairman From the GPESPN Asks ASN to Support NQSA's Project," July 26, 2014, <http://www.nqsa.org/news-events/single/article/a-new-support/event-day/26/event-month/07/event-year/2014.html>.
- 29 Swiss Federal Department of Foreign Affairs, "The Montreux Document," December 14, 2015, <https://www.eda.admin.ch/eda/en/dfa/foreign-policy/international-law/international-humanitarian-law/private-military-security-companies/montreux-document.html>.
- 30 Author interviews with ASIS representatives from 2013–2015. See also ASIS International, "ISO to Develop New Global Private Security Quality Management Standard," August 6, 2013, <https://www.asisonline.org/News/Press-Room/Press-Releases/2013/Pages/ISO-to-Develop-New-Global-Private-Security-Quality-Management-Standard.aspx>, and US Office of the Assistant Secretary of Defense for Logistics & Materiel Readiness, "Private Security Companies," <http://www.acq.osd.mil/log/ps/psc.html>.
- 31 UK Department for Business Innovation & Skills, "Cyber Essentials Scheme: Overview," April 7, 2014, <https://www.gov.uk/government/publications/cyber-essentials-scheme-overview>.
- 32 According to the National Retail Federation's list of top 100 US retailers in 2015. National Retail Federation, "Top 100 Retailers Chart 2015," <https://nrf.com/2015/top100-table>. See signatories at Bangladesh Accord, "Signatories," 2015, <http://bangladeshaccord.org/signatories/>.
- 33 Steven Greenhouse and Stephanie Clifford, "U.S. Retailers Offer Plan for Safety at Factories," *New York Times*, July 10, 2013, http://www.nytimes.com/2013/07/11/business/global/us-retailers-offer-safety-plan-for-bangladeshi-factories.html?_r=0.
- 34 Walmart, "Standards for Suppliers," 2015, <http://corporate.walmart.com/global-responsibility/ethical-sourcing/standards-for-suppliers>; Walmart, "Audit Process," 2015, <http://corporate.walmart.com/global-responsibility/ethical-sourcing/audit-process>.
- 35 Steven Greenhouse and Stephanie Clifford, "Fast and Flawed Inspections of Factories Abroad," *New York Times*, September 1, 2013, <http://www.nytimes.com/2013/09/02/business/global/superficial-visits-and-trickery-undermine-foreign-factory-inspections.html>.
- 36 Julfikar Ali Manik and Nida Najar, "Bangladesh Police Charge 41 With Murder Over Rana Plaza Collapse," *New York Times*,

