Preventing Weak Links in Nuclear Security: A Strategy for Soft and Hard Governance

Summary Report & Initial Policy Recommendations

March 2014

NSGEG

*This report is based on discussions of the Nuclear Security Governance Experts Group (NSGEG) at its workshop on **Preventing Weak Links in Nuclear Security: A Strategy for Soft and Hard Governance** held on October 16-18, 2013 in Warrenton, Virginia. This workshop, part of a continuing project on nuclear security, was convened during the Stanley Foundation's 54th Annual Strategy for Peace Conference and organized by the Stanley Foundation with support from the Asan Institute for Policy Studies and Partnership for Global Security. This report and its recommendations draw upon major strands of discussion developed at the workshop and in its papers. They do not necessarily reflect the views of individual NSGEG members or other workshop participants who neither reviewed nor approved this document.*

The Asan Institute for Policy Studies
ideas & praxis

The
Stanley
Foundation

Creating a Legacy for the Nuclear Security Summits: Preventing Weak Links in Nuclear Security

Summary Report and Initial Policy Recommendations

The Nuclear Security Governance Experts Group (NSGEG) considers the Nuclear Security Summit (NSS) process to be a unique opportunity for world leaders to take needed actions to strengthen today's nuclear security system and eliminate and prevent weak links in this regime. The first two summits in Washington and Seoul succeeded in expediting the removal of dangerous nuclear materials, establishing nuclear security centers of excellence, and strengthening national legislation. However, the summits have neglected to address many of the important governance challenges that allow weak links in the international nuclear security system to exist and persist.

The third summit in The Hague in March 2014 provides an important opportunity for summit leaders to pivot toward resolving the nuclear security governance challenge in order to craft a sustainable legacy of nuclear security improvement, robustness, and adaptability. A successful strategy for eliminating and preventing weak links in nuclear security will need to couple a long-term vision with a practical step-by-step process. The goal is to create a more comprehensive and durable nuclear security regime with the dynamism to respond effectively as new challenges emerge.

Achieving this end state will require the implementation of a mix of soft and hard governance approaches over a period of time. Soft governance approaches involve voluntary measures that promote a culture of continuous improvement and incentivize new norm development without legally-binding requirements. They can maximize the effectiveness of the disparate parts of the current regime, promote communication for confidence-building, improve nuclear security performance through incentive-based and voluntary mechanisms, and utilize culturally-sensitive best practices and peer review. Hard governance approaches consist of legally-binding tools to codify norms and standards. These measures, in turn, can reduce the fragmentation of the international nuclear security framework; promote a robust regime at the international, regional, national, and facility levels; and create a platform for the regime's continuous improvement.

Initiating progress through a combination of innovative soft and hard governance steps at the 2014 summit is critical to ensuring that the NSS process results in significant improvements to the global nuclear security regime, continued high-level attention toward nuclear security after the 2016 NSS in the United States, and the creation of an enduring legacy of effective nuclear security improvement.

The Nuclear Security Governance Experts Group (NSGEG) believes that during the 2014 Nuclear Security Summit in The Hague, world leaders should address five important dimensions of nuclear security governance and develop a strategy for their implementation at the 2016 summit in the United States. Together these actions will begin to eliminate the weak links that currently exist in the global nuclear security system.

1. Maximize and universalize the current nuclear security regime and learn from the related nuclear disciplines of safety and safeguards

2. Promote effective communication and expanded information-sharing to build international confidence in the implementation of nuclear security policies and practices

3. Develop and utilize incentives-based and voluntary mechanisms to improve nuclear security practices in the short– and medium–term

4. Expand the use of culturally-sensitive peer review and best practices in the nuclear security system at the global and regional level

5. Pursue the benefits of a framework convention on nuclear security as a long-term approach for the continuous improvement of global nuclear security system

Maximizing the Current Regime

A first step toward eliminating weak links in nuclear security governance is to take full advantage of the legal authorities in the current international framework. Comprised of hard and soft governance measures, the existing regime provides a degree of control over nuclear and radioactive materials. However, it lacks specific standards, performance requirements, as well as systematic review and improvement mechanisms. Given these shortcomings and the 21st century challenges the governance regime is facing, universalization of its existing components is important. But, it alone will not be sufficient to build the necessary international confidence in the security of nuclear materials and facilities and radiological sources into the future.

The current framework is built around two international conventions: the amended Convention on Physical Protection of Nuclear Materials (CPPNM/A) and the International Convention for the Suppression of Acts of Nuclear Terrorism (ICSANT). Their principles are reinforced and complemented by measures in the Nuclear Non-Proliferation Treaty (NPT), Convention on Nuclear Safety (CNS), Early Notification Convention, United Nations (UN) Security Council Resolution 1540, and International Atomic Energy Agency (IAEA) Safeguards and Additional Protocol agreements. The NSS process has emphasized the importance of these tools and sought to bring the 2005 Amendment to the CPPNM into force so that the treaty's protections may extend to materials in domestic storage as well as international transport. However, not enough countries will have ratified this amendment before the 2014 summit to allow its entry into force.

