International Physical Protection Advisory Service (IPPAS): 100 nuclear security good practices from 100 IPPAS missions

Nuclear Safety and Security Programme

IAEA

Nuclear
Safety and
Security

For more than a quarter of a century, the IAEA has been offering the International Physical Protection Advisory Service (IPPAS) to its Member States, with the aim of helping countries to strengthen their nuclear security regimes. One of the IAEA's peer review and advisory services, IPPAS focuses on the physical protection of nuclear and other radioactive material, as well as of associated facilities and associated activities.

The IPPAS programme was born in 1995, when the IAEA Board of Governors identified the need for this voluntary advisory service as part of the IAEA's assistance to Member States. Since then, 60 Member States have hosted 100 IPPAS missions.

From the first missions in Bulgaria and Slovenia in 1996 to the 100th IPPAS mission in Zambia in 2023, we have accomplished significant progress to offer a modular approach of assistance that can be customized to address Member States' needs. Demand remains high for IPPAS missions, and the IAEA looks forward to assisting many more Member States in the future.

This assistance has helped many countries to enhance and maintain physical protection in all types of facilities and uses of nuclear and other radioactive material, keeping them secure — as well as safe. Over the years, IPPAS missions have provided essential support to Member States in the effective implementation of the Convention on Physical Protection of Nuclear Material and its Amendment (A/CPPNM), of the Code of Conduct on the Safety and Security of Radioactive Sources, and of the IAEA nuclear security guidance.

As the nuclear security threat landscape continues to evolve, the IPPAS programme is poised to adapt as well. The addition to the scope of IPPAS of a module on information and computer security for physical protection in 2012, and the establishment of the IPPAS Good Practices Database in 2016, confirm the IAEA's agility and readiness to address the needs of its Member States.

The milestone of the completion of 100 IPPAS missions proves the value and importance of the programme and inspires all of us to keep working on strengthening nuclear security globally. Nuclear security is a national responsibility. We must continue asking ourselves if we are doing everything we can to secure nuclear and other radioactive material and associated facilities and activities.

I would like to thank all Member States who have provided their expert support for the last 27 years and encourage more Member States to make use and participate in these missions that support the IAEA's efforts to ensure robust and sustainable nuclear security globally.

Lydie Evrard
IAEA Deputy Director General and Head of the Department of Nuclear Safety and Security

The International Physical Protection Advisory Service (IPPAS) is an IAEA advisory service provided to Member States, upon their request, in support of their efforts to establish and maintain effective national nuclear security regimes. IPPAS, established in 1995, focuses on the physical protection of nuclear and other radioactive material, associated facilities and associated activities.

The requesting Member State can determine the scope of the IPPAS mission by selecting all five IPPAS mission modules or only those which are most relevant to its needs. A new sixth module is currently being developed to comprise the review of nuclear material accounting and control for nuclear security purposes. The entire IPPAS process is flexible and each mission is therefore customized to address the needs of a specific Member State.

The IAEA compiles each IPPAS team to match the competencies required for the review of the modules requested by the Member State. The team composition is then proposed to the host country for confirmation.

Each IPPAS team consists of an experienced team leader and internationally recognized experts, specially trained in the IPPAS process. The team is multinational and multidisciplinary and includes one or more IAEA technical officers as well. Dependent upon the number of modules selected, the IPPAS team visits the Member State approximately for a period of two weeks to conduct the mission.

Members of the IPPAS team at a site visit during a mission in Netherlands in 2012.

The mission allows for a confidential peer-to-peer exchange of experiences and good practices. The agenda includes discussions with the host country experts and officials, visiting facilities, observing practices, and even reviewing national legislation and regulatory practices. IPPAS missions provide Member States recommendations on meeting international obligations, such as the A/CPPNM and the United Nations Security Council Resolution 1540. During the mission the team of experts reviews the Member State's nuclear security practices on the protection of nuclear and other radioactive material, associated facilities and associated activities against the IAEA nuclear security guidance published within the Nuclear Security Series (NSS).

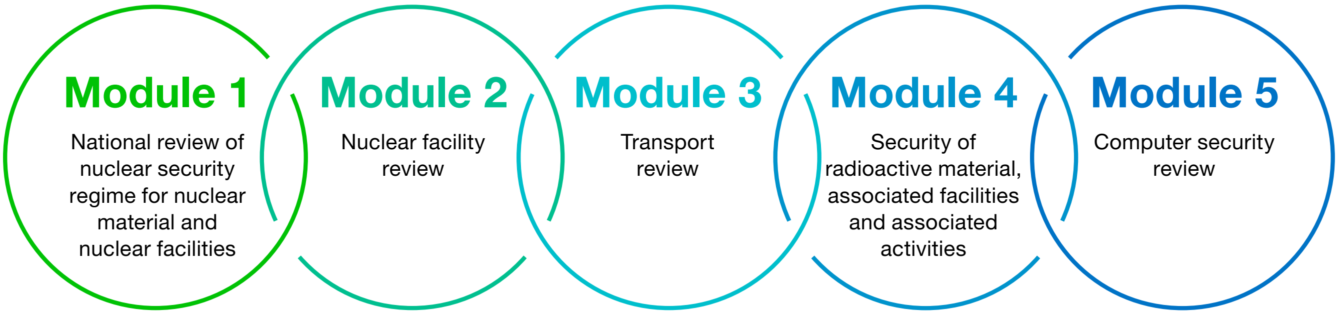

Module 1
National review of nuclear security regime for nuclear material and nuclear facilities
Module 2
Nuclear facility review
Module 3
Transport review
Module 4
Security of radioactive material, associated facilities and associated activities
Module 5
Computer security review

Figure 1. IPPAS missions consist of five independent modules, which can be selected by a Member State based on their needs.

