IAEA 60 Years
Atoms for Peace and Development

Information Circular

INFCIRC/908
Date: 9 January 2017

General Distribution
Original: English

Communication dated 22 December 2016 received from the Permanent Mission of the United States of America concerning a Joint Statement on Mitigating Insider Threats

Joint Statement on Mitigating Insider Threats

1. The Secretariat has received a communication dated 22 December 2016 from the Permanent Mission of the United States of America on behalf of the Governments of Armenia, Australia, Belgium, Canada, Chile, Czech Republic, Finland, Georgia, Germany, Hungary, Israel, Italy, Japan, Jordan, Kazakhstan, Republic of Korea, Mexico, Morocco, the Netherlands, Nigeria, Norway, Romania, Spain, Sweden, Thailand, the United Kingdom and the United States of America, and of INTERPOL, requesting the Secretariat to bring the communication and its attachment to the attention of all IAEA Member States.

2. As requested, the communication and its attachment are herewith circulated for the information of all Member States.

030/2016

NOTE VERBALE

The Permanent Mission of the United States to the United Nations Organizations in Vienna presents its compliments to the International Atomic Energy Agency and, on behalf of the Governments of Armenia, Australia, Belgium, Canada, Chile, Czech Republic, Finland, Georgia, Germany, Hungary, Israel, Italy, Japan, Jordan, Kazakhstan, Mexico, Morocco, the Netherlands, Nigeria, Norway, Republic of Korea, Romania, Spain, Sweden, Thailand, United Kingdom, United States and INTERPOL, has the honor to request that the IAEA Secretariat bring the following note verbale and its attachment to the attention of all IAEA Member States.

At the IAEA International Conference on Nuclear Security: Commitments and Actions, the United States, as sponsor of this Joint Statement, announced that it will be open for all Member States to subscribe to the goals and commitments as described. IAEA Member States wishing to subscribe to this Joint Statement on Mitigating Insider Threats are encouraged to notify the United States and inform the IAEA Secretariat via note verbale, and request such official communication be circulated as an INFCIRC document to all IAEA Member States.

The Permanent Mission of the United States avails itself of this opportunity to renew to the IAEA assurances of its highest consideration.

Attachment: Joint Statement on Mitigating Insider Threats

United States Mission to the International
Organizations in Vienna,
December 22, 2016.

Joint Statement on Mitigating Insider Threats

This joint statement records the intent of Armenia, Australia, Belgium, Canada, Chile, Czech Republic, Finland, Georgia, Germany, Hungary, Israel, Italy, Japan, Jordan, Kazakhstan, Mexico, Morocco, the Netherlands, Nigeria, Norway, Republic of Korea, Romania, Spain, Sweden, Thailand, United Kingdom, United States and INTERPOL to establish and implement national-level measures to mitigate the insider threat.

Insiders generally possess access rights which, together with their authority and knowledge, grant them far greater opportunity than outsiders to bypass dedicated nuclear and radiological security elements or other provisions such as safety systems and operating procedures. Insiders, as trusted personnel, are capable of methods of defeat that may not be available to outsiders. As such, insiders—acting alone or in concert with outsiders—pose an elevated threat to nuclear security.

To establish an integrated, graded approach to mitigating insider threats, nuclear and radiological security programs should include national-level and agency- or facility-specific Insider Threat Mitigation policies and programs, training and awareness activities, and collaboration between facility-level organizations. The Insider Threat Mitigation Program should include strong control and accountability measures for special nuclear material that rigorously assess and continually monitor insider human reliability, deter insiders from theft/diversion, limit their access, and provide prompt detection of theft/diversion.

1. **States commit to supporting the International Atomic Energy Agency (IAEA) to develop and implement an advanced, practitioner-level training course on preventive and protective measures against insider threats.**

The IAEA, with the assistance of Member States, has developed and implemented a basic training course to help mitigate insider threats. With support from partner Member States, and in response to IAEA basic insider threat mitigation course participant survey responses, States will support the IAEA with the development of an advanced, practitioner-level training course on preventive and protective measures against insider threats. This more advanced course will provide member states with hands-on training, guidance documents and related self-assessment and training materials. Similar in format to the IAEA's International Training Course on Physical Protection, the course could be piloted in Member States with appropriate facilities, and then transitioned to Nuclear Security Support Centers and Centers of Excellence (NSSC/COEs) in partner

States. The training course will focus on physical protection of materials, facilities, and sensitive information from insider threats, as well as Nuclear Material Accounting and Control (NMAC), trustworthiness program, nuclear security culture, and other methodologies to protect against theft of nuclear materials and sabotage of facilities. Future instructors from NSSC/COEs would receive special preparatory training, and then help teach the pilot course and both regional and national NSSC/COEs may adapt the courses as appropriate to meet the threat-based needs of the Member States.

2. **States will implement measures to mitigate insider risks using a risk-informed graded approach by taking actions that may include one or more of the following:**

- Developing and implementing a national-level policy on insider threat mitigation, identifying all relevant stakeholders and information sources, and implementing agency-specific training and education.
- Developing or maintaining an outcome focused regulatory approach that will assist those responsible to think more holistically about security risks and mitigations.
- Taking specific steps to facilitate collaboration and information sharing among relevant national organizations (e.g., facility security, human resources, personnel security, national security, counter-intelligence and law enforcement).
- Establishing or strengthening NMAC programs for nuclear security purposes, and regulations for implementation, including, for example,

    - Systems to identify nuclear material status, movement, and changes. These may include appropriate NMAC software, secure electronic data transfer between facilities and to the national or regional level, and established national- or regional-level plans to respond to suspected theft/diversion;
    - Facility-level Material Control & Accountability (MC&A) programs to detect theft/diversion through modern nuclear material accounting system software, including peer review of software;
    - Regional-, National-, and facility-level programs to conduct performance tests, self-assessments and peer reviews to assess and enhance effectiveness of insider threat mitigation programs to include NMAC systems.

- Establishing a nuclear security regime for protection of materials and facilities from insider activities, including, for example:

    - Development and implementation of a training program to mitigate insider risk to include topics such as the importance of the individual in recognizing and preventing insider threats; physical protection systems used to secure

materials at facilities and in transit; insider analysis, prevention, and mitigation; and how to develop trustworthiness programs;
  - Physical protection systems used in protection of materials and facilities;
  - Nuclear security culture;
  - Methodologies to protect against protracted and abrupt theft of nuclear materials;
  - Procedures for materials transfer;
  - Protection of materials at the target;
  - Access (e.g. two-person) rules and other administrative and technical measures against insider threats;
  - Defined physical protection design objectives and/or measures as they relate to sabotage and the potential insider threat; and
  - Maintaining good cyber hygiene procedures such as protective monitoring on cyber estate and ensuring user privileges are relevant and appropriate to their current role.

- Establishing insider trustworthiness programs that can include:
  - Defining eligibility requirements;
  - Clearly identifying and documenting roles and responsibilities;
  - Conducing background checks;
  - Initial and ongoing:
    - Vetting of personnel by law enforcement agencies;
    - Medical and psychological testing;

- Drug and alcohol testing;
  - Detecting and reporting aberrant behavior;
  - Process for no-fault self-reporting any condition that may affect an individual's ability to conduct security responsibilities and for reporting any other security concerns;
  - Providing personnel assistance programs to help mitigate life stressors that can impair ability to conduct security duties; and,
  - Regular security awareness training, including cyber security.