The IAEA's recommendations and guidance set out in its Nuclear Security Series and the Code of Conduct on the Safety and Security of Radioactive Sources (Code of Conduct) are among the most important soft governance documents steering the nuclear security regime. However, these documents are non-binding, unless they are embedded within domestic legislation or legal agreements between states. The IAEA also offers a range of review services, such as International Physical Protection Advisory Service (IPPAS) for nuclear security national systems evaluation, but IPPAS missions are voluntary and must be requested by states.

Many experts agree that better integration of nuclear safety, security, and safeguards disciplines would benefit the entire nuclear system. Each discipline is distinct, but also is closely intertwined with the others. The disciplines complement one another and, to a degree, each is reliant upon the successful functioning of the others. For example, both nuclear safeguards and nuclear security measures are aimed at detecting and deterring unauthorized removal of nuclear material, ensuring that all nuclear material is accounted for, and providing timely detection of lost or diverted material. However, unlike nuclear security, the IAEA safeguards regime operates under a well-established legal framework with structured verification mechanisms. In addition, closer interaction between the nuclear safeguards and security regimes could help identify what non-sensitive information is already being shared as a part of the safeguards regime and promote its application to nuclear security.

There are several “easy fixes” in the near-term that could promote a fuller implementation of the current nuclear security framework while working within the parameters of existing hard and soft governance measures.

- Universal and integrated implementation of the CPPNM/A, ICSANT, the Code of Conduct, and national accounting and control obligations in Safeguards Agreements;

- Improved interaction between the UN and the IAEA, which are treaty depositories with important implementation functions; and

- Establishment of stronger links between nuclear safeguards, safety, and security and identification of common interests, differences, and efficiency gains among the three.

Over the long-term, “phase-in” measures could be pursued to significantly strengthen and modernize the international nuclear governance framework, such as:

- Establishment of international nuclear standards to cover nuclear safety, nuclear security, accounting and control;

- Institutionalization of performance assessments;

- Introduction of a process to periodically review the effectiveness of the nuclear security legal framework; and

- Closing the gaps in the existing legal framework.

Recommendation 1: Ensure the universal implementation of the existing legal conventions.

Recommendation 2: Enhance information sharing about nuclear security among international and national officials and experts within the three major nuclear disciplines of safety, safeguards, and security.

Recommendation 3: Continue progress by institutionalizing performance assessments; addressing the gaps in the existing legal framework; and establishing international standards to cover nuclear safety, security, accounting, and control.

Recommendation 4: Identify non-sensitive information that is already being shared as a part of the safeguards regime that could also benefit the nuclear security regime.

Communication for Confidence-Building

Improving communication and information sharing related to nuclear security is essential and has many dimensions. Communicating during a crisis requires different strategies and tactics than communicating during routine operations, as the *what*, *how*, *when*, and *with whom* of information-sharing will depend upon the circumstances. Also, the quality and credibility of information provided to states, international institutions, media, and the public is critical to building confidence in the effectiveness of nuclear security measures taken at the international, regional, national, and facility level.

In all instances, a careful balance must be struck between sharing timely and useful data that builds confidence while protecting proprietary and sensitive information. Additional work must be done to define exactly what types of information can be safely shared to increase public confidence and how the information dissemination process can take advantage of new information technologies. The nuclear industry, centers of excellence (CoEs), and international institutions all have important roles to play in promoting effective communication that builds confidence while protecting sensitive information.

International confidence can be built through effective communication about the quality and effectiveness of a state or facility's security system. However, in attempting to build this confidence, one must be specific about identifying the desired stakeholder community and the level of confidentiality surrounding the disclosure. Some countries and companies may be willing to share some information with their peers, but not with the broader public. To this end, developing confidentiality guarantees could be a critical path forward in encouraging more non-sensitive information disclosures. Establishing a qualification system for nuclear security personnel and reporting on it also could build confidence in the quality and training of the personnel attending to these matters. Such information may include publicizing when force-on-force exercises have taken place, but not disclosing the timing, location, or other details of such activities.

As part of its series of Best Practice Guides, the World Institute of Nuclear Security (WINS) has published "Communicating Security Information: Striking a Balance," that identifies important steps that industry actors can take to communicate more effectively. It notes the importance of organizations adopting a "need to share" approach to information exchange, as opposed to following the traditional "need to know" framework. This shift of perspective is important. It can help companies better balance the risks of unintended data disclosures with the risk of failing to share information that could counter a threat or avoid an incident. WINS has found that organizations also need clear and consistent guidelines for communicating with different stakeholders. They need to better appreciate and harness the power of new information technologies and platforms to communicate the quality and effectiveness of their security system. In order to do so, they need to consider publicizing their efforts to run exercises, test physical capabilities, and implement best practices. This type of simple outreach is critical since losing public approval can have an existential impact on the industry, and it is much easier to lose the public's confidence than regain it.

