Critical thinking from Stanley Foundation conferences

POLICY dialogue BRIEF

Improved Nuclear Security Through Effective Information Sharing

Strengthening nuclear security at the national, international, and facility levels has been a high-priority objective of the nuclear security summit process. Although the process is coming to an end in 2016, the mission is not yet complete. The ability to exchange nuclear security-related information, standards, and best practices, as well as security culture in a timely manner is paramount to improving the effectiveness and accountability of the nuclear security regime. Sufficient information is necessary to identify credible threats and effective responses but must be weighed against the need to keep sensitive information confidential. Today's international nuclear security conventions merely encourage, but do not formalize, the exchange of information among state parties and international organizations in a manner that would sustain effectiveness. While information exchange among signatories is emphasized in international legal instruments, the formal obligation covers only a minimum of information. Examination of the legal instruments, voluntary agreements, and standards reveals untapped information-sharing options for strengthening global nuclear security.

Effective interaction and cooperation among a broad range of stakeholders have been identified as essential for meeting nuclear security objectives and for maintaining a strong nuclear security culture. However, the degree to which information is currently shared is not sufficient, and resulting information gaps exist between states and operators as well as within industry supply chains. In addition, there is a risk that unless they are performed with care, releasing information and increasing transparency could compromise nuclear security and decrease physical protection against theft, sabotage, or other unauthorized access to nuclear materials. Finding a balance between sharing nuclear security-related information while protecting its sensitive dimensions is a challenge that will remain after the nuclear security summit process has concluded.

On October 14–16, 2015, the Stanley Foundation convened a group of experts and policymakers from the United States and abroad to address these issues at its 56th Strategy for Peace Conference, held at Airlie Center in Warrenton, Virginia. The roundtable discussion identified providers and recipients of nuclear security information at the facility, national, and international levels and considered what kinds of nuclear security-related information are relevant to each group. The participants

56th Annual Strategy for Peace Conference

Sponsored by The Stanley Foundation

October 14–16, 2015 Airlie Center, Warrenton, Virginia

This brief summarizes the primary findings of the conference as interpreted by the rapporteur, Pia Ulrich; the chair, Anita Nilsson; and the organizer, Jennifer Smyser. Participants neither reviewed nor approved this brief. Therefore, it should not be assumed that every participant subscribes to all of its recommendations, observations, and conclusions.

also discussed the differences in sharing information during normal circumstances versus emergencies and how increased, regularized, and sustained information exchange may strengthen security regimes nationally, regionally, and internationally. In order to systematize their findings, they developed a matrix to share nuclear security information. As a practical example, the group also examined the flow of information gleaned from International Physical Protection Advisory Service (IPPAS) missions carried out by the International Atomic Energy Agency (IAEA) and how it can best be leveraged to improve confidence. This policy dialogue brief outlines the group's findings about the dimensions of information sharing in nuclear security.

A Matrix of Information Sharing

The roundtable began with participants acknowledging the complexity of information sharing in the nuclear security field, the broad range of stakeholders that provide and receive information, and the variety of substance covered in such exchanges. Their discussion of these factors, along with the recognition of how a nuclear emergency changed the state of play and the need to identify and maintain confidentiality of certain types of sensitive information, was captured in a matrix of nuclear security information. An initial draft of this matrix, developed by a subgroup of the Fissile Materials Working Group (FMWG) in early 2015, was an effort to systematize policy recommendations for the 2016 Nuclear Security Summit related to information sharing, standards and best practices, and security culture.[1] Roundtable participants built on and revised this draft FMWG matrix, outlining categories, recipients, confidentiality, and the value of information.

Categories of Information

The roundtable discussion highlighted the benefits of proper categorization of information for all nuclear security stakeholders and its contribution to increasing transparency. Nuclear security-related information can be grouped and categorized depending on its content. Finding a balance between the sharing of information and maintaining the confidentiality of its certain sensitive types can be facilitated by a logical system that groups data similar in nature and to which appropriate levels of confidentiality may be assigned. Categories of nuclear security-related information include legal and regulatory information, with policy-related background; information regarding implementation, internal working procedures, facility design, design basis threat; incident-related data; and response-related information, such as from first responders.

In its Nuclear Security Series (NSS) implementing guide No. 23-G, *Security of Nuclear Information*, the IAEA identifies categories of information in order to provide guidance on implementing the principle of confidentiality.[2] It is thus focused on protecting the distribution rather than identifying information that is useful to share or information that may be made available to states on a need-to-know basis. The group agreed that despite this focus on protecting the distribution, the categorization included in NSS No. 23-G could be adapted for the rationale of information sharing. Some participants pointed out that in rendering information confidential, the implementing guide's objective is easier to meet than the roundtable's recommendation to share nuclear security-related information and knowledge while maintaining confidentiality of sensitive information. Participants agreed that the overarching objective of sharing information is to strengthen nuclear security and build confidence about its effectiveness.

Stakeholders: Providing and Receiving Information

Nuclear security has a broad range of stakeholders, from those at the state level to the general public. At the state level, stakeholders include the executive and legislative branches, competent authorities (e.g., nuclear regulators), and law-enforcement agencies. Public stakeholders include media, academia, scientific institutes, and nongovernmental organizations. Industry may partly have an official role (e.g., as license holders) and at the same time be privately or publicly owned, if separate from the state. In addition, international organizations and other countries are stakeholders primarily as recipients of information.