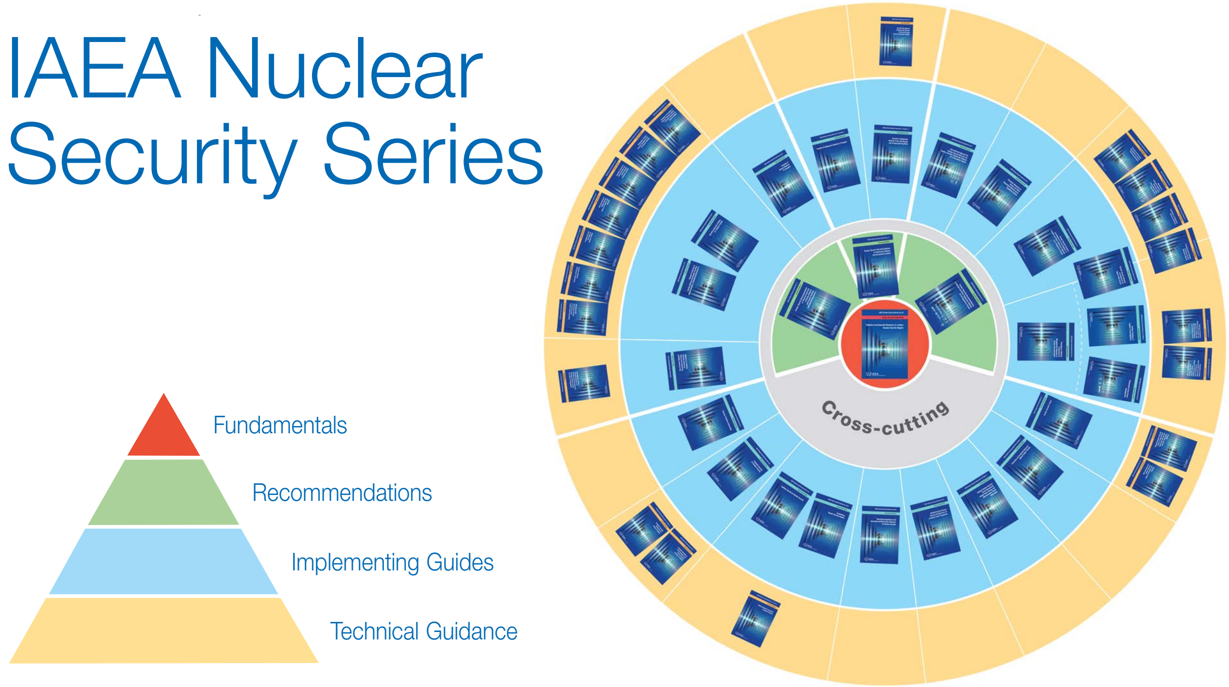


Figure 2. The IAEA Nuclear Security Series.

The outcome of the IPPAS Mission is a confidential report which includes a set of recommendations and suggestions for the host country implementation. It also includes good practices identified in a country. The confidential final report is relayed to the host country approximately two months after the conclusion of the IPPAS mission. A press release issued by the IAEA in the end of each IPPAS mission strengthens transparency and public awareness on nuclear security.

After the mission, the host country may elect to request assistance from the IAEA as a follow up activity, such as training on specific area identified by the mission, assistance in the development or revision of legislation or assistance in upgrading the physical protection systems at the facility or during transport. In case the Member State has an Integrated Nuclear Security Sustainability Plan (INSSP), these follow-up activities may also be conducted within the plan. Such follow-up activities are entirely voluntary for the host country. Similarly, the host country may decide to request a follow up mission three to four years after an IPPAS mission.

Follow-up missions allow a review of the Member State’s implementation of previous mission’s recommendations and suggestions, and may also include additional modules or review of nuclear security measures at other facilities, which were not visited during the previous mission. An essential feature of IPPAS is the availability, upon request, of IAEA follow-up assistance, such as training, technical support and more targeted assessments of various elements of national nuclear security regime. In such a manner, a Member State’s decision to request follow-up or subsequent IPPAS missions or other follow-up activities, provides for the continuous improvement in nuclear security.

IPPAS mission in Kuwait, 2023.

“With the experience of hosting three IPPAS missions (2009, 2012 and 2022), Finland strongly encourages the IAEA Member States to request such a mission. The mission not only provides excellent findings in order to further enhance national nuclear security measures, but allows the national experts opportunities for exchanging information on nuclear security with the team experts in confidential manner. This is one of the key benefits of IPPAS missions not available elsewhere. The latest IPPAS mission hosted in Finland 2022 provided excellent recommendations improving nuclear security regime in Finland and the findings are used for ongoing renewal of the Nuclear Energy Act. On the request of the IAEA, Finland has also provided experts for missions in other IAEA Member States and we believe these are one of the best opportunities for experts to learn from others. This knowledge can then also be used for national improvements.”