The newly-created centers of excellence around the globe also have an important role to play in improving nuclear security communication and confidence-building. At least a dozen countries have announced plans to establish CoEs related to nuclear security since the NSS process began in 2010. Some of these centers have been built as national enterprises and established with assistance from the IAEA and others. Many aspire to serve as regional hubs for continued learning and refinement of nuclear skills, including security. In addition to their value in promoting technical skills, CoEs hold great potential for identifying information that could be shared and improving the coordination of information. For instance, they could serve as the foundation of an international information sharing system that provides regular reporting on the status of nuclear security measures aimed at promoting understanding and building confidence both internationally and domestically. These centers also could distribute regular publications about their training activities and convene regulators, operators, security authorities, and other relevant actors to strengthen their joint collaboration. More ambitiously, if a professional association developed a qualification system for nuclear security personnel, CoEs could offer specialized courses that would allow personnel to become accredited.

International actors such as the IAEA, the European Nuclear Security Regulators Association, EURATOM's Ad Hoc Group on Nuclear Security, and the World Nuclear Association (WANO), also provide opportunities for improving communication between nuclear practitioners and the public. They have the potential to offer virtual platforms for information exchange, such as the IAEA Nuclear Security Information Portal. They also can convene high-level and multi-sector meetings and support exercises that involve a full range of international bodies and national organizations to test emergency situation systems coordination. Their work could further expand to initiating national and international reviews of document classification and information protection practices with an eye toward identifying information that could be released to further build trust in the nuclear enterprise.

While the list of important and useful vehicles for information-sharing continues to grow, not enough attention has been given to *what information* can be shared through them. There needs to be a common understanding about what information is truly sensitive and what information can be shared more easily with the public and international community. One way to think about this problem is by categorizing information across a spectrum of its sensitivity. WINS suggest thinking in terms of information that is easily shared, could be shared, not ready to be shared, and cannot be shared. This approach changes the frame of the dialogue from *What needs to be protected?* to *What can be shared?*

Recommendation 5: Create a list of "10 most important things that would increase international confidence in nuclear security" based on consultations with international officials, national representatives, industry, and experts. The focus should be on what information could be provided that would assure them that other countries are in control of and effectively operating their nuclear security systems.

Recommendation 6: Encourage organizations to adopt a need to share approach to information exchange rather than relying on a need to protect standard. Also, institute clear and consistent guidelines for communicating with different stakeholders, and utilize the WINS Best Practice Guides on communications.

Recommendation 7: Use CoEs as the foundation of an international information gathering and dissemination system. Encourage the regular publication of non-sensitive information about their training courses, exercises, and other measures. CoEs also could offer specialized courses for nuclear security personnel accreditation, if a qualification system can be developed by one or more professional organizations.

Recommendation 8: Encourage international organizations and initiatives to build confidence among stakeholders by: offering virtual platforms for information exchange; developing confidentiality guarantees to encourage non-sensitive information disclosures; convening high-level and multi-sector meetings; supporting exercises that involve diverse actors to test their systems; and assisting in national and international reviews of document classification and information protection practices to ensure that they protect only truly sensitive information.

Incentives-Based and Voluntary Regimes

Voluntary regimes are formal systems utilized by industries, governments, or other institutions and actors to encourage more responsible business practices and promote adherence to a set of principles beyond legal requirements. Applying the characteristics and principles used in other successful, incentive-based, voluntary regimes to the nuclear security area can facilitate the development of new norms that strengthen the global nuclear security system in the short- and medium-term. These interim steps are especially relevant in the absence of new legal mandates or a more unified international regime.

The drivers for actions beyond those legally required include leadership, long-term vision, public opinion, reputational concerns, financial incentives, accreditation, and market signals. To adapt and apply these motivations to the nuclear security regime, one must ensure that representatives from all relevant stakeholder communities are being engaged, essential best practices are prioritized within the initiative, and consideration is given to the business and financial benefits for making changes.

Successful voluntary regimes are employed by a diverse array of industries and typically have three common characteristics: multi-stakeholder cooperation, flexibility and adaptability, and the eventual evolution into established norms. Examples of such regimes include the following:

- The Extractive Industries Transparency Initiative (EITI) was developed as a response to governance challenges posed by mining and energy companies expanding into countries with underdeveloped legal institutions. It is an example of multi-stakeholder cooperation that utilizes a reputational and accreditation-based incentives structure. The implementation of EITI standards signals to companies that a country is a stable investment environment and to countries that they will be fairly compensated for their natural resources by the companies. EITI's multilateral effort and focus on governments, companies, and civil society is a good model institutionalizing transparency and best practices as a beneficial business procedure.

- The Leadership in Energy & Environmental Design (LEED) system is an internationally recognized process that uses a point scoring system to certify and designate a building's energy efficiency. It is an example of a voluntary regime that is flexible and adaptable and uses financial, reputational, and accreditation-based incentives. LEED accommodates a diversity of actors by maintaining different sets of standards for rating new construction, renovations, and historical sites while maintaining an overarching system that is applicable across borders and industries.

