Incentivizing Good Governance Beyond Regulatory Minimums: The Civil Nuclear Sector

Debra K. Decker,[1, 2] Kathryn Rauhut[3]

[1] Senior Advisor, Stimson Center

[2] Corresponding Author, ddecker@stimson.org

[3] Non-Resident Fellow, Stimson Center

[*see Author Capsule Bios below*]

Abstract

The consequences from a blended cyber-physical terrorist attack on a nuclear power plant are potentially catastrophic. Sabotage of the plant or theft and subsequent use of radiological materials can potentially lead to blackouts, deaths, and injuries and even a release of radiological materials. This threat continues to evolve in sophistication and complexity and is outpacing the ability and resources of governments to anticipate risks and to protect their critical infrastructure and the public from harm. Policymakers are working to keep up with the rapid onset of these threats to reinforce the resilience of critical infrastructure. Cyber vulnerabilities including insider threats are also evolving, with cyberattacks on nuclear facilities the tip of the iceberg as more sophisticated advanced persistent threats develop. This paper suggests governments look beyond regulations and policy directives to harness the power and energy of the market to incentivize operators to voluntarily adopt security measures beyond regulatory requirements.

Good organizational governance is important and necessary to secure critical infrastructure including nuclear facilities and increasingly can be rewarded by the market. The definition of what is good organizational governance matters to investors, lenders, insurers, regulators, and the public. Is the organization going to be able to function effectively as an enterprise and provide a return to investors, pay back its loans, protect its workers and community, including the environment? In the nuclear field, the stakes can be high—with stakeholders depending on a stable baseload electric supply without safety or security incidents, especially of a radiological nature.

 doi: 10.18278/jcip.4.1.15

This article documents findings from a multi-year project to identify incentives for nuclear security beyond regulatory minimums, with a focus on nuclear power plants. We assessed the importance of standards and developed a "Good Governance Template" to support owners/managers in obtaining benefits and reducing potential liabilities. We found that market incentives are developing in areas such as insurance, credit, and other rating systems to support the development of good governance, including incentives for companies to demonstrate due care in the management of risks, especially cyber risks. Building a business case for nuclear security based on these incentives is an important step forward in securing our nuclear future, especially in terms of cyber risks.

Keywords: Governance, nuclear security, nuclear safety, nuclear power, regulation, standards, guidance, incentives, liability, cyber, insurance, credit ratings, ESG ratings, sustainability, due care

Introduction

The nuclear sector, like other critical infrastructures, will continue to be a target—for terrorists, domestic activists, and foreign state actors penetrating domestic critical infrastructures. Given these threats with new avenues like cyber for attack and the potentially high consequences of any incident, ensuring nuclear safety and security remains a critical issue. By definition, critical infrastructure performs essential functions for a community. The designation of what constitutes critical infrastructures may differ somewhat between countries and across regions, but the approaches to managing risks and the oversight mechanisms to ensure safe and secure performance are similar. Regulatory authorities establish minimum baseline requirements. Policy directives supplementing these are put forth from a central authority such as through an Executive Order or a European Union Council Directive. Oversight of compliance and implementation is complex, especially in sectors that present high risks. With all this, however, the policy goals are the same—to have the critical infrastructure organization internalize some of the external costs from potential malperformance.

Although regulations and directives may be essential to ensuring some minimum levels of protection, performance, and resilience of critical infrastructures, compliance may not be achieved and is by no means sufficient. Some countries' regulatory authorities may not have the capacity or capability to provide adequate oversight to ensure compliance or to insist on performance improvements. Even in countries that have well-developed oversight authorities, regulations and other requirements typically do not keep up with the emerging challenges in to-

day's fast-paced societies. Overly prescriptive regulations can be not only costly and burdensome but also counterproductive by impeding optimization of organizational safety and security. Technological innovations, increased digitization and adoption of novel processes may present efficiencies but can also pose new risks beyond what regulators and policymakers conceived. Recognizing this, some oversight authorities like the US Nuclear Regulatory Commission (NRC) are moving towards performance-based systems.[1]

Thus, to ensure safe and secure performance of our most critical assets and systems, owners as well as managers and operators must be incentivized to invest in good governance in a dynamically changing world. Safety and security must not be costly burdens seen to constrain but optimized to also benefit business and ensure balanced investment in managing across risks.

This project on incentivizing good performance in the civilian nuclear industry sector started with the Obama Administration's goal of strengthening nuclear security internationally, including in the United States, as interest in nuclear energy increases—not just for power but also for other industrial and research purposes. The four international Nuclear Security Summits under U.S. President Obama from 2010 to 2016 helped to raise awareness of nuclear risks, with some nuclear materials and facilities vulnerable to extremist and terrorist threats and insiders always a concern. The civil nuclear industry is slowly growing worldwide although plants are closing domestically. The drivers for nuclear's global growth include increasing energy demand as the world population grows and the need for carbon-free energy as well as desalination. New advanced reactors are also part of the energy mix that are expected to be less expensive, safer and more secure. These may well jumpstart future new nuclear growth.

The goal of our research was to find whether security could be embedded in the interests of nuclear licensees, as safety is embedded: Is there a way to ensure civil nuclear security beyond regulatory minimums? Security is part of overall safety. Security violations can become safety violations in the view of nuclear regulators. In many languages, safety and security are in fact the same word. Safety incentives should logically work to incentivize security. We attempted to identify the right business case that could cause licensees to properly adjust their performance to a new fast-changing environment that regulations and directives could not quickly anticipate and regulate. We sought the "holy grail": a market-based incentive or incentives that could apply benefits to reward good governance not only to the nuclear power industry but also to the broader nuclear sector, such as nuclear fuel facilities, transport, and research/test reactors. If incentives could work in the nuclear sector, they could be applied across the spectrum of other critical infrastructure sectors as well.

1 See, for example, guidance from the U.S. NRC at: https://www.nrc.gov/reading-rm/doc-collections/nuregs/brochures/br0303/index.html

In interviewing nuclear industry stakeholders, we found that cybersecurity was one of the major operator concerns. The Obama Administration had itself recognized that cybersecurity of critical infrastructure is a major source of risk, so it worked with stakeholders to develop a Cybersecurity Framework and explored incentives to foster adoption (U.S. Department of the Homeland Security Integrated Task Force, 2013). Many of those incentives required legislation and political will, which were slow to arise. Only recently have government mandates and incentives matured, with the Cyberspace Solarium Commission recommendations and related legislation (Cyberspace Solarium Commission n.d.). The Solarium Commission and earlier reports recognized that market forces can work to mitigate risks.

We sought to identify and help magnify those forces that could apply to better managing not just cyber risks but also other sources of risk. We found new market incentives evolving as States' regulatory systems are unable to keep pace with risks from technological changes in and outside facilities, including blended physical-cybersecurity threats and new types of possible incidents such as those involving drones or deep fakes.