Most of these stakeholders produce, receive, and employ different categories of nuclear information, depending on their interests and responsibilities. In their discussion, roundtable participants considered whether a stakeholder primarily provides or receives information, as this may be important and necessary to know when determining constraints of information sharing.

Information Flows and Channels

Roundtable discussion focused on how different channels of communication are used for different kinds of information, depending on whether there is an urgent need for the information to reach a targeted recipient, such as in an emergency, or whether the reach out is more general. For example, the legal framework, the regulatory framework, and general conclusions regarding implementation are expected to be published and thus be available to all. Other information, such as inspection results and license conditions, are of interest primarily to the operator or license holder and would normally only be shared in restricted numbers of hard copies. A summary of this information, after the removal of sensitive details, would also be of general interest and value. Still other information is

strictly confidential, as is also reflected in its distribution. Not all stakeholders are interested in or need the same types of information.

Roundtable participants also discussed information sharing in emergencies and recognized the need to distinguish between emergency preparedness information and the actual information distributed in case of an emergency. For some recipients, emergency preparedness information is very different from information received in case of an emergency. For example, while an assurance regarding the presence of a contingency plan and an adherence to certain standards is sufficient in terms of emergency preparedness, the public will expect to receive quite different information during emergencies and in their wake.

Maintaining Confidentiality of Sensitive Information

Identifying sensitive information and protecting its confidentiality in a way that can be employed globally and across a variety of different actors requires a common denominator on how to distinguish between sensitive and nonsensitive information. After examining categories of information and definitions used, roundtable participants acknowledged that the coexistence of different terms in documents issued by various organizations and authorities calls for an analysis of their compatibility. With regard to the matrix, they agreed that a clear understanding and a common approach is needed to unambiguously set standards for determining confidentiality.

Participants also discussed if existing standards could be adapted from IAEA NSS No. 23-G. As noted earlier, this guide is geared to maintaining confidentiality, whereas the matrix's aim is to identify information that can be shared freely, thereby contributing to strengthening and building confidence about effective nuclear security. Roundtable participants agreed that the matrix would benefit from employing internationally accepted standards for determining confidentiality. It was then decided that in order for the matrix to be most useful, it should be organized as complementary to IAEA NSS No. 23-G.

Strengthening Global Nuclear Security Through Information Sharing

It is widely recognized that the exchange of information (i.e., documented knowledge, conclusions, incidents, and effectiveness criteria) is vital to identifying relevant state needs and improving the effectiveness of nuclear security worldwide. Presently, insufficient information is available to obtain confidence that a national nuclear security regime (i.e., the essential elements of the nuclear security infrastructure in a country[3]) is established and operates as intended. While the threat of nuclear terrorism is well known and feared, the response, internationally and nationally, to protect nuclear and other radioactive materials from being used in malicious acts is much less publicized. This gap may be bridged by the provision of information that has a value in identifying and/or supporting improved or strengthened nuclear security from a global perspective. The matrix is a first step toward bridging this gap.

Roundtable participants agreed that the primary and overarching objective of the matrix is to strengthen nuclear security. They discussed ways in which a platform that facilitates and improves information sharing among a variety of actors in the nuclear arena may help build public confidence, identify weaknesses, and, as a result, contribute to strengthening nuclear security. The providers of information (e.g., operators) may be encouraged by incentives to share information. By examining each contribution's value to the bigger goal of improving global nuclear security, stakeholders become aware of the importance of their role. Incentives, or recognition of their contributions, may also provide positive feedback. This added value is reflected in the matrix's column "Value to assess the effectiveness (completeness, update, and possible gaps) of the global nuclear security regime, and for confidence building." Ideally, such a tool would also highlight incentives and benefits to providing information and the value of the information shared to strengthen nuclear security.

The Information Matrix: A Dynamic and Unique Nuclear Security Tool

The matrix provides an overview of a broad range of stakeholders, information providers, and recipients; the various categories of information; and needs to maintain confidentiality. As a result, it may reveal needs for improvements and needs to close gaps in the nuclear security arena. The matrix and its explanatory text draw on the value of providing information, ultimately to enhance nuclear security globally, build public confidence, and underpin the standing of the operator or competent authority.

Balancing Information Sharing and Confidentiality

Information about civil nuclear materials and facilities is present in official documents and reports. In some countries, government officials and nuclear industry operators, as part of their licensee conditions, also have legal obligations to disclose information, including data related to nuclear security, and tools such as the US Freedom of Information Act can also make this information available to the public. Because information that is publicly disclosed also becomes accessible

to terrorists and other malicious actors, there is a need to assess the sensitivity of information, including information that is releasable through such public-disclosure statutes.

Roundtable participants discussed various types of information and whether they should be publicly disclosed. Information that contains factual data with regard to existing physical protection systems, or other data that perpetrators can use in the planning of an offence, should be kept confidential. This kind of information is referred to as sensitive. On the other hand, information about the regulatory system, including results of general reviews, can and should be disclosed to the public. Likewise, information about security incidents, with an appropriate level of detail, is deemed reasonable for public presentation. Ongoing investigations, however, justify keeping some of the information in the law-enforcement area protected.