- The chemical industry's Responsible Care program, the American Petroleum Industry's (API) guidance documents, and the U.S. healthcare industry's Joint Commission on Accreditation of Healthcare Organizations (JCAHO) demonstrate how voluntary regimes can evolve over time into widely-accepted industry norms and standards. To raise performance levels without regulation, Responsible Care uses a financial and reputational incentives structure, API employs accreditation and reputational incentives, and JCAHO utilizes accreditation and financial incentives.

Voluntary regimes to raise performance often develop after a significant catalyzing event. For example, the Bhopal Disaster in India set the stage for the chemical industry to develop of Responsible Care. However, voluntary regimes have developed as preventative measures in other areas; proactive local governments and business leaders have come together to combat climate change. A willingness to exercise leadership is the critical element in getting any new regime off the ground, and important lessons for nuclear security may be learned from better understanding how other successful voluntary regimes were initiated and nurtured.

One example of a new incentive-based model is the approach being taken by the United States to address cybersecurity. Following the failure of cybersecurity legislation in the U.S. Senate in August 2012, the President issued Executive Order 13636 that directs government agencies to use their existing authorities to improve cybersecurity for critical infrastructure. It includes a Cybersecurity Framework provision under which the Departments of Homeland Security, Commerce, and Treasury are working to identify incentives for companies to cooperate with them. Preliminary findings from the departments focus on direct and indirect financial incentives, such as insurance benefits, grants, process preference, liability limitations, and rate recovery for price-regulated industries. While these cybersecurity policies are still under development, it is telling that policymakers are turning to incentive-based voluntary mechanisms to address one of the most complex and significant transnational challenges of the 21st century.

For nuclear security, financial and reputational incentives are likely to be the most important elements driving additional self-regulation. Existing nuclear industry organizations that focus on safety, particularly the Institute of Nuclear Power Operations (INPO) and WANO, have not been eager to expand their focus into security. However, they could become incubators for the development of a voluntary regime to raise performance standards in nuclear security that are both innovative and cost-effective. Enhancing nuclear security does not simply mean investing more money in guns, guards, and gates. Instead, it should involve innovating efficient solutions to meet security challenges.

Recommendation 9: Examine closely how industries and institutions have implemented incentives-based voluntary performance enhancement regimes. Identify the benefits and drivers and assess their potential application to nuclear security.

Recommendation 10: Identify potential leaders in the nuclear area that can spearhead the creation of an incentives-based nuclear security improvement process.

Recommendation 11: Encourage WANO, INPO, and other nuclear industry professional and trade associations to become incubators for innovative and cost-effective voluntary regime development that raise nuclear security performance levels while providing financial and related business benefits.

Culturally-Sensitive Peer Review and Best Practices

National culture, defined as common vision, values, and beliefs, plays an important role in the development and implementation of nuclear security practices. The roles of peer review and best practices, therefore, need to be adapted to different national and regional cultures. They cannot be “one size fits all.”

Peer review is a form of evaluation designed to enhance the quality of work, and effectiveness of performance, and identify best practices by inviting outsiders in to assess a site or system. Best practices refer to professional techniques or procedures that have consistently been shown to provide superior results. Peer reviews and the dissemination of best practices are critical to enhancing effectiveness in fields where no international standards exist, like nuclear security.

The global application of effective nuclear security measures is a daunting mission, given the scale of the task and differences among national systems and cultures. Understanding the cultural environment in which individual nuclear security systems operate provides a fuller picture of effectiveness and where improvements can be made at the facility, national, and international levels. Without a strong understanding of the prevailing cultural norms, one cannot truly understand the reasoning behind the management and response structures that have been built. However, culture should not be used as an impediment to peer review and best practices; instead, exercising cultural sensitivity can help improve their acceptance, use, and results.

Early engagement with stakeholders in the process of planning peer reviews is important for understanding the cultural contexts in which they will take place. It can head off confusion about terminology, interpretation, and other issues that may arise from language issues and threat perceptions. Cultural considerations can add to the robustness and validity of reviews and foster the development of relationships based on respect. It also can facilitate the use of culturally appropriate methods, knowledge, and data interpretation. However, cultural sensitivity cannot be used as a reason or excuse for accepting weak oversight, governance, or inadequate nuclear security practices.

One way to decrease cultural tensions that may arise with new nuclear security practices is to move toward a performance-based approach, rather than pursing prescriptive standards across all regions. This approach does not replace the need for nuclear security minimum benchmarks, but it does allow for culturally acceptable solutions to be crafted within the international system. Utilizing best practices and peer review are important ways for countries to demonstrate that they are living up to the expectations of the public and the international community in the responsible use of nuclear and radioactive materials.

In the NSS process the focus has been on IAEA's IPPAS missions as the preferred form of nuclear security peer review. IPPAS missions are confidential, voluntary reviews during which each participating state decides what the team of international inspectors will examine. Most often the examination involves a state's implementation of national rules, regulations, and international best practice recommendations and conventions, as well as sometimes selected facilities. International experts are assigned to IPPAS missions based on their expertise, but host countries have the prerogative to reject certain inspectors. Recently, several countries, including nuclear weapon states, have requested first-time IPPAS missions. The IAEA has the capacity to conduct about 10 missions a year, and they cost approximately 50,000 Euros each.

