IAEA
International Atomic Energy Agency

Guidelines for the ITDB States’ Points of Contact

Vienna, December 2023

IAEA Services Series 49

IAEA SAFETY STANDARDS AND RELATED PUBLICATIONS

IAEA SAFETY STANDARDS

Under the terms of Article III of its Statute, the IAEA is authorized to establish or adopt standards of safety for protection of health and minimization of danger to life and property, and to provide for the application of these standards.

The publications by means of which the IAEA establishes standards are issued in the **IAEA Safety Standards Series**. This series covers nuclear safety, radiation safety, transport safety and waste safety. The publication categories in the series are **Safety Fundamentals**, **Safety Requirements** and **Safety Guides**.

Information on the IAEA's safety standards programme is available at the IAEA Internet site

www.iaea.org/resources/safety-standards

The site provides the texts in English of published and draft safety standards. The texts of safety standards issued in Arabic, Chinese, French, Russian and Spanish, the IAEA Safety Glossary and a status report for safety standards under development are also available. For further information, please contact the IAEA at: Vienna International Centre, PO Box 100, 1400 Vienna, Austria.

All users of IAEA safety standards are invited to inform the IAEA of experience in their use (e.g. as a basis for national regulations, for safety reviews and for training courses) for the purpose of ensuring that they continue to meet users' needs. Information may be provided via the IAEA Internet site or by post, as above, or by email to Official.Mail@iaea.org.

RELATED PUBLICATIONS

The IAEA provides for the application of the standards and, under the terms of Articles III and VIII.C of its Statute, makes available and fosters the exchange of information relating to peaceful nuclear activities and serves as an intermediary among its Member States for this purpose.

Reports on safety in nuclear activities are issued as **Safety Reports**, which provide practical examples and detailed methods that can be used in support of the safety standards.

Other safety related IAEA publications are issued as **Emergency Preparedness and Response** publications, **Radiological Assessment Reports**, the International Nuclear Safety Group's **INSAG Reports**, **Technical Reports** and **TECDOCs**. The IAEA also issues reports on radiological accidents, training manuals and practical manuals, and other special safety related publications.

Security related publications are issued in the **IAEA Nuclear Security Series**.

The **IAEA Nuclear Energy Series** comprises informational publications to encourage and assist research on, and the development and practical application of, nuclear energy for peaceful purposes. It includes reports and guides on the status of and advances in technology, and on experience, good practices and practical examples in the areas of nuclear power, the nuclear fuel cycle, radioactive waste management and decommissioning.

GUIDELINES FOR THE ITDB STATES' POINTS OF CONTACT

The following States are Members of the International Atomic Energy Agency:

AFGHANISTAN
ALBANIA
ALGERIA
ANGOLA
ANTIGUA AND BARBUDA
ARGENTINA
ARMENIA
AUSTRALIA
AUSTRIA
AZERBAIJAN
BAHAMAS
BAHRAIN
BANGLADESH
BARBADOS
BELARUS
BELGIUM
BELIZE
BENIN
BOLIVIA, PLURINATIONAL STATE OF
BOSNIA AND HERZEGOVINA
BOTSWANA
BRAZIL
BRUNEI DARUSSALAM
BULGARIA
BURKINA FASO
BURUNDI
CABO VERDE
CAMBODIA
CAMEROON
CANADA
CENTRAL AFRICAN REPUBLIC
CHAD
CHILE
CHINA
COLOMBIA
COMOROS
CONGO
COSTA RICA
CÔTE D'IVOIRE
CROATIA
CUBA
CYPRUS
CZECH REPUBLIC
DEMOCRATIC REPUBLIC OF THE CONGO
DENMARK
DJIBOUTI
DOMINICA
DOMINICAN REPUBLIC
ECUADOR
EGYPT
EL SALVADOR
ERITREA
ESTONIA
ESWATINI
ETHIOPIA
FIJI
FINLAND
FRANCE
GABON
GAMBIA
GEORGIA
GERMANY
GHANA
GREECE
GRENADA
GUATEMALA
GUINEA
GUYANA
HAITI
HOLY SEE
HONDURAS
HUNGARY
ICELAND
INDIA
INDONESIA
IRAN, ISLAMIC REPUBLIC OF
IRAQ
IRELAND
ISRAEL
ITALY
JAMAICA
JAPAN
JORDAN
KAZAKHSTAN
KENYA
KOREA, REPUBLIC OF
KUWAIT
KYRGYZSTAN
LAO PEOPLE'S DEMOCRATIC REPUBLIC
LATVIA
LEBANON
LESOTHO
LIBERIA
LIBYA
LIECHTENSTEIN
LITHUANIA
LUXEMBOURG
MADAGASCAR
MALAWI
MALAYSIA
MALI
MALTA
MARSHALL ISLANDS
MAURITANIA
MAURITIUS
MEXICO
MONACO
MONGOLIA
MONTENEGRO
MOROCCO
MOZAMBIQUE
MYANMAR
NAMIBIA
NEPAL
NETHERLANDS
NEW ZEALAND
NICARAGUA
NIGER
NIGERIA
NORTH MACEDONIA
NORWAY
OMAN
PAKISTAN
PALAU
PANAMA
PAPUA NEW GUINEA
PARAGUAY
PERU
PHILIPPINES
POLAND
PORTUGAL
QATAR
REPUBLIC OF MOLDOVA
ROMANIA
RUSSIAN FEDERATION
RWANDA
SAINT KITTS AND NEVIS
SAINT LUCIA
SAINT VINCENT AND THE GRENADINES
SAMOA
SAN MARINO
SAUDI ARABIA
SENEGAL
SERBIA
SEYCHELLES
SIERRA LEONE
SINGAPORE
SLOVAKIA
SLOVENIA
SOUTH AFRICA
SPAIN
SRI LANKA
SUDAN
SWEDEN
SWITZERLAND
SYRIAN ARAB REPUBLIC
TAJIKISTAN
THAILAND
TOGO
TONGA
TRINIDAD AND TOBAGO
TUNISIA
TÜRKİYE
TURKMENISTAN
UGANDA
UKRAINE
UNITED ARAB EMIRATES
UNITED KINGDOM OF GREAT BRITAIN AND NORTHERN IRELAND
UNITED REPUBLIC OF TANZANIA
UNITED STATES OF AMERICA
URUGUAY
UZBEKISTAN
VANUATU
VENEZUELA, BOLIVARIAN REPUBLIC OF
VIET NAM
YEMEN
ZAMBIA
ZIMBABWE

The Agency's Statute was approved on 23 October 1956 by the Conference on the Statute of the IAEA held at United Nations Headquarters, New York; it entered into force on 29 July 1957. The Headquarters of the Agency are situated in Vienna. Its principal objective is "to accelerate and enlarge the contribution of atomic energy to peace, health and prosperity throughout the world".

IAEA SERVICES SERIES No. 49

GUIDELINES FOR THE ITDB STATES' POINTS OF CONTACT

INTERNATIONAL ATOMIC ENERGY AGENCY
VIENNA, 2023

Marketing and Sales Unit, Publishing Section
International Atomic Energy Agency
Vienna International Centre
PO Box 100
1400 Vienna, Austria
fax: +43 1 26007 22529
tel.: +43 1 2600 22417
email: sales.publications@iaea.org
www.iaea.org/publications

For further information on this publication, please contact:

Information Management Section
International Atomic Energy Agency
Vienna International Centre
PO Box 100
1400 Vienna, Austria
Email: Official.Mail@iaea.org

GUIDELINES FOR THE ITDB STATES’ POINTS OF CONTACT
IAEA, VIENNA, 2023
IAEA-SVS-49
ISSN 1816-9309

Printed by the IAEA in Austria
December 2023

FOREWORD

Established in 1995, the Incident and Trafficking Database (ITDB) is the IAEA’s information system on incidents of illicit trafficking and other unauthorized activities and events involving nuclear and other radioactive material out of regulatory control.

The ITDB facilitates the exchange of authoritative information on relevant incidents among States on a voluntary basis, which assists participating States and international organizations to combat illicit nuclear trafficking and to strengthen nuclear security. The information provided by participating States, which is collected in the database, is analysed to identify common trends and patterns, to assess threats and to evaluate weaknesses in material security, as well as in detection capabilities and practices. The ITDB is an essential component of the information platform supporting the implementation of the IAEA’s Nuclear Security Plan.

IAEA Nuclear Security Series No. 15, Nuclear Security Recommendations on Nuclear and Other Radioactive Material out of Regulatory Control, provides recommendations on international cooperation that specifically relate to information exchange mechanisms such as the ITDB. However, the IAEA has not published any guidelines on the details of how the database’s information is managed and exchanged on a national level. States participating in the ITDB programme have expressed the need for such guidelines.

This publication addresses these topics and provides suggestions for integrating the programme into a national nuclear security regime. It has been developed for explanatory purposes only and its application is not mandatory. The descriptions are not intended to interfere with other IAEA and States’ obligations outlined in relevant conventions and agreements. In particular when a State reports an incident to be included in the database, such reporting will not release the State from any other obligations or arrangements for reporting information about incidents involving nuclear or other radioactive material to the IAEA. These include, for example, obligations under the Convention on Early Notification of a Nuclear Accident, the Convention on Assistance in the Case of a Nuclear Accident or Radiological Emergency, IAEA safeguards agreements, State systems of accounting for and control of nuclear material, and the Convention on the Physical Protection of Nuclear Material and its Amendment.

These suggestions were compiled by experts in the IAEA with the assistance of Member States. The IAEA officers responsible for this publication were J. Garcia Sainz and A. Gredinger of the Division of Nuclear Security.

EDITORIAL NOTE

This publication has been prepared from the original material as submitted by the contributors and has not been edited by the editorial staff of the IAEA. The views expressed remain the responsibility of the contributors and do not necessarily represent the views of the IAEA or its Member States.

Guidance and recommendations provided here in relation to identified good practices represent expert opinion but are not made on the basis of a consensus of all Member States.

Neither the IAEA nor its Member States assume any responsibility for consequences which may arise from the use of this publication. This publication does not address questions of responsibility, legal or otherwise, for acts or omissions on the part of any person.

The use of particular designations of countries or territories does not imply any judgement by the publisher, the IAEA, as to the legal status of such countries or territories, of their authorities and institutions or of the delimitation of their boundaries.

The mention of names of specific companies or products (whether or not indicated as registered) does not imply any intention to infringe proprietary rights, nor should it be construed as an endorsement or recommendation on the part of the IAEA.

The IAEA has no responsibility for the persistence or accuracy of URLs for external or third party Internet web sites referred to in this publication and does not guarantee that any content on such web sites is, or will remain, accurate or appropriate.

CONTENTS

1. INTRODUCTION

1.1. BACKGROUND

Since its inception in 1995, the Incident and Trafficking Database (ITDB, the “Database”) has been a reliable information system for voluntary information sharing among its participating States and the International Atomic Energy Agency (IAEA) regarding incidents[1] involving nuclear and other radioactive material out of regulatory control. Provision of this information to the IAEA falls under the purview of the national ITDB points of contact (PoCs) who are responsible for providing reports of incidents to the ITDB secretariat at the IAEA (the “secretariat”). PoCs receive information and reports about illicit trafficking and other unauthorized activities involving nuclear and other radioactive material out of regulatory control produced by the secretariat. They also facilitate the national response to secretariat enquiries on specific incidents.

1.2. OBJECTIVE

The purpose of this publication is to:

- Describe all relevant elements of the ITDB programme (the “programme”)[2];
- Assist participating States in designing and implementing approaches, within the context of the programme, for the collection, analysis and dissemination of information on incidents involving nuclear and other radioactive material out of regulatory control at the national level with PoCs of other States and with the IAEA;
- Describe the roles and responsibilities of PoCs and the practices that empower them in exercising their roles and responsibilities;
- Assist PoCs with collecting relevant information from multiple sources, transmitting such information to the secretariat and sharing the programme’s analytical outputs with their respective competent authorities on a need-to-know basis in accordance with the recommendations contained in Refs [1, 2];
- Provide an overview of information management between the secretariat and States’ PoCs (“ITDB network”, the “Network”) by describing the practices and processes of the ITDB programme.

Thus, this publication provides guidelines for the programme that supports participating States in meeting recommended nuclear security practices on a national level, through enhancing their awareness of the benefits of the comprehensive reporting to, and the analysis provided by, the Database. It assists States and their national PoCs and complements the ITDB Terms of Reference (ToR) and Conceptual Framework.

1.3. SCOPE

This publication addresses the IAEA’s ITDB information exchange mechanism and specifically its processes and benefits for nuclear security purposes. It provides a general introduction to the

[1] An incident within the scope of the ITDB (hereinafter referred to as ITDB incident) is an event arising under any of the circumstances described in the ITDB’s Conceptual Framework, which identifies, among other things, incident types relating to nuclear or other radioactive material out of regulatory control. The types of ITDB incidents are listed in Appendix II and in the Glossary of this publication.

[2] “ITDB programme” refers to the programme of activities associated with administering the database.

programme and its fundamental concepts, procedures for becoming a participating State, the nomination process of PoCs, with specific references regarding their roles and responsibilities, with an overview of the tools that are available to PoCs and other authorized users.