Methods and Results

This paper is the summation of five years of research, interviews and roundtables which considered various incentives that could motivate operators to voluntarily adopt security measures beyond regulatory minimums. We went through a systematic series of questions and developed and tested hypotheses around different market levers. We started first by considering who, in addition to regulators, were looking at nuclear performance and how those evaluations might be used in the market. We then considered how voluntary consensus standards could be used to bring external benefits to operators and recognized that standards compliance was not enough in itself. Good governance as well as stewardship of nuclear materials is required. Low probability, high consequence events like terrorism demand difficult tradeoffs and resources may not always be readily available. Strong security does not necessarily mean more security but can often mean a rightsizing of existing resources (Forging Strong Security Norms, Kempfer, Rauhut, Umayam, 2018). With stakeholders, our team developed and discussed a "Good Governance Template" that could guide senior leadership in their decision-making processes to ensure and demonstrate good security without revealing sensitive information. The template is a set of principles with related questions (e.g., on resilience and contingency planning) which help owners/operators illustrate and track "reasonableness" by providing a transparent statement of criteria evaluated by those managing risks. The template is a written set of risk mitigation protocols that illustrate regular risk assessments and corresponding personnel training and document best practices, thus garnering benefits for good governance from regulators, insurers, financiers/investors, judges, and attorneys.

The largest benefit we identified from an initial roundtable of stakeholders was reduction in potential liability for an incident as well as the significant potential loss of reputation from that incident. Subsequently, we found that credit ratings, which measure many factors including general governance, influence funding costs and are thus a concern of owners/managers. Also helping to drive good governance, including over security, is the development of cyber ratings and ESG—environmental, social, and corporate governance—ratings. These are independent factors influencing some investors, financiers and insurers but also are becoming factors for credit raters. The Governance Template, a simple tool, if properly applied, could help owners and managers improve their ratings.

Who, in addition to regulators, is addressing nuclear security?

The International Atomic Energy Agency (IAEA), the UN-affiliated agency established to promote the "safe, secure and peaceful use of nuclear technologies," defines nuclear security accordingly: "Like nuclear safety, nuclear security aims to protect people, property, society and the environment from harmful effects of ionizing radiation" (International Atomic Energy Agency n.d.).

The IAEA develops guidance documents for nuclear security—but these are guidance only, slow to be published and the world changes quickly. The IAEA has many types of review missions. Countries have taken advantage of its Integrated Nuclear Security Support Plan (INSSP) peer-reviews that over the past five years include a cyber security component for both operations and infrastructure derived from IAEA published guidance. On a facility basis, the IAEA conducts International Physical Protection Advisory Service (IPASS) missions and has started including cybersecurity in these. However, ensuring performance improvements requires follow-up missions and the funding, staffing and resources do not always exist for such follow up missions. These are confidential missions with only some states revealing their performance assessment. This lack of transparency may make the reviews more attractive to some operators but limit their utility for market rewards and benchmarking by other states.

Nuclear facilities/materials should be secure from sabotage or theft and safe from all hazards, including accidents and other incidents. The World Association of Nuclear Operators (WANO), whose U.S. office sits with the Institute for Nuclear Power Operations (INPO), does full peer reviews of nuclear operators every four years with interim reviews every two years, but these consider safety and reliability and exclude security. WANO is also working with other organizations such as the IAEA and the Japan Nuclear Safety Institute to see what other reviews can be judged as equivalent to WANO peer reviews. Although WANO might not directly review security, cyber security and supply chain security are of high concern within the nuclear industry; their inclusion in future reviews appears inevitable.

The World Institute for Nuclear Security (WINS) has supported the development of professional training and certifications for nuclear security officers. Some country regulators have minimum requirements for nuclear security officers. Such professional certifications can help evidence good security training but not necessarily performance. Others support nuclear security, such as with exercises, but not necessarily the development of good, embedded standards. And almost all these efforts are not made public so cannot get rewarded.

Some press investigations have consolidated public information of US nuclear power plant ratings, including the Nuclear Regulatory Commission scoring as part of its reactor oversight process—but these are time-consuming, occasional efforts (Proctor 2018).

Could Voluntary Consensus Standards Help Reduce Risks?

To develop a business case for nuclear security, we hypothesized with industry stakeholders how they could come together to decide on what good practices are necessary as well as sufficient to merit rewards. At industry's request, we presented a paper making the case for voluntary consensus standards at the joint Industry-Civil Society Nuclear Summit in 2016 (Nuclear Energy: Securing the Future – A Case for Voluntary Consensus Standards, Decker and Rauhut 2016).

The paper points out the plethora of standards development bodies around the world beyond the International Standards Organization (ISO) and includes statements from industry calling for some standards particularly for managing cyber risks. This was a new development as U.S. private sector participants working with the U.S. Department of Homeland Security (DHS) and the National Institute of Standards and Technology (NIST) on cyber security had wanted to ensure that NIST developed a cybersecurity framework not a standard.

We were thus encouraged to explore the standards development world. If you were compliant with some performance standards, could you get benefits from insurers, financers, regulators, the public? We looked at what standards had been developed already in the nuclear area and whether standards really work to ensure better quality practices in those who follow them, including within the nuclear industry.

Some guidance for security that could lend itself to standards development comes from many treaties, conventions and UN Security Council resolutions that call for nuclear safety and security, in particular the Amendment to the Convention on the Physical Protection of Nuclear Material and related IAEA guidance. This prompted our study of where standards can best be applied (The Quest for Nuclear Security Standards, Decker and Rauhut 2016).

ISO, American Society of Mechanical Engineers (ASME) and its N-Stamp, ASTM, ASIS, and others have developed voluntary consensus standards for prod-

ucts and quality performance. Management standards in safety/risk management, such as ISO quality management (ISO 9000 series) and its risk management guidance (ISO 31000), are generally not used in the nuclear industry. However, the industry has strong standards over product quality.

There has been a move to develop specific standards in the nuclear industry for quality management, such as for nuclear supply chain management, but these are not yet widely adopted. On security, the IAEA just issued in 2021 guidance on computer security that suggests "competent authorities" may look to some ISO/IEC [International Electrotechnical Commission] 27000 series information security management standards (IAEA 2021).

In discussions with these official standards organizations as well as some private providers of rating services in other fields, we found that organizations who went through the process to be shown compliant by ISO or other standards did so as a contractual requirement of performance or as a market differentiator. The U.S. Department of Defense asked ASIS, an official American National Standards Institute developer which is known for its security standards certifications, to develop standards for private security forces with certified training and then required those certifications for securing related Defense Department contracts.