One of the participants noted that in 2008 in the United Kingdom, multiple information requests regarding nuclear facilities and vulnerable nuclear material were made as a result of the broad evaluation of future nuclear energy. It was recognized that it was necessary to find a balance between the public's right to information, including under the public-disclosure statute, and legitimate security concerns on the part of the government and industry. Guidance on how to reach that balance was drafted.[4] This guidance is still used today in order to ensure sufficient public access while protecting confidentiality and mitigating security concerns.

In the roundtable discussion, participants examined the dimensions of confidentiality and how to best balance those dimensions with information sharing. A participant noted that although information from one dataset may not pose a risk, sensitive data may be compromised when it is coupled with information from other sources. This mosaic effect poses a challenge to finding a balance and demonstrates that the release of information has to be evaluated from a holistic point of view.

The group then focused on the resulting question of whether the objectives of information sharing can be met when only fragmented information is made available. A participant noted that the US Department of Energy inspector general's report on the 2012 break-in at the Y-12 National Security Complex in the United States was a good example of a balance.[5] The report acknowledged weaknesses and proposed actions without giving detailed information about the targets and creating vulnerabilities.

Circumstances, such as an emergency, may make it necessary to share information with new groups of actors based on a reassessment of the need to know. Further, in all scenarios, information providers and recipients must distinguish between essential data and data that are nice to have but redundant. Some participants pointed to the fact that the balance of sharing information and keeping sensitive parts of it confidential must be sufficiently dynamic to ensure the need-to-know basis in specific situations or circumstances.

Roundtable participants stated the necessity of finding a balance between the public's right of information and the need of government and industry stakeholders to maintain confidentiality of sensitive information.

Cybersecurity

Strengthening cybersecurity requires sharing sufficient information on attempted or successful attacks, even if such information may indicate vulnerability, among various stakeholders. Protection against cyberattacks is essential for effective nuclear security. The prevailing risks are well illustrated in open sources of information for various applications. One of the roundtable participants cited a publication that draws on information gathered from open sources and personal interviews in order to highlight cybersecurity risks in civil nuclear installations.[6]

Participants discussed the importance of security culture and risk management and recognized that cybersecurity constitutes the next big challenge. The implications for information and information-technology-system management at nuclear facilities, by governments and supporting infrastructure, are clear. The group agreed that governments and industry need to take action and work toward a significantly reduced cyberthreat by introducing and maintaining an adequate information-technology structure designed to mount effective cybersecurity. It concluded that addressing cybersecurity threats requires a comprehensive understanding of all dimensions, with up-to-date information and the ability to adapt to changing and evolving threats. Some participants pointed out that information sharing and discussion of possible risks in the public domain may also contribute to improved information-technology-security culture.

Information Contributed by IPPAS Missions

The roundtable discussion then turned to the information that could be gleaned from the IAEA's International Physical Protection Advisory Service (IPPAS) missions. The objective of the IPPAS missions is to promote better nuclear security by reviewing and assessing how well the state has implemented obligations in international agreements and IAEA nuclear security guidance. One of the roundtable participants explained the process, which starts four to eight months ahead of the

mission with a preparatory meeting in the host country. During the mission, the team, consisting of several multinational, recognized, and experienced experts, examines the national nuclear security regime and how physical protection of nuclear material, facilities, and transports are established in the country.

The purpose of an IPPAS mission is to equip states with recommendations to strengthen their national nuclear security regime by identifying gaps and best practices vis-à-vis published IAEA guidance and recognized best practices. Thus, the result of the IPPAS examination is relevant for many nuclear security stakeholders, such as regulators, operators, the IAEA, and the public. However, IPPAS mission results are not publicly available, as IPPAS reports are classified by the IAEA as highly confidential, and the distribution of the report is determined by the host country.

Roundtable participants pointed out that since the IPPAS mission primarily reviews the national nuclear security regime, which is founded on state policy and regulations, the degree of implementation of the regime is not, by definition, confidential. This has also been confirmed by countries such as the Netherlands, Hungary, and Canada, which have chosen to publicize their IPPAS results. These countries have recognized that transparency on the degree to which the country has implemented the national nuclear security regime and its progress over time are strong builders of nuclear security confidence, including with the public and neighboring states.

The group then discussed the contributions of IPPAS missions to global and national nuclear security. Participants agreed that the information included in an IPPAS report that refers to the national nuclear security regime and the official physical protection requirements (e.g., the regulatory system, with licensing or reporting requirements) is or should be accessible to the general public. This information is of interest to the several different actors in the matrix and is well suited/leveraged both for confidence building with the public and as a tool to assess effectiveness of nuclear security in a broader, global perspective. Some participants also debated the dilemma of openness versus confidentiality in reporting IPPAS mission results.

Participants, convinced of the value of IPPAS, elaborated on how mission reports could be better utilized for confidence-building purposes. Some noted that compilation of results may facilitate the identification of gaps and weaknesses, but the methodology needs to be carefully selected. For example, a statistical measure of the number of recommendations may be misguiding, as it depends on several independent factors such as the degree to which information is made available by the country and the ability of the team to assess the information. Others pointed out that even a rough tool to share more information from IPPAS missions will provide an important contribution to global nuclear security.

