International Journal of Nuclear Security

Volume 6 | Number 1 Article 8

7-6-2020

Challenges and Opportunities for Sharing Threat Information with Radioactive Materials Operators

Raphael Duguay
Canadian Nuclear Safety Commission

Challenges and Opportunities for Sharing Threat Information with Radioactive Materials Operators

Cover Page Footnote

The author wish to acknowledge the valued contributions and comments from Ali El-Jaby, Jodi Peloquin, Michael Beaudette, Patrick Adams, Craig Thompson, Fred Morris and Chris Englefield.

International Journal of Nuclear Security, Vol.6, No.1, 2020

Challenges and Opportunities for Sharing Threat Information with Radioactive Materials Operators

Raphaël Duguay

Senior Security Advisor, Nuclear Security Division

Canadian Nuclear Safety Commission (CNSC)

"All that is necessary for the triumph of evil is that good men do nothing." Edmond Burke

Abstract

Operators are required to implement security measures to address requirements set by the regulatory body or competent authority. These security requirements are generally based on the national threat level and information provided by the relevant law enforcement authority, intelligence agencies, and other relevant stakeholders. However, not all States can share this information with those who hold radioactive materials (e.g., operators), especially if they take a more prescriptive approach to regulation on security. The same situation often exists when a performance-based approach is used because there are multiple barriers that restrict the competent authority from sharing threat information. For example, competent authorities need to protect confidentiality and comply with national laws, regulations, and other information security considerations. In this paper, the author presents some challenges and opportunities relevant to exchanging threat information. The objective is to reflect on current practices, including good practices at the state and operator levels, to facilitate cooperation

between regulatory bodies and operators. The purpose is to increase awareness about the threats and techniques used by adversaries and to assist stakeholders in maintaining vigilance without compromising the security and confidentiality of the information.

1. Introduction

When protecting high-risk radioactive materials against malicious actors, it is important to implement security measures that are based on threats and potential consequences following a graded approach in relation to the overall level of risk. The International Atomic Energy Agency (IAEA) has developed a set of recommendations and guidance documents to help Member States develop and implement a nuclear security regime to adequately manage the safety and security of radioactive materials. Based on the IAEA Code of Conduct on the Safety and Security of Radioactive Sources ("The Code of Conduct") **[*1*]**, every state should define its domestic threats and assess their vulnerability with respect to the various materials used in the country. However, there are several challenges in sharing threat information. Some of these issues are related to confidentiality, the need to protect national security or trade secrets, and compliance with national privacy laws, regulations, policies, and directives. In addition, there are legal protection concerns such as copyrights, trademarks, and the general fear of losing control of the information. To share this type of sensitive information, the competent authority needs the consent of the owner as well as assurances from the receiver that they will not disclose this information without proper authorization. This last criterion often is harder to achieve because organizations need to develop and implement contractual arrangements and maintain trusting relationships will the relevant stakeholders. Therefore, it takes time, human and financial resources, and the will to work in collaboration with other stakeholders. In this paper, the author presents some challenges and opportunities to facilitate sharing threat information between regulatory bodies and operators. The objective is to enhance and strengthen awareness on current and evolving threats and techniques used by adversaries and to assist stakeholders in being better prepared to address the threats without compromising national security and confidentiality.

This paper focuses on the nuclear industry, and in particular, operators that use, store, and transport high-risk radioactive materials. It excludes nuclear power plants and other high security nuclear facilities because these operators usually have more resources to assess threats to their facilities and operations as well as established communication networks with government organizations, law enforcement agencies, and other intelligence security services. In this paper, the author assumes that the regulatory body is involved in the development of the domestic threat statement for the variety of radioactive materials used within its territory.