That the nuclear industry has not widely adopted third-party quality management standards is clearly due to lack of perceived benefits from external certifications/accreditations. That said, the industry generally operates to its own high standards, which get even more stringent after each major incident. On safety, INPO has done many trainings and certifications; but regulators such as the U.S. Nuclear Regulatory Commission require these (Institute of Nuclear Power Operations n.d.). WINS has certified more than 400 professionals in nuclear security, often with financial support. Without regulatory requirements or external funding, it is unclear to what extent such initiatives would persist.

Unfortunately, standards can become a check-the-box routine without significant national and organizational commitment to the good governance that can drive good safety and security cultures. In Korea in 2012, the testing of nuclear power plant parts was discovered to have been falsified, costing billions of dollars and sending many to jail (Park 2013). The Fukushima nuclear power disaster, although precipitated by a tsunami, was more attributable to poor management and "regulatory capture," with the regulators more controlled by the nuclear industry than regulating it (Kaufmann and Penciakova 2011).

This became clearer as we pursued discussions with the Organisation for Economic Co-operation and Development's Nuclear Energy Agency (NEA) in our quest to find the conditions from which benefits could accrue for good security. How can you demonstrate good security? The NEA has heavily emphasized the importance of human and organizational elements in nuclear safety culture. In

discussions with the NEA, we agreed that good governance was the key to good security just as it is to safety. Standards may be good but are not sufficient—governance drives culture which drives adherence to the spirit of any adopted standards (Decker 2016).

Doubling Down on Security Culture: Good Governance is Good Business

Culture is important to good performance. Some recent examples of accidents where safety culture was identified as a contributing cause include BP's Texas City refinery explosion in 2005 (Chemical Safety Board), the Washington Metropolitan Area Transit Authority Metrorail collision in 2009 (National Transportation Safety Board), the Deepwater Horizon oil spill in 2010 (United States Coast Guard), and the Upper Big Branch mine explosion in 2010 (Mine Safety and Health Administration).

A lot of work has been done on safety culture and some work has been done on security culture, but leaders and how they govern drive culture. Good leadership and good safety and security culture are closely related. In the nuclear area, a U.S. Nuclear Regulatory Commission study of INPO's safety culture evaluations and plant performance showed the correlation between culture and fewer unplanned scrams, forced outages and better overall operating performance (Morrow and Barnes 2012).

Creating a governance framework for good nuclear security could prove cost-effective for operators, that is, it could derive licensee benefits from using it, we hypothesized. This would not be an in-depth standard or IAEA guidance, but a framework for management—for reflection, review, documentation and perhaps also a tool for communicating with stakeholders that demonstrates managements' due diligence, that management has seriously reflected on and pursued good security measures.

Industry was already thinking along these lines and had presented an initial security governance framework at the 2016 Nuclear Industry Summit in their report "The Role of the Nuclear Industry Globally." We took that initial draft of a governance framework and further developed it in discussions with operators, insurers, regulators, lawyers, and others who could help provide insight on possible incentives for good governance. We looked to other industry sectors, such as aviation and maritime and especially the chemical industry—and built out the framework in more detail. We supplemented it with IAEA guidance, WINS guidance, and incorporated WANO/INPO leadership principles (Duncan 2019).

The result was a Good Governance Framework that could be used by operators and was tested with stakeholders (Stimson Center n.d.). The team discussed the tool with various stakeholders and across various cybersecurity hypothetical

scenarios. Although the Framework uses the term "Security" throughout, changing this to "Safety and Security" was deemed to provide even broader benefits.

We also investigated evaluations of governance and how those were evolving beyond just the maritime, chemical and aviation sectors and looked to the assessment of insurers and other evaluators of good governance. We found that rating systems help assess an organization's governance and reassure stakeholders of effective oversight and management as well as secure returns. Good governance can also help protect owners/managers from some potential liability. More investors, lenders and the public are looking to environmental, social, and governance factors in their assessment of organizations, and ratings have been developed in that area. Insurers and credit rating agencies are also becoming more sophisticated as more data become available, especially in the area of cyber risks.

Discussion

The journey to finding overall good governance as the basis for potential market rewards was a long one. This was an iterative process, with the framework being tested and refined across many stakeholder groups, with a focus on those conveying benefits.

Regulatory Benefits

Could you gain some regulatory benefits from owners, managers and operators doing a self-assessment of security using a Good Governance Framework? Although we were exploring benefits to be derived from the external market, we found that regulators are always a primary concern of licensees.

What did regulators say about supporting the nuclear security governance framework we were developing:

- Yes! It's another tool in the regulatory toolkit.
- If we know that an operator has not been doing well but is working on bettering their governance model, we can give them the benefit of the doubt in some of our oversight evaluations.

This stakeholder approval was a by-product of the effort, but an important one.

Insurance Benefits

As part of risk management, organizations take out insurance. Many countries require operators to be insured to demonstrate that the country is compliant with international treaties (World Nuclear Association 2021). Commercial insurers generally exclude nuclear risks, thus specialized nuclear insurers exist that provide coverage for nuclear operators. They share risks among themselves by es-

tablishing pools of insurance within and across countries (Nuclear Risk Insurers n.d.). Thus, we hypothesized that insurance had to be a lever for good governance internationally.

Insurers evaluate risks for underwriters and help operators in pre- and post-incident performance. They recommend ways to reduce the likelihood of a loss and its consequences. They also can assist in reducing the consequences of an incident by providing advisory services and assistance post incident.

The two major categories of insurance are property insurance, which includes business continuity, and liability insurance, which covers third parties' losses. Other specialized insurances exist, including for cyber coverage. Cyber is one of the key areas that worry nuclear insurers. With plants becoming more digitized, potential attack vectors increase—with increased risks to software and hardware, to information technology and operational technology. The electric sector is a prime target for advanced persistent threat actors who act through trusted parties, including managed service providers. Supply chain and cyber-related risks including ransomware attacks worry the sector.

Policies in the past had been silent on cyber coverage, so these were deemed by default to be covered risks. However, now they are generally excluded and must be specifically written back into a policy or obtained through a separate cyber risk policy that details coverage.

The specialized nuclear insurers survey nuclear power plants to assess plant performance and the insurance risk presented. As only 441 power plants currently operate in the world, with 56 under construction (primarily in China), specialized assessors—typically engineers and nuclear professionals—are hired by insurers to survey these plants (WNA 2021 and Reitsma 1998). While security and security culture are not standalone parts of the structured assessments, engineering consultants and pool representatives informed us that it is incorporated into their overall assessment. In the United States, which has the largest number of nuclear power plants, American Nuclear Insurers (ANI), a joint underwriting association, and Nuclear Electric Insurance Limited (NEIL), a mutual insurance company, respectively cover primarily liability and property insurance. Each operator takes on the risk of the others. Risk assessments and to some extent pricings for coverage are informed by confidential ratings that INPO issues. We also found that evidence of good governance, such as the model we developed, could help inform insurance underwriting.