However, there is a sense among some experts that the highly-confidential and voluntary nature of the IPPAS mission is not sufficient to develop the high confidence in the nuclear security system over the long-term. One reason is that the lessons learned from IPPAS are not broadly shared with others which prevent states from learning from each other's experiences. The Netherlands is the first country to publicly discuss the non-sensitive elements of its IPPAS mission. If more countries emulate this precedent, it would have a positive impact on the dissemination of international best practices.

The Director General of the IAEA suggested ahead of the July 2013 IAEA *International Conference on Nuclear Security* that the nuclear security system should utilize the peer review process, citing the effectiveness of the system used for nuclear safety. Under the safety regime, there is an international systems-level review under the CNS, a national level review from the IAEA, and an operator level review from WANO. WANO reviews are not mandatory, but the organization has created an expectation that its members undergo a peer review every three years. Creating this type of system in the international nuclear security regime will be difficult and could thus be phased-in. To begin promoting a peer review expectation, the IAEA could adopt an “opt-out” approach to IPPAS by offering missions to states that could then be declined, rather than relying on countries to request them. To build support for such changes, consideration must be given to the incentives for undergoing IPPAS reviews, such as reputational enhancement and demonstrating good performance to the international community.

Recommendation 12: Establish the processes and incentives for regular nuclear security peer reviews, the sharing of non-sensitive lessons learned, and the use of performance-based assessments.

Recommendation 13: Employ cultural-sensitivity to improve the acceptance and use of peer reviews.

Recommendation 14: Encourage the IAEA to offer IPPAS missions, which the states could choose to decline rather than waiting for a nation to request the mission.

Hard Governance and a Framework Convention

A long-term sustainable approach to the improvement of nuclear security governance necessitates maintaining broad public confidence in the operation of the nuclear enterprise. Achieving this goal will require progressing from today’s patchwork nuclear security system toward one in which hard and soft governance coexist within a unified framework. There are precedents for framework conventions in other fields, such as environment, health, human rights, and nuclear safety. They include:

- United Nations Framework Convention on Climate Change
- Part XII of the United Nations Convention on the Law of the Sea
- World Health Organization’s Framework Convention on Tobacco Control
- Campaign for the Framework Convention on Global Health
- Council of Europe’s Framework Convention for the Protection of National Minorities
- Convention on Nuclear Safety

These examples of framework convention share common themes. They recognize the importance of cooperation, involve an incentives-driven process, and have in place implementation and monitoring mechanisms. They also acknowledge the global implications of each challenge and the shared responsibility countries have in addressing them. The relevancy of these themes to the nuclear security mission suggests that states should at least consider a framework approach to nuclear security before opting for only non-binding guidelines and codes of conduct.

Applying a framework governance approach to nuclear security would involve supplementing the existing fragmented legal regime with general and comprehensive legal norms. A nuclear security framework agreement would not replace the current international arrangements, or infringe on commitments and obligations states may have made elsewhere. Instead, it would complement and unify the existing international measures. Some soft governance approaches could become codified into hard governance measures under a framework agreement, but a wide range of voluntary measures would continue to exist and play a critical role in the regime's advancement.

The nuclear security framework agreement would need to allow for continuous development and change to keep pace with evolving threats and developments. It would be structured to fill the gaps in the current regime while remaining dynamic enough to accommodate changes as nuclear energy expands and its challenges evolve. It would establish a clear definition of "nuclear security" and allow for the establishment of specific, practical goals. It also could be equipped with cooperative mechanisms to ensure that resources are channeled to help certain states that want to meet its standards but lack implementing capacities.

Recommendation 15: Develop the text of a draft nuclear security framework convention that establishes a clear definition for nuclear security, incorporates new tools for cooperation and assistance, and remains dynamic enough to accommodate changes as nuclear energy expands and new challenges emerge.

Cyber Security and the Nuclear Industry

Cyber attacks are a tactic that adversaries may employ for achieving their objectives. Unlike a physical attack, cyber attacks do not require physical proximity to the target. This increases the pool of potential targets and actors involved. Low-skill threat actors can recruit people with higher skills and direct them to the target without the need to ever meet them or personally visit the target. Collusion among cyber threat actors, including hacktivists, nation states, and extremist groups, can range from the development of cyber tools to direct operational support.

The most infamous nuclear cyber-attack to-date, Stuxnet, targeted the industrial control systems of Iran's enrichment facility at Natanz. This was the first time cyber weapons were known to have caused physical damage by targeting industrial control systems. This attack raised new questions about cyber vulnerabilities in critical infrastructure and industrial facilities around the world.

Policy responses for combating cyber threats must be clear in their objectives, identify the assets they intend to protect, and allow for continuous development and adaptation to a dynamic threat environment. Determining the right policy approach often entails a collaborative process between industry actors and government agencies. At nuclear plants, addressing cybersecurity challenges necessitates high-level, performance-based policies that allow for flexibility and provide clarity on the threat and the desired policy outcome.

