International Transport Security Symposium

Tokyo, Japan

12-14 November 2019

Ministry of Foreign Affairs of Japan

JAEA

National Nuclear Security Administration

Table of Contents

Introduction

The United States Department of Energy (DOE) National Nuclear Security Administration (NNSA), the Ministry of Foreign Affairs of Japan, and the Japan Atomic Energy Agency (JAEA) convened the inaugural International Transport Security Symposium (ITSS) in Tokyo, Japan during 12-14 November 2019. The purpose of this Symposium was to support the 2017 Joint Statement on Transport Security of Nuclear Materials (INFCIRC/909), to strengthen the security of nuclear and radiological materials in transport, and to seek solutions from the international community to counter threats during the transport of these materials around the world.

In 2017, recognizing the importance of working together as a global community to further improve security in the transport of nuclear and other radioactive materials, Japan sponsored the IAEA Information Circular 909 (INFCIRC/909), Joint Statement on Transport of Nuclear Materials. INFCIRC/909 now has 17 subscribing countries who have expressed their commitment to further exchange national practices on the transport security of nuclear and radioactive materials and actively support the IAEA, Global Initiative to Combat Nuclear Terrorism, and the Global Partnership Against the Spread of Weapons and Materials of Mass Destruction in advancing nuclear transport security obligations. The International Transport Security Symposium created a forum for the international community to discuss this important topic.

Objectives

Threats to the secure transportation of nuclear and radiological materials pose a significant risk to the future of the nuclear and radiological community as a whole. The intention of this Symposium was to examine these threats and engage the international community to seek solutions to counter the threats as well as strengthen the security regimes for these materials in transport. The ITSS provided a forum for partner countries to discuss their good practices and exchange knowledge to improve existing regimes when addressing Transportation Security. Through the Symposium dialogue, focus areas for future exchanges and coordination were identified. The ITSS was intended to foster a network of competent authorities, regulators, operators, industry, law enforcement, and response organizations as the stakeholders of global Transportation Security. The network and topics identified at the ITSS were designed to build momentum and increase willingness for additional international cooperation on the topic of Transportation Security.

The Symposium was also designed as a mechanism to showcase INFCIRC/909, identify areas where INFCIRC/909 subscribers should be focusing their efforts, and to encourage further subscribers.

Key Themes

Transport Security, why is it important to the International Community?

In this panel discussion, participants identified the reasons that transport security is vital to the international nuclear community and sought to identify some key challenges that transport security is facing now and in the future.

Members of various stakeholder organizations offered insights and perspectives into the importance of ensuring the security of nuclear and radioactive material transport throughout the world. The panelists included a representative from the International Atomic Energy Agency (IAEA) and members of the International Nuclear Services (United Kingdom), the International Maritime Organization, and SOGIN (Italy).

Without transportation security, nuclear materials would not be able to move through the nuclear fuel cycle from mines to fabrication facilities to power plants. This would leave countries without power and unable to decommission facilities. Hospitals and universities would not be able to do research and various medical procedures would be impossible. However, due to the global complexity of transport security, there are also unique challenges that the international community must address. These challenges include operating in the public domain, reliance on technology and the growing cyber threat, risks in the supply chain, delay and denial of shipments, intermodal changes, armed robbery, and piracy. Multiple panelists and participants placed great emphasis on information security vulnerabilities. There are a lot of people involved in transporting nuclear and radiological materials with different requirements and it is a big challenge to maintain the restriction of information.

Key Takeaway: Transport can be one of the most attractive areas of the nuclear fuel cycle to adversaries due to its unique challenges.

"Transport is the most exciting part of the nuclear sector – it binds the whole sector together."
-Ben Whittard, INS

Building an International Solution to Transport Security

The first Nuclear Security Summit in 2010 raised the importance of transport security. In this panel, members of the regulatory agencies in Canada and Romania, both signatories to INFCIRC/909, discussed the measures they are currently putting in place to improve transport security and what challenges lie ahead.

Security challenges are constantly evolving and panelists discussed the key role international organizations can play in helping to build capacities with countries. Canada is a proponent of the IAEA's International Physical Protection Service (IPPAS) and has hosted IPPAS missions where recommendations for transport security were highlighted. They are focusing current efforts on tracking technology for radioactive sealed sources, table-top exercises, and integrating security exercises for licensees using, storing, and transporting category III nuclear and radioactive material.