Strengthening the Impact of IPPAS Missions

Roundtable participants noted that while IPPAS missions are not mandatory, they are the best mechanism in place to review a state's compliance with international obligations and nuclear security guidance. The group expressed general agreement on the need to provide incentives for states to request a mission and subsequently invite a follow-up mission to review progress on the implementation of recommendations. Such application of IPPAS would lead to a larger number of missions, strengthen IPPAS as a tool, and increase global nuclear security.

Comparing the Approach for IPPAS With ICAO Missions

One roundtable participant offered the example of audits conducted by the International Civil Aviation Organization (ICAO) to assure security of passenger air travel. A specialized agency of the United Nations, ICAO promotes the safe development of civil aviation and sets standards and regulations necessary for aviation safety, security, and efficiency, and can be seen as the IAEA's aviation counterpart. ICAO is the permanent body administrating the principles to which its contracting states consented, and its inspections are mandatory by the decision of the ICAO Assembly and follow the objective to audit compliance.

Participants then focused on comparing and contrasting IPPAS and ICAO missions. Whereas IAEA IPPAS missions are voluntary and their objective is to provide advice, ICAO inspections are based on a binding convention that enables ICAO to issue binding regulations for aviation safety and security, as well as performing regular inspections of aviation control in member countries. ICAO and IPPAS differ significantly on information sharing: while ICAO reports are confidential, significant information is shared through a secure web interface and cleared when the issue in question is corrected; IPPAS reports are, as a rule, classified as highly confidential and not shared unless the host country decides to the contrary.

Roundtable participants discussed and recognized the value of ICAO-type performance reviews and emphasized the structural differences between the mandate of ICAO and the IAEA. They further pointed out that in anticipation of a larger number of IPPAS missions, more international IPPAS experts need to be trained and prepared. In this regard, the ICAO University's approach of training experts for missions provides a valuable model for the IAEA to learn from.

The Joint Initiative to Strengthen Nuclear Security Implementation

The existing nuclear security framework offers potential to further strengthen the security system. An initiative proposed at the 2014 Nuclear Security Summit titled "Strengthening Nuclear Security Implementation" was supported by 35 nations and was later published by the IAEA as INFCIRC/869.[7] The initiative calls for voluntary actions by individual countries to strengthen the security of their nuclear materials by implementing IAEA guidance (the Nuclear Security Fundamentals—Essential Elements of a Nuclear Security Regime) and to meet the intent of the nuclear security recommendations, as documented.

The initiative commits countries to implement the IAEA guidance through their regulations. This is mostly open source information. The initiative also commits countries to host peer reviews (IPPAS) periodically and act on the recommendations provided. This may also be seen as information related to the country's compliance with its political commitment. Through INFCIRC/869, the initiative is open to all IAEA member states and was lifted from the nuclear security summit sphere to last beyond the summit process.

Roundtable participants agreed that strengthening nuclear security, including through information sharing, will use the existing nuclear security framework as a foundation, recognizing that the present system has gaps. While some participants noted that the future goal should be to fill those gaps, there was agreement that the existing legal framework should serve as the basis for IPPAS missions in the short term.

International Reporting

The current nuclear security framework provides different reporting and reviewing mechanisms. Participants discussed the similarities between reporting requirements in UN Security Council Resolution 1540, the Convention on the Physical Protection of Nuclear Materials and its amendment, and the International Convention on the Suppression of Acts of Nuclear Terrorism. Reporting, in some way, is a mandatory and important part of each regime. In addition, in these international legal instruments, exchange of information and interaction among state parties are anticipated and recommended. Exchange of information is necessary for implementation.

However, in a fragmented regime, the reporting and reviewing mechanisms generate overlap that could be streamlined to improve information sharing and reduce the countries' reporting burden.

Recommendations

Establishing effective and balanced best practices on information sharing is an essential part of an effective, global, nuclear security regime. Roundtable participants agreed on the following recommendations to strengthen information sharing:

- **Promote increased, more effective reporting, as outlined in the Nuclear Security Information Matrix.**

  Incentives and benefits to providing and sharing information are important tools to strengthen nuclear security at facilities, in nations, and internationally.

  The roundtable recommended that more attention be given to increasing the exchange of information, to recognizing the value of providing and receiving nuclear security related information, and to finding a suitable balance between the values of information sharing and legitimate requirements to maintain confidentiality of sensitive information, as outlined in the Nuclear Security Information Matrix.

  In finding the right balance, roundtable participants noted that:

  - Information sharing promotes building a nuclear security culture among all stakeholders, one that will also help strengthen global nuclear security. A culture of informed risk management will require sufficient information to enable the threat to be addressed and reassessed, from time to time, also in relation to safety, security, and transparency.
  - Confidentiality of information assessed to be sensitive—such as specific information on vulnerable material, physical protection arrangements, transport routes, and personnel data—should be maintained.
  - In an emergency, a reassessment of the need-to-know basis should be made, as the nature and content of information to be shared will be different in emergencies compared with routine situations.

- **Consolidate reporting requirements.**

  Each agreement comes with its own, often overlapping, reporting requirements. With reporting requirements for UN Security Council Resolution 1540 and the Convention on the Physical Protection of Nuclear Materials and its amendment, countries are to provide different but similar sets of information in different contexts.

  The roundtable recommended that a strategy be developed for consolidated and more-consistent reporting; that would also provide incentives for

more-effective reporting while avoiding reporting fatigue.