2. Definitions from IAEA Nuclear Security Series

- ***Representative threat statement (RTS)****:* A description of the motivations, intentions, and capabilities of potential adversaries that are less rigorous and formal than the approach used to establish a design basis threat **[*2*]**.
- ***Competent authority****:* A governmental organization or institution that has been designated by a state to carry out one or more nuclear security functions. For example, competent authorities

include regulatory bodies, law enforcement, customs and border control, intelligence and security agencies, and health agencies **[*3*]**.

- ***Design basis threat (DBT)****:* A comprehensive description of the motivations, intentions, and capabilities of potential adversaries against which protection systems are designed and evaluated **[*4*]**.
- ***Sensitive information****:* Information, in whatever form, including software, that the unauthorized disclosure, modification, alteration, destruction, or denial of use of could compromise nuclear security **[*5*]**.
- ***Threat assessment****:* An evaluation of the threats — based on available intelligence, law enforcement, and open material information — that describes the motivation, intentions, and capabilities of these threats **[*3*]**.
- ***Threat statement****:* A document that summarizes the threat assessment and has been modified to account for policy considerations. The DBT is an example of a threat statement (developed after extensive consultation in Member States) **[*6*]**.
- ***Threat information****:* To the extent the threat information is provided by the regulatory body, it describes the information in sufficient detail to indicate how the security system is designed to protect against both external and internal threats. Also indicates who is responsible for receiving threat information and how such information is shared with operator personnel who have a need to know **[*4*]**.

In this paper, the term "threat information" expands to include details about potential terrorist groups, criminals, or insiders that have the intent and/or are capable of conducting a malicious act with radioactive materials. This may include, for example:

- relevant information on the *modus operandi* or previous malicious acts
- lessons learned from security events or incidents
- security events or security information reported from competent authorities to operators and from operators to competent authorities
- guidance to enhance readiness and situational awareness of users, operators, and/or security personnel

3. International Threat Assessment Methods for Radioactive Materials

This section describes practices recommended by the International Atomic Energy Agency (IAEA) for conducting threat assessments for radioactive materials and how threat information may be integrated into regulatory frameworks.

The Code of Conduct **[*1*]**, the IAEA Nuclear Security Series (NSS) No. 14 *Nuclear Security Recommendations on Radioactive Material and Associated Facilities* **[*3*]**, and the revised IAEA NSS No. 11 *Security of Radioactive Materials* **[*4*]** mention that the Member State can use a domestic or national

threat assessment to determine credible motivations, intentions, and the capabilities of potential adversaries that could cause harm through the sabotage of a facility or the unauthorized removal of a radioactive material for malicious purposes. The State is responsible for undertaking the task of conducting a threat assessment. Different methods exist for assessing the threats at a strategic, operational, and tactical level. However, there is not an international standard or agreed minimum level of threat. Also, there is not a common international threat assessment method regarding international transport for high-risk radioactive materials. Because the responsibility for nuclear security rests entirely with the State, threats during international shipments of radioactive materials are harder to assess and must be considered in the shipment risk assessment. The responsibility for this risk assessment usually falls on the operator and must be verified and validated by the relevant competent authorities.

The information from the Threat Assessment can be used by a competent authority, such as a regulatory body, during the development, implementation, and maintenance of the security regulations and requirements for radioactive materials. However, this threat information is usually not specific to facilities and sometimes is too generic to provide relevant and useful information to operators responsible for physical protection programs at facilities and for transport.

Typically following a threat assessment, the Competent Authority will develop a design basis threat (DBT) to protect nuclear material and nuclear facilities. The DBT is a rigorous process that includes consultation with multiple organizations. It provides threat information on the motivation, capabilities, modus operandi, and tools used by a potential external and/or insider adversary. Implementing a DBT for radioactive materials requires more resources and is difficult to maintain for countries that are in the process of developing their regulations and have limited resources. The DBTs are considered a classified document by national competent authorities; therefore, it cannot easily be shared with private organization operators without proper information security arrangements, nondisclosure agreements, contractual arrangements, or an equivalent safeguard.