However, insurance costs are a very small part of a nuclear power plant's cost. Capital costs (for the facility itself) and salaries are the largest expenses with fuel costs much lower than gas or coal plants (WNA 2021). Treaty terms cap liability limits for radiological events, while governments typically absorb much of the liability costs of the operators which keeps insurance rates low. Also, note that in-

surance did not factor into some large nuclear events like Chernobyl and Fukushima.[2] We found possible better insurance terms from better nuclear security, but these were not a driver of many operating decisions.

Also, insurers do not base their prices solely on risk, so demonstrating good governance and reducing risks would not necessarily lead to better insurance terms. Insurers also price based on portfolio performance, their loss experience and market competition.

The only lever insurance can provide to promoting good governance is the question of an entity's ability to obtain insurance at all. In only a few cases internationally have insurers requested changes in an enterprise's operating procedures before confirming underwriting. Insurers' engineers, while undertaking surveys, will influence operators to improve resilience to cyber incursions. They provide recommendations and promote best practices observed internationally, such as from the IAEA, NEA, WINS, and national regulatory bodies.

This may change. Small modular reactors (SMRs) and advanced modular reactors (AMRs) are likely to become a significant part of the future nuclear power industry. With different cyber risk exposures than legacy nuclear systems, these new plants will present insurers with new challenges. An advantage of digital systems utilized for SMRs and AMRs is that they will be designed and manufactured to work in the digital age, with associated security concerns addressed from the initial design. They are also much more digitally complex than older legacy systems that have backfitted digital systems and hardwired safety systems. SMRs and AMRs with remote monitoring systems will have to be assessed to be reliable and resilient. Assessment of their safety and security will be tied not only to their having safety and security "by design" but also to their having a "commoditized" approach to their manufacture and performance. This will make supply chain even more important. New types of insurance might be needed with more attention to governance quality standards as cyber and supply chain risks become better understood.

The nuclear pools have followed the market trend, i.e., to specifically exclude cyber in property insurance policies, and operators have shown a lack of interest to separately insure it. They self-insure or do not insure. The pools concluded that operators were comfortable managing the cyber risk themselves within their safety and security frameworks.

The pools do not exclude cyber from nuclear third-party liability cover for radiological events, but as mentioned earlier these are generally capped. However,

2 See: https://www.oecd-nea.org/law/table-liability-coverage-limits.pdf. Note that Chernobyl and Fukushima were not privately insured (https://www.oecd-nea.org/ndd/workshops/nuclearcomp/presentations/documents/1.SebastiaanReitsma-OECD-NEALiabilityWorkshop-December2013.pdf). Japan was not party to a convention until after the Fukushima incident, and the Soviet Union's responsibilities for the Chernobyl incident were limited under the then-existing convention details (https://www.oecd-nea.org/law/chernobyl/LAMM.pdf).

potential liability from events not involving radiological releases must be considered as cyber risks increase. Lloyd's, the specialist insurance/reinsurance market, has called for better clarity in policies and noted the major and potentially catastrophic impact of a cyberattack on an electric grid (The Council of Insurance Agents and Brokers 2019 and Lloyd 2015).

The importance of good governance and stewardship of nuclear assets including management of cybersecurity and supply chains cannot be understated. New technologies, including deep fakes, can escalate the impact of cyber incidents. Owners/managers must assess risks as part of good governance; and transferring some risks to insurers should be better studied and well considered. The insurance industry's assessment of cyber risk is quickly increasing with insurance becoming more costly as underwriters handle more cyber incidents and want to manage their exposures.

Reduced Liability and Increased Reputational Benefits

Two effective inducements for incentivizing security governance were operator concerns for reputation and liability from events without radiation releases. The international liability regime covers incidents that release or threaten to release radiation; a blackout or other disruption to the power supply at a nuclear power plant would not be covered (Nuclear Energy Agency 2019). In the aftermath of a terrorist incident at a nuclear facility, an operator could be held liable for negligence, that is the failure to act reasonably and adequately to protect the public and environment from harm. To demonstrate this, we held several roundtables in London with judges, attorneys, regulators, insurers, and operators. We developed hypothetical cybersecurity scenarios in which there was a blackout at a nuclear power plant with catastrophic consequences. One roundtable featured a mock trial in which former judges heard evidence about the hypothetical incident and ruled on whether the operator of the hypothetical plant in question would be held liable for civil and criminal charges for failure to prevent or mitigate a cyber terrorist-related event[3] (Stimson 2017 and Stimson 2018). In order to do so, the group tested iterations of the Good Governance Template and whether or not use of the template could have prevented or mitigated the effects of an incident.

The purpose of these roundtables was to explore liability mechanisms to identify economic incentives to make business decisions above and beyond compliance with regulatory minimums. Reasonable precautions must be taken to have systems and processes in place to address incidents with due diligence to ensure that processes are working consistently, reasonably and in accordance with industry norms. These factors are required to evidence an operator's duty of care. In

3 See some summaries at https://www.stimson.org/wp-content/files/file-attachments/LiftingTheLid-R4-WEB.pdf and, an earlier event, at https://www.stimson.org/2017/demonstrating-due-care-cyber-liability-considerations-nuclear-facilities/.

addition, operators must operate with continuous improvement and look to best practices in managing their facility.

The importance of developing and implementing a good model of governance and transparently reporting on that model proved to provide public assurance and support owners' and managers' self-attestations of operating with due care (World Institute for Nuclear Security 2018). It was found that significant civil and criminal liability can be reduced if operators have taken reasonable measures to protect the public and environment.

These personal impacts from demonstrating good governance proved to be compelling. Some benefits from good governance go even further. Entities can apply in the United States for certain protections from litigation if they comply with principles under the Homeland Security Act of 2002 known as the SAFETY Act. Enacted after 9/11, it was intended to motivate production of anti-terrorism products and services. The Act provides a unique way for organizations to limit liability in the event of a cyber or physical act of terrorism. It provides significant protection for products and services that meet specific anti-terrorism performance metrics. Security companies that have received SAFETY Act protection include ABM Security Services and Wackenhut Security. The National Football League, Major League Baseball and National Basketball Association have also had their security and best practices certified, and finally, the Southern Company obtained Safety Act coverage for its cyber/risk mitigation program for its electricity generation, transmission and distribution, gas services, business corporate services, and other activities.[4]

Finance and Investor Benefits

We next explored the issue of financing and whether demonstration of good governance of security and safety could attain better financing terms? Nuclear facilities are very expensive to build and require many investors and lenders (although this will likely change with SMRs and AMRs). Public companies, private companies, utilities that have nuclear generation, government-owned entities can all get rated, rating agencies explained. Because an entity is publicly owned does not mean that it is not subject to a rating review.