- **Encourage periodic IPPAS missions with information sharing.**

  IPPAS is a key contributor to monitoring the effectiveness of nuclear security globally and nationally. In anticipation of increased, and periodic, use of IPPAS missions, attention should be given to identifying how IPPAS results may be compiled and shared to contribute to a process aimed at assessing nuclear security effectiveness at the national level and globally.

  Therefore, the roundtable recommended that:

  - Nonsensitive information related to the national nuclear security regime, its legislative and regulatory systems, and infrastructure support included in IPPAS mission reports be shared through an open information platform.
  - An information portal be created where countries may store additional IPPAS information they can share with others.
  - A database on best practices be established.

Endnotes

1 Fissile Materials Working Group, *The Results We Need in 2016*, June 2015, *www.fmwg.org/FMWG_Results_We_Need_in_2016.pdf*.

2 International Atomic Energy Agency (IAEA), *Security of Nuclear Information*, 2015, *http://www-pub.iaea.org/MTCD/Publications/PDF/Pub1677web-32045715.pdf*.

3 IAEA, *Objective and Essential Elements of a State's Nuclear Security Regime*, 2013, *http://www-pub.iaea.org/books/IAEABooks/10353/Objective-and-Essential-Elements-of-a-State-s-Nuclear-Security-Regime*.

4 United Kingdom Office for Nuclear Regulation, *Finding a Balance (Version 3): Guidance on the Sensitivity of Nuclear and Related Information and Its Disclosure*, April 2, 2014, *www.onr.org.uk/ocns/balance.pdf*.

5 Inspector General, US Department of Energy, *Inquiry Into the Security Breach at the National Nuclear Security Administration's Y-12 National Security Complex*, Special Report IG-0868, August 29, 2012, *energy.gov/ig/downloads/special-report-ig-0868*.

6 Caroline Baylon, Roger Brunt, and David Livingstone, *Cyber Security at Civil Nuclear Facilities: Understanding the Risks*, Chatham House, September 2015, *https://www.chathamhouse.org/sites/files/chathamhouse/field/field_document/20151005CyberSecurityNuclearBaylonBruntLivingstone.pdf*.

7 IAEA, "Communication Received From the Netherlands Concerning the Strengthening of Nuclear Security Implementation: Joint Statement on Strengthening Nuclear Security Implementation," October 22, 2014, *http://www.iaea.org/sites/default/files publications/documents/infcircs//infcirc869.pdf*.

NUCLEAR SECURITY INFORMATION MATRIX			
Type of info	**Subset info**	**Information provider and channel used**	**Information recipient**
1. Information related to the national nuclear security regime			
National security policies	**Decisions and related background information related to national acts or arrangements for nuclear security**	Government: records of established policies and related decisions in printed-copy text	All: the public, competent authorities, operators, law enforcement
Explanations and clarifications to national security policies	**Document that elaborates on or provides guidance on the implementation of a national policy that has earlier been issued by the government**	Government and/or regulator or competent authorities: official documents, publications	Operator or license holders, technical and scientific institutes that may benefit from additional information about the policy to facilitate implementation; for nonsensitive documents, also media and the public
National security regulations	**National security regulations governing the use of nuclear material or other radioactive material; requirements related to nuclear and other radioactive materials out of regulatory control**	Nuclear regulatory body; other competent authorities involved in the control of or response to incidents with nuclear and other radioactive materials that are out of regulatory control	All: the public, operators, law enforcement, technical and scientific institutes, governments, and international organizations
Guidance on regulations	**Specifications, explanations, and further details related to national security regulations and their implementation**	Same as for national security regulations	Operators or license holders; technical and scientific institutes with a role to support implementation; media and public for supplementary, nonsensitive guidance

Need to protect sensitive information	**Value to assess the effectiveness (completeness, update, and possible gaps) of the global nuclear security regime, and for confidence building**
Documentation produced by the originator, subsequent distribution through electronic media; this kind of information is not sensitive	The information provides assurances that nuclear security remains a governmental priority and provides background on arrangements included in the national nuclear security regime.
An assessment is to be performed in the individual case. Information that may relate to security specifications (e.g., response times, target protection) should be identified and treated as sensitive information. Other information (e.g., requirements to coordinate arrangements among different authorities) is not sensitive and can be shared publicly.	Explanations and clarifications provide further information about the national nuclear security regime and how it is set up. If the information contained is sensitive, the document title and date of issue still offer contributing value.
This kind of information is not sensitive.	The regulatory system is the backbone structure in the national nuclear security regime; the awareness of its principles, requirements, and reach are of great value nationally as well as internationally for confidence building.
In most cases, supplementary guidance on national security regulations does not contain sensitive information. However, an assessment on the security classification will be done to identify technical or equipment specifications or other details that could be used by adversaries in planning a malicious act. In such cases, the information will be protected as sensitive.	The regulatory system and the guidance on regulations constitute the core that build up the national nuclear security regime. Awareness and knowledge of its principles and understanding the operational mode are important for maintaining its effectiveness, and to identify needs of improvements. This understanding is supported and facilitated by a system that is open, with a minimum of sensitive, protected information.