In the proposed revision of NSS No. 11, the IAEA recognizes the existence of Representative Threat Statements (RTS). An RTS follows a similar process as the DBT but is more flexible. In both approaches, the DBT and RTS could be used in developing regulatory security requirements for radioactive materials and could achieve the same goal. Figure 1 shows how threat information is used to define requirements for security systems.

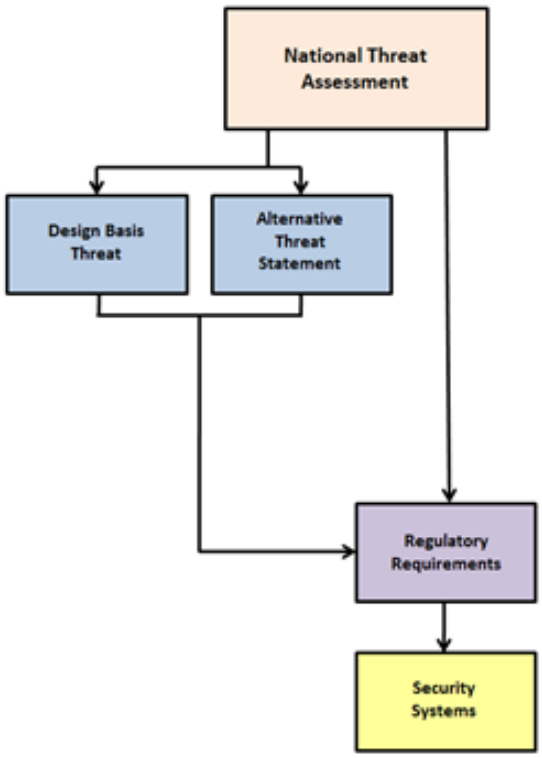

Figure 1: IAEA Revised NSS 11 Process for Using Threat Information

In both cases, there are also commonalities in using threat information to characterize the credible threats. For example, both DBTs and the RTS use a threat matrix or threat profiles. The difference is that a state may decide to use a DBT for nuclear materials and an RTS for other radioactive materials. The DBT can be used to protect materials and the RTS for lower risk materials. Also, during their development process, both documents may involve different organizations that are more relevant to the type of material. According to the IAEA, an RTS is typically used to develop a more prescriptive regulatory approach and requirements. The RTS is also considered to follow a less rigorous process.

Figure 2 is an example of a generic table of attributes and characteristics for hypothetical threats based on IAEA guidance documents and is not to be taken as a true illustration.

	Description of attributes and characteristics	**Terrorist group X**	**Criminal Group Y**	**Activists/ Demonstrators Group Z**
Motivation	*Political, financial, ideological, personal*	Political	Financial	Ideological/ Political
Level of commitment	*Disregard for personal health, safety, well-being, or survival (Choose from low to high.)*	High	Medium	Low
Intentions	*Unauthorized removal, material or facility sabotage, public panic and disruption, political instability, mass injuries and casualties, loss of*	Sabotage and theft	Theft	Disruption of activities, media

	reputation, unavailability of facilities, demonstrations (choose theft and/or sabotage)			attention, business reputation
Group size	*Attack force, coordination, support*	5-8	8-10	10-20
Weapons	*Types, numbers, availability, improvised*	Semi-automatics, handguns, explosives	Handguns, knives	Handheld tools, banners
Tools	*Mechanical, thermal, manual, power, electronic, electromagnetic, communications equipment*	Power tools, hand-held tools	Power tools, hand-held tools	Hand-held tools, masks, backpacks
Modes of transport	*Land, water, air; type, number, availability*	Land, 4 x 4	Land, 4 x 4	Land, 4 x 4, rental truck
Technical skills	*Engineering, use of explosives and chemicals, radiation protection, communication skills*	Basic, explosives	Basic	Basic knowledge of radiation protection
Computer skills	*Skills to compromise computer systems and components and the availability, integrity, and confidentiality of the data processed, stored, or forwarded in computer systems and components*	Low	Medium	High (hacking likely)
Knowledge	*Targets, site plans and procedures, security measures, safety and radiation protection procedures, operations, potential use of radioactive material*	Low	Medium	Low
Funding	*Material, amount, availability*	$10,000	unknown	Low, under $10,000
Insider issues	*Collusion, passive/active, violent/nonviolent, number of insiders*	Collusion, passive insider	Collusion, passive/active insider	Collusion with passive insider
Support structure	*Local sympathizers, support organization, logistics*	Unknown	Medium, local sympathizers	International fund-raising website
Tactics	*Covert and overt*	Both	Covert	Both