- *Export finance banks*: We researched export financing and spoke with several export banks. We found countries are looking to support their exports and build strategic relationships and are not that concerned about getting paid back over the many decades the financing would likely be outstanding, or so it seemed.

- *New builds:* Security risk is also not a concern for others financing new builds—project overruns are. Initial funding arrangements were all based on strategic

4 See currently approved SAFETY Act technologies at: https://www.safetyact.gov/lit/at/aa.

country decisions, project-specific financing and country-related overall risk profiles—not the potential risks inherent in the eventually operational plants.

- *Operational Plants:* For going concerns—enterprises that were already operating—security can be a factor. Organizations are sensitive to changes in their risk profiles because they get evaluated by credit rating agencies like Standard & Poor's, Moody's and others around the world. Stock analysts and investor advisors all have a lot to say. What does good governance of security mean to them? If an entity's ratings go down, the cost of borrowing goes up including on new debt issues. The value of the company itself can go down with lower stock ratings for poor governance. This impacts both public and private equity investors' valuations of the company.

We found that good credit ratings can translate to better financing terms for organizations and the ability to tap into a larger investor group. Some investors such as pension funds can only invest in certain grades of investments. *The Economist* notes, "A downgrade can cause a company's funding costs to rocket, or a run on a bank. It can also force a corporate or sovereign borrower out of an index, draining the pool of investors willing or permitted to lend to it" (*The Economist* 2020).

Until now, most companies in the nuclear sector have had their credit ratings affected more by the general outlook for nuclear or the country risk of where they are located than by their individual performance, according to our interviews. This is changing somewhat as more data-driven risk evaluations are occurring in the rating agencies and as more investors consider sustainability and ESG goals in their portfolio holdings.

Credit, ESG and Cyber Ratings Driving Change

Credit rating agencies assess the ability of a country or entity to repay a debt. "Sovereign ratings" are given to a country to assess its political stability, foreign reserves, and other information. Ratings are also assigned to public and private companies and their various debt instruments. The rating agencies also give "ratings outlooks" that give their analysts' opinions regarding the direction of the rating for a future period given an entity's performance and anticipated market conditions.

The United States Securities and Exchange Commission recognizes nine credit rating agencies. (U.S. Security and Exchange Commission n.d.) The biggest are Moody's, Standard & Poor's (S&P) and Fitch. These three globally dominate, but other rating authorities in Europe, Switzerland, China, Russia and elsewhere recognize others also. Of particular interest—given where nuclear facilities are located—may be the European credit authorities' lists and rules, the Russian credit rating organization ACRA that partners with China, and Chinese rating agencies like China Chengxin Credit Rating Group that has a subsidiary joint venture with Moody's.

Credit rating agencies are not without controversy. The 2008 financial crisis highlighted the inability of the agencies to rate accurately, with misleading ratings on many financial instruments. Conflict of interest questions relate to how ratings agencies are paid; in the U.S., the organization being rated pays.

Given perceived overreliance on such agencies, the European Union and other members of the G20 took steps to ensure "that banks, market participants and institutional investors make their own credit assessments and not rely solely or mechanically on CRA [credit rating agency] ratings" (European Commission 2013). The EU cited the lack of transparency in agencies' sovereign ratings among other issues.

Given these and other concerns, under international regulatory requirements, banks have to risk-weight their assets (Chen 2020). Banks use complex rating systems beyond the rating agencies to make judgments on credit quality. Published operating information of a company is just one factor used in these assessments. But some lenders are beginning to look at textual information including public sentiment in assessing credit risks. And public sentiment is affected by entity and media reporting as well as credit ratings. This is significant with companies now clearly needing to manage their public reputations as part of good governance and good ratings.

Cyber risks in the electric utility area and nuclear sector in particular are indeed already concerns of analysts, as this sector is well known to be a target of terrorists, other States and hacktivists; and cybersecurity is increasingly affecting ratings. In 2017, the U.S. credit bureau Equifax suffered a major cyberbreach that released the personal information of nearly 150 million people (Fruhlinger 2020). [Note that credit bureaus rate individuals while credit rating agencies rate entities, so this was a release of individual's data.] The CEO resigned and asserted that the failure of one person in IT had left the company exposed to the exploit (Bernard and Cowley 2017). The company faced fines and class-action lawsuits that led Moody's to downgrade the company's ratings; this was one of the first time that Moody's had taken a negative rating action due to a cyber incident (Moody's 2019, 5). This affected the value of the company and its share price declined. However, as so many companies have experienced cyber incidents, the stock market appears to be suffering from breach fatigue and Equifax' share price has since rebounded (Osborne 2021). Early in 2021, it was found that Eletrobras, the largest power utility company in Latin America, was hit with a ransomware attack including as a target Eletronuclear, its subsidiary involved in the construction and operations of nuclear power plants (Cyber Reports 2021). Moody's, for one, deemed this a credit negative.

Analysts say that key to maintaining value after a cyber incident is to react quickly, responsibly and transparently to the incident. To attempt to quantify a company's cyber risk exposure—both IT and OT—and measure its resilience, in

2021 Moody's invested in BitSight and VisibleRisk to bring big data and more analyses to its cyber risk assessments (Moody's n.d. and VisibleRisk n.d.).

Investors look beyond credit ratings to other ratings and assessments of organizations. These investors can be individual ones looking not just for performance based on risk and returns but also for ethical matches for their portfolios. Shareholder activism has forced increased management interest in good governance (Broadridge n.d.). Investor and lender interest has led to Environmental, Social and Governance evaluations—or ESG, an outgrowth of earlier efforts at corporate social responsibility. The increase in interest in companies with good ESG profiles comes from individual investors as well as pension funds and other controllers of large sources of wealth, known as asset managers. This is not just about investors gaining more of a conscience, but also about analysts recognizing that such companies attract talent and have lower turnover thus potentially higher profits and better long-term sustainability, or at least that is the thinking (Thygensen 2019). And good governance is important. McKinsey notes, "Frequent governance reviews are … simply good corporate hygiene" (Birshan et al. 2020).

Approaches to ESG and sustainability reporting are proliferating, but their governance evaluations do not yet directly address oversight of safety/security for protection of workers and the environment (*The Economist* 2020). We see this changing, especially as we see ESG and credit ratings being developed into more finely tuned and integrated models—although some ESG may look at nuclear negatively (nuclear waste disposal) or positively (low carbon), which Canada's Bruce Power is capitalizing on with its green financing framework (Bloomberg News 2021). The ratings agencies' governance assessment differs from the internal good governance measures that we used in our model. Their models have higher-level measures that may include, for example, board structure, independence, diversity, and compensation but do include risk oversight (ISS n.d.). Some agreement on acceptable/important ESG indictors may well be forged as countries issue their own ESG rules, with the EU just publishing new disclosure rules on sustainability (think climate effects) for fund managers that the U.S. looks set to emulate (Eaglesham and Hirtenstein 2021 and Gnanarajah and Shorter 2021).