Romania emphasized the importance of creating regulatory frameworks that include all of the stakeholders involved in transporting nuclear and radiological materials. Regulators need to demand comprehensive transport security plans and use proactive assessments to ensure industry implements these plans appropriately. Additionally, with the implementation of the defense in depth concept measures can include mitigation of insider threats, secure communications, and a redundant method of communication (including a contingency plan to alert the monitors without letting the adversary know), and a two-person rule for drivers.

Another solution to building transport security regimes internationally includes countries subscribing to INFCIRC/909. By subscribing, countries demonstrate their willingness to share, learn, and contribute in the areas of transport security with their international partners who are also subscribers. Subscribing to INFCIRC/909 can also influence policymakers and budgets by giving visibility to transport security and potentially allowing for the allocation of more resources to transport security.

Key Takeaway: Threats to Transportation Security are constantly evolving. One of the key roles of regulators is to ensure that operators implement proper security for shipments to include producing and adhering to robust transport security plans.

Threat Issues that Impact a Transport Security Regime

In this panel a number of key threats were discussed from the varying perspectives of industry and research.

Ensuring that transport is economically viable is a key part of creating an appropriate transport security regime – if this is not the case, it threatens the ability of the nuclear community to function. Nuclear and radiological material is one of the nine dangerous goods classes that require security during transportation. However, nuclear and radiological materials include a variety of different types of shipments, so, unlike safety, there can be no uniform type of security. Regulators and industry must establish an appropriate base level of security, which is then augmented depending on the consequences of the material and the threat posed by the situation where it is being transported. Security must meet the needs of the regulator and material, but disproportionate security measures can make it harder or impossible to perform a shipment within a reasonable budget.

A major evolving threat to transport security is cyberattacks. Modern vehicles have a very large number of cyberattack surfaces, either through attacking the car itself or through the infrastructure. Security measures have not kept up with these features. Communications with all larger vehicles are published where attackers can access them, posing an even larger risk, whereas smaller, passenger cars have proprietary data that is not published. The extent that vehicles can be kept disconnected and information off of the internet can help prevent cyberattacks. However, this is not entirely possible, so some mitigation strategies include performing a complete inventory of the electronic features of each vehicle at the time of purchase, purchasing software verification tools for periodic assessment, performing tamper checks, developing or purchasing a network scanning tool, deploying tactics and procedures to develop redundant communications and navigation, and training personnel on how to find handheld transmitters.

Another key threat to the secure transportation of nuclear and radiological material is the delay and denial of shipments. The solution to this issue is not simple. However, one mitigation strategy would include providing education on understanding the cargo and knowing why it is important to transport these materials. A second mitigation strategy is to work through the IAEA and have Member States confront those that do not allow the transport of these materials.

Security culture is a key area which can be improved to help ensure the secure transportation of nuclear and radiological materials. The promotion of an effective security culture must start with the management of an organization; leadership must be focused on and dedicated to proper security. However, the regulator also has a role to play in ensuring that this culture is verified and properly monitored and maintained through periodic reevaluation.

Key Takeaway: A successful transport regime must balance economic realities with the security requirements of the material and the threats posed. The threats are constantly evolving, and transport operators must be flexible.

Engaging Industry and Other Non-State Stakeholders in Transport Security

This panel provided representatives of industry and non-state organizations a forum to consider how industry can become more engaged in creating a strong transport security regime and discuss the concept that transport activities are an economic activity that impacts how different stakeholders consider security issues. A graded approach to security was highlighted as an important factor in facilitating the transport of nuclear and radiological materials. Industry must be able to make the business case for security.

Creating a strong relationship between regulator and industry was once more put forward as a route to a stable transport security regime. To increase the cooperation between regulation and industry, it was suggested that regulators take advantage of trade unions and industry associations such as the WNA and WNTI, which already have established lines of communication. Regulatory agencies can aid industry by supporting communications between shippers and receivers and by trying to actively achieve harmonization in security regulations across borders. This remains a difficult goal to achieve because, unlike for safety, the threats are very different in different countries (e.g. internal issues, criminal threats at ports and borders, etc.).