Figure 2: Generic Table of Attributes and Characteristics for Hypothetical Threats based on IAEA NSS 14 and 11

When developing security requirements for radioactive materials, a state may use a prescriptive approach, and the regulatory body may impose security requirements without sharing threat information with operators. A state may also wish to implement a performance-based approach where the responsibility of defining the threat and implementing mitigating measures is mostly on the operator. In this case, the operator has to submit their proposal to the competent authority and/or regulatory body for their approval. Operators are responsible to gather threat information from open materials, records of incidents, and from local police forces regarding local crime, past incident reports, or other sources of information. This can be a challenge for operators that do not have access to threat

information and have limited resources. Finally, States may choose to adopt a combined performance and prescriptive approach to protect radioactive materials. In all approaches, using threat information is a common vector, but there are challenges in sharing this information that will be explored in the following section.

4. Challenges for Sharing Threat Information

This section explores challenges for acquiring and sharing threat information between the different stakeholders, starting from the regulatory body to the operators' level.

A. National Sovereignty and National Security

Information regarding threats to national security is usually treated as sensitive and classified information under national laws relevant to public safety and national security. External stakeholders, such as an operator's staff, find it difficult to acquire threat information from the competent authority (e.g., national intelligence service, law enforcement agencies, regulatory body, etc.) because government rules for security clearance and requirements for handling secure information are not the same for the operators. The necessary level of security clearance, trustworthiness verification, and/or criminal background check required by national security regulations are directly related to the capability to receive, manage, and disseminate classified information on threats to radioactive materials.

In addition to these difficulties, some countries have conducted sabotage studies, vulnerability assessments, and other sensitive research on radioactive material attractiveness that cannot be shared with stakeholders because of their confidentiality. These studies identify weaknesses and vulnerabilities and are classified to maintain national security and protect global security.

B. Legal Provisions, Privacy Laws, and Regulations

National laws and regulations on information security usually dictate how to label, classify, and manage information for government agencies and other competent authorities. These requirements apply to public organizations but not necessarily to operators using radioactive materials. In some States, there are legal provisions for copyright protection, trademarks, and intellectual property that can pose additional barriers for sharing information.

Privacy laws and regulations can restrict the disclosure of private information with other organizations. All organizations are required to protect private information and implement protective measures to meet legal and regulatory requirements.

C. Administrative Arrangements

To protect threat information and maintain a trusting relationship among public and private organizations, contractual or written agreements are implemented between the parties for sharing sensitive information. Organizations may be required to implement memoranda of understanding and nondisclosure agreements as part of these arrangements. In addition, the competent authority or regulators must get consent from the owner of the information, usually a law enforcement organization,

before sharing it with private sector operators. These administrative and bureaucratic arrangements take effort and time to develop, implement, and maintain. They can slowdown the process for sharing timely sensitive threat information among stakeholders.

D. Other Barriers and Challenges

Challenges may also exist in sharing threat information within an organization. This can be caused by compartmentalization of classified information, business silos, poor security culture, and inadequate integration of security threats and risks in the organizational structure and the management decision process.