Moody's has been working on an effort to integrate ESG concerns into its overall ratings. Some cyber issues fall into ESG evaluations and could directly affect credit ratings, e.g., data privacy issues in the health care or financial services sectors. But other ESG effects on an entity's credit worthiness are more subtle. In discussions with Moody's, it was noted that operational aspects and risk transfer aspects of organizations' cyber risk profile are not fully captured in ESG ratings. For the Governance rating, 30-40 questions are considered with 80-90 sub-questions. Questions concern, for example, board structure, policies and procedures; board independence; compliance and reporting. Management credibility and track record are important, e.g., the organization performs as management plans

and says it will. Controversies in the news are tracked and included in evaluations. Moody's, as an SEC-approved credit agency has access to operations, information and internal reports that go beyond companies' public reporting. The INPO rating system for nuclear performance is shared with Moody's and other approved credit rating agencies (as well as insurers and INPO members, as earlier mentioned). Moody's executives noted that good governance of security affects environmental and social evaluations, and that ESG ratings should not be stove-piped. Indeed, the company is right now trying to integrate all evaluations.

Morningstar is an investment research organization that provides evaluations of relative risk and returns with a star-rating system. Its Morningstar ratings and its analyst recommendations are highly influential among fund managers. The firm has expanded its services into credit ratings and ESG ratings. Morningstar's Sustainalytics, an ESG rating organization, explained the ratings basis for its ESG system including such factors as overall industry exposure to ESG risks. Importantly, the firm monitors 70,000 news sources bi-weekly to rate the news' risk and impact on organizations and how that news might affect shareholders and stakeholders. In terms of evaluating governance, the firm considers business ethics and a company's handling of adverse events.[5]

The move toward greater evaluations of governance and reputation in assessing ESG ratings, and the move toward integration of evaluations (within ESG ratings, with credit ratings and from news sources), demonstrate that good governance of security should help in the future drive for better ratings and their benefits. Some aspects of security governance are already starting to affect ratings, at least in the cyber area. A rating can be affected but not so substantially—yet! The financial materiality of cybersecurity is only now being identified.

Other Efforts

Some press investigations have consolidated public information of U.S. nuclear power plant ratings (Cascadia Times 2013), including the Nuclear Regulatory Commission scoring as part of its reactor oversight process—but these are time-consuming efforts (Proctor 2018). Note, we did not look at National Nuclear Security Administration (NNSA) Performance Evaluations—although that would be an interesting exercise given the many past issues of government nuclear facilities.[6]

5 For other information on Sustainalytics, see: https://www.sustainalytics.com/about-us.

6 For some recent performance evaluations of government-owned but contractor-managed nuclear facilities, see: https://www.energy.gov/nnsa/articles/nnsa-releases-performance-reports-labs-plants-and-sites. Some issues on management of these facilities can be found in press reports as well in analyses of the Project On Government Oversight and the Exchange Monitor. Some good early work on incentives for nuclear security in government facilities with nuclear warheads and weapons-usable materials (before the advent of WINS in 2008), can be found at: https://scholar.harvard.edu/files/matthew_bunn/files/incentives_for_nuclear_security.pdf.

An INPO tactic that drives security and managers' quest for good ratings is management's consideration of quest for a good rating and thus a good reputation amongst peers. Peer pressure is perceived to be important. In 2019, the "Federal Energy Regulatory Commission (FERC) and North American Electric Reliability Corporation (NERC) issued a joint white paper proposing to 'name and shame' electric utilities violating NERC Critical Infrastructure Protection (CIP) Reliability Standards" (Jeweler et al. 2019). The organizations were receiving many Freedom of Information Act requests for these, and the thinking was that public exposure of noncompliance notices could lead to better compliance. However, fearing that this could also lead to even worse security breaches, the proposal was abandoned in 2020. In any event, reputation concerns can lead owners/managers to have better security governance, and enhanced reputation can then feed into credit, ESG, insurer benefits and better performance.

Conclusion

We have explored how market incentives could be used as a force multiplier to incentivize nuclear security beyond regulatory minimums and found that evidence of due care is a necessary prerequisite for achieving benefits. Recognizing that complete security can never be achieved, facilities could be inspired to good security and safety governance beyond regulatory minimums through a Good Governance Template that inspires reflection, requires systematic reviews and transparent risk assessments, and demonstrates due care.

We found that judgments of rating agencies, insurers, courts, and financiers can motivate good security performance of a nuclear facility operator by affecting public reputation and by modifying potential liability of the facility's owners/operators in the event of an incident. Evidencing good performance also potentially affects the availability of financing/investment as well as financing terms and conditions. Insurance availability, especially for cyber coverage, will become a more important incentive for good governance as owners/operators have expanded exposure to more complex technologies and an enlarged threat surface.

Each potential lever of influence has certain limitations, but when taken as a whole—as a reflection on a company's reputation—are very important. The overall reputation of a company is an important consideration in the judgments these parties make, and positive judgments bring benefits to the entities. Overall reputational considerations—not one individual market benefit—appear to drive owner/managers in a more holistic way. Peer judgments are important to an operator's own self-assessment, which should not be undervalued. Further, reputation influences regulators as well as the public and employees.

In sum, we found that the whole of incentives is bigger than the sum of its parts—that multiple and collective incentives promote the best security state of

practice and obtain the most benefits. Continual improvement, doing the right thing, right-sizing security, supporting a questioning attitude, seeking and adopting best practices—these are all mantras in the nuclear industry that the industry itself should continue to foster in licensees. Licensees will then benefit from better stewardship and governance of their facilities in the virtuous circle of knowledge and continuous learning.

Acknowledgements and Funding

The authors thank the John D. and Catherine T. MacArthur Foundation, the Carnegie Corporation of New York, the Stanley Foundation as well as the governments of Canada, Finland, and the United States for their financial support.

We would also like to give special thanks to the law firm of Pillsbury Winthrop Shaw Pittman and many of its staff for all their *pro bono* support and especially to Elina Teplinsky a partner at Pillsbury who has supported this work from its beginning. We also want to recognize the World Institute for Nuclear Security for collaborating with us—in particular, Roger Howsley, its former Executive Director, who was a visionary and gave this project his unwavering support. There were so many others who advised on this project, including Symantec and Lofty Perch on cyber issues, Moody's Corporation and Sustainalytics on ratings' incentives, Edlow International on transport risks and Nuclear Risk Insurers, the Nuclear Energy Institute and the Canadian Nuclear Association—to name just a few. We also want to recognize two remarkable leaders who are no longer with us: Frank Saunders, formerly with Bruce Power, and Greg Kaser, formerly with the World Nuclear Association. Thank you all. We deeply appreciate your contribution to helping us seek ways to make the world safer and more secure. We also would like to thank Stimson Research Intern Jerry Zhang for helping to edit this paper.