Any nuclear or other radioactive material that goes out of regulatory control may represent an actual, potential or perceived radiological hazard to human health, society and the environment. Therefore, while not within the scope of this publication, the PoCs should be well acquainted with their States' obligations and arrangements associated with nuclear and radiological emergency response, in order to understand and assist, as appropriate, with necessary obligatory or voluntary actions, including notifications and reporting.

These include the principal (but not necessarily exclusive) obligatory or voluntary reporting arrangements related to IAEA safeguards agreements; States' systems of accounting and control of nuclear materials; the Convention on the Physical Protection of Nuclear Material (CPPNM) and its Amendment [3]; the Convention on Early Notification of a Nuclear Accident and the Convention on Assistance in the Case of a Nuclear Accident or Radiological Emergency [4]. They also include associated operational arrangements in accordance with IAEA Safety Standards No. GSR Part 7, Preparedness and Response for a Nuclear or Radiological Emergency[3] [5], and those governed by the Operations Manual for Incident and Emergency Communication (EPR–IEComm 2019) [6]. Specifically, the Unified System for Information Exchange in Incidents and Emergencies (USIE) is the secure 24/7 IAEA website for designated contact points in IAEA Member States to exchange urgent information during nuclear or radiological incidents and emergencies, regardless of whether they arise from accident, negligence or deliberate act.

The ITDB reporting system is entirely separate and independent from the above mentioned mechanisms, tools and arrangements for information exchange, communication and transmission of information.

Throughout this publication, there are certain terms that are used and intended to be interpreted in the context of the programme and that also have connotations or actual definitions associated with response to nuclear and radiological emergencies. In such cases, this publication will provide a clarification of the definition for use under the programme upon the first use of the terms as well as in the Glossary.

1.4. STRUCTURE

Following the introduction in Section 1, Section 2 describes the history and structure of the ITDB programme, including its purpose and scope, its Conceptual Framework and the consultation process within it.

Section 3 presents the necessary information for joining, and the benefits of participation in, the ITDB programme.

Section 4 explains the procedures for the appointment of PoCs and alternate PoCs. It also includes the necessary references to their desired competences and technical capabilities.

[3] GSR Part 7 [5] establishes requirements for ensuring an adequate level of preparedness and response for a nuclear or radiological emergency, irrespective of its cause.

Section 5 provides advice on the empowerment of the PoCs. It does so by situating the ITDB programme in the context of the national nuclear security regime and by describing the requirements for PoCs to fully exercise their responsibilities.

Section 6 depicts the main roles and responsibilities of PoCs.

Section 7 provides references for the information exchange in the ITDB programme, including States' reporting in a complete, comprehensive and timely manner. Additionally, this Section describes how the secretariat shares ITDB information with international and regional partners as well as relevant national competent authorities.

Section 8 describes the existing information tools developed by the secretariat that are available to PoCs and other authorized users through the IAEA Nuclear Security Information Portal (NUSEC).

Appendix I presents the historical milestones of the ITDB programme. Appendix II contains the grouping of types of incidents as defined by the Conceptual Framework. Appendices III, IV and V include information exchange models for reporting incidents to the Database, for sharing information with national stakeholders and for a national network.

The Annex contains three templates (sample letters) for requesting participation in the ITDB programme, nomination of PoCs and alternate PoCs, and updating contact details. These templates can serve as a reference for States' competent authorities.

2. THE HISTORY AND STRUCTURE OF THE INCIDENT AND TRAFFICKING DATABASE

2.1. HISTORY

The last decade of the twentieth century saw the first documented cases of nuclear smuggling, a new phenomenon that represented a serious threat to international peace and security. Member States turned to the IAEA for assistance, and, at the March 1995 meeting of the Board of Governors, the Director General presented a report on Measures Against Illicit Trafficking in Nuclear Materials and Other Radioactive Sources (GOV/2773/Add.1) [7]. The Board thereupon requested the Director General to carry out the proposed activities, including the development of a reliable database of information on incidents of illicit trafficking, to assist Member States and to better inform the public. In August 1995, Member States were notified that the IAEA was prepared to accept information on illicit trafficking incidents and begin issuing periodic summary reports. The IAEA invited States to indicate their interest in participating in the programme and to identify their PoCs.

In March 2002, the ITDB — known as the Illicit Trafficking Database prior to 2012 — was identified as an integral part of the Director General's report on IAEA's plan of activities for Protection Against Nuclear Terrorism: Specific Proposals (GOV/2002/10) [8]. The collection, evaluation, use and dissemination of information on illicit trafficking in nuclear and other radioactive material was recognized as a key contribution to the development and implementation of measures to help strengthen nuclear security worldwide and prevent nuclear and radiological terrorism.

The Database continues to play an important role in the implementation of the IAEA's Nuclear Security Plans and the IAEA nuclear security programme.

2.2. PURPOSE AND SCOPE

The purpose of the ITDB has not changed substantially since its inception in 1995 and, as described in its current ToR, serves the following purposes:

(1) Assist States with the timely[4] exchange of authoritative information on incidents involving illicit trafficking and other related unauthorized activities involving nuclear and other radioactive material;
(2) Maintain and analyse reported information with a view to identifying common threats, trends and patterns; to assist States in determining what actions may need to be taken with respect to particular events or to help formulate policy towards combating illicit trafficking of such materials; and support the IAEA's nuclear security activities;
(3) When appropriate, to provide a reliable source of basic information to the media concerning trafficking incidents by providing authoritative information about such events.

In 2000, the Database's scope was expanded to include not only the illicit trafficking of nuclear and other radioactive material, but also other unauthorized activities involving such materials. This change in the scope was one of the recommendations on the reporting of incidents contained in the meeting report of the PoCs meeting of 15–17 November 2000. The current ToR reflect the expanded scope. They include, but are not limited to, incidents involving illegal trade and movement of nuclear or other radioactive material across national borders. They also cover incidents involving unauthorized acquisition (e.g. through theft), supply, possession, use, transfer or disposal of nuclear and other radioactive material, whether intentionally or unintentionally, with or without crossing international borders. The scope also covers unsuccessful or thwarted acts of the above type, as well as the loss of material and the discovery of uncontrolled material. States are also encouraged to report scams — that is, incidents involving the intentional offering for sale of benign material that is purported to be nuclear or otherwise radioactive.

The importance of the expanded scope is evident by the adoption in 2012 of "Incidents of nuclear and other radioactive material out of regulatory control" as the official subtitle for the ITDB.

2.3. CONCEPTUAL FRAMEWORK

Owing to the Database's expanded scope, in 2006, the secretariat began to categorize incidents into three groups for communication and analysis purposes. However, this initial grouping did not provide a clear indication as to which incidents were related, or potentially related, to trafficking. Providing an indication of trafficking is considered an important objective, since

[4] The use of the term 'timely' in the ToR should be understood as the shortest possible time that is necessary for an PoC to obtain sufficient (accurate and comprehensive) information about an ITDB incident that will allow the PoC to complete an incident notification form and submit it to the secretariat. The ToR encourage States to provide, if possible, information on an incident within 24 hours. While this is a targeted reporting time frame, it is rarely accomplished in practice. See additional information on this in Section 7.1.

the original rationale for establishing the Database was its function as a repository of information related to trafficking.

Progress towards this objective was hindered for many years because of difficulties in developing a suitable definition of 'trafficking' for the Database's purposes. In 2015, an appropriate definition was developed that provided the basis for designing a new system consisting of three groups for categorizing incidents based on whether they were related, potentially related or unrelated to trafficking (or malicious use).

A Conceptual Framework that integrated the above fundamental concepts was agreed to at the triennial meeting of the PoCs at IAEA Headquarters in Vienna on 28–31 July 2015. The three principal elements on which the Conceptual Framework was established are: (1) a definition of trafficking for ITDB communication purposes only; (2) the categorization of reported types of incidents into three groups; and (3) a list of types of incidents that indicate their relationship to the aforementioned three groups and the supporting reporting guidelines for incidents.

As described in the Conceptual Framework, the new categories of incident types are the following:

- Group I: incidents that are, or are likely to be, connected with trafficking or malicious use;
- Group II: incidents of undetermined intent;
- Group III: incidents that are not, or are unlikely to be, connected with trafficking or malicious use.

Additional information regarding the group structure, including associated types of incidents as defined in the Conceptual Framework, can be found in Appendix II.

2.4. CONSULTATION PROCESS WITHIN THE PROGRAMME

The programme is implemented by the secretariat based on the IAEA Statue and Nuclear Security Plans and in accordance with the Database's ToR. The secretariat regularly consults with PoCs on issues related to the implementation of the programme, including review of its priorities, draft analysis reports and changes to administrative procedures. PoCs provide important feedback regarding the day-to-day operation of the programme and are encouraged to do so on their own initiative as well as when requested by the secretariat. Additionally, the secretariat regularly convenes Triennial PoCs meetings, in order to review past activities and define future priorities. Changes to the ToR are the responsibility of the participating States and the IAEA Secretariat, as appropriate.

3. PARTICIPATION IN THE INCIDENT AND TRAFFICKING DATABASE PROGRAMME

3.1. BENEFITS OF PARTICIPATION

By joining the programme, participating States are able to receive information on incidents reported by other States, access analysis reports and become part of the ITDB network.

The secretariat notifies all PoCs when a new incident is reported, which allows participating States to share all or part of the reported information with their national competent authorities, including those associated with nuclear security response activities such as law enforcement, border guards and customs, or intelligence agencies, as appropriate.

Access to the Database by PoCs and other authorized users is obtained through the NUSEC ITDB restricted area (see Section 8). This access is provided effectively through the users' personal access to the IAEA secure servers in the Internet domain. Access to ITDB officially confirmed data allows PoCs to, inter alia:

- Raise and maintain an enhanced situational awareness among national competent authorities and stakeholders;
- Contribute to national threat assessments, design basis threat and Integrated Nuclear Security Support Plans (INSSP) development and review;
- Identify seized material by cross-checking identification markings or through image comparison;
- Prepare case studies for training based on realistic scenarios.

The Network has become increasingly valuable as the Database demonstrates how nuclear or radioactive materials are leaving regulatory control far from the points at which they are subsequently detected. In this context, the Network may complement other international and regional security information exchange initiatives[5] and contribute to spreading knowledge and good practices in relation to the detection of, and response to, nuclear security events involving nuclear and other radioactive material out of regulatory control, as well as nuclear or radiological emergencies involving such materials. The Network offers unique collaboration opportunities. In addition to the support provided by the secretariat, States' PoCs may also seek support from their peers in other States to share or obtain additional information on relevant specific incidents, particularly when their respective States may be affected by the same or similar incidents. This improves the PoCs' knowledge of specific incidents and their causes so that they can swiftly assess current incidents and suggest measures to prevent further occurrences.

The secretariat regularly organizes PoCs training activities to enhance the familiarity of PoCs with the ITDB reporting system as well as the benefits obtained from the use of its products; to familiarize PoCs with necessary actions to collect data for the submission of incident reports to the Database; and to assist the PoCs in the subsequent dissemination of ITDB data to their network of national competent authorities. These activities also acquaint new PoCs with the ITDB's information exchange practices and reporting procedures and tools.

3.2. PARTICIPATION BY STATES

Joining the ITDB programme is a process that is open to all States on a voluntary basis, regardless of whether or not they are Member States of the IAEA.

States wishing to join the programme need to submit the formal nomination, by post or email (official.mail@iaea.org), to the IAEA Division of Nuclear Security through the official

[5] Relevant international networks and resources include the Geiger database, an analytical platform that collates law enforcement data on incidents involving radiological or nuclear material maintained by the International Criminal Police Organization (INTERPOL). Other regional information exchange initiatives include the specialized working group on illicit trafficking of nuclear and other radioactive material of the Southern Common Market (MERCOSUR), the CBRN Working Group of the European Explosive Ordnance Disposal Network (EEODN) managed by the European Law Enforcement Agency (EUROPOL) and the European Union Agency for Law Enforcement Training (CEPOL).

channels (i.e. Permanent Mission, Ministry of Foreign Affairs, or a national competent authority for nuclear security matters). The Annex contains three templates (sample letters), which could be used as a reference, for requesting participation in the programme, nomination of PoCs and alternate PoCs and updating contact details.

In addition to a point of contact, States are encouraged to nominate one alternate point of contact who may represent the same or a different national competent authority. Information on the programme, the procedures for accessing the NUSEC ITDB restricted area and for reporting incidents will be sent to the officially nominated PoCs.

Participation in the programme does not entail an obligation on the part of the participating State to report incidents in the scope of the Database. However, and as recommended in existing IAEA nuclear security guidance [1], the Database may be used by States to report cases of nuclear security events involving nuclear or other radioactive material or seizures thereof in accordance with their international obligations and national legislation, without prejudice to States' obligations and arrangements associated with nuclear and radiological emergencies involving nuclear or other radioactive material, IAEA safeguards agreements, State systems of accounting and control of nuclear material) and the CPPNM and its Amendment, as specified in Section 1.3. Reported incidents need to be categorized by three groups, in accordance with the ITDB Conceptual Framework. Appendix II describes the types of incidents to be reported and provides detailed examples and guidelines to facilitate the reporting of incidents.