In the United States, the Nuclear Regulatory Commission's (NRC) requirements for cyber security are performance-based and not prescriptive. Licensees may choose their own methods for meeting the objective of protecting digital equipment within nuclear plants from cyber attacks that would impact operational safety, security, or emergency response capabilities. While the NRC's cyber regulations take less than two pages of text, hundreds of pages of supporting documents and implementation guidance have been produced to assist licensees. This guidance can be easily adapted to new threats without the need to change the law.

Staying ahead of cyber threats requires continuous monitoring, assessment, and information sharing. A digital system that is completely secure today can become insecure overnight. Maintaining awareness of cyber attacks in other industrial sectors also is a critical element of preparedness, as adversaries may be testing their attacks vectors against other targets.

For the U.S. nuclear power sector, US-CERT (Computer Emergency Readiness Team) and the industrial control system community are the main information sharing venues, but many all-hazards information sharing centers also include a cyber-defense component. Most of the information that comes through these channels involves past incidents, but in the coming years, more real-time information sharing is possible. Information also is shared among industry actors themselves, and all systems breaches are required to be reported to the NRC, which can then choose to share non-sensitive information about them more broadly. Cooperation with intelligence agencies also is important. There are people within the U.S. nuclear industry with top-secret level clearance which allows them to be briefed on the latest threats.

Insider threats, supply chain concerns, and unintended access points to isolated systems are among the range of threats that impact the nuclear industry's cybersecurity decision making. Just as in the physical world, quality assurances and exercises are employed to test how well the cyber security systems at nuclear plants are operating. However, not every cyber threat is equal or can be avoided. With this in mind, business control systems are kept separate from operational controls, and resources are more highly focused on the operation side where a penetration could result in radiological sabotage that threatens the health and safety of the public.

Recommendation 16: Continue to pursue high-level, performance-based cyber security policies that allow for flexibility and provide clarity on both the threat and policy objectives.

Recommendation 17: Remain apprised of cyber attacks in other industrial sectors to understand cyber-attack trends, patterns, and other information that will assist the cyber preparedness of nuclear facilities.

Recommendation 18: Support public-private information sharing partnerships and collaborative responses to emerging cyber challenges.

A Strategy for Improving Global Nuclear Security Governance

The NSS process has grown in scope and scale since its initiation in 2010. While the Washington summit in 2010 focused exclusively on fissile materials and talked little about transparency, the Seoul summit in 2012 succeeded in broadening the agenda to more fully encompass the nuclear security mission. This trend has created the opportunity for The Hague summit to bring governance issues to the table. Further innovations at the 2014 summit are critical to achieving significant improvements to the nuclear security regime by 2016, when the heads-of-state NSS process will likely conclude.

The summits have been an important force in bringing together stakeholders from government, industry, and civil society to work on the common objective of ensuring the security of nuclear materials and facilities in order to protect the public and the environment. The NSS process has created a valuable base of more than 50 countries that are now active in nuclear security. However, continued progress will likely rely on a small core of countries within this group pushing the global community toward more ambitious goals and objectives. Action-oriented joint statements, "gift baskets," and multilateral initiatives offered at the 2014 summit are one way that progress can be made.

The concept of multinational commitments was introduced into the NSS process in 2012, and they are important vehicle that could be used to introduce governance at the 2014 NSS. They are a valuable tool for empowering countries to drive the system forward with work plans that are in line with but go beyond the summits' consensus communiqués. A 2014 gift basket in which countries committed to maximizing the current regime and evaluating new ideas for strengthening global nuclear security would provide an important platform from which countries could drive future progress.

Support has been growing for the pursuit of new actions to eliminate weak links in the nuclear security regime, including greater international harmonization of nuclear security standards, confidence-building through non-sensitive information sharing, the concept of continuous improvement, and culturally-sensitive peer review. The Asia-Pacific Leadership Network, which includes numerous former government officials from the region, issued a statement ahead of the 2012 summit calling for binding nuclear security standards, an international mechanism for reporting on nuclear security performance, and peer review to improve the regime. At the Seoul summit, then-Australian Prime Minister Julia Gillard gave an intervention endorsing a nuclear security accountability framework and more peer review. Ahead of the IAEA's July 2013 *International Conference on Nuclear Security*, Director General Yukiya Amano penned an op-ed in which he called nuclear security peer review a "no-brainer" way to improve performance. Others, including former U.S. officials, Secretaries of State George Shultz and Henry Kissinger, Secretary of Defense William Perry and Senator Sam Nunn, have called on world leaders at The Hague Summit to "commit to develop a comprehensive global materials security system."

A determination on the post-NSS political structure for improving nuclear security seems to have been deferred to the 2016 summit in the United States. However, it is a critical question that requires significant consideration to ensure that the momentum and gains created by the NSS process will be preserved. The IAEA certainly will remain the premier technical entity for nuclear security after the summit process concludes, but there are concerns about whether it is well-suited to the political challenges of advancing the agenda. Important questions have been raised about whether it has the necessary tools, resources, and flexibility to maintain high-level political attention on nuclear security. These challenges are not insurmountable, but overcoming them will require countries to exercise considerable leadership within the IAEA.