Type of info	Subset info	Information provider and channel used	Information recipient
Security reports	**Security reports compiled and issued periodically by the regulator or another competent body (e.g., annual reports) that contain information of the completeness and effectiveness, as a whole, of the national regulatory system; security reports with results of national inspections, assessments, and investigations of, and related to, the operation of physical protection systems, specific equipment, or staff performance**	Regulator or other competent body; annual reports published and made available in open media, including Internet; security reports with results of inspections, assessments, or investigations are issued in printed copy made available to the target audience only	The public; government; national, regional, and international organizations; IAEA; technical and scientific organizations; operator or license holder that has been subject of an inspection, evaluation, or investigation
International peer reviews	**Results of international peer review of the national nuclear security regime**	Evaluation report issued by the lead organization for the evaluation, normally the IAEA Evaluation of the regulatory system, its supporting guidance, and its effectiveness is documented in a printed copy. After screening, the report may also be made available publicly.	Regulator, government, public, media
Security performance reports	**Performance reports, as required by an operating license; review of performance during a reporting period, security plans, and staff development; reports may cover physical protection access control, detection and alarm, barriers, IT security, staff development, exercises, coordination with regulatory and competent authorities, emergency response, and law enforcement**	Operator or other license holder; printed report in limited number Implementation of a regulatory requirement to issue security performance reports contributes information that may be made available to the public.	Regulator

Need to protect sensitive information	Value to the regime and for confidence building
Annual or periodic security reports will be assessed on the sensitivity of their content. There must be a balance between providing information for awareness and knowledge of, and understanding the effectiveness of, the national nuclear security regime and the need to protect sensitive information. A periodic report will describe maintained effectiveness, thereby deterring an adversary from carrying out a malicious event. Security reports that examine security arrangements at facilities or for license holders are likely to contain sensitive information and should only be provided on a need-to-know basis, primarily to the operator or license holder. Information in these reports may be used by a perpetrator in planning a malicious event and should therefore be protected.	Annual or periodic security reports issued by the regulator or any competent authority are essential for all stakeholders to understand the implementation of national policy, the regulatory system, and interaction among those involved. The reports will help maintain effectiveness and identify needs for improvements. Thus, national reports may also contribute to maintaining effectiveness of the global nuclear security regime. Security reports that are the results of inspections, assessments, evaluation, and investigation of the operation of physical protection or other security systems at facilities and by license holders are key to maintaining effectiveness in the operation of security systems. These reports will feed into, for example, an annual security report.
Security evaluation reports are to be assessed with respect to inclusion of sensitive information. Traditional approach is to classify an evaluation report as sensitive and maintain confidentiality of the report as a whole. However, the evaluation of the regulatory system (i.e., the national nuclear security regime) does not normally contain information that could be used by an adversary and may therefore be published (e.g., online). Press releases, media interviews, and commentary reports may be treated in a similar manner.	International peer reviews are deemed to be objective, thorough, and constructive. The value of periodic peer reviews is high, in the first place for the national nuclear security regime and its effectiveness, but also for the global system. Evaluation of regular peer reviews will contribute to identifying needs to strengthen the global nuclear security regime. International peer review results contribute to confidence building, nationally and internationally and with neighboring countries.
Security performance reports are deemed to contain sensitive information of physical protection, vital areas, equipment used, and staff-related issues. This information is sensitive and would be of use to an adversary planning to target the facility in a malicious act. The report is, by default, sensitive, requiring protection at the appropriate classification level.	Security performance reports issued by the operator are essential to maintain effectiveness of the security system implemented at a facility or a location and to identify needs for improvement. While the individual security performance report is sensitive, the existence of such reports giving feedback on the implementation of security regulations constitutes an important input for summary annual reports. General conclusions and initiatives taken to improve the national nuclear security regime may be reflected in the annual report of the regulator. Such general feedback will contribute to confidence building and to strengthening the international nuclear security regime.

Type of info	Subset info	Information provider and channel used	Information recipient
Security incident report	Report of a security incident or event; trafficking of nuclear or radioactive materials, attempts of intrusion at or attacks on a facility, or attempts to steal nuclear or radioactive materials	Operator or license holder; for incidents that relate to material not under regulatory control, law-enforcement organizations IAEA, as the holder of the Incident and Trafficking Database, to disseminate information obtained from the regulatory body or the point of contact of the database	Initial report to be provided to the regulatory body or competent authority; for trafficking incidents, report to the IAEA Incident and Trafficking Database; press release or other information to be provided to the media and public; timely follow-up with additional information as the incident or event is examined or investigated
Emergency announcement of a security event	Information aimed at the public that a security incident or event may result in or has resulted in the dispersal of radioactivity; information about actions to take, precautions, and forecast of recommended actions in the near future	National disaster management organization; regulator; information provided in printed copy and through Internet	Public, media, government
Emergency/ incident communication of facility or operator	**Communication that contains information about the event and first actions taken by the operator or facility**	Operator	Public, media
Incident/ emergency planning	**Contingency and Response Plans**. Response planning is compulsory at nuclear facilities. Such planning for security incidents is part of the International Atomic Energy Agency (IAEA) guidance requirements. The planning includes verification of alarm, first response plan, and forensics planning, including so-called nuclear forensics. Radiological response, should there be a release of radioactivity, is normally integrated with the response planning performed for radiation safety purposes.	Operator: provides the planning records to the regulator and other competent response organizations Regulator: summary versions may be shared with the public to communicate the planning and for overall preparation purposes	Regulator, public