States that are not participating in the programme may also report incidents to the Database through their national competent authorities and have done so in the past. However, these States do not receive, and cannot access, ITDB data, since that information is only available to officially nominated PoCs, other authorized users, participating States and relevant international organizations.

3.3. PARTICIPATION BY INTERNATIONAL ORGANIZATIONS

International organizations with roles and responsibilities within the scope of the ITDB may request participation in the programme. Such organizations can access a limited and predefined amount of information. Interested international organizations need to send a letter to the IAEA's Division of Nuclear Security that identifies the scope of their activities under which they wish to cooperate with the ITDB programme and assigns their PoCs. The secretariat will determine if the request for participation is granted. The secretariat will send information to the eligible organization's PoCs regarding the programme, the procedures for accessing the NUSEC ITDB restricted area and the tools and products accessible to the organization.

Participating international organizations may be invited to attend ITDB outreach activities and contribute to the development of specific projects or products. They may also be invited to attend parts of the triennial PoC meetings as observers.

4. SELECTION OF INCIDENT AND TRAFFICKING DATABASE POINTS OF CONTACT AND ALTERNATE POINTS OF CONTACT

As specified in the ToR, each State participating in the programme needs to appoint an official with the appropriate managerial and technical capabilities and competences to serve as a point of contact or alternate point of contact. The PoCs should be empowered with the appropriate authority, resources and infrastructure to fulfil their duties and be available to do so.

PoCs will provide reports of incidents to the secretariat, receive information and reports produced by the IAEA and be able to provide answers to the secretariat to enquiries on specific incidents.

The point of contact could be assisted by an alternate point of contact from the same or another relevant competent authority for better information management coordination, control of information dissemination and reporting. If a State needs to nominate more than one point of contact or alternate point of contact, effective coordination among them at the national level is required in regard to reporting to the secretariat and to disseminating ITDB information nationally, in order to avoid the duplication of efforts or prevent any inaction and to minimize the possibilities of processing conflicting information from various PoCs acting independently from each other.

Information on incidents in the scope of the ITDB may be considered classified within a national information security policy. For this reason, States need to ensure that the point of contact and alternate point of contact are cleared to process classified information and reports with relevant State competent authorities and that relevant national processes are adhered to.

4.1. COMPETENCES AND TECHNICAL CAPABILITIES

PoCs need to have expertise and experience in nuclear security. A scientific or technical background in nuclear related sciences is an advantage. Overall, the PoCs need to seek the following competences and technical capabilities:

- Basic knowledge of technical aspects of nuclear security, such as detection instruments, radiation measurement units and radiation protection terminology;
- Knowledge of national governmental structures and of legislation and activities in nuclear security;
- Working experience in international nuclear security programmes and initiatives;
- Ability to identify, analyse and collate requisite information for submitting comprehensive incident reports;
- Ability to identify information needs from stakeholders;
- Good report writing skills;
- Adequate computer skills;
- Good team player skills;
- Good command of the English language.

Prospective or new State PoCs are encouraged to participate in the International Training Course for New and Prospective PoCs for the ITDB.

5. EMPOWERMENT OF THE INCIDENT AND TRAFFICKING DATABASE POINTS OF CONTACT

5.1. THE INCIDENT AND TRAFFICKING DATABASE PROGRAMME IN THE CONTEXT OF THE NATIONAL NUCLEAR SECURITY REGIME

When a State applies for participation in the programme, consideration needs to be given to integrating this new activity into its national nuclear security regime. The programme should not be implemented as a stand-alone activity. A State may collaborate or have agreements with other States or international organizations for the exchange of nuclear security information.

These arrangements and other factors need to be considered when identifying the most appropriate authority that will take the lead for the programme. Moreover, participation in the programme allows States to fulfil the nuclear security recommendations in Ref. [1] that recommends that States should provide information concerning any loss of control over nuclear or other radioactive material with potential transboundary effects to potentially affected States through bilateral or multilateral mechanisms. Additionally, PoCs should keep in mind relevant State obligations under the international legal instruments related to the nuclear and radiological emergencies involving nuclear or other radioactive material out of regulatory control, IAEA safeguards agreements, State systems of accounting and control of nuclear material and the CPPNM and its Amendment, as outlined in Section 1.3 and foreseen in Refs [3–5].

In accordance with the nuclear security recommendations specified in Ref. [9], PoCs should be part of States' competent authorities and have adequate authority, competence and resources to fulfil their assigned responsibilities. Furthermore, States need to ensure that PoCs have access to information from other competent authorities and governmental organizations on incidents in the scope of the Database and that they are informed in a timely manner of such incidents [9]. To this end, States need to ensure that all authorities actively involved in the programme collaborate in the exchange of information. This collaboration should preferably be formalized through suitable arrangements that identify competent authorities and stakeholders and their roles and responsibilities with appropriate procedures for an effortless flow of information. Nuclear security recommendations specified in Ref. [2] encourages States to consider establishing suitable arrangements to enable them to participate in international information exchange such as the ITDB for the purpose of reporting nuclear security events. Formal information exchange arrangements involving PoCs will allow States to address this recommendation. Depending on the State system, such provisions could be included in the national legislation or implemented through other agreements between authorities (e.g. memoranda of understanding, cooperation agreements). This formalization will ensure continuity in the information management process among the involved entities irrespective of the persons responsible for it at any given time.

In some cases, States may designate a contact point to cover multiple reporting or communication functions. These may comprise the roles of ITDB PoCs and PoCs under the arrangements for a nuclear and radiological emergency [3–5], including information exchange via USIE, as described in Section 1.3. Providing information to the IAEA through the ITDB or USIE is the prerogative of the State and will be decided on a case-by-case basis by the State, taking into account the purposes of both systems. Because nuclear and other radioactive material out of regulatory control is the primary concern of both information exchange systems, in the situation where the PoCs are from different organizations, States are encouraged to ensure an open and active dialogue between them in order to maximize the potential for information exchange and to ensure 24/7 information exchange in an emergency. PoCs may also have other reporting responsibilities, including those under IAEA safeguards agreements, as well as State systems of accounting and control of nuclear material and the CPPNM and its Amendment. Where PoCs do not have formal reporting responsibilities, there may be a need for them to ensure that the appropriate national authorities are informed of relevant ITDB incidents.

5.2. EMPOWERMENT

Since PoCs report incidents on behalf of their respective State, they need formal authority to fulfil their tasks such as data collection, reporting incidents, informing other national competent authorities or negotiating new developments of the programme. Specifically, they need to:

- Be formally recognized within the State as the official focal point with the legal ability to liaise with the IAEA on ITDB matters and interact with the national competent authorities to collect, process, analyse, report and share information in the scope of the ITDB;
- Represent the State when communicating with the secretariat and within the Network, including the transmission of information as well as taking a position regarding the developments and implementation of the programme;
- Have the authority to submit reports to the Database in a timely manner;
- Communicate with other States' PoCs (e.g. bilaterally) in case of ITDB incidents with international nuclear security implications;
- Facilitate the dissemination of ITDB information to the national competent authorities and other stakeholders with a role in nuclear security;
- Promote the Database nationally through training and other awareness activities as required, including engaging other national authorities to participate in regional or international ITDB outreach activities.

There is a need to have formal arrangements within participating States to describe the roles and responsibilities of the PoCs in a way that allows them to fulfil their tasks. However, States are responsible for determining the procedures on how these tasks are to be accomplished.

6. ROLES AND RESPONSIBILITIES

PoCs represent an important element of a nuclear security information exchange system at both the national and international levels. As described in the ToR and explained in this publication, the responsibilities of PoCs are not limited to reporting incidents to the Database; they also help to build and maintain national nuclear security networks for information exchange purposes.

The main responsibilities and activities of PoCs may vary depending on their specific position within a State's nuclear security system and the support available from both their own agencies and other competent authorities. Consequently, PoCs may delegate or share some of their following main responsibilities:

- Lead the information exchange process with the secretariat, submitting accurate and complete incident reports in a timely manner and update reports if appropriate.
- Promote and help to maintain a practicable national ITDB incident reporting mechanism and guidelines to ensure completeness, comprehensiveness and timeliness of incident reporting.
- Ensure coordination among national competent authorities and other stakeholders in disseminating appropriate ITDB information and analysis frequently within the national network.
- Foster and encourage ITDB incident reporting behaviour within competent authorities and other stakeholders.
- If possible, establish and maintain a national registry of incidents in the scope of the Database that includes both reported and unreported incidents. Unreported incidents could include incidents for which the PoCs are still gathering information or waiting for clearance for reporting to the secretariat. This registry will facilitate a smooth transition for future PoCs and is a valuable resource for the evaluation of the national situation. It also assists in producing analyses and trend reports, as required.

- Manage access permissions of national authorized users, other than the PoCs, to the NUSEC ITDB restricted area. This includes replacing, granting or revoking users' access rights when the responsiblities of national authorized users change.
- Actively participate in national coordination meetings at which the PoCs can promote and raise awareness of ITDB activities and exchange related information within the national nuclear security network.
- Regularly participate in ITDB meetings and workshops to foster a desired level of nuclear security information exchange and coordination with other States' PoCs as well as contribute to the implementation of ITDB projects and activities.
- Be familiar with the existing functions and tools in the NUSEC ITDB restricted area which PoCs can use to access data and manage information exchange.
- Ensure that law enforcement agencies are included in the information exchange network, since these agencies may report incidents that they are investigating only to judicial authorities. Therefore, these incidents may not be brought to the attention of the PoCs.

Since the PoCs may receive information on a single incident from multiple sources, they need to coordinate with each reporting authority and agree on what information may be shared with the ITDB according to established national procedures.

If there is more than one national point of contact, it is recommended for each State to have a single person responsible for overall management of the programme and to coordinate the response to the secretariat for reportable incidents, as well as to coordinate any document review, comments, feedback or questions regarding the States' programme.

7. NUCLEAR SECURITY INFORMATION EXCHANGE

The ITDB information exchange framework comprises four main data flows:

(1) Reporting by States (PoCs) to the secretariat;
(2) Information sharing among States' PoCs;
(3) Information sharing by the secretariat with States and other partners;
(4) Information sharing by States' PoCs with national competent authorities and other stakeholders.

States' PoCs should be able to communicate with all relevant national competent authorities to allow for information exchange on incidents in the scope of the ITDB. This would allow the PoCs to learn about relevant incidents promptly and officially; collect the necessary information and transmit it to the secretariat; and provide feedback, advice and analysis to the information providers, as appropriate.

As stated in the ToR, all disseminated or shareable ITDB data is for States' official use only. Therefore, the PoCs or other national competent authority should unequivocally inform the recipients about this restriction when disseminating such data. Recipients of data within a State should be restricted to the officials of national relevant authorities with a role and responsibility in nuclear security that justifies their need-to-know and access to such data. A State should not make other States' data publicly available without prior consent of these other States.The IAEA publicly shares limited aggregated information about ITDB statistics through the factsheet, which is published at the beginning of each year on the IAEA website. The factsheet contains aggregated general statistics on the number of incidents reported to the Database. Statistics taken from the Database are also published in reports submitted to the IAEA Board of Governors and General Conference, such as the IAEA Annual Report and the Nuclear Security Report, which are made public in accordance with the usual practice for these documents.

7.1. COMPLETENESS, COMPREHENSIVENESS AND TIMELINESS

Reporting to the Database should be aligned with its scope in accordance with the Conceptual Framework and its reporting guidelines, which provide the necessary details regarding the information needed in an incident report.

Complete, comprehensive and timely reporting are the main elements that characterize effective reporting to the Database. The secretariat provides advice and guidance to PoCs on reporting practices in general, and in particular on the use of the online reporting tool and its standard reporting forms (online incident notification forms WebINF and Batch WebINF) to report and update incidents if appropriate.

States need to submit an incident report when they have sufficient information available on the incident. It is the responsibility of the PoCs to ensure that all relevant information that is to be reported (subject to information security requirements of the State) is included in the WebINF. At a minimum, the following information (Part 1 of the WebINF) should be identified, together with a basic narration of the incident facts for the incident summary (Part 2 of the WebINF), to submit an incident report:

- Date of the incident;
- Location of the incident;
- Incident group;
- Type of incident;
- Material involved in the incident, if available;
- Information of whether the material was recovered, seized or otherwise placed under regulatory control.

Timely reporting is encouraged, especially when there is evidence or suspicion that an ITDB incident has potential international nuclear security implications. This could be the case of nuclear or other radioactive material detected in trafficking incidents that involve citizens of various nationalities or when the origin of the seized materials is unknown. It could also apply to orphan sources detected in unauthorized shipments along international supply chains when the materials detected in one State have originated from, or passed through, third States undetected. The PoCs need to make every effort to report incidents with potential nuclear security links to other States as soon as practicable, in particular when there is evidence of trafficking or malicious use[6]. Timely reporting allows for timely analysis. While reporting of historical events has benefits to States when considering what may happen in the future, it is more beneficial to analyse incidents in their actual spatial and situational contexts, which are time dependant.

[6] However, the ITDB is not designed and implemented as an alert system or an emergency response tool. See Section 1.3 for further reference on obligatory and voluntary reporting via USIE of the nuclear and radiological emergencies involving nuclear and other radioactive material outside of regulatory control.