However, positive signs include the elevation of the Office of Nuclear Security within the agency's structure, and the successful July 2013 conference in which the IAEA blended together the technical and policy communities. However, there are still countries that are very cautious about giving the IAEA too much power. The agency's high-profile activities and strongest mandates are for safeguards and safety; security comes third and this hierarchy. Further, IAEA countries that have not been a part of the NSS meetings may be negative about the IAEA taking over the agenda of a process that they weren't invited to join.

Because the nuclear security regime's challenges are primarily political, not technical, there needs to be a process separate from the IAEA that deals with the issue from a political perspective. The establishment of this political track has been one of the great contributions of the NSS. A nuclear security framework convention with a conference of parties is one way to provide a forum for continued political discussion of nuclear security in the absence of regular, high-level summits. Such a structure would complement and work with the IAEA and existing soft and hard governance measures, not supplant them.

Recommendation 19: Encourage action-oriented joint statements at 2014 summit through which countries can commit to maximizing the current regime, evaluate new ideas for strengthening global nuclear security, and provide a platform for further progress in 2016 and beyond.

Recommendation 20: Evaluate options for maintaining high-level political momentum after the summit process concludes, such as a nuclear security framework convention, in order to provide a high level forum for political discussion and concerted action.

Nuclear Security Governance Experts Group Workshop on Preventing Weak Links in Nuclear Security: A Strategy for Soft and Hard Governance

Airlie House, Warrington, VA
October 16-18, 2013

Agenda

Day 1

8:00 - 8:10 pm	**Opening Remarks**	
	Kenneth Luongo, The Partnership for Global Security	
	Shin Chang-Hoon, The Asan Institute for Policy Studies	
	Jennifer Smyser, The Stanley Foundation	
8:10 - 9:30 pm	**Session I**	**Maximizing the Current Regime**
	Discussion Leader	**Anita Nilsson**, AN & Associates
	This session will discuss how to utilize all elements of existing nuclear instruments to the fullest extent and universalize implementation of all relevant international agreements and IAEA recommendations.	

Day 2

9:00 - 10:45	**Session II**	**Hard Governance**
	Discussion Leader	**Chang-Hoon Shin**, The Asan Institute for Policy Studies
	This session will provide an update on the development of draft articles for a nuclear security framework convention and an opportunity to discuss its roll-out strategy.	

11:00 - 12:00	**Session III**	**Culturally-Sensitive Peer Review and Best Practices**
	Discussion Leader	**Jiyoung Park**, The Asan Institute for Policy Studies
	This session will assess how to develop states' opportunities to learn from peers and others' nuclear security experiences to better recognize the unique cultural contexts in which national nuclear security systems and personnel operate. It will consider how some best practices may not be easily transferrable from one culture to another, and how some cultures may perceive information sharing and peer review as overly intrusive, even if the information being exchanged is not truly sensitive.	
2:00 - 3:30	**Session IV**	**Communication for Confidence-Building**
	Discussion Leader	**Sharon Squassoni**, Center for Strategic and International Studies
	This session will focus on how to more effectively communicate information about nuclear security in a way that protects truly sensitive information while building international confidence. It will explore how centers of excellence, industry practices, and international institutions and initiatives can guide the development of information exchanges that balance sovereignty with global responsibility. It will also include a presentation by Trevor Findlay on adapting international emergency preparedness and response mechanisms that were developed with nuclear safety in mind to nuclear security.	

3:45 - 5:30	Session V	Incentives-Based and Voluntary Regimes
	Discussion Leader	**Sarah Williams**, Partnership for Global Security
	This session will examine approaches to accreditation and certification, financial benefits, and reputational enhancements that have been used by other industries to exceed minimum legal requirements and build new norms. They can serve as models for developing new non-binding actions to improve nuclear security.	

Day 3

9:00 - 10:00	Presentation	Cybersecurity and the Nuclear Industry
	Discussion Leader	**William Gross**, Nuclear Energy Institute
	This presentation will offer an overview of the nuclear industry's perspectives on cybersecurity, including threats, vulnerabilities, and strategies for minimizing risk. It will place this issue within the broader context of cyber threats to the private sector and provide insight on the continued evolution of policy approaches to countering cyber threats.	
10:15 - 11:45	Session VI	Creating a Core of Countries to Drive the Agenda
	Discussion Leader	**Ken Luongo**, Partnership for Global Security
	This session will develop a strategy for creating political incentives to improve nuclear security and identify forward-looking countries willing to commit to greater responsibility beyond the existing rules. It will also explore how inclusion of a nuclear governance gift basket in the 2014 Nuclear Security Summit (NSS) outcome documents would allow states to evaluate and demonstrate new nuclear security concepts. It will also discuss potential group activities throughout 2014 and in the lead up to the 2016 NSS in Washington.	
11:45 - 12:00	Closing Remarks and Next Steps	