Need to protect sensitive information	Value to the regime and for confidence building
An assessment of the sensitivity of the information contained in the security incident or event reports will be done and sensitive information protected at the appropriate level. Nonsensitive parts of reports are to be made available to all and published online (e.g., via press release, media interviews). Follow-up and periodic summary reports containing information about the impact of the event, any damage or potential damage, including radiological	Incident reports provide information that relates to the security situation, including interest in and actual perpetrations or attempts to disturb or attack a facility, material that is subject for trafficking. The reports contribute to the awareness of the need to maintain effective security systems. Follow-up information with factual information provided to the public is essential to build confidence in the effectiveness of the nuclear security regime as a whole.
The information is aimed at the public and organizations and should be drafted in a manner that provides sufficient substance to support the emergency report and the advice given to the general public, at the same time excluding sensitive information that may negatively affect management of the emergency situation.	Public and international confidence in the national emergency response planning, the regulator, and other organizations that may contribute response in the emergency situation
An assessment of information sensitivity will be required. The operator is responsible for security arrangements at the facility and for its operation. It will therefore be expected that the operator will communicate to the public and media about an event that has occurred or is unfolding. The information provided should be assessed as nonsensitive.	Communication by the operator contributes confidence in responsibility to operate and maintain security systems at the facility. The communication may indicate initial actions taken to protect staff vis-a-vis the emergency response organizations.
The detailed response plans will be assessed for sensitivity of data contained. The detailed plans may contain sensitive information and be protected from public distribution. Summary versions with planning purpose, objective, actors involved, and planned activities—without details, may be helpful for effective implementation. The communication of such information will also provide important contributions to the nuclear security regime.	The knowledge and awareness of plans and preparedness for security incidents or events are important contributions in the nuclear security regime, at the national as well as international levels. Absence of information may be seen as absence of planning, which indicates gaps and vulnerabilities in the nuclear security regime.

Type of info	Subset info	Information provider and channel used	Information recipient
Threat assessments and security alerting	**Design Basis Threat (DBT).** This is the basic level of threat against which a physical protection system shall be effective. The DBT is normally developed by the regulator, with the contribution of the operator, law enforcement, and intelligence, as well as other organizations that may contribute information or assessment regarding the threat situation. **Alert function**. In the event of a security incident/event, a warning or alert is issued by either the operator, nearby law enforcement, or the regulator. In the early stage of an alert situation, the warning may be directed to a few persons or organizations. Later, the alert function may have to reach the local population and the public.	Operator or law-enforcement organization (e.g., local police), regulator, or representative of another competent authority	The DBT is normally issued by the regulator for national use, primarily by the operator or manager of nuclear facilities, or other establishments with significant amounts of radioactive substances. The warning or alert in case of a security event (e.g., theft of material, attempt to perform an act of sabotage) will first be issued by the operator to local law enforcement and to the regulator. Depending on events, a public alert or warning may have to be issued. The radiological emergency warning or alert will be integrated into the alert.
2. Information on nuclear material, radioactive materials, and inventories			
Inventory records at facilities and locations where radioactive materials are used or stored	The **records** contain detailed information about the nuclear material used or stored, and about radioactive sources or other radioactive substances.	Operator: updated records are submitted by the operator to the regulator, and in some cases to the IAEA. These records and technical reports may contain specific information about the nuclear material that is normally not public. Summary records (e.g., for use in annual reports of the operator) may give an overview of value for a broader audience. Regulator: national summary records, without specific storage details, may be of interest to and shared with the public.	**IAEA, bilateral authority** The IAEA receives periodic reports of materials in use of storage, information that is used in a broader perspective (e.g., regional summaries).

Need to protect sensitive information	Value to the regime and for confidence building
The DBT, almost by default, contains sensitive information: the characteristics of an intrusion (e.g., number of people, arms, level of knowledge) against which the physical-protection system is designed. This information is by default sensitive, to be protected as highly sensitive, by the operator, the regulator, or other competent authority and strictly shared on a need-to-know basis. The sensitivity of an early alert that a security incident is ongoing, or has happened, has to be assessed in the individual case. In suspected cases of theft, confidentiality may be initially justified during a first period, but with time, it becomes appropriate that the event is made known more broadly, including to the public.	The general information about the existence and role of the DBT is deemed to be important in building confidence that the physical-protection system at a nuclear facility is deemed to be effective. The DBT sets the requirements for the operator, and in cases where the threat goes beyond the DBT, the national response will be added. This general information will be important in understanding the allocation of responsibilities among the operator, the regulator, and the government. Early warnings and alerts are seen as key indicators of an effective system. Postponed release of information about a security event needs to be explained in light of the evolution of the incident or event. Continuous feedback on the incident's development will be seen as evidence of competence and responsibility.
Reports with specific technical information (e.g., quantities, radioactivity) primarily submitted in controlled printed reports through secured channels will be assessed for sensitivity of data contained. Detailed information about nuclear material or radioactive sources is normally classified as sensitive. The sensitivity may be balanced by making information available that is less detailed, presented in a general, summary form.	General or summary information regarding inventory of nuclear material or radioactive sources is expected to be accepted and appreciated by the public.