Petteri Tiippana, Director General of the Radiation and Nuclear Safety Authority (STUK), Finland

Evolution of the IPPAS programme

Since the IPPAS establishment, the number of practical applications for nuclear and other radioactive material, as well as their global footprint, have grown and evolved significantly. The IAEA's Power Reactor Information System (https://pris.iaea.org/PRIS/home.aspx) database estimates there are more than 400 nuclear power reactors operating in over than 30 Member States worldwide. An additional number of 30 States are considering the potential establishment of nuclear power programmes in order to meet future energy demands in a carbon-neutral manner. Even more broadly, the use of radioactive sources to meet a range of United Nations sustainable development goals (SDGs) in agriculture, industry, education, and medicine make them a vital resource for all States.

Like nuclear safety, nuclear security protects people, property, society and the environment from the harmful effects of ionizing radiation. To this end, the IPPAS programme's focus on nuclear security systems and measures has evolved to address the evolution of the international security threat landscape. Adequate and effective nuclear security practices — especially for the physical protection of nuclear and other radioactive material, associated facilities, and associated activities — allow Member States to fully harness powerful technologies and materials by ensuring that they are not misused.

At the early phase of the IPPAS programme the emphasis was on the physical protection of nuclear material and nuclear facilities. The scope was later extended on preventing the sabotage of nuclear and other radioactive material at facilities, during transport, and during associated activities.

Estimates cite over 20 million consignments of sealed radioactive sources annually, a number that grows significantly with each year. Recognizing the universal importance of such sources, the IPPAS programme first began addressing radioactive sources security in 2007 during a mission in Ghana. Following work to develop such a module, as well as practical experience gained by addressing radioactive sources security during missions in Georgia (2008) and Bangladesh, Finland, Singapore and Turkmenistan (2009), a new IPPAS module titled "Security of radioactive material, associated facilities and associated activities" was officially added to the IPPAS programme in November 2014.

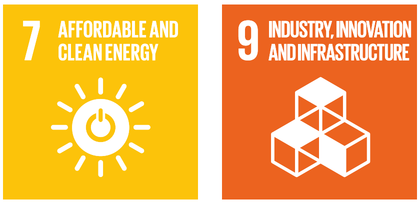

7 AFFORDABLE AND CLEAN ENERGY
9 INDUSTRY, INNOVATION AND INFRASTRUCTURE

Figure 3. Nuclear security enables countries to achieve the United Nations SDGs, and specifically the SDGs 7 and 9.

With the rise of computer-based security events in industrial and government sectors worldwide, the IPPAS programme began in 2011 the development of an information and computer security module. Later that year, an IPPAS mission to the United Kingdom was the first IPPAS mission to feature a review of practices for information and computer security. In 2012, the IPPAS programme was enhanced to include a new comprehensive module on information and computer security. This module includes a review of national policies, looking specifically at computer security regulations, sensitive information assets, and related supply chain security considerations. At the facility level, the computer security review looks at computer security management, access controls, defensive computer security architecture, and other areas.

Cross-cutting nuclear security areas such as risk management, threat assessment, implementation of graded approaches, nuclear security culture, safety-security interfaces and human resource management are assessed as well during an IPPAS mission.

By September 2023, 60 countries in all corners of the world have received an IPPAS mission.

100 nuclear security good practices from 100 IPPAS missions*

Module 1 - National review of nuclear security regime for nuclear material and nuclear facilities

Strategy, policy and nuclear security culture

1. A nuclear security coordination group/council has been established with representatives of all involved agencies, to address and advise on nationwide strategic nuclear security issues.
2. A working group on the physical protection of nuclear material and facilities provides for the coordination and cooperation between the relevant authorities.
3. Detailed Memoranda of Understanding have been developed to establish specific roles and responsibilities of entities involved in the physical protection, and establish procedures and processes to ensure effective communication between those parties.
4. Expectations are documented in the relevant national policy to establish a nuclear security culture programme within the civil nuclear industry sector.
5. Workshops and roundtables are routinely held to develop nuclear security culture in the nuclear industry.
6. A national centre for nuclear security culture has been established to develop and maintain a strong nuclear security culture.
7. The operator conducts regulator on-line surveys to assess the state of nuclear security culture within the organization.
8. Safety, security and safeguards reside within the same regulatory organization, promoting greater synergies between the three regulatory disciplines.
9. The regulator has ‘resident inspectors’ at power reactors and category I facilities, to provide a continuous on-site presence.
10. Stakeholders are routinely involved in the regulatory rule making process, resulting in rule making that is more accepted by stakeholders, and more effective.