From the industry perspective, regulatory frameworks that allow for innovation are to be encouraged. For example, the United Kingdom has moved away from a prescriptive regime to a performance-based regulatory framework. Performance-based regulation specifies a threshold of acceptable performance and a means for verifying that the threshold has been met. While this allows Government and industry more flexibility in adapting to the evolving threats it does require a higher degree of knowledge, potential costs and expertise on the part of industry. Innovation can help mitigate against the expense of providing appropriate security.

The participants and panelists discussed many aspects of design basis threats (DBT) and noted that appropriate DBTs are key to industry being able to meet regulatory requirements. Generally, DBTs are developed by a government entity. The DBT itself is sometimes shared with key people within industry, but some countries choose to keep the DBT secret and only make industry aware of

changes in procedures. It was also noted that there are other industries with DBTs and that the nuclear and radiological industry is not unique in needing security.

Once more the issue of appropriate security balanced with economic realities was discussed. Industry has been utilizing new technologies to drive costs down and, where possible, limit the reliance on expensive labor. Other strategies, such as the separation of shipments into smaller quantities so that they become a lower category shipment, can make transportation less expensive. To ensure an appropriate balance between cost and security, a number of companies are starting to integrate security analysis within the management system, in particular in risk analysis and risk mitigation strategies.

Key Takeaway: The relationship between regulators and industry must include effective and timely communication in both directions. Economics is a major driver in the realities of providing secure transportation and industry as well as the regulator has a vital role in ensuring that an appropriate balance is maintained.

International and Regional Cooperation in Capacity Building and Assistance

Transport security lends itself to regional and international cooperation due to the cross-border nature of many radiological and nuclear shipments. In this panel, participants heard how international and regional cooperation is currently underway, and panelists and participants were asked to identify areas for future engagement and effort in this area.

The importance of regional cooperation was emphasized, and some examples were given where through regional cooperation transport security protocols, plans, and procedures had been amended and improved. Sharing of information (both internally and internationally), including best practices and threat data, was identified as an important route to improving global transport security. INFCIRC/909 aims to be part of the framework through which information sharing is facilitated. Participants identified the need to develop a network of resources that countries can use to enhance their Transportation Security framework. The IAEA noted that it is not up to the Agency to determine what is considered a 'good practice'; instead, international experts and Member States identify examples and, ideally, add them to the IAEA's good practices database.

The panelists noted the following:

- The importance of understanding local culture and identifying local experts.
- The delivery method of courses should vary according to the local culture. For example, battle boards in transportation can be very effective for some agencies and participants but would not work as effectively with leadership in Asian cultures.
- Subject matter experts are not always the best people to deliver these training courses.

Effective evaluation of the programs is also a vital step in increasing the effectiveness of a training course over time. The Middle East Scientific Institute for Security (MESIS), the Integrated Support Center for Nuclear Nonproliferation and Nuclear Security (ISCN), and the IAEA use pre-, during, and post-surveys at the individual and organization level to make sure that the content is useful and being used once the participants return to their respective organizations. However, the long-term effect of training remains a challenging area to evaluate.

Scenario Based Exercise

The Symposium also included an extended scenario-based exercise designed to stimulate discussion amongst the participants. Each exercise session comprised of a hypothetical video scenario with follow up facilitated questions with the audience and a panel of experts. The hypothetical scenarios are designed to demonstrate multiple failures of security culture and the problems that can arise from an inadequate regulatory environment. During the discussion, a number of key themes were covered, both internal and external to the organization, including developing appropriate insider threat mitigation programs, creating clear and robust security plans, and developing strong relationships with key stakeholders such as the regulator and first responders.

The initial scenario introduced a fictitious nuclear facility, Kiku Nuclear Fuels, where a new employee is preparing a shipment of nuclear material. The scenario examines the many and varied challenges and issues the employee comes across whilst preparing the nuclear shipment and introduces a terrorist group, Clan Yagami, that is a likely threat to the fictitious city and nuclear facility.