For small companies or public facilities like hospitals or universities, the operators may not have adequate resources to assess their threat environment and integrate this information in their physical protection program. Other challenges include:

- The presence of "optimism bias" contributes to the perception that this (i.e., threat to radioactive materials) won't happen to "us," making these additional efforts is not worth it or necessary.
- Public sector operators, such as universities, hospitals and medical facilities, have a strong organizational structure of transparency.
- Sharing information specific to one organization and compartmentalizing intelligence information with another: In some cases, the competent authority may decide to share threat information with one operator and not the entire industry to protect ongoing investigations and avoid spreading confidential information.
- Over-classification of information results from the absence of guidance on classification and inconsistent handling requirements. Also, data or information deemed classified by one organization may be considered unclassified by another due to subjectivity or misinterpretation of classing rules.
- Cleared individuals may lack experience in handling sensitive/confidential information resulting in them not understanding how to manage this information.
- A security clearance from one operator may not be compatible with the standard and requirements from another operator.
- The increasing use of the internet, emails, and electronic storage media and the need to protect confidentiality in a more digital environment is becoming more complex and expensive for some organizations.
- The lack of security culture and awareness on how to handle classified and sensitive information

According to Morris et al. (2013) **[*7*]**, there appear to be several reasons for the failure to fully appreciate the threats, including:

- The lack of a precedent leads to the assumption of low risk threat: "No one has successfully stolen a radioactive material and used it in a dirty bomb in a given state (or sabotaged a radioactive material in place)."

- In a state without a nuclear program, there may be no institutional infrastructure or familiarity with the applicable analytical methods to conduct a national threat assessment, design basis threat, or equivalent threat definition for radioactive materials.
- States which lack a significant domestic terrorist movement may simply adopt the view that "it can't happen here."
- A common perception is that radioactive materials are self-protecting – an inaccurate view given the increase in suicidal terrorist attacks and the willingness of potential adversaries to accept a lethal radiation dose and that such lethal doses may not be sufficiently incapacitating to prevent theft or sabotage. There is a misbelief that radiation is a deterrent and helps to prevent unauthorized removal because it will incapacitate the adversary. This statement is false, since malicious actors are ready to sacrifice their lives to conduct their attacks and that the radiation dose they may get will not immediately incapacitate them.

In addition to these challenges, the amount of effort and resources needed to share classified information with radioactive material operators is significant. It usually deters an organization's leaders from investing in human and financial resources because there are no data on the return on investment and how it can benefit the organization. It is also hard to measure the effectiveness of these programs, and there is little research or studies on their impacts. Fortunately, there are opportunities for implementing a collaborative framework with industry to share threat information. There are also good practices between public and private organizations that strengthen vigilance and information sharing. In the next section, we will explore opportunities and share some good practices that can facilitate the sharing of classified information.

5. Opportunities to Facilitate Sharing of Threat Information

There are multiple benefits in establishing a collaborative framework for exchanging information between public and private organizations.

Benefits	
Nuclear Regulator	**Radioactive Material Operators**
Increases communications and information sharing with industry representatives Assists in establishing a trusting relationship Encourages reporting of suspicious events Establishes more cooperation mechanism with relevant stakeholders	Increases awareness of potential threats to operations Increases vigilance Provides additional information that can be used to influence decision makers or enhance security measures Provides additional material that could be used in training, drills, and exercises

Figure 3: Table of Direct Benefits

Figure 3 identifies direct benefits for the regulator and the operators. There are also indirect benefits, such as increasing networking among security points of contacts, establishing cooperation against common threats or security issues, and increasing the knowledge and awareness of participants. The table excludes law enforcement agencies, custom border services, and security intelligence organizations since they already have established networks and mechanisms with private organizations to share threat information, including reporting of suspicious events. This is typically part of their intelligence mandate.

Some of the barriers identified in section B cannot be easily changed because they are linked to national sovereignty. Privacy laws and regulations, legal provisions, national security directives, and policies have to be followed when handling classified information to protect the confidentiality, availability, and integrity of the information. Therefore, compliance with these rules is required and should set the foundation of all cooperation and coordination arrangements between the public and private organizations.