Threat assessment and Design Basis Threat (DBT)

11. A regular, annual budget has been established for a working group to assess and identify methods to address insider threats.
12. A nuclear security organization was formed to centralize the employee vetting process and help decompartmentalization of information gathered on nuclear security threats, in order to deliver this information to other relevant ministries.
13. A secure platform has been established for relevant agencies to securely exchange classified information in relation to nuclear security.
14. Clear and effective measures have been established for the designation, storage, transmittal, reproduction, and destruction of sensitive documents.
15. Resources have been established so that any organization with nuclear security repsonsibilities may require their staff to be subject to vetting by the relevant government security office.
16. Close and effective links have been established between the competent authority, intelligence agencies, police, and armed forces to support development of threat assessments.
17. A full time inspector position has been established to assess relevant international threats and to share the information relevant for deciding on the facility operating modes.
18. Strong arrangements and procedures exist to help address and implement any necessary day-to-day changes of the threat level.
19. A two level DBT, one level for the nuclear energy sector and one level for each specific facility, has been established so as to allow consideration of the unique circumstances and considerations in different areas/locations.
20. A DBT is provided to new facilities at the very early phase of project implementation, to apply ‘security by design’ for increasing nuclear security efficiency.

Contingency plans, preparedness and response

21. A high level coordinating body has been established for responding to nuclear safety and nuclear security incidents and for the development of national contingency plans.
22. A security hotline has been established so anyone can report potential nuclear security events.
23. A computerized system has been established whereby, when a call is received on the general emergency number, an alert will automatically advise the responder about the existence of radioactive material in the facility for the deployment of an appropriate response force.
24. Awareness of first responders is strengthened through periodic training and encouraging the public to report any security related observations.
25. Contingency plans for response to nuclear security events are regularly exercised by all license holders and relevant authorities, with a comprehensive, national level joint exercise conducted each year.

* The list of good practices has been extracted from the IPPAS Good Practices Database and edited with the aim to remove any sensitive information pertaining to specific host countries and to facilitate public’s understanding on the technical areas reviewed.

26. ‘Flapsheets’ — clear and concise instructions containing the actions to be taken in the event of nuclear security incidents—have been developed by the operator, negating the need for police personnel to trawl through larger documents when timeliness may be critical to success or failure.

27. A common, encrypted communications system is used throughout the nuclear sector and state security organizations to ensure that there is well-coordinated command and control during emergencies.

28. An emergency operating procedure has been established to provide the main control operator with a procedural guideline to give clear instructions of how to shut down the reactor in the event of an adversary making an intrusion into the vital area.

Module 2 – Nuclear facility review

29. Nuclear material holdings have been consolidated between sites, significantly reducing the nuclear material footprint, associated security requirements, and the risk of theft.

30. The inclusion of yellowcake production and material is subject to prudent management practices.

31. A centralized database has been established to record all personnel either authorized for or denied access to any of its sites, with access rights that can be limited to any (or all) of the nuclear power plants (NPP) sites.

32. The badges/passes of personnel on sick leave, long business trips, or no longer on contract at each site are promptly disabled via the access control system.

33. The facility has a policy to effectively limit the number and type of vehicles that are allowed access to the protected area.

34. An off-site distribution centre has been established to reducing risks to the site by screening deliveries remotely; reducing the number of shipments and deliveries; allowing for secure freight forwarding; and introducing system to improve delivery monitoring, tracking, and communication.

35. A designated guard monitors access to the vital area, thus ensuring immediate detection of possible malicious acts.

36. The operations CCTV system supports the work order permit system and the surveillance of maintenance and service tasks undertaken in sensitive areas of the facility.

37. A system has been established for communicating the status of alarms at the NPP to the local police authorities.

38. The effectiveness of the onsite response forces for the research reactor is regularly tested by multiagency force-on-force exercises.

39. A committee has been established to address physical protection issues in an integrated manner, involving all relevant stakeholders.

40. A security management system has been established including associated plans and procedures as a component of the integrated management system, which has been certified by an independent third party to assure quality.

41. The security culture of the facility has been enhanced by management actions, including the mandatory rotation of duties so that staff experience many different security functions/responsibilities.

42. Security guards accompany operating personnel during walk downs to provide familiarity with normal plant conditions that is useful during an onsite response and support nuclear security culture.

43. Safety and security themed playing cards, with 52 good practices, have been distributed to employees and used to motivate operator personnel to report on safety and security events.

44. Regular benchmarking sessions for physical protection approaches at similar nuclear facilities are used to enhance security awareness and capabilities.

45. Easy to use flowcharts to assess alarms and initiate a response are used by control center operators.

46. A security officer and assistant security officer from the regulatory body are available onsite during public holidays, weekends, and after working hours, providing additional security competencies to the security guard service.

47. The facility undertakes efforts to retain their guard staff, ensuring that persons staffing the security desk are experienced and knowledgeable.

48. The use of a state of the art central alarm station (CAS) simulator that mimics the CAS design and layout is used for the training and qualification of operators.

49. Site specific training is required for all employees and visitors entering the protected area, with relevant physical protection information.

50. Every new employee is required to meet with the security manager, to support the employee’s increased understanding of security issues and measures and for the security manager to become acquainted with the new staff member.

51. Maintenance results are analyzed and equipment and systems are periodically assessed to identify trends and point out potential problems, reducing operation failures, detecting obsolete equipment and allowing anticipation of equipment replacement needs.

52. No-fault, beyond-DBT type scenarios are used during force-on-force exercises and inspections, providing operators and regulators to learn in a less stressful environment.

53. Each vehicle of the off-site response forces is equipped with a personal radiation dosimeter and the off-site response forces are trained to operate them.

54. The information given to the response forces in order to plan and exercise response is not limited to the location of a set of vital areas, but rather based on a defence in depth concept that enables a flexible response.