The PoCs need to ensure that previously reported incidents are updated when new information becomes available. This is particularly important for incidents involving material that was out of regulatory control but later recovered; when the correct identification of seized material entails a lengthy analytical process; or when the prosecution of a criminal case delays the release of key information on the exact type of material involved in an incident (Part 1 of a WebINF) or of other relevant circumstantial information (Part 2 of a WebINF). This updated information is important for the ongoing analysis of ITDB data.

7.2. REPORTING BY STATES TO THE SECRETARIAT

The data flow covered in this section concerns information transmitted by States to the secretariat and comprises incident reports and related technical information.

Since information about incidents in the scope of the ITDB may originate from various sources, it is important that information about these incidents reach the national PoCs in a timely manner. Upon verification, data consolidation and authorization to transmit the information, PoCs are expected to report the incidents in question to the secretariat through the standard ITDB incident notification form. Therefore, a functioning national network is important to support the necessary information exchange needed by the programme.

When building a national network, the State needs to identify not only the PoCs, but all other competent authorities that may receive information on incidents relevant to the ITDB. Their number and characteristics will depend on the national nuclear security regime and may include the following:

- National authority for nuclear and other radioactive material (e.g. regulatory authority);
- National border control authority reporting centre or focal point for nuclear and radiological incidents;
- National, regional or other law enforcement agencies (especially those responsible for the detection of, and response to, incidents involving nuclear or other radioactive material out of regulatory control);
- Intelligence services personnel concerned with nuclear or radiological incidents and related investigations;
- National, regional or other emergency response organizations with a role in detecting or responding to incidents involving nuclear or radiological material out of regulatory control, including those responsible for identifying characteristics of material out of regulatory control or responding to transport related incidents;
- Relevant facilities (e.g. hospitals) that possess nuclear or other radioactive material in use, storage or transport or where such materials are likely to be detected when out of regulatory control (e.g. metal recycling companies).

PoCs should provide information to approved entities on the reporting needs (e.g. types of incidents, material involved) to ensure effective and comprehensive ITDB incident reporting. Since the above mentioned competent authorities have different roles, responsibilities and capabilities in nuclear security, each of them is likely to detect different types of incidents. Therefore, PoCs may need to apply different approaches to their national competent authorities and other stakeholders. For further reference on this, see the information exchange models included in Appendix III. PoCs may use or adapt the existing ITDB incident notification form, including its translation into their national language as necessary, for facilitating their collection of relevant data on incidents in the scope of the ITDB and its transmission among national competent authorities and other stakeholders.

It is the State's responsibility to ensure that procedures on reporting and information-sharing thresholds are established between the above mentioned competent authorities and the PoCs. If these procedures are not established, the PoCs should identify necessary competent authorities to develop these procedures and work to implement these partnerships. This includes, in particular, those incidents that are subject to judicial investigations. Information-sharing requirements in these incidents may include timely sharing of minimum data (e.g. Part 1 of a WebINF) and identifying the information that may be suitable for an updated incident report at a later stage. An example of suitable information may include details regarding the types of perpetrators (e.g. thief, terrorist), their intent and the status of the law enforcement investigation that may have been considered sensitive information from a national perspective at the time, or shortly after, the incident occurred. Personal information of perpetrators or individuals involved in an incident should be excluded from an ITDB incident report.

Ideally, the PoCs should have access to a registry or database of national incidents. If the national registry is wider than the scope of the ITDB, then Database reportable incidents should be clearly identified in the registry. The ITDB online reporting tool automatically stores all submitted incident reports and any subsequent updates. This functionality provides PoCs with a registry of their incidents submitted via WebINF without the need to create one. However, a State may need more information than the one contained in the online reporting tool. Therefore, only a national registry or database would fulfil all national needs.

PoCs should ensure that they are included in other incident reporting or related networks to aid them in identifying domestic incidents that may be relevant to report to the Database. The PoCs may also wish to look into whether any regional systems exist that may have information of other reportable incidents.

7.3. INFORMATION SHARING AMONG STATES' POINTS OF CONTACTS

The data flow covered in this section concerns bilateral and multilateral collaboration among States. Information exchange with the secretariat does not exclude bilateral or multilateral contacts. These could be important especially with neighbouring States. The secretariat maintains an updated list of States' PoCs available in the NUSEC ITDB restricted area and remains available to support PoCs as necessary. Furthermore, the secretariat promotes regional cooperation and networking through the organization of regional workshops and other training events.

In some regions, there are collaboration initiatives that have been developed to strengthen nuclear security regionally and that can support the work carried out by the PoCs. If compatible with their function, States' PoCs may consider developing or cooperating with international meetings, working groups and initiatives that support bilateral or multilateral information sharing with other States and organizations relevant to the ITDB.

Information exchange does not need to be limited to other PoCs in the region. If a State has reasons to believe that another State may be able to assist in providing information in relation to an investigation involving nuclear or other radioactive material out of regulatory control, it may be beneficial to engage in bilateral information sharing to support the investigation. For instance, if an investigation reveals that such material originated in another State prior to discovery outside of regulatory control in the PoCs' State, the PoCs network can prove a valuable tool for sharing information with relevant foreign competent authorities. These competent authorities may assist the investigation to identify how the material in question arrived within the reporting State and whether it did so through authorized transportation. These relationships can also be beneficial to prevent double entries that involve the same incident to the Database and coordinate information exchange to assist and improve the overall quality of the incident report.

7.4. INFORMATION SHARING WITHIN THE IAEA SECRETARIAT, WITH STATES AND OTHER PARTNERS

The data flow covered in this section concerns information transmitted from the secretariat to the participating States and international organizations, as well as internally within the IAEA Secretariat (i.e. the Department of Safeguards and the Incident and Emergency Centre in the Department of Nuclear Safety and Security). Appendix III illustrates this specific information flow.

All participating States, the IAEA's Department of Safeguards and the Incident and Emergency Centre receive the full incident reports as submitted by the reporting State. In some cases, the reporting State has restricted the dissemination of Part 2 of the incident report due to the sensitivity of the information. In such cases, only Part 1 of the incident report is incorporated into the ITDB analysis and shared with participating States and internally within the IAEA until the reporting State lifts the restriction on Part 2 data. The participating international organizations receive only Part 1 of the incident report in all cases as set forth in the ToR.

The secretariat shares quarterly bulletins on analysis products with participating States and international organizations. However, the biennial analysis report is only shared with States, since it includes information from Part 2 of the incident reports that is not shared with international organizations.

Both participating States and international organizations have access without restrictions to the ITDB Dashboard within the NUSEC ITDB restricted area. This tool does not include information from Part 2 of the incident reports.

Additional information on ITDB incidents is shared through lectures or presentations delivered by the secretariat to promote the programme and to raise awareness on the security concerns of nuclear and other radioactive material out of regulatory control.

7.5. INFORMATION SHARING BY STATES' POINTS OF CONTACT OF THE INCIDENT AND TRAFFICKING DATABASE WITH NATIONAL COMPETENT AUTHORITIES AND OTHER STAKEHOLDERS

The data flow covered in this section concerns information received from the secretariat that is forwarded by States' PoCs to the national competent authorities in their respective national networks. It may include incident reports, analysis reports and other ITDB data reports as agreed between States' competent authorities and other relevant stakeholders.

Comprehensive information sharing for providing and receiving information entails a two-way exchange between PoCs and their national competent authorities and other stakeholders. Information sharing should not be restricted to just information being received by the PoCs from national competent authorities and other stakeholders. The distribution of information from the PoCs to national stakeholders is also important. Information sharing by the PoCs can greatly support relationships with national competent authorities and other stakeholders and encourage continued support and improvement of both national nuclear security interests and the programme.

PoCs play a key role in raising and maintaining awareness nationally on incidents reported through the Database by disseminating information to their national networks in accordance with their established practices. PoCs may directly retrieve and circulate ITDB information through internal communication channels. Alternatively, PoCs can also grant representatives of other competent authorities access to the NUSEC ITDB restricted area. Presently, up to five national users, including the point of contact and alternate point of contact, can have access to the restricted area, which provides sufficient access to the main competent authorities. PoCs should ensure that appropriate information-sharing arrangements are implemented with alternate PoCs, authorized users and other national competent authorities.

PoCs should make certain that ITDB data shared within their national competent authorities and other stakeholder networks is relevant to the competent authorities involved. For example, some States may choose to adopt information models that share particular incidents or events with specific competent authorities and other stakeholder groups[7]. Some competent authorities and other stakeholders may only need to receive Group I or II incidents or incidents that have domestic or regional impacts.

Since ITDB information is for official use only, PoCs should ensure that this information is shared only with persons and organizations which meet this requirement and that its further dissemination is controlled effectively. Furthermore, PoCs should ensure that additional national users with access to the NUSEC ITDB restricted area remain active and access rights are revoked if appropriate.

8. INCIDENT AND TRAFFICKING DATABASE RELATED INFORMATION TOOLS

8.1. INTRODUCTION TO THE IAEA NUCLEAR SECURITY INFORMATION PORTAL (NUSEC)

The secretariat uses NUSEC as the communication channel with its PoCs and authorized users. NUSEC is a secure, centralized and interactive web environment that is designed to strengthen the nuclear security community worldwide by facilitating communication and providing the most up-to-date information on the IAEA's activities related to nuclear security. It is a non-public, password-protected online platform through which Member States and other IAEA partners can showcase their nuclear security activities, including publications and contact details. NUSEC provides access to specialized IAEA resources and data on multilateral and national activities of relevance to its various user groups, which also showcase all activities relevant to the IAEA's Division of Nuclear Security. All NUSEC authorized users may access the unrestricted part of each of these user groups to view an introduction to the topic, background documents and contact details of the respective managers.

[7] Canada has incorporated two information dissemination groups. One group mostly comprising law enforcement, intelligence and border officer contacts receive information on Groups I and II ITDB incidents which have, or may have, a connection to trafficking or malicious use. A second smaller group receives information on Groups I, II, and III ITDB events to ensure that all events are reviewed for lessons learned and good practices by other reporting states.

8.2. REGISTRATION IN THE IAEA NUCLEAR SECURITY INFORMATION PORTAL

Membership to NUSEC is open to all government officials from IAEA Member States and relevant international organizations that are nuclear security professionals or are involved in IAEA nuclear security activities. The registration process involves three steps:

(1) Creation of a NUCLEUS user account;
(2) Request access to NUSEC;
(3) Request access to specific NUSEC user groups, if applicable.

NUCLEUS (Step 1) is the common access point (single sign-on system) to the IAEA's scientific, technical and regulatory information resources. NUCLEUS is available to the public with access limited to free and unrestricted IAEA resources. Access to NUSEC (Step 2) is granted by the portal administrators upon verification of the user profile and the user's justification for access to nuclear security information. Access to NUSEC user groups (Step 3) is granted by the respective managers of the user groups.

The secretariat confirms the permissions of all PoCs for the NUSEC ITDB restricted area. Once PoCs have been granted access, they can then independently manage the access rights of additional national users to a maximum of five individuals per State, including the PoCs and alternate PoCs (see Section 7.5). PoCs can manage their national users' access rights through a specific tool that is included in the NUSEC ITDB restricted area (see Section 8.4).

8.3. THE RESTRICTED AREA OF THE INCIDENT AND TRAFFICKING DATABASE IN THE IAEA NUCLEAR SECURITY INFORMATION PORTAL

All ITDB products and tools produced and maintained by the secretariat are accessible through the NUSEC portal.

PoCs and other authorized users are granted access to resources within the NUSEC ITDB restricted area, which offers the following benefits:

- Since NUSEC is a password protected secure portal that obliges authorized users to log in through individual user profiles, information is disseminated via secure means to a restricted community of users;
- Better control of information dissemination on a national basis, since access is personalized to authorized users that include PoCs and other national users whose access rights are managed by their respective PoCs;
- Additional information is available to PoCs and other authorized users at all times through the ITDB Dashboard, a tool designed to retrieve ITDB data;
- The online reporting tool (WebINF) allows PoCs to securely report, update and review their respective incidents.

Access to the NUSEC ITDB restricted area has an additional layer of security that consists of a two-factor authentication. Authorized users have the following two options for two-factor authentication:

(1) Receive a numerical code by email sent to the email address linked to the user's NUCLEUS account.
(2) Generate the code with one of the many publicly available authenticator applications (e.g. Google Authenticator).

8.4. CONTENTS OF THE RESTRICTED AREA OF THE INCIDENT AND TRAFFICKING DATABASE IN THE IAEA NUCLEAR SECURITY INFORMATION PORTAL

PoCs and authorized users can access a wide range of ITDB products and tools that vary depending on the specific user profile. There are three different profiles:

(1) User of the secretariat;
(2) Member State user;
(3) International organization user.

Users at the secretariat have access and editing rights to all content, the ability to create or remove additional pages and manage all users' access rights. Member States' users have access to all products and tools, and PoCs can manage the access rights (i.e. grant or revoke access) of their respective national authorized users. Users from international organizations have limited access that includes only Part 1 of submitted incident reports, quarterly bulletins, ITDB Dashboard, Access Management (for their respective officials), the PoC Monitor and ITDB events. The page contents of the NUSEC ITDB restricted area, as available to States' PoCs and other authorized users, is summarized below. If a page is not available to PoCs from international organizations, it is noted in the description.

