The
Stanley
Foundation

209 Iowa Avenue
Muscatine, IA 52761 USA
563·264·1500
563·264·0864 fax
stanley@stanleyfoundation.org
www.stanleyfoundation.org
Richard H. Stanley, Chair
Keith Porter, President

Policy Memo

DATE: October 28, 2013

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

Summary

In just five months, more than 53 heads of state will convene in The Hague, often referred to as the legal capital of the world, for the third Nuclear Security Summit (NSS). Participants have the opportunity to use this summit to go beyond the actions taken to secure fissile material and radioactive sources at previous summits and begin to address the underlying governance challenges that the regime faces in today's evolving, globalized threat environment. Initiating progress on a combination of hard- and soft-governance steps is critical to ensuring that the NSS process results in significant improvements to the global nuclear security regime and continued improvement thereafter if the high-level summitry concludes after the 2016 NSS in the United States.

At its 54th annual Strategy for Peace Conference, the Stanley Foundation, together with the Partnership for Global Security and the Asan Institute for Policy Studies, convened a workshop of the Nuclear Security Governance Experts Group on October 16-18, 2013. The topic of discussion was "Preventing Weak Links in Nuclear Security: A Strategy for Soft and Hard Governance." This policy memo offers highlights of the discussion and recommendations of roundtable participants.

Maximizing the Current Regime

A first step toward eliminating weak links in global nuclear security governance is to take full advantage of the legal authorities that exist in the current international framework, which covers the peaceful use of all nuclear and radioactive sources. Universal adherence to and implementation of the nuclear security regime is a key goal of the summit process but one that will not be fully achieved in 2014. The current framework consists of, *inter alia*, two main hard-governance 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), and soft-governance documents, chiefly nonbinding guidance and recommendations issued by the International Atomic Energy Agency (IAEA).

The discussion at the workshop centered on ways to leverage the implementation of this framework to remedy the absence of performance requirements, standards, and system overview and improvement mechanisms in the current nuclear security regime. This process should begin with a focus on:

- Universal implementation of existing legal platforms.
- Integrated implementation of CPPNM/A and ICSANT.
- Improved interaction and assistance opportunities between the IAEA, the United Nations (UN), and member states.
- Enhanced communication/information sharing related to nuclear security.
- Establishment of links between safeguards, safety, and security; and identification of common interests, differences, and efficiency gains.

This process could be followed with phase-in measures, including:

- Establishing international nuclear standards to cover nuclear safety, nuclear security, and materials accounting and control.
- Institutionalizing performance assessments.
- Introducing a process to review effectiveness of the nuclear security legal framework.
- Reviewing the role of the IAEA/UN.
- Addressing the gaps in the present legal framework.

During discussions on how to better integrate the ways that nuclear safety, security, and safeguards are addressed, participants honed in on what the nuclear security regime could learn from the safeguards regime. Both nuclear safeguards and nuclear security measures are aimed at deterring and detecting unauthorized removal of nuclear material, ensuring that all nuclear material is accounted for, and providing timely detection of lost or diverted material. Unlike nuclear security, however, the IAEA safeguards regime operates under a well-established legal framework with structured verification mechanisms. Learning from the safeguards regime to determine what nonsensitive information shared as a part of safeguards could be more broadly exchanged to improve nuclear security is an important way to strengthen the regime and protect the public.

Participants explored the evolution of the peer-review concept in nuclear security. There was some consensus that the highly confidential and voluntary nature of the IAEA’s International Physical Protection Advisory Service (IPPAS) was not sufficient for a sustainable nuclear security regime over the long term. In turn, participants examined other viable peer-review models, such as those used by the World Association of Nuclear Operators, and discussed how the IPPAS structure could evolve into a more effective tool. To this end, there was agreement that given the evolving threat environment and gaps in today’s nuclear security regime, universalization of its existing components alone would not be able to build confidence and support a robust and adaptive peaceful nuclear enterprise into the future.

Communication for Confidence Building

The importance of peer reviews and exchanging information while protecting truly sensitive data was highlighted in the consensus documents of the 2010 and 2012 Nuclear Security Summits. These types of communications build confidence in the effectiveness of the existing and ongoing nuclear security measures being undertaken at the international, regional, national, and facility levels. The discussion thus centered on the role of industry, centers of excellence, and international institutions in promoting effective communication while protecting sensitive information.