The participants noted that the following areas are important to ensure the safe shipment of nuclear fuels:

- Clear communication of the roles and responsibilities of all stakeholders in advance of the shipment
- Ensuring adequate preparation
- Developing procedures on how to share information and ensuring all knowledge is kept to approved individuals on a need to know basis
- Trustworthiness/insider threat programs must be in place to adequately vet all those involved in the shipment
- Ensuring clear and up-to-date threat assessments

When polled, the majority of the audience identified scheduling a pre-departure security meeting with all departments as the top priority, followed by ensuring the transport security plan was tested and validated, confirming the trustworthiness of all individuals involved in the shipment, requiring the use of encrypted communication and, lastly, conducting a table-top exercise of the contingency plan(s) for the shipment. Some participants noted that because all types of threats are constantly evolving, there should be more of an emphasis on requiring the use of encrypted communication than the poll shows. It was also mentioned that conducting a table-top exercise of the shipment and contingency plans is key in ensuring that the shipment plans are robust, and everyone knows how to respond if an incident occurs.

In the second hypothetical video scenario, the shipment of nuclear materials takes place with a few changes from the plan and is eventually intercepted by Clan Yagami during transport. It is shown that there was an insider in Kiku Nuclear Fuels, the supervisor of the new employee, who relayed information about the shipment to the terrorist organization. In the discussions following the video, the panelists weighed in on how they would know a truck was hijacked during transport. This depends on the material type, but there are a variety of ways, including driver contact, the truck diverts from the geofence causing an alarm, an escort could report the hijacking, the real-time

tracking system could show the truck is deviating from the route, if the vehicle did not show up on time, and others. In the Philippines, all category one and two materials have tracking mechanisms that are being monitored and that is how they would know if the truck was hijacked.

The participants were asked to rank the issues at Kiku Nuclear Fuels that would be easy for Clan Yagami to exploit. The majority of participants said that the careless protection of sensitive information and minimal/no vetting of new drivers were the easiest, followed by lack of a detailed transport security plan, weak regulatory compliance, and unreliable GPS equipment or transport trucks. The panelists agreed that the careless protection of information was the easiest issue to exploit and that the minimal or no vetting of drivers was also a significant issue. The panelist from the Philippines raised the issue of a lack of coordination with first responders, including law enforcement, which led to an inadequate response.

The group also discussed what actions should be taken after it is discovered that the shipment was hijacked. Though immobilizing the vehicle is an option to consider, there was a robust discussion around ensuring that this is the best response as it could cause more problems than it fixes. A question was also raised on who has the authority to immobilize a shipment. The participants also placed importance on notifying local law enforcement as the first step and that you want to get response going as quickly as you can from all of the organizations that have the responsibility to respond. In regard to informing the public, the panelists agree that generally the regulatory body, such as the US NRC and Romania's regulator, have a public affairs office that handles informing the public. It was also noted that contingency plans must be in place, not just for malicious acts, but also for other emergencies such as earthquakes.

Focus Areas

Laws and Regulatory Framework

In this session, participants were engaged in discussions on how to identify the good practices, common challenges, and possible solutions to transport security through laws and regulatory frameworks. The participants were asked to consider three objectives:

1. Discuss the role of a sound regulatory structure and how it may influence effective protection strategies of shipments.
2. Identify challenges and obstacles in implementing a comprehensive framework.
3. Discuss potential gaps or needs analysis as it pertains to developing or upgrading current regulations to align with current international guidance in order to achieve an effective transport security regime.

Participants for this small group interactive session were broken into three groups and asked to consider these objectives from the focus of a regulator, operator, and law enforcement personnel.

From the regulatory perspective, the participants discussed how effective coordination among competent authorities (e.g. regulator, operator, and law enforcement) is key to developing effective regulations. Some countries have multiple agencies that overlap in their functions. Developing

clear roles as well as communication procedures is necessary to effectively prepare for a transportation security event. Another good practice would be from the competent authorities to be mindful of the "3S" (security, safety, and safeguards) areas when forming regulations to make them more comprehensive and holistic. Many of the participants also brought up the presence of a high-level National Committee or Memorandum of Understanding (MOU) custom. These agreements and structures help the coordination of responders like firefighters, police forces, and others. This type of organization also allows for exercises to determine gaps between responders, competent authorities, operators, and others.