55. An overall maintenance programme covers the security system components so that they benefit from the same strict maintenance regimes, including preventative ad corrective maintenance, and in-service inspections and periodic testing, as the safety systems.

56. To support the effectiveness of defense in depth for defined areas with graded access authorization levels, the trustworthiness of all personnel is also graded with regards to assigned access authorization.

Module 3 – Transport review

57. Per policy, a transport vehicle driver, in addition to the responsible operator, help to assure continuous security of sources being transported.

58. A dedicated transport control centre and a tracking system to monitor the location of all transports in real time, help assure effective response to nuclear security incidents.

59. International shipments from the border are escorted to their final destination by a car staffed with personnel with a knowledge of the region well and the local language to ensure prompt and efficient communication with response forces, if necessary.

60. A national emergency operations centre is used as a transport control centre during the transport of nuclear material with its communication channels and role in coordinating all stakeholders allowing an effective, secured exchange of security related information.

Module 4 – Security of radioactive material, associated facilities and associated activities

61. A secure national registry, containing detailed information, exists for radioactive sources of categories 1 to 5.

62. Active bilateral cooperation is intensive and provides for a specific mechanism to follow the developments in neighboring States in the field of radioactive sources security through the semi-annual meetings at the Head of State level.

63. Repatriations of disused radioactive sources from the host country and utilization of alternative technologies, where possible, has led to increasing efficiencies through savings of human and financial resources.

64. The demonstrated proactive dissemination of information on nuclear security incidents to the international community, the host country exemplifies a good practice that considerably advances an understanding of existing threats worldwide.

65. International cooperation is used to harness available donor resources, to cover security of radioactive sources.

66. Technical cooperation has been established between intelligence organizations of other States in the region to exchange information about shared threats regarding radioactive sources and events related to such material.

67. Efforts are being made to maintain regulatory control of radioactive sources throughout the country, including transfers and safe storage of sources where the licensee loses control of radioactive sources for any reason, and interaction with companies that possibly possessing unlicensed sources on their premises that predate regulatory control.

68. In cases of portable radioactive sources, the license specifies the exact place(s) of storage to which sources must be returned after usage.

69. The nuclear regulatory authority's board of directors is comprised of representative from each of the primary ministries involved in radioactive sources security, in order to facilitate the development and maintenance of a comprehensive framework.

70. Radiation protection training and seminars are held regularly to share information with first responders, including the background on nuclear security fundamentals and location and type of radioactive sources.

71. The national counterterrorism unit maintains an information package on radioactive sources, providing tactical decision makers with information that would be useful in resolving a nuclear security event at the site.

72. By regulation, the national emergency centre must be activated at least once a year to perform training exercise to test plans for response to radiological emergencies.

73. Customs conduct no-notice, scenario-based radiological security exercises at border checkpoints.

74. Export requests are evaluated using a risk-informed and systematic approach, with particular attention given to the end-use, end-users, safety and security, importing State particulars, final and immediate consignees, as well as other information from open sources, and domestic and foreign watch lists.

75. Radioactive source security during transport has been strengthened by developing and operating a web-based source tracking management system to facilitate the detection and recovery of missing or stolen radioactive sources.

76. A two person rule applies during the transport of radioactive sources off-site, during which time the vehicle may not be parked or abandoned, and all sources must be transferred back to their storage location at the end of each working day.

77. To ensure the security of category 4 and 5 radioactive sources, a declaration of conformity is required from operators assuirng that the transport is carried out in accordance with regulatory security requirements.

78. Prior to the issuance of security regulations for radioactive material, graded security measures were required with redundant and diverse measures for defence in depth, serving as a model also for countries lacking detailed regulations for the nuclear security of radioactive material.

79. A two-person rule and key control management procedures have been established for storage containers for category 4 portable density gauges.

80. Multiple physical barriers and anti-tamper measures inside radioactive source storage containers provide defence in depth and protective layers.

81. Access control is strengthened through the use of multiple, dual authentication systems such as biometric systems and card access readers to control access to restricted areas with high activity radioactive sources.

82. Duress devices have been strategically located to immediately alert security response personnel in the case of security breach, intrusion, or personnel being forced to operate under duress conditions.

83. Tamper indicating devices exist on machines containing high activity radioactive sources in order to deter, detect, and prevent insider threats.

84. A Master's degree programme on nuclear security has been established on the subject of nuclear security of radioactive sources.

Module 5 –Computer security review

85. Good practices, inclusive of gate passes and hard drive encryption, have been established for the removal of computer equipment off-site. All staff, contractors and visitors are required, on entry, to register and seek approval to remove any information assets from the facility.

86. The computer security team is involved in all physical protection procurement and commissioning activities, to ensure appropriate identification and protection of critical digital assets important to nuclear security.

87. The successful implementation of dedicated portable memory sticks that constitute the only means of data transfer in and out of 'stand alone' network environments provide rigorous control of potential malware migration.

88. A comprehensive centralized computer security monitoring centre has been established to collect relevant information from different networks and domains and to assists in the early detection of anomalies or intrusion attempts.

89. National level resources with specialized information and computer security capabilities are made available to support operators and authorities.

90. A facility computer security officer solicits the opinion of safety experts and the information technology (IT) system users when developing computer security measures in order to ensure that the implemented computer security measures do not adversely affect safety measures and the operation of the facility.