8.4.1. Recent Incident Notification Forms

It contains the electronic copies of all incident reports submitted by States; they are displayed in chronological order by month, from most recent to oldest. This page does not contain all incident reports submitted to the Database throughout its history. Once the secretariat publishes a quarterly bulletin, all incident reports included in that analysis product are removed from this page. However, PoCs and authorized users who are interested in any of the incident notification forms that are no longer available in this page may obtain an electronic copy from the secretariat upon request. This page is not available to users from international organizations.

8.4.2. International organizations' view of Incident Notification Forms

It contains Part 1 of all incident reports submitted by States with the same characteristics and limitations explained under 'Recent incident notification forms' above. This page is where users from international organizations can access Part 1 of submitted incident reports in accordance with the ITDB dissemination policy.

8.4.3. Points of Contact List

It contains one document in PDF format – the list of States' PoCs – which is regularly updated by the secretariat.

8.4.4. Quarterly Bulletins

It contains all published quarterly analysis bulletins for the past five years. PoCs and authorized users who are interested in any of the quarterly analysis bulletins that are no longer available on this page may request a copy from the secretariat.

8.4.5. Analysis Reports

It contains all published analysis reports since 2003. The analysis reports are conducted on a biennial basis. The reports are archived chronologically by reporting period and remain available for download. Additionally, the secretariat uses this page to post analysis reports on major public events (MPEs) that can be downloaded by the PoCs of the State hosting the MPE. These reports are produced exclusively for the PoCs of the host State and are available only to the host State for a limited amount of time. Reports on MPEs are removed when the host State's PoCs confirm that they have downloaded them. This page is not available to users from international organizations.

8.4.6. Draft Analysis Reports

It contains the draft biennial analysis reports posted by the secretariat that are under review by PoCs. PoCs can then download the report, review it and post their comments in this page. This page remains empty when no draft report is being reviewed. This page is not available to users from international organizations.

8.4.7. Incident and Trafficking Database Dashboard

This page allows authorized users to search, retrieve and compare statistical data. This is done through a simplified interface containing a data search screen with 13 parameters that can be combined to conduct complex searches. Search results are presented either in a tabular format (tab 'Data') or a graphic display (tab 'charts').

The search screen incorporates a button to run the search (labelled ‘Search’) and a button to clear the selected search parameters (labelled ‘clear’). Since this interface allows for combined searches, search parameters added to a search may be deselected individually. The button labelled ‘clear’ is useful when users wish to start from a blank screen after building a complex search involving many different parameters. The search screen includes the following 13 parameters:

(1) IAEA key: this is the unique reference number automatically generated by the database and assigned to each recorded incident. Incidents are automatically assigned a serial number that begins with the year and month in which the incident is recorded in the database and ends with a three-digit sequential number starting at ‘001’. Users can search for specific incidents by its unique reference number.
(2) Incident date: this is the date when the incident occurred as reported by the State. Users can search by a specific date or by a date range.
(3) INF date: this is the date when the incident notification form (INF) is submitted to the secretariat. The WebINF tool sets this date automatically to the actual submission date by PoCs. Users can search by a specific INF submission date or by a date range.
(4) Incident group: this allows users to search incidents by the groups (i.e. Groups I, II and III), in accordance with the Conceptual Framework. Users can combine any of the three groups in a single search.
(5) Incident type: this allows users to search incidents by any of the 14 types of incidents defined in the Conceptual Framework, some of which comprise completed and attempted subtypes. For example, ‘unauthorized trade’ applies to a completed illegal sale or purchase of nuclear or other radioactive material, and ‘attempted unauthorized trade’ applies to acts of the same nature that were prevented, typically as a result of law enforcement activity. Users can combine any of the 14 types of incidents in a single search.
(6) Region: this allows users to search incidents by the region in which they have occurred. There are six predefined regions: Africa; North and Latin America; Eastern Europe; Western Europe; Middle East and South Asia; and Southeast Asia, Pacific and Far East. Users are not able to combine the regions in a single search.
(7) Country: this allows users to search by the country that reported the incident (i.e. the country under whose jurisdiction the reported incident occurred). Users can combine any countries in a single search.
(8) Material involved: this allows users to search incidents by type of material involved: nuclear, radioactive, or radioactively contaminated or other material (RCOM). Users can combine any of the three types of material in a single search.
(9) Type of material: this allows users to further filter material involved by subtypes. Nuclear material subtypes include: plutonium, thorium, depleted uranium, natural uranium, high enriched uranium (HEU), low enriched uranium (LEU), uranium-233, and uranium of unknown enrichment. Radioactive materials may be further filtered as sealed or unsealed sources. Lastly, RCOM may be further filtered by manufactured goods or parts, scrap metal, naturally occurring radioactive materials (NORM), non-radioactive material (i.e. scams), other material, package or container and unknown. Users can combine any of the subtypes of material in a single search.
(10) Material nuclide: users can search by any of the 107 listed nuclides, individually or combined with other nuclides, which also include the options ‘other’ and ‘unknown’.
(11) RS-G-1.9 category: users can search by any of the five categories of radioactive sources defined in IAEA Safety Standards No. RS-G-1.9, Categorization of Radioactive Sources [10], individually or combined with other nuclides.

(12) Material recovered: users can search by incidents in which materials were seized or recovered, totally or partially, or not seized or recovered. This option is particularly interesting for materials involved in thefts and losses, since it gives an indication of how many materials reported initially as missing remain out of regulatory control due to intentional (theft) or unintentional (loss) acts.

(13) Border detection: users can search for incidents that have been detected at borders by selecting the option 'Yes' in this question. This question may be relevant for border guards or customs authorities, since many of the reported border detections correspond to the routine activities of such agencies.

The tabular format incorporates the options of customizing the retrieved data by selecting different columns and exporting the outputs as an Excel file.

The graphic display includes 12 graphs to visualize statistical data on the following parameters in the retrieved data: total number of incidents; regions; incident groups; recovery of material; border detections; types of material; incidents by type and group; number of nuclear material items by type; radioactive sources by nuclide; radioactive sources by RS-G-1.9 category; RCOM by type of material; and RCOM by nuclide.

8.4.8. Incident and Trafficking Database Online Reporting Tool

The WebINF is the online reporting tool developed by the secretariat; it provides a secure transmission of incident reports by States as well as storage of draft and submitted reports. The paper-based INF remains as an alternative if the WebINF tool is unavailable or if national restrictions affect the electronic transmission of nuclear security information.

The WebINF was updated following the development of the new database (ITDB Plus) and the subsequent migration of all existing data from the old database in 2017. The advantage of the updated online reporting tool over the original version is that it has the same structure as the database (i.e. each data field in the WebINF form has its correspondent field in the database). As such, the synchronization of data fields between the reporting tool and the database allows a direct data import that saves processing time and adds transparency because incident data is recorded exactly as reported by the States. The automated process eliminates manual data processing by the secretariat that was necessary with the old database. For these reasons, States are strongly encouraged to report all incidents through the WebINF tool.

From a Member State user's perspective, one of the main advantages of the WebINF application is that all reported incidents are kept in the application and can be consulted at any time. This is important when new PoCs replace the previous ones. Since the reported incidents are linked to a State profile and not to an individual, no data is lost. This allows the new PoCs to learn what has been reported, when it was reported, and to update incident reports easily, as appropriate. This is done by editing the original incident report and resubmitting it to the Database.

Additionally, the WebINF tool incorporates the online version of the old Batch INF. At the request of PoCs, the Batch INF was created as a simplified reporting form designed for incidents that created a burden for some PoCs owing to their less serious nature but high frequency. The Batch INF contains a limited number of data fields designed to report on a quarterly basis exclusively Group III incidents (excluding thefts) that involve RCOM or radioactive sources of less than 100 MBq. Incidents involving thefts, any type of nuclear material or radioactive sources with an activity of 100 MBq or higher are to be reported through WebINF.

The new Batch WebINF is a more streamlined, user-friendly reporting form than the old Batch INF. It is easy to complete, process and submit updates, if required.

The WebINF page contains three instructional documents that can be downloaded in PDF format:

(1) The New WebINF Page: this document explains the structure of the WebINF and the available options to select single or batch reporting forms and check submitted or draft reports;
(2) How to Fill out WebINF: this document includes step-by-step instructions on how to process a single incident report or WebINF;
(3) How to Fill out Batch WebINF: this document includes step-by-step instructions on how to process a batch incident report or Batch WebINF.

The WebINF page is not available to users from international organizations.

8.4.9. Access Management

This page allows PoCs to manage the permissions of their respective national users (for PoCs from Member States) or other officials (for PoCs from international organizations) to access the NUSEC ITDB restricted area. This page displays two tables: an upper table, NUSEC Users Who Have Access to ITDB Restricted Area, and a lower table, NUSEC Users without Access to ITDB Restricted Area. As indicated by its title, the upper table displays the users who have access to the NUSEC ITDB restricted area. The lower table displays all national users who have access to the NUSEC portal but not to the ITDB restricted area. PoCs can grant access to a maximum of five authorized users in total, including themselves (see Section 7.5).

It is the PoCs' responsibility to manage access to the restricted area for their State (excluding other PoCs or alternate PoCs users whose access rights are managed by the secretariat). Granting and revoking access of authorized users is a simple procedure that requires PoCs to follow the instructional document that is distributed to upon their nomination. PoCs may also grant authorized users additional permissions to draft and submit incident reports, if appropriate.

8.4.10. Incident and Trafficking Database Point of Contact Monitor

It contains all published issues of the Point of Contact Monitor (the "PoC Monitor"). It is an informative document designed to update PoCs and other authorized users on the implementation of the programme's projects and activities. It is issued twice a year: the first issue reporting on the period January–June and the second issue reporting on the period July–December.

The PoC Monitor contains only administrative and programmatic information. This includes data on the number and type of incident reports (e.g. WebINF, Batch INF) received by the ITDB. Incident related information and statistics are not included. Such information can be found in the ITDB analytical products and tools that are available in the NUSEC ITDB restricted area.

The PoC Monitor shares information on a regular basis on the programme and the team's activities. It reports on the progress of relevant ITDB projects, provides reminders for meetings and updates information regarding ITDB staff and PoCs changes. It also includes information on incident reporting tips.

8.4.11. Incident and Trafficking Database Events

It contains information about all meetings and outreach activities, including the triennial PoCs meetings, regional or national workshops and consultancy meetings. A page for each event usually contains the agenda, list of participants, presentations delivered, photographs and other relevant material.

The purpose of this page is twofold: (1) it allows the Network to keep track of past activities; and (2) it allows participants to access and download the relevant materials of the activities in which they have participated. This avoids the problems encountered with transferring data via portable storage devices or data limits on emails. The secretariat usually updates this page within a week of completion of a meeting or other outreach activity.

8.5.INFORMATION SECURITY

The IAEA categorizes all information submitted and contained within the restricted area as 'Restricted Information'[8], unless otherwise stated by the submitting State. Any confidential documents submitted through other secure channels are clearly identified as such and stored separately from the incident record. Confidential information as designated by the Member State or the IAEA is not stored in the ITDB restricted area.

The protection of the information within the restricted area is a shared responsibility between the IAEA who provides the portal and the PoCs who access the data. The PoCs should follow best security practices in safeguarding both their credentials for accessing the system and any data extracted from the restricted area.

Information technology (IT) security controls implemented for the restricted area consist of a combination of technical and administrative controls that have been designed based on guidance from ISO/IEC 27002:2013, Information Technology – Security Techniques – Code of Practice for Information Security Controls[9] and other international IT security best practices. The technical controls implement multilevel protection utilizing a security zone architecture, firewalls, anti-malware protection, vulnerability scanning, as well as comprehensive secure configuration and patching procedures. Additionally, enhanced protections are implemented for the privileged access to systems required by administrators.

[8] The IAEA defines the term 'Restricted Information' as "Information in relation to which unauthorized disclosure or unauthorized access could be prejudicial to the interests of the Agency, i.e. have effects which are undesirable and/or could cause inconvenience and embarrassment".

[9] This standard was superseded and replaced in February 2022 by ISO/IEC 27002:2022, Information Security, Cybersecurity and Privacy Protection – Information Security Controls.

Appendix I.

INCIDENT AND TRAFFICKING DATABASE MILESTONES

In 1995, the IAEA set up the ITDB as an information system on incidents of illicit trafficking and other unauthorized activities and events involving nuclear and other radioactive material out of regulatory control. This appendix summarizes the main developments and achievements of the ITDB since 1995.

1995. On 3 August, the IAEA formally announces in writing that the ITDB programme has been implemented and invites Member States to report incidents. States' official reporting commences and includes some previous incidents, the earliest dating back to 1992.

1996. The incident notification form (INF) is divided into two parts to allow for the restriction of certain data in Part 2.

1998. The first PoCs meeting is held in Vienna.

2000. The second PoCs meeting is held, and subsequently is convoked on a triennial basis. Acting on the recommendations of the meeting, the scope of the Database is expanded to include and distinguish between illegal transfers, inadvertent movement, contaminated scrap and other trivial events.