The participants discussed three sets of recommendations. The first set of recommendations was for industry, including the need to adopt a “need-to-share” rather than a “need-to-know” approach; create clear, consistent guidelines for communication with each stakeholder; and use new information technologies to their greatest advantage. The second set of recommendations focused on the role that centers of excellence can play in improving communication by helping to establish an international information disclosure system; regularly publishing information about training efforts; improving collaboration among domestic parties and the public; and establishing a cadre-qualification system in each country. The third set of recommendations focused on what contributions international institutions and initiatives could make, including conducting regular multilateral drills; enhancing the IAEA Nuclear Security Information Portal; adopting a nuclear security event scale; conducting IAEA high-level meetings that include industry; communicating results of IPPAS missions; and initiating national and international reviews of document classification and information protection.

Participants agreed that confidence can be built through effective communication about the quality and effectiveness of one’s security system. All participants also recognized the importance of distinguishing and tailoring different types of communication strategies and tactics to meet specific needs, such as what information is provided in an emergency situation versus what is provided during normal operations. It is also essential to consider how to make technical information more understandable to the public and navigate what can be disclosed and to whom regarding procedural, proprietary, and truly sensitive information. Additional work must be done to define exactly what types of information can be safely shared to increase public confidence and take advantage of new information technologies.

Incentives-Based and Voluntary Regimes

Voluntary regimes are systems organized by industries, government, or through their cooperation to encourage more-responsible business practices and adherence to a set of principles beyond legal requirements. They are an important tool in the development of new norms over time. A diverse array of industries are successfully employing them, including the multisector Extractive Industries Transparency Initiative, the flexible and adaptable Leadership in Energy & Environmental Design, and a variety of voluntary initiatives in US health care that have led to the long-term development of industry norms, such as the Joint Commission on the Accreditation of Health Care Organizations. New incentives-based models also are being developed to deal with transnational challenges in the cyberrealm.

Applying the characteristics and principles used in successful, incentives-based and voluntary regimes to nuclear security can enable the development of new norms that strengthen the global nuclear security system in the medium term, especially given the absence of new government mandates or a more unified international legal regime. Drivers of this type of self-regulation include leadership, long-term vision, public opinion and reputation concerns, financial incentives, and accreditation and market signals. To adapt and apply these motivations to the nuclear security regime, one must ensure that representatives from all relevant industries are being engaged, essential best practices are prioritized within the initiative, and consideration is given to the business case for making changes.

Participants discussed the challenge of comparing the nuclear industry to other industries, especially in crafting incentives for reducing the threat of nuclear terrorism, a scenario which has never happened. There was some disagreement on the drivers of self-regulation and whether these would be more financial or reputational in the case of the nuclear industry. However, participants agreed that leadership would be needed to launch any meaningful initiative, and additional research should be done to understand how other successful voluntary regimes originally got off the ground. Participants debated whether any of the existing nuclear safety industry organizations could be persuaded to expand their focus into security and how to encourage nuclear security innovations that are cost effective.

Culturally Sensitive Peer Review and Best Practices

National culture, defined as common vision, values, and beliefs, not only affects but also has a role to play in the implementation of nuclear security peer review and best practices. Understanding the cultural environment in which nuclear security systems operate provides a fuller picture of their effectiveness and where improvements can be made. Without a strong sense of the prevailing cultural norms, one cannot truly understand the management and response structures that have been built. To this end, culture is not an impediment to peer review, but cultural sensitivity can help improve its acceptance and use.

The discussion focused on three recommendations for how to better utilize culture in enhancing nuclear security:

- Engage stakeholders in planning since the engagement process begins with understanding culture and developing procedures for working together.
- Give consideration to culture since it can add to the robustness and validity of reviews.
- Differentiate practices in order promote different approaches to different groups with shared cultures.

The participants discussed specific examples of how culture affects peer review and best practices in specific regions, for example, East Asia, Russia, and Europe. Opinions diverged on the importance of cultural sensitivity in peer review since deviation for culture may weaken international governance. However, participants agreed that one way to decrease tension with cultural issues is to move nuclear security assessments toward a performance-based approach, as opposed to one that is prescriptive. To this end, culture is important, but it doesn’t replace the need for minimum benchmarks. Participants agreed that national nuclear security culture can also change with the evolution of international nuclear security culture.

Hard Governance

Participants discussed the need to move away from a patchwork nuclear security governance approach toward a sustainable regime in which hard and soft governance could coexist. They identified precedents for framework convention approaches in other areas of policy, such as the environment (United Nations Framework Convention on Climate Change, Part XII of the United

Nations Convention on the Law of the Sea); health (World Health Organization's Framework Convention on Tobacco Control, Campaign for the Framework Convention on Global Health); human rights (Council of Europe's Framework Convention for the Protection of National Minorities); and nuclear safety (Convention on Nuclear Safety). These framework approaches share common themes: they recognize the importance of cooperation, global implications, and shared responsibility; they involve an incentives-driven process; and they have in place implementation and monitoring mechanisms.