91. A facility computer security officer works together with the property/process owner to conduct a threat assessment for each new asset and to determine the appropriate characterization and protective measures prior to placement on the facility network, ensuring minimum exposure to an attack.

92. The NPP site has a dedicated test environment that mirrors the facility target digital environments and allows for the aggressive and effective performance-based testing of strategies for computer security without impacting the safety and security of operating facility systems.

93. The policy of isolating the operation and automation network from external traffic has resulted in a demonstrable decrease in malware occurrences across the more sensitive network.

94. A computer security group and procedures related to group assembly, roles and responsibilities, communication, officers on duty, have been established for NPPs. The NPP computer security group works closely with external national level organizations with cybersecurity responsibilities.

95. A special directorate on computer security has been established to plan, coordinate, and manage the competent authority's computer and information security activities, including a cyber assessment team to monitor threats.

96. The competent authority regularly undertakes a cross departmental information exchange on the development of computer-based threats and vulnerabilities.

97. A performance-based approach, detailed in a cyber DBT and IT security guidelines, provides a flexible framework to prevent and protect nuclear installations from cyber attack.

98. There is a single computer security concept for all vital sectors under one leading competent authority.

99. Information analyses of real world events and potential events in the energy sector, including the nuclear sites, is shared with all relevant computer security authorities and operators.

100. A national level computer security council has been established from different agency stakeholders, academia, and the public and private sectors, in order to share information amongst relevant stakeholders.

Year	Milestone
1995	IPPAS programme established
1996	First IPPAS missions to Bulgaria and Slovenia
1999	First IPPAS guidelines are published as Service Series 3
2012	Training material developed and first national and regional IPPAS workshops held
2012	Information and computer security added to IPPAS missions
2013	First international seminar on sharing experience and good practices from conduct of IPPAS missions
2014	Revised IPPAS Guidelines document published as Service Series 29
2014	First IPPAS international training course conducted for potential IPPAS team members
2016	Establishment of the IPPAS Good Practices database
2021	25 years anniversary since the first IPPAS mission
2023	100th IPPAS mission conducted (Zambia)

Figure 4. Important milestones for the IPPAS programme.

How to request an IPPAS mission

An interested Member State can request a meeting with an IAEA representative to discuss the IPPAS programme. An IPPAS workshop can be also conducted, on request, to provide detailed information on the issues related to IPPAS.

If the Member State decides to proceed, a formal request for an IPPAS mission (through or copied to its Permanent Mission) shall be submitted to the IAEA's Division of Nuclear Security.

The host country should designate a point of contact (name/organization) responsible for further communication with the IAEA on planning the mission and making practical arrangements.

More information on requesting an IPPAS mission can be found in the IPPAS Guidelines: www-pub.iaea.org/MTCD/Publications/PDF/SVS-29_web.pdf

> The IPPAS mission to Kuwait in 2023 was an enlightening experience that highlighted the shortcomings of some practices and areas that require further attention. The expert mission gave excellent advice and recommendations on best approach, suggestions and resolutions to those shortcomings. Some of the recommendations, in general, touch on developing and/ or enhancing of quality assurance programme, integrated management system, risk assessment. One of the highlights of the mission was pointing out the ambiguity of responsible body when it comes to nuclear security and risk management, and the overlap of responsibilities between different government bodies, which hopefully be fixed with amendments to current regulations. In the future, these recommendations will be taken into serious consideration to further upgrade and enhance regulatory structure in Kuwait. The mission highlighted as well some best practices that Kuwait applies in its regulatory system."
>
> **Elham Al Fares,** Director, Radiation Protection Department, Kuwait

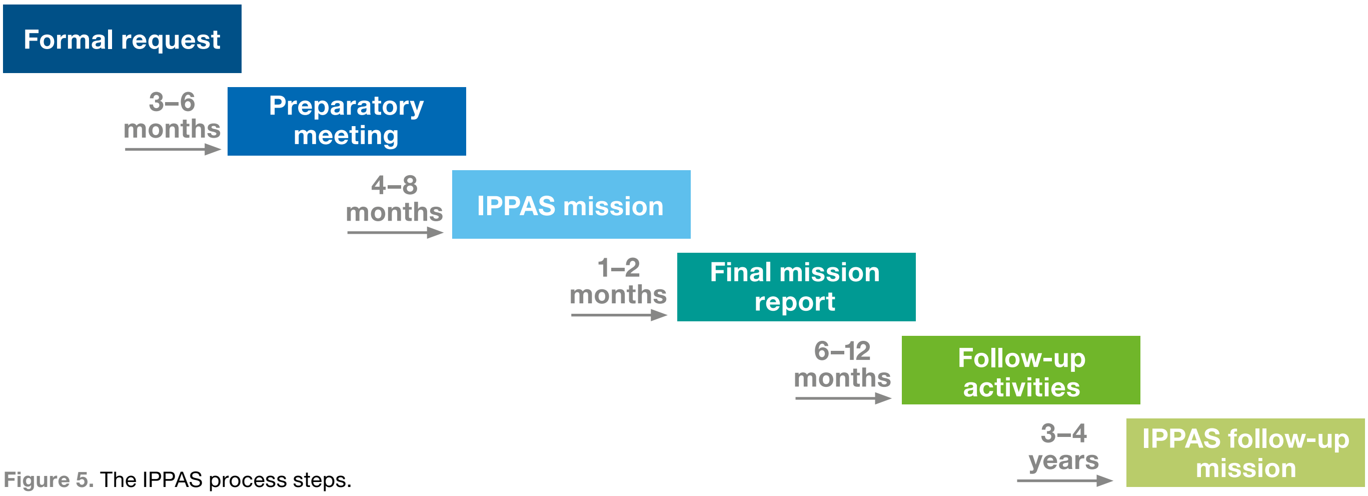


Figure 5. The IPPAS process steps.