Type of info	Subset info	Information provider and channel used	Information recipient
Reports according to safeguards agreements	**Reports** on inventory and inventory changes, technical specifications of material items, as well as explanatory notes are issued periodically by the operator or the regulator, or another competent authority that is assigned the reporting responsibility according to safeguards agreements.	The operator (in Europe) and the regulator or another competent body with reporting responsibility will issue the reports to the IAEA. The reports are normally transferred as electronic files.	The IAEA receives the safeguards reports and, as a rule, protects the reports as confidential.
Historical records related to nuclear research and development and activities	Throughput, capacity, and historical throughput on facility under safeguards; archive documents and electronic files	Operator	Regulator, IAEA
3. Transport of nuclear material and of radioactive substances			
Transport of nuclear material and radioactive substances	Specific information of nuclear material or radioactive materials transport; summary information of transports completed	Operator, regulator	Regional and international governments, the public
4. Other information of relevance for implementation at facilities of the national nuclear security regime			
Corporate reports	Corporate reports reflecting company policy on security, investments made, and resources allocated to maintain effective physical protection, equipment, coordination, and staff development	Operator, as part of the corporate periodic report	Public, media
Personal/personnel information	Information about appointments and significant changes in staff, in particular when security-related functions are involved	Operator, regulator	Public, media, local community

Need to protect sensitive information	Value to the regime and for confidence building
Some countries treat the safeguards reports as nonsensitive, available to anyone on request. The IAEA treats them as confidential, which demonstrates a difference in approach. In some cases, it may be assessed that the information contained is sensitive.	As required by safeguards agreements, and in some cases by bilateral agreements. Access to the reports will contribute confidence regarding fulfillment of international obligations.
Sensitivity of the contained information will be assessed. It is not likely that historical records will contain information that remains sensitive. The historical data will have to be archived for a minimum time period, at least five years.	As required by national laws and safeguards agreements with the Additional Protocol
Sensitive information shared only on a strict need-to-know basis, distributed within membership channels. Transports are seen as potentially more vulnerable than when the material is kept within facilities or locations. Information provided ahead of transports may help adversaries plan malicious acts. When the transport is completed, the information may be released.	Information about transports will contribute to better understanding of the movement of radioactive substances and related circumstances. It will also contribute to an informed public.
Public report. The corporate report, by default, does not contain security-sensitive information.	Provides insight into corporate policy vis-a-vis security and the priority given to nuclear security in the corporate approach. Increases confidence in the priority given to security in the management of the facility.
Not sensitive	Contributes to confidence building and awareness of efforts made to implement effective nuclear security systems. Particularly important for local communities.

Type of info	Subset info	Information provider and channel used	Information recipient
Decommissioning and other nuclear investments or changes	**Plans to decommission or shut down nuclear facilities, other plans for new activities or changes in ongoing activities**	Operator, regulator	Public, media, local community
Security related to nuclear technology	**Evaluations performed on existing or new nuclear technologies and related security impact**	Operator, regulator	Competent authorities, government, public, media

Participants

Roundtable Organizer

Jennifer Smyser, Vice President and Director of Policy Programming Strategy, The Stanley Foundation

Chair

Anita Nilsson, President, AN & Associates

Rapporteur

Pia Ulrich, International Nuclear Policy Analyst, Federation of American Scientists

Participants

Rob Anderson, Counselor, Political Department, Embassy of the Kingdom of the Netherlands to the United States

Roger Brunt, Security Consultant, Grosmont Howe Ltd.

Bart Dal, Consultant, Ministry of Foreign Affairs, Netherlands

Miroslav Gregoric, Consultant, Miroslav Gregoric S.P.

Corey Hinderstein, Senior Coordinator, Nuclear Security Summit and Nonproliferation Policy Affairs, National Nuclear Security Administration, US Department of Energy

Igor Khripunov, Distinguished Fellow and Adjunct Professor, Center for International Trade and Security, University of Georgia

Anya Loukianova, Graduate Fellow, University of Maryland, College Park

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

Samantha Pitts-Kiefer, Senior Program Officer, Scientific and Technical Affairs, Nuclear Threat Initiative

Need to protect sensitive information	Value to the regime and for confidence building
Not sensitive	Contributes to confidence building and awareness of efforts made to implement effective nuclear security systems. Particularly important for local communities.
Normally not sensitive. In some cases, sensitive information included in the evaluation may have to be protected.	Contributes to confidence building and awareness.

Peter Rickwood, Founder, Atomic Reporters

Warren Stern, Senior Advisor, National Security and Nonproliferation, Brookhaven National Laboratory

Page Stoutland, Vice President, Scientific and Technical Affairs, Nuclear Threat Initiative

Cindy Vestergaard, Senior Researcher, International Security, Danish Institute for International Studies

Rodney K. Wilson, Director, Center for Global Security and Cooperation, Sandia National Laboratories

Timur Zhantikin, Deputy Chairman, Committee for Atomic and Energy Supervision and Control, Ministry of Energy of the Republic of Kazakhstan

Affiliations are listed for identification purposes only. Participants attended as individuals rather than as representatives of their governments or organizations.

The Stanley Foundation

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

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

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

209 Iowa Avenue
Muscatine, IA 52761 USA
563-264-1500
563-264-0864 Fax
info@stanleyfoundation.org

The Stanley Foundation

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

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

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

209 Iowa Avenue
Muscatine, IA 52761 USA
563-264-1500
563-264-0864 Fax
info@stanleyfoundation.org

PRINTED ON RECYCLED PAPER | 1/16 750