Acronyms and Abbreviations

AMR	Advanced modular reactor
ANI	American Nuclear Insurers
DHS	U.S. Department of Homeland Security
ESG	Environmental, Social, and Governance
FERC	Federal Energy Regulatory Commission
IAEA	The International Atomic Energy Agency
INPO	Institute for Nuclear Power Operations

INSSP	Integrated Nuclear Security Support Plan
IPASS	International Physical Protection Advisory Service
ISO	International Standards Organization
NEA	Nuclear Energy Agency
NEIL	Nuclear Electric Insurance Limited
NERC	North American Electric Reliability Corporation
NIST	National Institute of Standards and Technology
NRC	Nuclear Regulatory Commission
SMR	Small modular reactor
WANO	World Association of Nuclear Operators
WINS	World Institute for Nuclear Security

Author Capsule Bios

Debra K. Decker is a Senior Advisor at the Stimson Center, where she works on cyber and nuclear security issues. She has advised on strategy and risk management with private and public sector organizations, including the U.S. Federal Bureau of Investigation and the U.S Departments of Defense and Homeland Security. In the public sector, she has specialized in threats stemming from weapons of mass destruction and in the vulnerabilities of critical infrastructure. She was involved in the development of the National Institute of Standards and Technology first Cybersecurity Framework and the 2013 ASIS Technical Advisory Committee for developing a national risk assessment standard. Earlier in her career, she was a Research Associate at Harvard's Belfer Center for Science and International Affairs.

Kathryn Rauhut is Non-Resident Fellow at the Stimson Center. An attorney specializing in international security, she works primarily in the field of cyber and nuclear security accountability and liability issues. She is a member of the California Bar Association, the American Bar Association, and the International Nuclear Lawyer's Association. She has completed a decade of international work in Europe while living in Vienna, Austria. Prior to her work with Stimson, she was Strategic Advisor to the World Institute for Nuclear Security and the Internet Security Alliance. Before that, she was Deputy General Counsel of Lawrence Livermore National Laboratory in California, where she had earlier served as a prosecutor. Ms. Rauhut, along with Ms. Decker, have been advisors to the International Atomic Energy Agency on supply chain risk issues.

References

Bernard, Tara, and Stacey Cowley. 2017. "Equifax Breach Caused by Lone Employee's Error, Former C.E.O. Says." *The New York Times*. October 3, 2017. https://www.nytimes.com/2017/10/03/business/equifax-congress-data-breach.html.

Birshan, Michael, Madelein Goerg, Anna Moore, and Ellora-Julie Parekh. 2020. "Investors Remind Business Leaders: Governance Matters." McKinsey & Company. October 2, 2020. https://www.mckinsey.com/business-functions/strategy-and-corporate-finance/our-insights/investors-remind-business-leaders-governance-matters.

Bloomberg News. 2021. "Nuclear Energy Generator Splits ESG Buyers with Green Bond." November 18, 2021. https://www.bloomberg.com/news/articles/2021-11-18/nuclear-energy-generator-splits-esg-buyers-with-green-bond-sale.

Broadridge. "ESG Webinar: How to Engage Shareholders Through Technology." Accessed December 9, 2021. https://www.broadridge.com/webinar/esg-webinar?id=ICSCIO19jl5d4afe9903727e96f88518d91d37ee51&so=se&po=&di=&ct=&ot=wb&mt=ja&yr=20&rg=gl&on=01&ep=pd&gclid=EAIaIQobChMI66WXlozi6gIVSr7ACh0PuArMEAAYASABEgKuevD_BwE.

Cascadia Times. 2013. "The Most Dangerous Nuclear Power Plants in America." December 18, 2013. https://www.times.org/nuclear-power-back/2018/3/8/the-most-dangerous-nuclear-power-plants-in-america.

Chen, James. 2020. "Basel II." Investopedia. October 31, 2020. https://www.investopedia.com/terms/b/baselii.as.

Cyber Reports. 2021. "Eletrobras, Copel energy companies hit by ransomware attacks." February 7, 2021. https://cyber-reports.com/2021/02/07/eletrobras-copel-energy-companies-hit-by-ransomware-attacks/.

Cyberspace Solarium Commission. "Cyberspace Solarium Commission." Accessed December 9, 2021. https://www.solarium.gov/home.

Decker, Debra. "Before the Next Chernobyl." CNN Opinion. April 26, 2016. https://www.cnn.com/2016/04/26/opinions/chernobyl-nuclear-safety-opinion-decker/index.html.

Decker, Debra, and Kathryn Rauhut. 2016. *Nuclear Energy: Securing the Future – A Case for Voluntary Consensus Standards.* Washington, D.C.: Stimson Center. https://

www.stimson.org/2016/nuclear-energy-securing-future-case-voluntary-consensus-standards/.

Decker, Debra, and Kathryn Rauhut. 2016. *The Quest for Nuclear Security Standards.* Muscatine, IA: The Stanley Foundation. https://stanleycenter.org/publications/pab/Decker-RauhutPAB216.pdf.

Duncan, Brian. 2019. *WANO Principles: Nuclear Leadership Effectiveness Attributes*. PL2019-01. London, United Kingdom: The World Association of Nuclear Operators. https://www.wano.info/getmedia/f6e15600-4526-42f6-b77d-066deba2561d/PL-2019-01-Nuclear-Leadership-Effectiveness-Attributes-(A4).pdf.aspx.

Eaglesham, Jean, and Anna Hirtenstein. 2021. "ESG Disclosure Rule from Europe Challenge U.S. Fund Manager." *The Wall Street Journal*. March 22, 2021. https://www.wsj.com/articles/esg-disclosure-rules-from-europe-challenge-u-s-fund-managers-11616405401.

European Commission. 2013. "New Rules on Credit Rating Agencies (CRAs) – Frequently Asked Questions." January 16, 2013. https://ec.europa.eu/commission/presscorner/detail/de/MEMO_13_13.

Fruhlinger, Josh. 2020. "Equifax Data Breach FAQ: What Happened, Who was Affected, What was the Impact?" CSO. February 12, 2020. https://www.csoonline.com/article/3444488/equifax-data-breach-faq-what-happened-who-was-affected-what-was-the-impact.html.

Gnanarajah, Raj and Gary Shorter. 2021. *Introduction to Financial Services: Environmental, Social, and Governance (ESG) Issues*. CRS Report No. IF11716. Washington, D.C.: Congressional Research Service. https://crsreports.congress.gov/product/pdf/IF/IF11716.