How to become an IPPAS international team member

Responding to the growing demand for IPPAS missions, the IAEA has developed a range of information sharing platforms on the various aspects of requesting, planning, and conduct of an IPPAS mission.

With the aim to ensure the availability of geographically and subject-matter international experts for future IPPAS missions, the IAEA regularly conducts informational training courses for interested potential IPPAS experts. There have been more than 35 national and regional workshops and training courses held to date, hosting hundreds of participants. Examples of previous such informational workshops and training courses focused on sharing best practices and information on IPPAS, included:

- a series of International Seminars on IPPAS –France (2013), United Kingdom (2016); Austria (2021)
- a series of International Training Workshops for IPPAS potential new team members in Austria (2014, 2015, 2017, 2019, 2023).

> "The scope of the 100th IPPAS mission in Zambia was to review the security of radioactive materials, implementation of nuclear security measures at the radiotherapy, scientific and industrial research and interim radioactive waste facilities. Additionally, to review and evaluate practical security arrangements for transport of radioactive materials. This in line with the National Nuclear Policy for 2020 which requires Zambia to comply with all regional and international treaties and conventions pertaining to nuclear programmes and ensure that nuclear safety and security, environmental protection, safe management of radioactive waste, and compliance with international conventions, treaties and protocols relevant to the application of nuclear science and technology are adhered to. The Zambian Government has committed to addressing the various short, medium and long term milestones as recommended by the IAEA through missions such as the IPPAS. During the mission, a team of international experts provided recommendations which Zambia is expected to implement to enhance its nuclear security regime."
>
> **Melody M Nsofwa,** Manager, Department of Nuclear and Radiation Safety, Radiation Protection Authority, Zambia

Members of the IPPAS team visited the Cancer Diseases Hospital in Lusaka during the IPPAS mission in Zambia. (Photo: Radiation Protection Authority, Zambia)

IPPAS good practices database

The IAEA has maintained the IPPAS Good Practices Database since 2016 to share the findings of such missions with the international nuclear security community. Maintaining this database and sharing such examples with respect to confidentiality extends the benefits of IPPAS missions beyond the host country to the international nuclear security community, and multiplies the impact of the assistance offered by the IAEA to its Member States.

Currently the database includes 532 good practices, a result of 90 IPPAS missions conducted until the end of 2019. The database is accessible for designated Points of Contacts of the Member States.

> “Japan hosted an IPPAS mission in 2015 and its follow-up mission in 2018. In response to the IPPAS findings, we decided to strengthen the computer security measures and increase the number of inspectors with expertise in the field. In addition, the Nuclear Regulation Authority incorporated computer security threats in its national threat assessment and required licensees to take robust computer security measures, as well as to enhance the content of their computer security plans by incorporating countermeasures against cyberattacks. In spite of the preparation time and effort required to host the IPPAS missions, it was a valuable experience for Japan to review the status of nuclear security measures through IPPAS missions and to promote their enhancement based on the provided recommendation and suggestions.”
>
> **Hiroyuki Sugawara,** Director for International Nuclear Security in the Division of Nuclear Security, Nuclear Regulation Authority, Japan