2003. The responsibility for the ITDB within the IAEA is transferred from the Department of Safeguards to the newly created Office of Nuclear Security in the Department of Nuclear Safety and Security.

2006. The INF is updated for better identification of the materials involved and a clearer restriction for Part 2 information.

2006. Participants in the triennial PoCs meeting agree on the following topics:

- A revised version of the ToR, which include a redefinition of the ITDB scope;
- A new INF, which is maintained until the implementation of the ITDB Conceptual Framework in 2016;
- A request for the IAEA to develop a web-based platform for the dissemination of ITDB data.

2011. The IAEA launches NUSEC with a dedicated ITDB restricted area that has since served as the primary information exchange platform between the IAEA and the PoCs. NUSEC replaces sharing information via fax (INFs), hard copies (analysis reports), or CD-ROMs (aggregate yearly incidents).

2012. Participants in the triennial PoCs meeting agree to change the name of the database from 'Illicit Trafficking Database' to 'Incident and Trafficking Database' to align its name with the revised scope agreed upon in 2006. They also agree on launching a project for redesigning and modernizing the database.

2013. Dissemination of INFs via fax is discontinued and is now implemented exclusively via the ITDB restricted area in NUSEC.

2013. The IAEA begins the redesign of the database software, including a tool for the electronic submission of incident reports (WebINF).

2014. The secretariat officially launches the online incident reporting tool WebINF. This new tool quickly replaces the traditional paper-based INF as the preferred means to submit incident reports to the ITDB.

2015. The secretariat launches a data search tool with a graphic interface, known as ITDB Dashboard.

2015. Participants at the triennial PoCs meeting approve the ITDB Conceptual Framework, which is implemented in 2016. The Conceptual Framework includes a definition of trafficking for ITDB communication purposes and a new definition of incident groups that categorize incidents as related to trafficking or malicious use, unrelated to trafficking or malicious use, and undetermined trafficking or malicious use intent.

2017. A new database (ITDB Plus) is launched after the successful introduction of a new software solution and the migration of data from the old database. This is followed by a project on the standardization of migrated legacy data and the development of new tools:

- A new version of the existing online reporting tool WebINF;
- A new version of the ITDB Dashboard that replaces the old ITDB Dashboard and the old WebITDB tool by integrating a complex search functionality with outputs in table and graphic forms, both of which are exportable or downloadable.

2017. Information sharing between the secretariat and PoCs moves exclusively to NUSEC, and the possibility of reporting incidents to the Database via fax is discontinued.

Appendix II.

GROUPING OF TYPES OF INCIDENTS IN THE INCIDENT AND TRAFFICKING DATABASE CONCEPTUAL FRAMEWORK

As described in Section 2.3, in 2015, the secretariat together with the PoCs developed a Conceptual Framework that integrated a categorization of ITDB incidents based on whether they were related, potentially related or unrelated to trafficking or malicious use. This Conceptual Framework includes a definition of ‘trafficking’ that provides the basis for such categorization. Below is a summary of the categorization of reported types of incidents into three groups and a list of types of incidents that indicates their relationship to these groups as described in Section 2.3.

II.1. GROUP I: CONFIRMED OR LIKELY ACT OF TRAFFICKING OR MALICIOUS USE OR SCAM/FRAUD (INCLUDING ATTEMPTS THEREOF)

Incidents included are those for which there is sufficient information provided in the reporting State’s INF to determine that the incident is, or is likely to be, connected with trafficking or malicious use. The following types of incidents are included in Group I:

— **Malicious use**

— **Unauthorized trade** (further to the definition of trafficking)

— **Unauthorized movement** (further to the definition of trafficking)

— **Scam/fraud** (because the intent to commit such an act may provide an indication of the intent to acquire nuclear or other radioactive material, in particular, for trafficking or malicious use)

— **Unauthorized possession**

— **Theft (and attempt)**

when **the intent** to conduct an act of trafficking or malicious use has been clearly indicated by the reporting State

II.2. GROUP II: UNDETERMINED ACT OF TRAFFICKING OR MALICIOUS USE (INCLUDING ATTEMPTS THEREOF)

Incidents included are those for which there is insufficient information provided in the reporting State’s INF to determine that the incident is, or is likely to be, either connected or unconnected with trafficking or malicious use. The following types of incidents are included in Group II:

— **Missing**, since there is insufficient information to preclude theft

— **Unauthorized possession**

— **Theft (and attempt)**

when **the intent, or non-intent,** to conduct an act of trafficking or malicious use has not been clearly indicated by the reporting State, or has been reported to be unknown at that time

Reclassification into Group I or Group III can be made, should intent, or non-intent, be subsequently identified by the reporting State.

II.3. GROUP III: CONFIRMED OR LIKELY ABSENCE OF AN ACT OF TRAFFICKING OR MALICIOUS USE (INCLUDING ATTEMPTS THEREOF)

Incidents included are those for which there is sufficient information provided in the reporting State’s INF to determine that the incident is not, or is unlikely to be, connected with trafficking or malicious use. The following types of incidents are included in Group III:

- **Unauthorized disposal**
- **Unauthorized shipment**
- **Unauthorized or undeclared storage**
- **Loss**
- **Discovery**
- **Misrouting**
- **Other**
- **Unauthorized possession**
- **Theft (and attempt)**

} if the reporting State clearly indicates in its INF the **non-intent** to commit an act of trafficking or malicious use

Appendix III.

INFORMATION EXCHANGE MODEL FOR REPORTING INCIDENTS TO THE INCIDENT AND TRAFFICKING DATABASE

This appendix contains a graphic information exchange model (see Fig. 1) for reporting to the Database that includes an example of information flows from national stakeholders to their respective PoCs and from these to the secretariat.

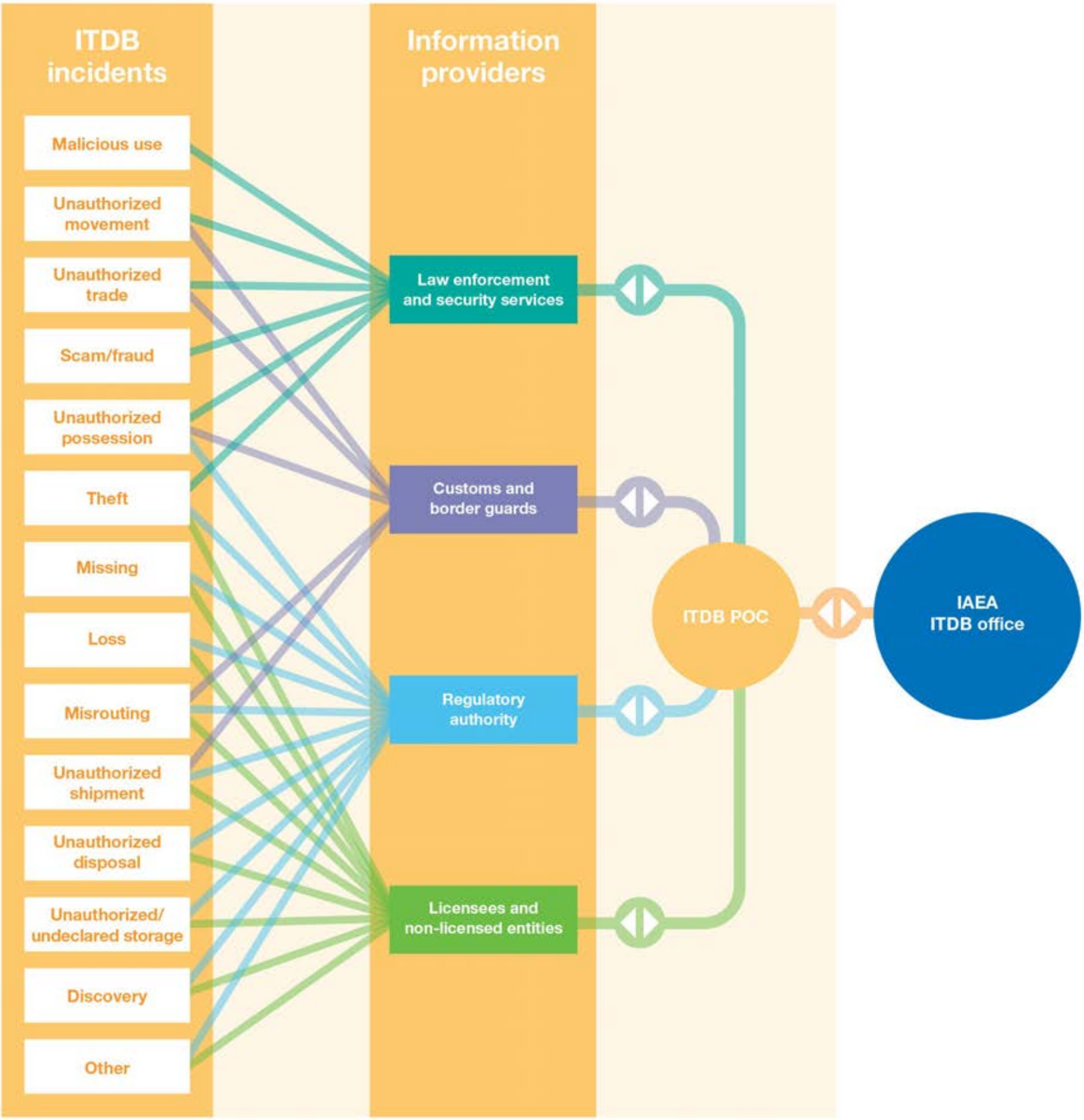

FIG. 1. Information exchange model for reporting incidents to the ITDB.

The left column in Fig. 1 identifies the 14 types of incidents categorized in the Database. The second column identifies the entities most likely involved in the detection of the incidents listed in the first column. Four main categories of national stakeholders are identified as the main sources of information on ITDB incidents: regulatory authorities; law enforcement and security services; customs and border guards; and licensees and non-licensed entities (such as metal recycling companies). These national stakeholders will ideally have formal working arrangements to report directly, or through other competent authorities, to their national PoCs to support the information exchange. However, information exchange arrangements vary from State to State according to their national legislation — which assigns responsibilities and capabilities to their competent authorities. Therefore, these examples are for reference only.

Table 1 shows the likely correspondence between the national stakeholders, their most likely sources of information, and the types of incidents that they are more likely to detect.

TABLE 1. OVERVIEW OF NATIONAL STAKEHOLDERS, THEIR RESPECTIVE SOURCES OF INFORMATION AND THE TYPES OF ITDB INCIDENTS THEY ARE LIKELY TO DETECT

Entity	**Source of information**	**Most common types of ITDB incidents**
Regulatory Authority	Inspections Reports from licensees Reports from non-licensed entities	Unauthorized possession Theft Missing Loss Misrouting Unauthorized disposal Unauthorized shipment Unauthorized/undeclared storage Discovery Other
Law Enforcement and Security Services	Reports from duty officers Investigations Intelligence	Malicious use Unauthorized movement Unauthorized trade Scam/fraud Unauthorized possession Theft Discovery
Customs and Border Guards	Border inspections Investigations Intelligence	Unauthorized movement Unauthorized trade Unauthorized possession Misrouting Unauthorized shipment Discovery
Licensees	Inventory checks Alarm systems	Theft Missing Loss Misrouting Unauthorized/undeclared storage Discovery
Non-licensed Entities	Detection equipment Accidental discovery	Unauthorized disposal Unauthorized shipment Unauthorized/undeclared storage Discovery

These examples of information flow in the ITDB information collation and reporting processes are included here for reference purposes. They are meant to assist States' competent authorities to design an information management framework that meets their requirements and the specifications of the programme.

Appendix IV.

INFORMATION EXCHANGE MODEL FOR SHARING INCIDENT AND TRAFFICKING DATABASE INFORMATION

Figure 2 illustrates the information flow from the secretariat to third parties (State PoCs, international organizations, as well as internally within the IAEA) and from third parties to their respective authorized users. The most likely use of this information is illustrated as well.

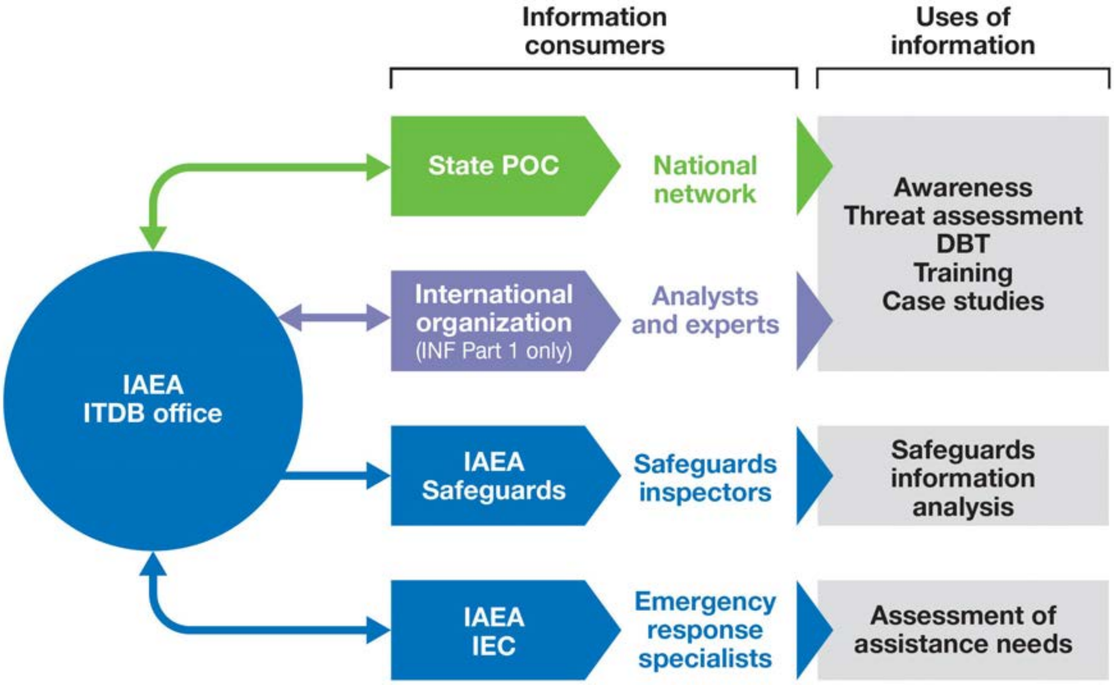

FIG. 2. Information exchange model between the secretariat and information consumers.