International Atomic Energy Agency, "Nuclear Security Series." Accessed December 9, 2021. https://www.iaea.org/resources/nuclear-security-series#:~:text=The%20IAEA%20establishes%20and%20maintains%20the%20guidance%20series,the%20environment%20from%20harmful%20effects%20of%20ionizing%20radiation.

International Atomic Energy Agency. "Overview of Management, Governance, and Organizational Structure." Accessed December 9, 2021. https://www.iaea.org/about.

International Atomic Energy Agency. 2021. *Computer Security for Nuclear Security*. Vienna, Austria: International Atomic Energy Agency. https://www-pub.iaea.org/MTCD/Publications/PDF/PUB1918_web.pdf.

Institute of Nuclear Power Operations. "About Us." Accessed December 9, 2021. http://www.inpo.info/AboutUs.htm#:~:text=Our%20National%20Academy%20for%20Nuclear%20Training%20provides%20training,and%20take%20the%20various%20online%20courses%20INPO%20offers.

ISS. "Governance Qualityscore." Accessed December 9, 2021. https://www.issgovernance.com/esg/ratings/governance-qualityscore/.

Jeweler, Matthew, Brendan Hogan, Richard Mroz, Robert Ross, and Cassie Lentchner. 2019. "Name-and-Shame Proposal of Electric Regulators Highlights Need for Cyber Insurance." November 5, 2019. https://www.pillsburylaw.com/en/news-and-insights/name-and-shame-proposal-of-electric-regulators-highlights-need-for-cyber-insurance.html.

Kaufmann, Daniel, and Veronika Penciakova. 2011. *Preventing Nuclear Meltdown: Assessing Regulatory Failure in Japan and the United States.* Washington, D.C.: The Brookings Institute. https://www.brookings.edu/opinions/preventing-nuclear-meltdown-assessing-regulatory-failure-in-japan-and-the-united-states/#:~:text=To%20a%20significant%20extent%2C%20it%20appears%20that%20regulatory,that%20the%20NRC%20is%20not%20effectively%20enforcing%20regulations.

Lloyd's. "Business Blackout." Accessed December 9, 2021. https://www.lloyds.com/news-and-insights/risk-reports/library/business-blackout/.

Moody's. "Moody's and Cyber." Accessed December 9, 2021. https://about.moodys.io/cyber.

Moody's. 2019. "Credit implications of cyber risk will hinge on business disruptions, reputational effects." Accessed December 17, 2021. researchdocumentcontentpage.aspx (moodys.com)

Morrow, Stephanie, and Valerie Barnes. 2012. *Independent Evaluation of INPO's Nuclear Safety Culture Survey and Construct Validation Study.* Rockville, MD: Nuclear Regulatory Commission. https://www.nrc.gov/docs/ML1217/ML12172A093.pdf.

Nuclear Risk Insurers. "Nuclear Pools." Accessed December 9, 2021. https://www.nuclear-risk.com/nuclear-pools/#.

Park, Ju-min. 2013. "South Korea Charges 100 with Corruption over Nuclear Scandal." Reuters. October 10, 2013. https://www.reuters.com/article/us-korea-nuclear-idUSBRE99905O20131010.

Proctor, Darrell. 2018. "Three U.S. Nuclear Plants Get Poor Marks from NRC." Power. May 30, 2018. https://www.powermag.com/three-us-nuclear-plants-get-poor-marks-from-nrc/.

Reitsma, Sebastiaan. 1998. "Nuclear Insurance Pools: World-Wide Practice and Prospective." Vienna, Austria: International Atomic Energy Agency. https://inis.iaea.org/collection/NCLCollectionStore/_Public/31/051/31051428.pdf.

Stimson Center. 2017. "Demonstrating Due Care: Cyber Liability Considerations for Nuclear Facilities." April 24, 2017. https://www.stimson.org/2017/demonstrating-due-care-cyber-liability-considerations-nuclear-facilities/.

Stimson Center. 2018. *Lifting the Lid on Nuclear Liability*. Washington, D.C.: Stimson Center. https://www.stimson.org/wp-content/files/file-attachments/LiftingTheLid-R4-WEB.pdf.

Stimson Center. "Nuclear Security Governance Template." Accessed December 9, 2021. https://www.stimson.org/2021/nuclear-security-governance-template/.

The Council of Insurance Agents and Brokers. 2019. "Lloyd's Moves to Address Silent Cyber Risk." July 11, 2019. https://www.ciab.com/resources/lloyds-moves-to-address-silent-cyber-risk/.

The Economist. 2020. "Markers Marked: Credit-rating Agencies are Back under the Spotlight." May 9, 2020. https://www.economist.com/finance-and-economics/2020/05/07/credit-rating-agencies-are-back-under-the-spotlight.

The Economist. 2020. "In the Soup: The Proliferation of Sustainability Accounting Standards Comes with Costs." October 3, 2020. https://www.economist.com/business/2020/10/03/the-proliferation-of-sustainability-accounting-standards-comes-with-costs.

Thygesen, Tine. 2019. "Everyone Is Talking About ESG: What Is It and Why Should It Matter To You?" *Forbes*. November 9, 2019. https://www.forbes.com/sites/tinethygesen/2019/11/08/everyone-is-talking-about-esgwhat-is-it-and-why-should-it-matter-to-you/?sh=2cf5219c32e9.

U.S. Department of Homeland Security Integrated Task Force. 2013. *Executive Order 13636: Improving Critical Infrastructure Cybersecurity, Incentives Study Analytic Report*. Washington, D.C.: Department of Homeland Security. https://www.cisa.gov/sites/default/files/publications/dhs-eo13636-analytic-report-cybersecurity-incentives-study.pdf.

U.S. Securities and Exchange Commission. "Current NRSROs." Accessed December 9, 2021. https://www.sec.gov/ocr/ocr-current-nrsros.html.

VisibleRisk. "Cyber Risk Qualification." Accessed December 9, 2021. https://visiblerisk.com.

World Institute for Nuclear Security. 2018. *Corporate Governance Arrangements for Nuclear Security.* Vienna, Austria: World Institute for Nuclear Security. https://www.wins.org/document/corporate-governance-arrangements-for-nuclear-security/.

World Nuclear Association. "Economics of Nuclear Power." Accessed December 9, 2021. https://world-nuclear.org/information-library/economic-aspects/economics-of-nuclear-power.aspx.

World Nuclear Association. "Liability for Nuclear Damage." Accessed December 9, 2021. https://www.world-nuclear.org/focus/fukushima-daiichi-accident/liability-for-nuclear-damage.aspx.

World Nuclear Association. "World Nuclear Power Reactors & Uranium Requirements." Accessed December 9, 2021. https://world-nuclear.org/information-library/facts-and-figures/world-nuclear-power-reactors-and-uranium-requireme.aspx.