- June 1, 2015, http://www.nytimes.com/2015/06/02/world/asia/bangladesh-rana-plaza-murder-charges.html?_r=0.
- 37 Truly independent audits are needed. One issue found even in the 2008 financial crisis was the lack of independence of the credit rating agencies, and that issue still has not been fully resolved. Gianluca Mattarocci, *The Independence of Credit Rating Agencies: How Business Models and Regulators Interact* (St. Louis: Academic Press, 2013), <http://librarytitles.ebrary.com/Doc?id=10793772>.
- 38 RightShip, Cargill, Huntsman Corporation and Unipeck UK Set New Industry Standard on Fuel Efficiency for chartering Vessels, February 10, 2012, <http://site.rightship.com/resources/news-releases/2012/10/02/cargill.-huntsman-corporation-and-unipeck-uk-set-new-industry-standard-on-fuel-efficiency-for-chartering-vessels/>; Lloyd's List Editorial, "72. Warwick Norman, RightShip," Lloyd's List Asia, December 12, 2014, <http://www.lloydslist.com/ll/news/article453092.ece>; and author confidential interviews with RightShip representatives, 2013.
- 39 ISN Insider, "ISN Partners With Canadian Nuclear Laboratories to Strengthen Workplace Safety," June 23, 2015, <http://www.isnworld.com/~isn/blog/?p=4372>; and author interviews with ISN representatives, 2015.
- 40 BSI Supply Chain Solutions, "Government Programs That We Support," 2015, <http://bsi-supplychainsolutions.com/en-US/about-us/government-programs/>.
- 41 International Laboratory Accreditation Cooperation, "About ILAC," 2015. <http://ilac.org/about-ilac/>.
- 42 Author interview with representative of Association of Public Health Laboratories, 2015.
- 43 International Civil Aviation Organization (ICAO), Convention on Civil Aviation (Chicago Convention), December 7, 1944, <http://www.refworld.org/docid/3ddca0dd4.html>. See in particular Article 37 of the convention.
- 44 Thormodur Thormodsson, "The ICAO Universal Safety Oversight Audit Programme," presentation at the ICAO-WHO CAPSCA Global Symposium, Montreal, April 2015, <http://www.icao.int/Meetings/CAPSCA2015/Presentations/DAY%202/Session%206/01%20USOAP%20for%20WHO%20presentation.pdf>.
- 45 Voice of America, "UN Agency Questions Thailand's Air Safety," December 9, 2015, <http://learningenglish.voanews.com/content/un-agency-questions-thailands-air-safety/2700345.html>.
- 46 IAEA, "Evolution From Voluntary Assessment to Mandatory Audits: Experience of the International Civil Aviation Organization," <http://www-pub.iaea.org/MTCD/meetings/PDFplus/2011/cn200/documentation/icao-infopaper3.pdf>; ICAO, "The Creation of the USAP," <http://www.icao.int/Security/USAP/Pages/The-Creation-of-the-USAP.aspx>.
- 47 United Nations, *Contribution of the International Maritime Organization (IMO) to the Secretary-General's Report on Oceans and the Law of the Sea, 2008*, 2008, http://www.un.org/Depts/los/consultative_process/mar_sec_submissions/imo.pdf.
- 48 International Maritime Organization, *The International Ship and Port Facility (ISPS) Code*, http://www.imo.org/en/OurWork/Security/Guide_to_Maritime_Security/Pages/SOLAS-XI-2%20ISPS%20Code.aspx; International Maritime Organization, "Maritime Security and Piracy," <https://www.imo.org/en/OurWork/Security/Pages/MaritimeSecurity.aspx>.
- 49 *The 9/11 Commission Report: Final Report of the National Commission on Terrorist Attacks Upon the United States*, official government edition (Washington, DC: Government Printing Office, 2004), p. 398, <http://govinfo.library.unt.edu/911/report/911Report.pdf>.
- 50 National Fire Protection Association, "NFPA 1600: Standard on Disaster/Emergency Management and Business Continuity Programs," <http://www.nfpa.org/codes-and-standards/document-information-pages?mode=code&code=1600>.
- 51 United States, *Implementing Recommendations of the 9/11 Commission Act of 2007* (Washington, DC: Government Printing Office, August 3, 2007), p. 465, https://www.nsa.gov/civil liberties/files/pl_110_53_sec_803_9_11_committee_act.pdf.
- 52 Federal Emergency Management Agency, "About PS-Prep," last updated October 6, 2015, <http://www.fema.gov/about-ps-preptm>.
- 53 US Department of Homeland Security, SAFETY Act, <https://www.safetyact.gov/pages/homepages/Home.do>.
- 54 ASIS, "ASIS Organizational Resilience Standard Receives Safety Act Certification," September 14, 2011, <https://www.asisonline.org/News/Press-Room/Press-Releases/2011/Pages/ASISOrganizationalResilienceStandard.aspx>.
- 55 Bernhard et al., *International Convention on Nuclear Security*.
- 56 ENCA, "S. Korea Angered by Reactor Fraud," May 31, 2013, <http://www.enca.com/world/s-korea-angered-reactor-fraud>.
- 57 After Fukushima, the public questioned nuclear power expansion. Yet concerns softened as the industry's potential contributions to slowing climate change were considered. NEI, "Public Favorability of Nuclear Energy Climbs for Today's Reactors, Future U.S. Development and Global Leadership," March 17, 2015, <http://www.nei.org/CorporateSite/media/filefolder/Backgrounders/Reports-Studies/Topline-Public-Opinion-Memo.-March-2015.pdf?ext=.pdf>. Note, an early 2015 report showed that 68 percent of US adults polled favor "the use of nuclear energy as one of the ways to provide electricity in the United States," <http://www.nei.org/CorporateSite/media/filefolder/Backgrounders/Reports-Studies/Topline-Public-Opinion-Memo.-March-2015.pdf?ext=.pdf>.
- 58 For example, the French nuclear safety regulator discusses some relative plant performance in *ASN (Nuclear Safety Authority) Report on the State of Nuclear Safety and Radiation Protection in France in 2014*, <http://www.french-nuclear-safety.fr/Information/Publications/ASN-s-annual-reports/ASN-Report-on-the-state-of-nuclear-safety-and-radiation-protection-in-France-in-2014>, Chapter 8. The US Nuclear Regulatory Commission reports on its reactor assessments at *Reactor Oversight Process (ROP)*, <http://www.nrc.gov/NRR/OVERSIGHT/ASSESS/#section2>, although security information is not reported.
- 59 The Global Initiative to Combat Nuclear Terrorism has as one of its principles the enhancement of security of civilian nuclear facilities and has expressed interest in promoting industry participation in its activities. See US Department of State, Global Initiative to Combat Nuclear Terrorism 2015 Plenary Meeting: Joint Co-Chair Statement, Washington, DC, June 17, 2015, <http://www.state.gov/r/pa/prs/ps/2015/06/243947.htm>.

THE STANLEY FOUNDATION

THE STANLEY FOUNDATION | 209 IOWA AVENUE, MUSCATINE, IA 52761 USA
563-264-1500 | 563-264-0864 FAX | INFO@STANLEYFOUNDATION.ORG

The Stanley Foundation advances multilateral action to create fair, just, and lasting solutions to critical issues of peace and security. Our work is built on the belief that greater international cooperation will enhance global governance and spur global citizenship. The foundation frequently collaborates with a wide range of organizations using different forums, formats, and venues to engage policy communities. We do not make grants.

Our programming addresses profound threats to human survival where improved multilateral governance and cooperation are fundamental to transforming real-world policy. Current efforts focus on policy improvement to prevent genocide and mass atrocities, eliminate the threat of nuclear terrorism, and drive collective and long-term action on climate change. The foundation also works to promote global education in our hometown of Muscatine, Iowa, and nearby.

A private operating foundation established in 1956, the Stanley Foundation maintains a long-term, independent, and nonpartisan perspective. Our publications, multimedia resources, and a wealth of other information about programming are available at www.stanleyfoundation.org.

The Stanley Foundation encourages use of this publication for educational purposes. Any part of the material may be duplicated with proper acknowledgement. Additional copies are available. This brief is available at www.stanleyfoundation.org/resources.