Good practices by module

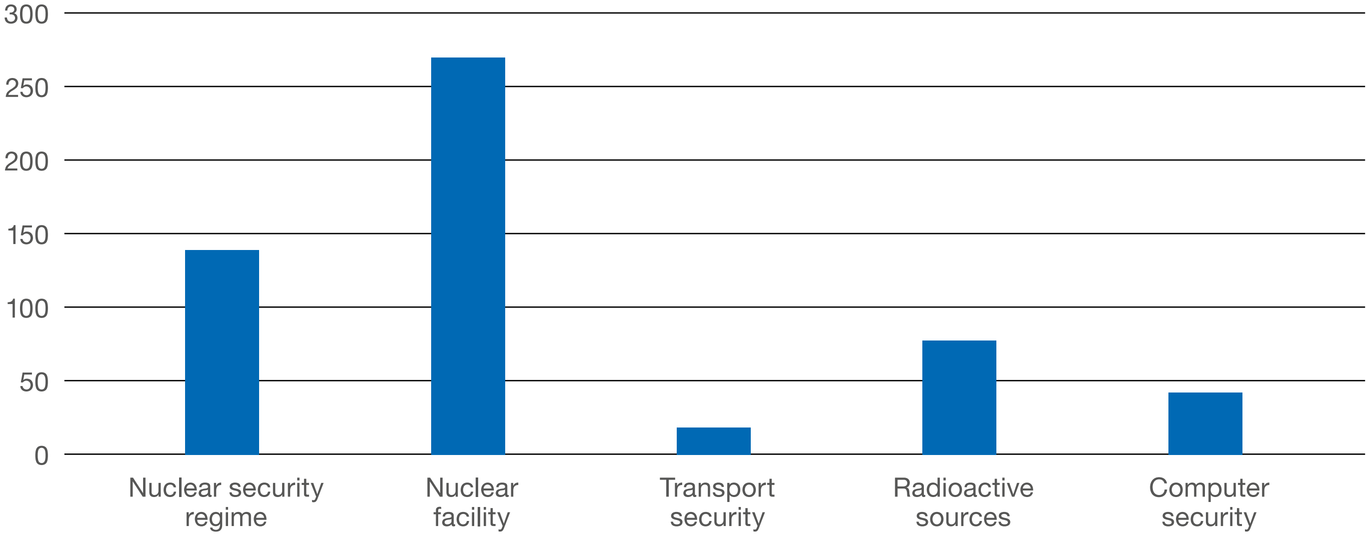
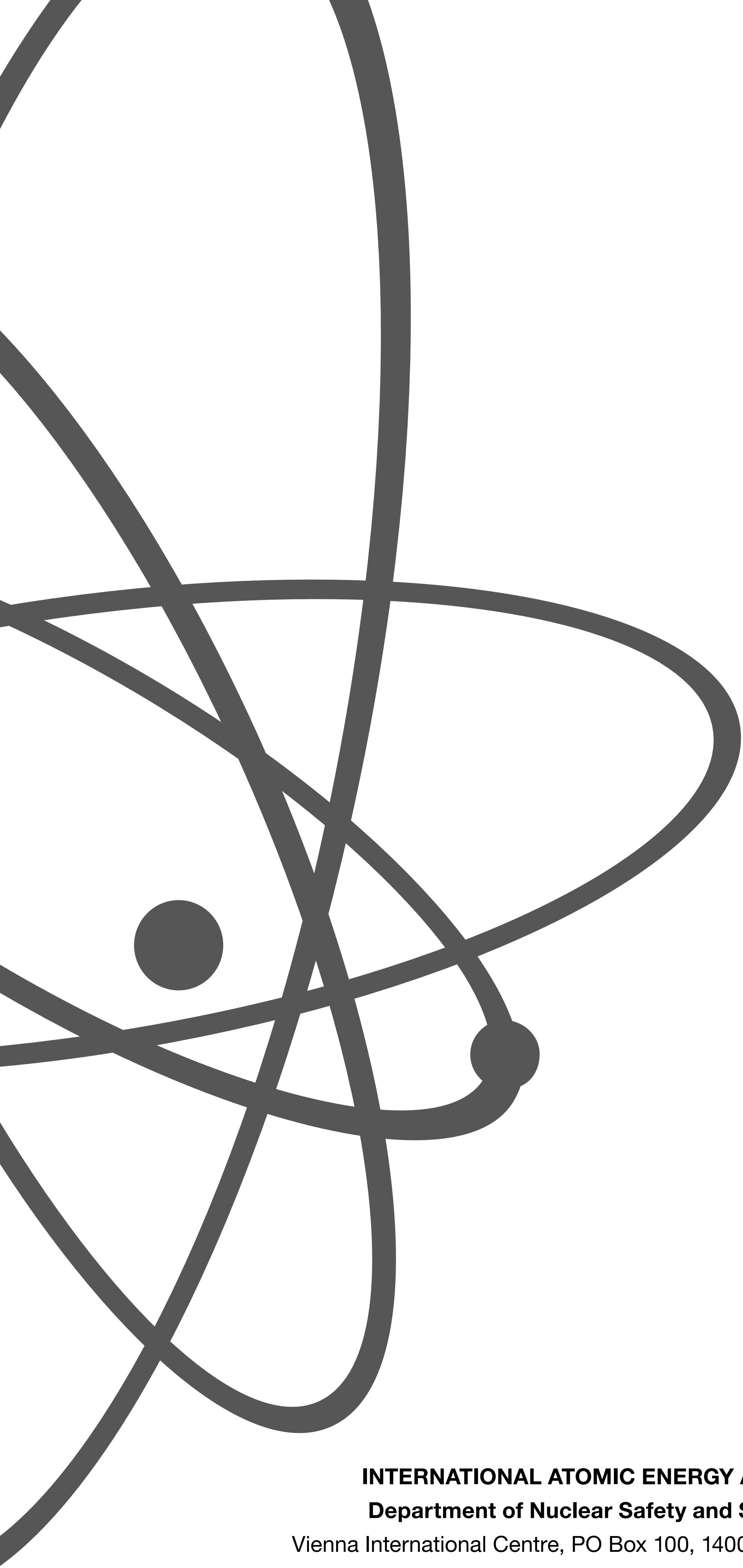


Figure 6. Number of good practices identified per IPPAS module.

Interested in becoming an IPPAS international team member?

Each Member State nominates individuals with relevant technical backgrounds to serve on IPPAS missions. Please contact the nuclear regulatory body in your country for more information.

Photos: IAEA and Member States



INTERNATIONAL ATOMIC ENERGY AGENCY
Department of Nuclear Safety and Security
Vienna International Centre, PO Box 100, 1400 Vienna, Austria
www.iaea.org/ns | Official.Mail@iaea.org

23-03843E