Similar to the information described in Appendix III, the parts of this model relating to entities other than the IAEA are hypothetical and are included here for reference purposes based on information provided by participating States and international organizations. Figure 2 is meant to assist States' competent authorities in designing an information management framework that meets their requirements and the specifications of the programme.

Appendix V.

INFORMATION EXCHANGE MODEL FOR A NATIONAL NETWORK FOR THE INCIDENT AND TRAFFICKING DATABASE

This appendix includes two information exchange models:

(1) A graphical model that displays a generic information exchange network for PoCs (see Fig. 3);
(2) A table with a suggested model for the dissemination of information on ITDB incidents (see Table 2).

Figure 3 illustrates the information exchange generic network model. This model includes several national stakeholders and the possible relationships established among them. It identifies the competent authorities responsible for the detection of, and response to, ITDB incidents; managing information and providing direct support on such incidents (primary network); and providing additional support and technical expertise as necessary (secondary network).

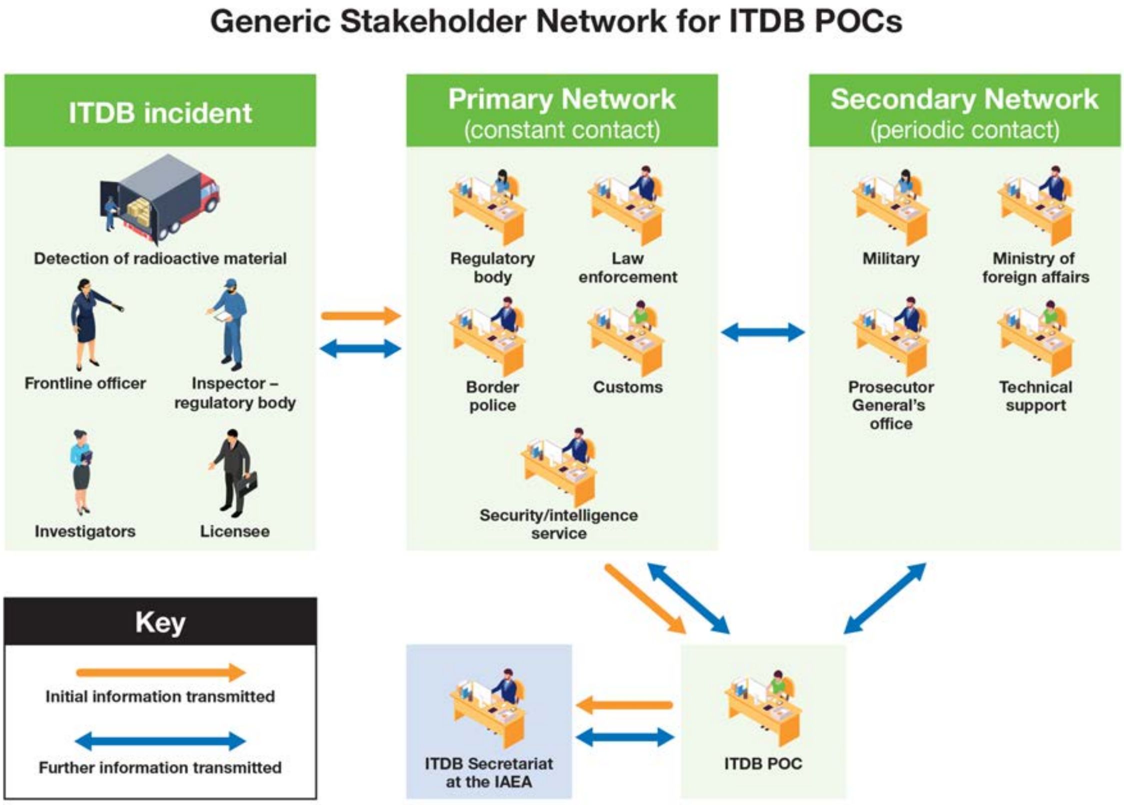
Generic Stakeholder Network for ITDB POCs
ITDB incident
Detection of radioactive material
Frontline officer
Inspector – regulatory body
Investigators
Licensee
Primary Network (constant contact)
Regulatory body
Law enforcement
Border police
Customs
Security/intelligence service
Secondary Network (periodic contact)
Military
Ministry of foreign affairs
Prosecutor General's office
Technical support
Key
Initial information transmitted
Further information transmitted
ITDB Secretariat at the IAEA
ITDB POC

FIG. 3. Information exchange model for a generic national stakeholder network for PoCs.

Table 2 shows a generic model for the dissemination of ITDB data to the national network based on the incident group classification and the nature of the stakeholders as identified in Appendices II and III. This model provides a reference for sharing such data within the national stakeholder network according to their needs.

TABLE 2. MODEL FOR THE DISSEMINATION OF ITDB INCIDENTS BY POCs TO NATIONAL STAKEHOLDERS

Group	Law Enforcement & Security Services	Customs & Border Guards	Regulatory Authorities	Licensees & Non-licensed Entities
Group I	Always	Case-by-case	Always	Case-by-case
Group II	Always	Case-by-case	Always	Case-by-case
Group III	Case-by-case	Case-by-case	Always	Case-by-case

PoCs should agree with the stakeholders on which incidents should be shared between them. Each stakeholder has different needs, therefore not everyone is interested in all types of incidents or in the whole set of data concerning an incident. Furthermore, the PoCs may wish to limit information sharing to only national, regional or global information depending on their national network, geographical location and stakeholder type. For example, each group of stakeholders may be interested in the following types of incidents:

- Law enforcement and security services:
  - All Group I and Group II incidents;
  - Group III incidents in which material left regulatory control as a result of an intentional act (e.g. Group III thefts);
  - Group III incidents in their region in which material is out of regulatory control and, as a result, available for trafficking or malicious use (e.g. loss).
- Customs and border guards: any type of incident of any group in which the detected material has crossed, or may cross, a national border, including unauthorized trade, unauthorized movement, unauthorized possession or misrouting involving more than one State, unauthorized shipments, thefts, losses and missing material[10];
- Regulatory authorities: all incidents without distinction;
- Licensees and non-licensed entities:
  - Any type of Group III incident that demands increased awareness among licensees. Incidents in which the affected party or the involved materials are similar to the licensee or their licensed materials would be of particular interest;
  - Thefts and losses, irrespective of the incident group, and missing material (Group II).

Other national authorities that are not mentioned in Table 2 may have a legitimate interest in accessing ITDB data depending on national responsibilities with regard to nuclear security. PoCs should have agreed in advance with their stakeholders which incidents, type of information from these incidents or related information products are relevant and beneficial for each of them.

[10] “Missing” is a type of incident in which materials are out of regulatory control as a result of either theft (intentional act) or loss (accidental, unintentional act) but where the available information does not allow establishment of the exact cause of loss of control. It is a Group II incident by definition. The clarification of the circumstances of the loss of control may result in its reclassification as theft or loss.

The examples shown in this Appendix serve as references that need to be adapted to the national context. The common point in all of these examples is the need to identify focal points for each stakeholder that is part of the national network. These focal points will liaise with the PoCs and will be responsible for deciding on the internal dissemination of the ITDB data received from the PoCs.

REFERENCES

[1] INTERNATIONAL ATOMIC ENERGY AGENCY, Nuclear Security Recommendations on Nuclear and Other Radioactive Material out of Regulatory Control, IAEA Nuclear Security Series No. 15, IAEA, Vienna (2011).

[2] INTERNATIONAL ATOMIC ENERGY AGENCY, Nuclear Security Recommendations on Radioactive Material and Associated Facilities, IAEA Nuclear Security Series No. 14, IAEA, Vienna (2011).

[3] The Convention on the Physical Protection of Nuclear Material, INFCIRC/274/Rev. 1, IAEA, Vienna (1980); Amendment to the Convention on the Physical Protection of Nuclear Material, INFCIRC/274/Rev.1/Mod.1 (Corrected), IAEA, Vienna (2021).

[4] INTERNATIONAL ATOMIC ENERGY AGENCY, Convention on Early Notification of a Nuclear Accident and Convention on Assistance in the Case of a Nuclear Accident or Radiological Emergency, Legal Series No. 14, IAEA, Vienna (1987).

[5] FOOD AND AGRICULTURE ORGANIZATION OF THE UNITED NATIONS, INTERNATIONAL ATOMIC ENERGY AGENCY, INTERNATIONAL CIVIL AVIATION ORGANIZATION, INTERNATIONAL LABOUR ORGANIZATION, INTERNATIONAL MARITIME ORGANIZATION, INTERPOL, OECD NUCLEAR ENERGY AGENCY, PAN AMERICAN HEALTH ORGANIZATION, PREPARATORY COMMISSION FOR THE COMPREHENSIVE NUCLEAR-TEST-BAN TREATY ORGANIZATION, UNITED NATIONS ENVIRONMENT PROGRAMME, UNITED NATIONS OFFICE FOR THE COORDINATION OF HUMANITARIAN AFFAIRS, WORLD HEALTH ORGANIZATION, WORLD METEOROLOGICAL ORGANIZATION, Preparedness and Response for a Nuclear or Radiological Emergency, IAEA Safety Standards Series No. GSR Part 7, IAEA, Vienna (2015).

[6] INTERNATIONAL ATOMIC ENERGY AGENCY, Operations Manual for Incident and Emergency Communication (EPR–IEComm 2019), IAEA, Vienna (2020).

[7] Measures Against Illicit Trafficking in Nuclear Materials and Other Radioactive Sources, Progress Report by the Director General, GOV/2773/Add.1, IAEA, Vienna (1995).

[8] Protection Against Nuclear Terrorism: Specific Proposals, Report by the Director General, GOV/2002/10, IAEA, Vienna (2002).

[9] INTERNATIONAL ATOMIC ENERGY AGENCY, Nuclear Security Recommendations on Physical Protection of Nuclear Material and Nuclear Facilities (INFCIRC/225/Revision 5), IAEA Nuclear Security Series No. 13, IAEA, Vienna (2011).

[10] INTERNATIONAL ATOMIC ENERGY AGENCY, Categorization of Radioactive Sources, IAEA Safety Standards Series No. RS-G-1.9, IAEA, Vienna (2005).

[11] INTERNATIONAL ATOMIC ENERGY AGENCY, IAEA Safety Glossary: Terminology Used in Nuclear Safety and Radiation Protection, 2018 Edition, IAEA, Vienna (2019).

ANNEX

TEMPLATES FOR REQUESTING PARTICIPATION IN THE INCIDENT AND TRAFFICKING DATABASE PROGRAMME AND FOR THE NOMINATION OF POINTS OF CONTACT AND ALTERNATE POINTS OF CONTACT

A–1. TEMPLATE FOR REQUESTING PARTICIPATION IN THE ITDB PROGRAMME

Permanent Mission of _________

[Address of Permanent Mission]

[Date]

Director
Division of Nuclear Security
Department of Nuclear Safety and Security
International Atomic Energy Agency
Vienna International Centre
P.O. Box 100
1400 Vienna
AUSTRIA

JOINING THE INCIDENT AND TRAFFICKING DATABASE (ITDB) PROGRAMME AND APPOINTMENT OF NATIONAL POINTS OF CONTACT

The [Government / Permanent Mission] of ________________ presents its compliments to the Secretariat of the International Atomic Energy Agency and would like to manifest interest in joining the Incident and Trafficking Database (ITDB) programme. In this regard, the [Government / Permanent Mission] of ________________ would like to draw your attention to the appointment of Mr/Ms __________________________________ and Mr/Ms __________________________________ as the national Point of Contact and Alternate Point of Contact respectively.

Their contact details are as follows:

Primary Point of Contact:
Mr/Ms [name of nominated person]
[Job position / role]
[Name of national agency]
[Address of national agency]

Telephone(s): _________________________
Email address: ________________________

Alternate Point of Contact:
Mr/Ms [name of nominated person]
[Job position / role]
[Name of national agency]
[Address of national agency]

Telephone(s): ______________________.
Email address: _______________________

Accept, [Sir/Madam], the assurance of our highest consideration.