Applying a framework approach to nuclear security would involve supplementing the existing fragmented legal regime with general and comprehensive legal norms. Most participants agreed on the need for a framework approach to nuclear security that would fill the gaps in the existing regime while enabling it to remain dynamic enough to adapt to the evolving transnational threats as well as to accommodate the future expansion of nuclear energy.

Cybersecurity and the Nuclear Industry

The participants examined the diverse landscape of cyberthreats, including advanced persistent threat actors, financial fraud actors, hacktivists, nation states, and extremist groups, as well as their objectives, which range from theft of secrets to denial of service to grid disturbance to sabotage of facilities. Thus, depending on the target—business assets, generation/transmission assets, and safety/security Internet Protocol systems—the responses in practice and in policy are dynamic and require a collaborative process within and between industries and government agencies.

Addressing cybersecurity challenges at nuclear plants requires high-level, performance-based policies that allow for flexibility and provide clarity on the threat and the policy's desired outcome. In the United States, the Nuclear Regulatory Commission's (NRC) requirements for cybersecurity are performance-based and not prescriptive. While the NRC's cyberregulations take up only a half-page of text, hundreds of pages of supporting documents and implementation guidance have been produced. This guidance can be easily adapted to new threats without the need to change the law.

The discussion centered on the need to draw a distinction between the threat of theft of nuclear materials and the threat of industrial sabotage. Sabotage, an attack that would challenge operational safety, security, or emergency response, is an incident which the current policy aims to prevent. Participants disagreed on whether industrial sabotage of nuclear facilities through cyberattacks would be a difficult feat, given the current practice of isolating process control and industrial control systems from the Internet, but the participants broadly expressed concern about the insider-threat potential. The discussion concluded with an assessment of the state of play in information sharing between companies in the nuclear industry, among industries using comparable systems, and with government actors.

Political Assessment and Strategy for Improving Global Nuclear Security Governance

A successful strategy for preventing weak links in nuclear security couples the long-term vision for a more comprehensive, universal, effective, and sustainable nuclear security regime with a step-by-step process that can lead to this vision. In this strategy, soft-governance approaches 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. In turn, a hard-governance measure can reduce the fragmentation of the international nuclear security framework and promote a robust regime at the international, regional, national, and facility levels.

The NSS process has grown in scope and scale since its initiation in 2010. Further innovations at the 2014 summit are critical in order to achieve significant improvements to the nuclear security regime by 2016, when the heads-of-state-level 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. Therefore, the discussion focused on identifying challenges to progress as well as opportunities for bolder action at the 2014 and 2016 summits.

Participants identified ways for the NSS process to result in a set of actions that would decrease the weak links in the nuclear security regime, build international confidence in it, and create a platform for continuous improvement and interaction among all stakeholders. The multinational commitments, or “gift baskets,” introduced into the NSS process in 2012, are one important vehicle for countries to drive the system forward with work plans that are in line with, but go beyond, the summits’ consensus communiqués. Participants agreed that a 2014 gift basket in which countries committed to maximizing the current regime and evaluate new ideas for strengthening it would provide an important platform for countries to drive future progress.

The discussion also examined what a post-NSS political structure for improving nuclear security might look like. While participants agreed that the IAEA would remain the premier technical entity for nuclear security after the summit process concluded, they questioned whether it was well suited to the political challenges of advancing the agenda. Most participants did not believe that the IAEA currently has the necessary tools, resources, or structure to maintain high-level political momentum on nuclear security issues.

This brief summarizes the primary findings of the conference as interpreted by rapporteur Michelle Cann, roundtable organizer Anya Loukianova, and cochairs Kenneth Luongo, Shin Chang-Hoon, and Jennifer Smyser. This Policy Memo does not necessarily reflect the views of the Stanley Foundation or any of the conference participants, but rather draws upon the major strands of discussion put forward at the event. Participants neither reviewed nor approved this document. Therefore, it should not be assumed that every participant subscribes to all of its recommendations, observations, and conclusions.

For further information, please contact Jennifer Smyser at the Stanley Foundation, 563-264-1500.

About The Stanley Foundation
The foundation seeks a secure peace with freedom and justice, built on world citizenship and effective global governance. It brings fresh voices, original ideas, and lasting solutions to debates on global and regional problems. The foundation is a nonpartisan, private operating foundation, located in Muscatine, Iowa, that focuses on peace and security issues and advocates principled multilateralism. Online at *www.stanleyfoundation.org*.