In the operator perspective session, participants discussed how clear requirements and guidance benefits not only the regulatory documents but also the implementation guidance for operators. One of the best ways to make regulations easier to understand for the operator is to consult operators in the drafting of regulations. Many countries already do this but toward the end of the drafting process. One suggestion was to incorporate the operators and other stakeholders more to increase the communication and, hopefully, improve the implementation and clarity of guidance. A major challenge identified in this session is the sharing of threat information. It is difficult for some threat information to be shared with the operators. This issue is mitigated in some countries due to operators being part of a government agency, but in countries where private companies are transporting materials, this continues to be a difficulty.

The participants in the law enforcement session discussed having a national CBRN Response Plan that would allow the different stakeholders an opportunity to communicate and prepare for a security response event. This helps law enforcement when they react to an event, it boosts communication with the regulator and gets multiple agencies together to create a plan. It also can help allow response agencies an opportunity to provide feedback to the regulator and have a say in the drafting of regulations. Another point of discussion was an MOU between the police and regulatory body to create a mechanism to allow communication and planning among response agencies. An issue that arose in this session was the fact that some countries do not have laws in place to criminalize the wrongful transport of nuclear and radioactive material. A lack of criminalization of these acts means that even if law enforcement detects or stops attackers, they are unable to do anything about it.

Physical Protection Systems and Response

In this session, participants were broken into small groups and engaged in discussions of physical protection systems (PPS) and response as it relates to transport security. The participants were asked to consider four objectives:

1. Discuss how an operator may analyze or assess the designed PPS (including response aspects).
2. Discuss key elements for enhancing PPS and response to a malicious event, including enhancement of detect, delay and response, communications, and interagency response.
3. Discuss how transport security responses may be incorporated into the National Response Framework.
4. Discuss how emerging technologies can strengthen an effective transport security regime and whether they may introduce vulnerabilities.

The participants identified numerous physical protection measures included to achieve detection, delay, and deterrence, including employing multiple layered systems, a verification process for PPS performance, having an effective inspections program and conducting rigorous multi-agency training exercises. All of these individual measures must be brought together to create a coherent system. However, it is important to remember that PPS requirements depend upon the country, material, and shipment profile.

Response capabilities identified in these sessions included coordination with law enforcement/security services (including EOD, escorts, and specialized response), conducting force-on-force exercises, creating awareness of National Response Frameworks, and ensuring a clear understanding of the roles and responsibilities of all parties (operators, regulatory bodies, military, and police). Many participants identified a need for further law enforcement training and cross-body training in search and recovery.

Some areas for further exploration include:

- Identifying measures that work at the interface of safety and security to save money and prevent repetition.
- Engagement with the regulator on contingency plans and the scenarios the contingency plans should cover.
- How are security responses incorporated into the National Response Framework?
- How can operators and regulators ensure that the 'need to know' basis is maintained whilst ensuring that enough information is shared to ensure appropriate responses? For example, how do you share information with first responders without compromising information security?
- How can those nations with less advanced capabilities ensure that the equipment they are buying is secure?

Insider Threats

In this session, participants were engaged in discussions of the role of information flow as part of a transport operation, the need for good operational security, and the ability to verify people's trustworthiness. The participants were asked to consider three objectives:

1. In the context of the video scenario, discuss the weaknesses that need to be addressed.
2. Give examples of vulnerabilities to transport security from an insider and/or the transfer of sensitive information.
3. Discuss what possible mitigation methods could be implemented to counter those issues, or what mitigation techniques are already being employed and showing success.

Participants for this small group interactive session were broken into three groups and asked to consider these objectives from the focus of a regulator, operator, and law enforcement personnel.

In the regulatory perspective session, participants identified that hypothetical video scenarios showed a lack of regulatory framework, which is required for all of the other parts of the shipment plan to fall into place. There also needs to be a validation of the regulatory framework to show that

it is in place by the operators and under inspection and control. Trustworthiness programs were also discussed, and these need to be laid out and in place to check employees. However, there is generally not a central background check among organizations and countries. Thus, what someone qualifies as being trustworthy may not qualify for someone else. Mitigation strategies are necessary to decrease the potential to have an insider threat and organizations should introduce a behavior observation program that tries to determine if there is something unusual going on with its employees. If an organization does not have a mindset of questioning itself, the process, the behavior of others, reporting, or being vigilant, it is tough to detect an insider.