To overcome institutionalized and administrative challenges for sharing sensitive or classified information, competent authorities can verify that persons receiving this information have a "need to know" based on their duties or related work activities. Also, they can require background checks, security clearance, or trustworthiness verification in accordance with national policy and be given guidance on how to protect this information from unauthorized disclosure. In addition, there are other alternatives identified in the lists below. The list identifies current good practices that exist to facilitate sharing threat information at the State and operator levels. It is not an exhaustive list. The intent is to share practical examples and alternatives that can enhance cooperation and communication.

E. Examples of Good Practices at the State Level

Practices	**Descriptions and Examples**
Institutionalized cooperation and coordination agreements	Establish good working relationships and arrangements to share sensitive information between the regulatory body and competent authorities, especially law enforcement and intelligence services. These arrangements can be formalized in a memorandum of understanding or other forms of written arrangements. Similar agreements can be implemented with industry operators or associations to share unclassified information. As a result, stakeholders follow national privacy laws and regulations as well as national security directives and other administrative and legal provisions.
Establish performance-based requirements for trustworthiness verification	In some states, multiple government programs require criminal background checks. This may be considered as equivalent to trustworthiness verification for operators. For example, as part of CNSC

and recognize other government security clearance programs	requirements, an individual that has unescorted access to high-risk radioactive sources needs to have a trustworthiness verification that includes a criminal record name check. This requirement also recognizes trusted travelers that undergo an FBI fingerprint verification and have a NEXUS card, or individuals that undergo criminal record verifications to get a valid firearms possession and authorization license.
Public/government security clearance sponsorship program for private industry	In Canada and the USA, there is the Information Sharing Network for Critical Infrastructure Protection that has programs to sponsor security clearance application from designated members of the industry with a security responsibility. The nuclear regulator may also sponsor private organization security clearance if they have a contractual agreement.
Establishing a National Nuclear Security Committee and/or working groups radioactive material security	Many States have national security committees that include representatives of industry operators and industry associations to increase the collaboration, cooperation, communication, and information for sharing on potential threats.
Participate with international and national networks that include industry representatives	There are many international organizations, such as IAEA, INTERPOL, Nuclear Security Contact Group, or state intelligence/policing services. Consideration should be given to using existing information sharing networks on radioactive materials. For example: Joining the IAEA Incident Trafficking database (ITDB), participating in the IAEA Working Group on Radioactive Material Security for national nuclear regulators, International Sealed Sources Suppliers and Producers Association (ISSPA), industry radiography associations, World Nuclear Transport Institute, etc. There are also national industry associations that can be leveraged to share information on recent nuclear security events, lessons learned, and good practices. During these meetings, the competent authority (ex: regulator or law enforcement agency) can provide unclassified information on current and emerging threats that can have an impact on operators.

Regular outreach, communication, and consultation to disseminate unclassified threat information	Conduct outreach and communication with relevant stakeholders periodically or on a regular basis with regard to threat information. This outreach can include annual or semi-annual intelligence discussions for staff and industry, conducted at the classified and/or unclassified level for stakeholder groups. Industry associations can invite representatives from the regulatory body and law enforcement to get updates on national threats or events that can have an impact on their operations.
Declassify sensitive information to an unclassified level	To be able to share threat information, law enforcement and intelligence services invest efforts in removing sensitive details and personal data to share unclassified information. This method is widely used to share laterally with other public law enforcement/government organizations and horizontally with industry security representatives or senior policy/decision makers. This is one of the most effective means of sharing threat information in a timely manner.
For international transport, establish bilateral/regional/multilateral agreements for sharing information between states	Recognition and promotion of cross-border security programs should be considered; for example, the Canada-USA-Mexico CT-PAT/PIP program provides benefits to members by getting access to security assessments and awareness sessions and facilitates international transport of radioactive materials across borders. Use pre-established communication methods with the Foreign Affairs Service for notification of international shipments. For example, embassy/diplomatic foreign affairs communication channels could be used to notify states when a shipment of category 1 radioactive material occurs that impacts their region. Example: Advance notification of maritime transport shipments to coastal states – using IAEA networks and nuclear security points of contacts for international information request.