[Signature]

[Title, Name]

A–2. TEMPLATE FOR THE NOMINATION OF POCs AND ALTERNATE POCs

Permanent Mission of _________

[Address of Permanent Mission]

[Date]

Director
Division of Nuclear Security
Department of Nuclear Safety and Security
International Atomic Energy Agency
Vienna International Centre
P.O. Box 100
1400 Vienna
AUSTRIA

APPOINTMENT OF NATIONAL POINT OF CONTACT FOR THE INCIDENT AND TRAFFICKING DATABASE (ITDB) PROGRAMME

The [Government / Permanent Mission] of ________________ presents its compliments to the Secretariat of the International Atomic Energy Agency and has the pleasure to draw your attention to the appointment of Mr/Ms __________________________________ and Mr/Ms __________________________________ as the national Point of Contact and Alternate Point of Contact respectively for the Incident and Trafficking Database (ITDB) programme.

Their contact details are as follows:

Primary Point of Contact:
Mr/Ms [name of nominated person]
[Job position / role]
[Name of national agency]
[Address of national agency]

Telephone(s): _________________________
Email address: ________________________

Alternate Point of Contact:
Mr/Ms [name of nominated person]
[Job position / role]
[Name of national agency]
[Address of national agency]

Telephone(s): _______________________.
Email address: _______________________

We reaffirm our commitment to be part of the ITDB.

Accept, [Sir/Madam], the assurance of our highest consideration.

[Signature]

[Title, Name]

A–3. TEMPLATE FOR THE UPDATE OF EXISTING POCs OR THEIR CONTACT DETAILS

Permanent Mission of _________

[Address of Permanent Mission]

[Date]

Director
Division of Nuclear Security
Department of Nuclear Safety and Security
International Atomic Energy Agency
Vienna International Centre
P.O. Box 100
1400 Vienna
AUSTRIA

UPDATE OF [NATIONAL POINT OF CONTACT / NATIONAL POINT OF CONTACT DETAILS] FOR THE INCIDENT AND TRAFFICKING DATABASE (ITDB) PROGRAMME

The [Government / Permanent Mission] of ________________ presents its compliments to the Secretariat of the International Atomic Energy Agency and has the honour to inform that the national Point of Contact and/or Alternate Point of Contact for the Incident and Trafficking Database (ITDB) programme have changed. With immediate effect, the contact details of said persons should read according to the information provided below:

Their contact details are as follows:

Primary Point of Contact:
Mr/Ms [name of nominated person]
[Job position / role]
[Name of national agency]
[Address of national agency]

Telephone(s): __________________________
Email address: _________________________

Alternate Point of Contact:
Mr/Ms [name of nominated person]
[Job position / role]
[Name of national agency]
[Address of national agency]

Telephone(s): ________________________.
Email address: ________________________

We reaffirm our commitment to be part of the ITDB.

Accept, [Sir/Madam], the assurance of our highest consideration.

[Signature]

[Title, Name]

GLOSSARY

The following definitions and explanations are specific to this publication and may not necessarily conform to definitions adopted elsewhere for international use.

alternate PoCs. Serve as a back-up to the PoCs in participating States or international organizations.

authorized user. Officials in participating States or international organizations who have been authorized by their respective point of contact or alternate point of contact to access the NUSEC ITDB restricted area. Participating States and international organizations may have up to five authorized users in total with access to the NUSEC ITDB restricted area, including the point of contact and alternate point of contact.

batch WebINF. An online reporting form used by States to report incidents of less serious nature to the secretariat in a batch form, normally on a quarterly basis. The Batch WebINF is a simplified version of the WebINF that facilitates the data processing by States. Batch WebINF may be used to report incidents that involve radioactively contaminated or other materials (RCOM) or radioactive sources of less than 100 MBq. Radioactive sources of or above 100 MBq and nuclear materials have to be reported via WebINF or INF.

high enriched uranium (HEU). Uranium containing 20% or more of the isotope ^{235}U. HEU is considered a special fissionable material and a direct use material [11].

incident and trafficking database (ITDB). IAEA's information system on incidents of illicit trafficking and other unauthorized activities and events involving nuclear and other radioactive material outside of regulatory control.

incident notification form (INF). The form used by States to report incidents to the secretariat. The INF was replaced in 2017 by an online reporting tool known as WebINF. The INF remains an alternative for reporting ITDB incidents but its use by States is discouraged.

ITDB incident. An event arising under any of the circumstances described in the ITDB's system of incident types relating to nuclear or other radioactive material. These types of incidents comprise the following: discovery; loss; malicious use; misrouting; missing; other; scam/fraud; theft; unauthorized disposal; unauthorized movement; unauthorized possession; unauthorized shipment; unauthorized trade; and unauthorized/undeclared storage.

low enriched uranium (LEU). Enriched uranium containing less than 20% of the isotope ^{235}U. LEU is considered a special fissionable material and an indirect use material [11].

participating international organization. An international intergovernmental organization that participates in the ITDB programme.

participating State. A State that participates in the ITDB programme. Being a Member State of the IAEA is not a requirement for participation in the ITDB programme.

PoCs. Points of contact of the ITDB programme in participating States or international organizations.

PoCs network. The community of users comprising all PoCs, including alternate PoCs, and the secretariat, as laid down in the ITDB Terms of Reference.

radioactively contaminated or other material (RCOM). Any item, object or collection of material that is contaminated with radioactive material or is naturally radioactive. Non-radioactive materials involved in scam/fraud incidents are also classified as RCOM in the ITDB for purposes of analysis.

trafficking. Any intentional unauthorized movement or trade of nuclear or other radioactive material, in particular, those with possible or proven criminal intent.

WebINF. The secure online incident notification form created in 2017 that replaced the traditional paper-based INF. The WebINF is available within the NUSEC ITDB restricted area and is the main means used by States to report incidents to the secretariat.

TYPES OF INCIDENTS IN THE SCOPE OF THE ITDB (SUMMARIZED FROM THE ITDB CONCEPTUAL FRAMEWORK AND ITS REPORTING GUIDELINES)

discovery. Incidents involving finding nuclear or other radioactive material that is out of regulatory control or for which no official control measures were in place (e.g. orphan source) outside a licensed (or otherwise controlled) facility or site.

loss. Incidents involving material that has been physically lost. The incident should be consistent with a loss in which a deliberate removal from control has been ruled out — as opposed to the possibly deliberate circumstances related to stolen or missing material.

malicious use (and attempt). An act (including attempts thereof) that involves any type or quantity of nuclear or other radioactive material for the purpose of harming humans, the economy or the environment.

misrouting. Incidents involving errors occurring during shipment of material, both domestic and international, that result in delivery (even if only temporarily) to incorrect addresses.

missing. Incidents involving the disappearance of material. The incident should show no evidence of theft, loss or misrouting.

other. Applied when the existing categories do not fit the circumstances of the incident. In this case, summary of the incident may help to determine the appropriate category.

scam/fraud. Non-radioactive material (or fictitious material) which was purposely advertised, or otherwise claimed, by the seller to be nuclear or radioactive for financial or material gain or threat of malicious use.

theft (and attempt). Incidents involving the theft (including attempts thereof) of nuclear or other radioactive material in which:

- Intent to conduct an act of trafficking or malicious use was clear from the State report (i.e. Group I incident), or
- Neither the intent nor non-intent to conduct a trafficking or malicious act was clear from the State report (i.e. Group II incident), or
- Non-intent to conduct a trafficking or malicious act was clear from the State report (i.e. Group III incident).

unauthorized disposal (and attempt). Incidents involving the unauthorized disposal (or attempts thereof) of any type or quantity of material.

unauthorized movement (and attempt). Incidents (including attempts thereof) which involve the intentional, unauthorized movement (e.g. by road, rail, air, ship) of material by an individual or a group of individuals particularly across international borders and believed to be related to an unauthorized trade or malicious use. The movement should not be of a type that may be associated with the abandonment of material. Nor should it be considered an unauthorized movement if it were to be covered normally by the following types of incidents: unauthorized shipment, unauthorized disposal, unauthorized storage or discovery.

unauthorized possession. Incidents which involve unauthorized possession by an individual or a group of individuals of any type or quantity of material in which:

- Intent to conduct an act of trafficking or malicious use was clear from the State report (i.e. Group I incident), or
- Neither the intent nor non-intent to conduct a trafficking or malicious act was clear from the State report (i.e. Group II incident), or
- Non-intent to conduct a trafficking or malicious act was clear from the State report (i.e. Group III incident).

unauthorized shipment. Incidents involving the shipment (domestic or international) of any type or quantity of material without the noted authorization. Such incidents should not be related to unauthorized trade, unauthorized movement or malicious use.

unauthorized trade (and attempt). An intentional, unauthorized transfer of ownership (including attempts thereof) whereby a material is sold, purchased or otherwise transferred by one party (individual or group of individuals) to another. Both parties are either aware, believe or require that nuclear or other radioactive material is involved.

unauthorized or undeclared storage. Incidents involving the discovery of nuclear or other radioactive material in a facility or site licensed for such material but had not been accounted for by the owner or operator of the facility. Alternatively, the site housed such material in excess of the amount specified in the licence.

ABBREVIATIONS

CBRN	chemical, biological, radiological or nuclear
CEPOL	European Union Agency for Law Enforcement Training
CPPNM	Convention on the Physical Protection of Nuclear Materials
EEODN	European Explosive Ordnance Disposal Network
EUROPOL	European Union Agency for Law Enforcement Cooperation
HEU	high enriched uranium
IAEA	International Atomic Energy Agency
INF	ITDB incident notification form
INSSP	Integrated Nuclear Security Support Plan
INTERPOL	International Criminal Police Organization
ITDB	Incident and Trafficking Database
LEU	low enriched uranium
MERCOSUR	Common Market of the South
MPE	major public event
NORM	naturally occurring radioactive material
NUSEC	Nuclear Security Information Portal
PoCs	ITDB points of contact
RCOM	radioactively contaminated and other material
ToR	ITDB Terms of Reference
USIE	Unified System for Information Exchange in Incidents and Emergencies
WebINF	Web Incident Notification Form

CONTRIBUTORS TO DRAFTING AND REVIEW

Case Lackner, S.	International Atomic Energy Agency
Cesarek, J.	Slovenian Nuclear Safety Administration, Slovenia
Dimitrovski, D.	International Atomic Energy Agency
Dugay, R.	Canadian Nuclear Safety Commission, Canada
East, C.	International Atomic Energy Agency
Finschi, E.	Comisión Chilena de Energía Nuclear, Chile
Garcia Sainz, J.	International Atomic Energy Agency
Gredinger, A.	International Atomic Energy Agency
Medici, F.	Swiss Federal Office of Energy, Switzerland
Nelson, T.	International Atomic Energy Agency
Nicholas, M.	International Atomic Energy Agency
Otukile, T.	Botswana Radiation Protection Inspectorate, Botswana
Purvis, S.	International Atomic Energy Agency
Quram, S.	Energy and Minerals Regulatory Commission, Jordan
Ramirez, R.	Instituto Peruano de Energía Nuclear, Peru
Roumie, M.	Lebanese Atomic Energy Commission, Lebanon
Sunden, E.	Swedish Radiation Safety Authority, Sweden
Svyslotsky, G.	State Nuclear Regulatory Inspectorate of Ukraine, Ukraine
Takam, R.	Office of Atoms for Peace of Thailand, Thailand
Thompson, C.	Canadian Nuclear Safety Commission, Canada
Tottie, N.	International Atomic Energy Agency
Zhu, B.	International Atomic Energy Agency

Consultants Meetings

Vienna, Austria: 29–30 January 2018; 27–29 March 2019

ORDERING LOCALLY

IAEA priced publications may be purchased from the sources listed below or from major local booksellers.

Orders for unpriced publications should be made directly to the IAEA. The contact details are given at the end of this list.

NORTH AMERICA

Bernan / Rowman & Littlefield

15250 NBN Way, Blue Ridge Summit, PA 17214, USA
Telephone: +1 800 462 6420 • Fax: +1 800 338 4550
Email: orders@rowman.com • Web site: www.rowman.com/bernan

REST OF WORLD

Please contact your preferred local supplier, or our lead distributor:

Eurospan Group

Gray's Inn House
127 Clerkenwell Road
London EC1R 5DB
United Kingdom

Trade orders and enquiries:

Telephone: +44 (0)176 760 4972 • Fax: +44 (0)176 760 1640
Email: eurospan@turpin-distribution.com

Individual orders:

www.eurospanbookstore.com/iaea

For further information:

Telephone: +44 (0)207 240 0856 • Fax: +44 (0)207 379 0609
Email: info@eurospangroup.com • Web site: www.eurospangroup.com

Orders for both priced and unpriced publications may be addressed directly to:

Marketing and Sales Unit
International Atomic Energy Agency
Vienna International Centre, PO Box 100, 1400 Vienna, Austria
Telephone: +43 1 2600 22529 or 22530 • Fax: +43 1 26007 22529
Email: sales.publications@iaea.org • Web site: www.iaea.org/publications

INTERNATIONAL ATOMIC ENERGY AGENCY
VIENNA