The participants taking on an operator perspective discussed the need for safe and secure communications during the planning and executing of the shipment. These needs are to ensure that the information is properly compartmentalized for staff and to prevent potential insiders and outsiders from gathering the information. It was also discussed that it is important to look into training programs for new staff and to have personnel reliability programs that incorporate elements that mitigate employee dissatisfaction and identify possible employee conduct and characteristics that may place the employee or workplace in jeopardy of compromise (e.g. workplace, financial, or other).

The sharing of information with law enforcement is necessary so that they know the shipment is occurring and can respond or participant in the shipment accordingly. The organization and/or regulator has to determine how long in advance and which personnel it is appropriate to share information within law enforcement. The participants in the law enforcement perspective session also discussed that creating procedures and MOUs with law enforcement is important so that agencies and operators know their own roles and responsibilities in the transport and in case of emergency. Lastly, it was discussed that law enforcement can provide vetting processes and background checks as well as share relevant threat data with the operator.

Conclusion and Next Steps

At the conclusion of the Symposium, a shared commitment to keep the conversation on transport security going was agreed upon by the participants. INFCIRC/909 as it currently stands does have value in terms of raising awareness of transport security and allowing subscribers to show their willingness to engage with other subscribers. One of the key issues highlighted during the symposium was identifying the benefits to new subscribers to INFCIRC/909.

Closing panelists emphasized the importance of raising awareness about Transportation Security through existing international frameworks such as ICONS 2020, the IAEA Technical Meeting on Transportation Security in 2020, and the NSSC Network. These efforts are in addition to continued bilateral and multilateral exchanges to follow in 2020. Follow up exchanges will likely focus on areas of Transportation Security identified during the ITSS. The most common sub-topics of discussion throughout the ITSS were Regulatory Development and Implementation, Insider Threat Mitigation as it relates to transport, Information and Cyber Security, Physical Protection Systems, Response Capabilities to transport events and Conduct Training and Exercises. The next event for INFCIRC/909 related efforts will be a read-out of the ITSS during a side event at the ICONS 2020 meeting.

GMS Takeaways and Actions

Through the planning stages if the ITSS, GMS learned lessons that may prove useful for the planning of future regional and international events. One challenge that GMS faced that was specific to the ITSS was navigating the relationship with our partners in Japan. The interaction was necessary in this case due to the nature of Japan's lead role on INFCIRC/909. Due to lead role within the Japanese government by Japan's Ministry of Foreign Affairs' on INFCIRC/909, there was a level of deference from ISCN/JAEA to Japan's Ministry of Foreign Affairs. The wait for official approval at times caused delays in reviewing materials, approving the participants list, and sending out invitations. The GMS planning team found more success when it was able to handle these issues itself, which was evidenced by the successful coordination internally with GMS country and Regional Project Managers to identify and invite participants. For future exchanges, the ITSS team would recommend the GMS internal team to take the lead which should limit the delays in planning preparations. Furthermore, the planning team found more success reaching out to prospective participants directly, or through direct GMS counterparts, than going through official diplomatic channels.

The conduct of the ITSS demonstrated some key lessons learned. One positive outcome of the ITSS was the impact of breakout sessions. As detailed in the "Focus Areas" section above, the breakout sessions provided an opportunity for participants to engage where they might not have otherwise in the larger group sessions. The breakout sessions will be replicated in future Transportation Security Regional Events to encourage greater discussion. Also, one area that could be improved was the preparation for Bi-Lat meetings among the high-level GMS representatives at the event. Events like the ITSS are a great opportunity to accomplish face-to-face meetings, and in future it may be possible to procure a specific meeting room for pull-aside meetings. It will also be valuable to hold a dedicated pre-planning meeting for GMS to properly coordinate the side meetings.