Example of Good Practices at the Operator Level

Practice	**Description and example**

Implement an effective security program to protect radioactive materials and sensitive information	• Comply with national laws, regulations, and security requirements • Conduct a Threat and Vulnerability Assessment • Establish security and contingency plans • Implement security policies and procedures • Use the information from the national DBT or RTS to assess the effectiveness of physical protection measures • Establish drills and exercises program • Implement a security awareness program and training • Promote nuclear security culture • Report nuclear security events and other suspicious incidents
Participate industry contact groups, outreach activities, teleconferences, and workshops relevant to nuclear security for radioactive materials	These industry associations already exist and are very useful forums to exchange information. For example: International Sealed Sources Suppliers and Producers Association (ISSPA), Candu Owner Group (COG), and Nuclear Power Operations (INPO). There are also associations for specific industry groups, such as the Canadian Industrial radiography association (CIRCA), Canadian Radiation Protection Association (CRPA), etc. In some instance, these groups share sensitive information among stakeholders, including newsletters and bulletins.
Designate or delegate one individual or team on how to handle classified information	A private organization can identify, train, and designate one security point of contact. This function can also be delegated to another support group within the organization. This designated officer can undergo the security clearance process (e.g. trustworthiness verification) to be able to receive information from other organizations.
Designate a security outreach officer or point of contact (e.g. liaison officer)	Some organizations designate a security outreach officer to promote good security culture within the organization.
Consult and communicate with local law enforcement agencies	The local law enforcement agency can provide valuable support, including information on local crimes and threats. They often publish reports and criminal statistics, and they can be very useful for alerting the population in case of life-threatening events.

Leverage open source information on nuclear security	Hire a consultant or analyst or use open source information software and tools to gather relevant information on threats to physical, cyber, and personal assets in the nuclear industry.

As mentioned by the World Institute on Nuclear Security **[*8*]**, "It is the State's responsibility to obtain, collate and analyze threat information and ensure it is comprehensive and up-to-date. However, operators also have valuable contributions to make to the threat assessment due to their specialized knowledge of transport routes and potential problem areas that should be avoided; consequently, they should be encouraged to contribute to the process." The IAEA also published important guidance for States on the security of nuclear information [5] This document identifies specific considerations for sharing and disclosing sensitive information. An important guiding principle is the need to balance the benefit of sharing the information and the need for security. This is a golden rule to ensure organizations share relevant, accurate, and timely information without compromising confidentiality.

Another good practice is getting law enforcement organizations involved and increasing their awareness regarding the risks and threats to radioactive materials. Law enforcement communities are a great resource to share threat information. They are an important player in the nuclear security regime for response. Typically, law enforcement organizations have competing priorities and need to risk manage their resources. Operators may find it difficult to communicate with the right law enforcement officer or to get them involved in alarm response training or site familiarization. The regulator, as a public and governmental organization, can greatly influence the relationships with police and security forces. To follow international recommendations, national competent authorities should require operators to establish arrangements with local law enforcement agencies to facilitate alarm response and to ensure timely and effective deployment in case of a security event. As mentioned by Mr. John Buchanan **[*9*]** from the radiological and nuclear terrorism prevention unit with Interpol, "*Building relationships with all law enforcement stakeholders to fight the illicit smuggling of radiological and nuclear materials is essential.*" From his perspective, it is important to develop networks and connections and to strengthen multiagency partnerships to protect nuclear and other radioactive materials.