Participant List
(in alphabetical order)

1. Anita Nilsson
   Executive Director, AN & Associates, LLC

2. Anya Loukianova
   Program Officer, The Stanley Foundation

3. Bart Dal, Advisor
   Nuclear Security and Safeguards, Ministry of Foreign Affairs, Netherlands

4. Caroline Jorant
   President, SDRI Consulting

5. Jennifer Smyser
   Director of Policy Programming, The Stanley Foundation

6. John Bernhard
   Former Ambassador of Denmark to the IAEA and Permanent Representative to the CTBTO

7. Kenji Murakami
   Visiting Professor of Nuclear Safety Engineering, Tokyo City University

8. Kenneth N. Luongo
   President, Partnership for Global Security

9. Lee Dong-Hwi
   Professor, Institute of Foreign Affairs and National Security, Korea National Diplomatic Academy

10. Michelle Cann
    Senior Budget and Policy Analyst, Partnership for Global Security

11. Page Stoutland
    Vice President, Nuclear Materials Security Program, Nuclear Threat Initiative

12. Park Jiyoung
    Research Fellow, Asan Nuclear Policy and Technology Center, The Asan Institute for Policy Studies

13. Rodrigo Alvarez
    Associate Researcher in the Doctoral Program at the Institute of Advance Studies, University of Santiago of Chile

14. Sarah Williams
Nuclear Policy Analyst, Partnership for Global Security

15. Sharon Squassoni
Senior Fellow and Director, Proliferation Prevention Program, Center for Strategic and International Studies

16. Shin Chang-Hoon
Director, Asan Nuclear Policy and Technology Center, and Director, International Law and Conflict Resolution Program, The Asan Institute for Policy Studies

17. Togzhan Kassenova
Associate, Nuclear Policy Program, Carnegie Endowment for International Peace

18. Trevor Findlay
Senior Research Fellow, Project on Managing the Atom/International Security Program; Professor, Norman Paterson School of International Affairs, Carleton University

19. William Gross (presenter)
Manager, Security Integration and Coordination, Nuclear Energy Institute

20. Yosuke Naoi
Deputy Director, Integrated Support Center for Nuclear Nonproliferation and Nuclear Security; Japan Atomic Energy Agency

Workshop Papers and Authors

- Maximizing Implementation of the International Framework for Nuclear Security
    - Authors – Anita Nilsson and Kenji Murakami
- Culturally-Sensitive Peer Review and Best Practices
    - Authors – Jiyoung Park and Rodrigo Alvarez
- Communication for Confidence-Building
    - Authors – Sharon Squassoni, Caroline Jorant, Yosuke Naoi, Roger Howsley
- Incentivizing Voluntary Improvements to Nuclear Security: Concepts and Case Studies
    - Authors – Sarah Williams, Caroline Jorant, Everett Redmond
- Preliminary Political Assessment and Strategy for Improving Global Nuclear Security Governance
    - Authors – Kenneth Luongo, John Bernhard, Irma Arguello, Kenneth Brill

Nuclear Security Governance Experts Group (NSGEG) Members

Rodrigo Álvarez – Global Consortium on Security Transformation (Chile)
Irma Arguello – The NPSGlobal Foundation (Argentina)
John Bernhard – Former Ambassador to IAEA (Denmark)
Kenneth Brill – Former Ambassador to IAEA (U.S.)
Trevor Findlay – Canadian Centre for Treaty Compliance, Carleton University (Canada)
Han Yong-Sup – Korea National Defense University (South Korea)
Roger Howsley – World Institute for Nuclear Security (Austria)
Caroline Jorant – SDRI Consulting (France)
Jun Bong-geun – Korea National Diplomatic Academy (South Korea)
Togzhan Kassenova – Carnegie Endowment for International Peace (U.S.)
Lee Dong Hwi – Institute of Foreign Affairs and National Security (South Korea)
Anya Loukianova – The Stanley Foundation (U.S.)
Kenneth Luongo – Partnership for Global Security (U.S.)
Kenji Murakami – Tokyo City University (Japan)
Yosuke Naoi – Japanese Atomic Energy Agency, Integrated Support Center (Japan)
Anita Nilsson – AN & Associates, LLC (Sweden)
Everett Redmond – Nuclear Energy Institute (U.S.)
Andrew Semmel – A.K.S. Consulting (U.S.)
Shin Chang-Hoon – The Asan Institute for Policy Studies (South Korea)
Sharon Squassoni – Center for Strategic and International Studies (U.S.)
Page Stoutland – Nuclear Threat Initiative (U.S.)
Yoo Hosik – Korea Institute of Nuclear Nonproliferation and Control (South Korea)

Nuclear Security Governance Experts Group (NSGEG)

The NSGEG is a globally diverse group of experts assessing the current state of nuclear security governance and developing a realistic and comprehensive set of policy recommendations intended to facilitate the evolution and improvement of the nuclear security regime.

NSGEG