GMS is already moving forward on the next steps following ITSS. The ICONS 2020 side event and the NNSA/JAEA Exchange on Next Steps occurred in February 2020 and laid out the path forward on Transport Security. A regional transport security event is planned to be hosted by Colombia from March 24-26, 2020, and another is planned to be hosted by Romania in September 2020. The IAEA Technical Meeting on Transport Security will be July 6-10, 2020, and the next IAEA International Training Course on Transport Security will be hosted by Japan in February 2021. The upcoming INS Expo will also highlight cooperation on Transport Security for GMS partners. In addition to these events, the ITSS has provided momentum for raising the profile of Transport Security among GMS peers and partners. The effort to continue this momentum includes gaining traction with both working level counterparts and high-level decision makers. A GMS goal that remains is to encourage more partner countries to become subscribers to INFCIRC/909. To reach that goal, GMS can build upon the ITSS by raising awareness and stressing the importance of Transport Security to counterparts, encouraging follow up events like those scheduled in Colombia and Romania, and engaging with the IAEA and other leading countries that can share their experience and expertise in areas of Transport Security.

Appendix I: List of Participating Countries

1. Argentina
2. Armenia
3. Bangladesh
4. Belarus
5. Cambodia
6. Canada
7. China
8. Colombia
9. Czech Republic
10. Egypt
11. France
12. Ghana
13. Hungary
14. India
15. Indonesia
16. Italy
17. Jordan
18. Kazakhstan
19. Kenya
20. Lao PDR
21. Malaysia
22. Mexico
23. Morocco
24. Nigeria
25. Philippines
26. Romania
27. Russia
28. Saudi Arabia
29. Spain
30. Ukraine
31. United Kingdom
32. Uzbekistan
33. Vietnam
34. United States
35. Japan
36. IAEA

Appendix II: IAEA Information Circular 909 (INFCIRC/909)

10 January 2017

Joint Statement on Transport Security of Nuclear Materials

Introduction

On the occasion of the Third Nuclear Security Summit held in The Hague, in the Netherlands, on March 24-25, 2014, the leaders of the participating States of the Transport Security Gift Basket, namely France, Japan, the Republic of Korea, the United Kingdom, and the United States, issued a Joint Statement to express their commitment to work together to further improve security in the transport of nuclear and other radioactive materials.

In the 2014 Joint Statement, the participating states of this Gift Basket expressed their intention to consider conducting table-top exercises for all transport modes (road, rail, maritime, and air) and proposed, among other actions, to share the good practices of above-mentioned activities with the International Atomic Energy Agency and other States while protecting sensitive information in order to actively contribute to the IAEA's drafting efforts of the Nuclear Security Series. The participating countries also stated that additional participating States were welcome, especially those that had experience in transport of nuclear materials.

On December 1-3, 2015 the above five countries, joined by Canada, Hungary, and Kazakhstan, met in Tokyo, Japan and committed to continuing the implementation of the 2014 Joint Statement. Furthermore, Japan, Kazakhstan, the United Kingdom, and the United States, with assistance from other participating States, produced four good practices guides for air, rail, road, and sea transport modes. Each of these guides is based on the way the lead country conducts its operations, so the subjects of emphasis vary from guide to guide. These four guides exemplify how these States implement the relevant international documents in their national systems, based on their experiences with and knowledge of the respective transport mode.

Initiatives

On the occasion of the Fourth Nuclear Security Summit held in Washington DC on March 31 to April 1, 2016, the Governments of Australia, Canada, Czech Republic, Finland, France, Hungary, Italy, Japan, Kazakhstan, Morocco, Spain, the Republic of Korea, Thailand, the United Kingdom, and the United States reaffirmed their will to further improve the overall security in the transport of nuclear and other radioactive materials and, in this regard, expressed their commitment to:

- Further exchanging national practices with other countries through the IAEA and the Global Initiative to Combat Nuclear Terrorism (GICNT). In this respect, the four "good practices guides," which are attached to this Joint Statement, may provide practical examples of how States can put into practice their international obligations and take into account international recommendations.

- Actively supporting the IAEA as the central organization for coordinating activities and developing guidance documents, and supporting the GICNT and the Global Partnership Against the Spread of Weapons and Materials of Mass Destruction in developing and implementing its activities, both of which are for the implementation of nuclear transport security obligations after the Nuclear Security Summit 2016.