6. Analysis and Thoughts

The establishment of a "Nuclear Security Culture" is based on a belief that the threat is real and credible. Therefore, it is important that stakeholders are engaged in this discussion and establish industry contact groups. An important element of information sharing moves from the state to the operator, but just as important is information sharing from the operator to the state. For example, it is critical to share lessons learned from security incidents to enable competent authorities to collect and compile national threat data and analyze trends, methods, relationships, and hot spots. Security incident reporting by operators should be encouraged and/or required by the state through regulation. Outreach with the industry can also be used to share information on radioactive material security and to increase awareness of relevant stakeholders and decision makers without compromising confidentiality requirements

To help users and operators understand what they are protecting against, it is necessary to inform and educate them about the threats. Radioactive materials are used worldwide in several medical, research, and industrial sectors; the regulator should focus efforts to target these specific industries and associations to develop their networks. Communication already exists with licensing and compliance programs; therefore, nuclear security should be part of the overall communication strategy with operators.

When competent authorities communicate with operators to share relevant and accurate threat information effectively, it is important to set objectives and measure their effectiveness to report to senior and executive managers. This can include direct and indirect benefits in building trustful relationships with relevant stakeholders.

Operators need to stay vigilant and informed on the motivation, intention, and capacity of the adversary. Cooperation in this aspect through timely and continuous sharing and dissemination of threat information is of particular importance to improve radiological security.

To increase prevention and detection of potential adversary attacks on radioactive materials, it is necessary to test the capacity to share threat information with relevant stakeholders in an effective and timely manner through regular training, drills, or tabletop exercises. These communication channels are crucial when a reported security incident occurs, and they help to keep stakeholders and the public informed.

Finally, to enhance the relationship between nuclear regulators, competent authorities and industry representatives, in particular operators handling high-risk radioactive materials in the private sector, should implement institutionalized coordination and cooperation mechanisms. Theses forums should use contractual relationships **[*10*]** with written agreements and a formal memorandum of understanding to facilitate the exchange of threat information and promote nuclear security culture, good practices, and lessons learned among relevant industry stakeholders and front-line response organizations.

Communication, coordination, and cooperation are usually shared responsibilities among nuclear security stakeholders. Therefore, there is a need to unify efforts, get leadership support, and invest resources at the national level to make a positive change and to strengthen communicating threat information. These “3 C” principles were identified as keys to secure radioactive material globally at the International Nuclear Security Conference highlights in 2018. It may be time to move from a “need to know” approach to a “need to share” threat information between competent authorities and radioactive materials operators to strengthen communication and trust as well as empower further cooperation for nuclear security.

7. WORK CITED

1. International Atomic Energy Agency, *Code of Conduct on the Safety and Security of Radioactive Sources* (2004).

2. *Security in the Transport of Radioactive Material* (Internat. Atomic Energy Agency, Vienna, 2008), *IAEA nuclear security series Implementing guide*.

3. International Atomic Energy Agency, *Nuclear Security Recommendations on Radioactive Material and Associated Facilities* (IAEA, Vienna, 2011).

4. *Development, Use and Maintenance of the Design Basis Threat: Implementing Guide* (International Atomic Energy Agency, Vienna, 2009).

5. International Atomic Energy Agency, *Security of Nuclear Information: Implementing Guide* (2015).

6. International Atomic Energy Agency, *Objective and Essential Elements of a State's Nuclear Security Regime: Nuclear Security Fundamentals* (2013; http://www-pub.iaea.org/MTCD/Publications/PDF/Pub1590_web.pdf).

7. F. Morris, B. R. Reed, A. Murray, in *Proceedings of an International Conference* (International Atomic Energy Agency, Abu Dhabi, United Arab Emirates).

8. World Institute for Nuclear Security Academy, *Textbook for the WINS Academy Course Module on Transport Security Management* (WINS, Vienna, Austria, 2015).

9. International Atomic Energy Agency, Working Group of Radioactive Materials Security presentation from Mr. John Buchanan (2017).

10. T. J. Walsh, R. J. Healy, ASIS International, Eds., *Protection of Assets* (ASIS International, Alexandria, VA, 2011).