Nuclear Security Summit, Seoul, March 2012: Multinational Statement on Nuclear Information Security

1. In the principal communiqué here at the Nuclear Security Summit in Seoul, all participants reaffirm their commitment to the security of nuclear information as follows:

> We recognize the importance of preventing non-state actors from obtaining information, technology or expertise required to acquire or use nuclear materials for malicious purposes, or to disrupt information technology based control systems at nuclear facilities. We therefore encourage States to: continue to develop and strengthen national and facility-level measures for the effective management of such information, including information on the procedures and protocols to protect nuclear materials and facilities; to support relevant capacity building projects; and to enhance cyber security measures concerning nuclear facilities, consistent with the IAEA General Conference Resolution on Nuclear Security (GC(55)/Res/10) and bearing in mind the International Telecommunication Union Resolution 174. We also encourage States to: promote a security culture that emphasizes the need to protect nuclear security related information; engage with scientific, industrial and academic communities in the pursuit of common solutions; and support the IAEA in producing and disseminating improved guidance on protecting information.

2. Without prejudice to the peaceful uses of nuclear energy, we the parties to this additional statement on nuclear information security, declare our further commitment to:

    a. Developing and strengthening our national measures, arrangements and capacity for the effective management and security of such information;

    b. Enhancing our related national security culture;

    c. Engaging with our national scientific, industrial and academic communities to further raise awareness, develop and disseminate best practice, and increase professional standards;

    d. Supporting, drawing on and collaborating with the IAEA, other key international organizations and partner countries to facilitate mutual achievement of these aims.

3. In particular we commit to action including some or all of the following, as appropriate to our national contexts, standards and frameworks:

    • Conduct of a national assurance exercise to help identify strengths and areas for development in the current practice of information security;

    • Development and/or optimization of a set of national guidance and grading systems for nuclear information security, including on what information can be publicly disclosed;

    • Implementation into national practice of the IAEA's guidance on Computer Security at Nuclear Facilities and its expected improved guidance on the Protection and Confidentiality of Nuclear Information;

- Full national implementation of information security-related elements of international instruments such as UNSCRs 1540 and 1887 and, as appropriate, of export control regimes that assist in regulating material and technology transfers;

- Recognition of the important role of industry in promoting and exchanging best practice as appropriate, including the promotion of the reflection in to national practice of best practice guides related to nuclear security culture and communicating nuclear security information;

- Promotion of the reflection in to national practice of international standards related to information security and cyber security, such as those produced by the International Organisation for Standardisation and the International Telecommunication Union;

- Further development of national expertise and skill levels in the practice of nuclear security, including information security, by drawing on the increasing opportunities offered by the IAEA's International Nuclear Security Education Network and other international organizations;

- Further improvement of security culture and information security practice through training or other professional development activities provided via existing or planned national and regional Nuclear Security Support Centres/Centres of Excellence;

- Development and implementation of national legislation and/or regulation as necessary to ensure that all nuclear industry staff are vetted for security purposes to a high standard;

- Specific provision in training or other professional development activities for raising awareness and skill levels among industrial security practitioners to reduce potential risk from the 'insider threat';

- Encouragement and facilitation of the elaboration and implementation of ethical codes or other self-governance pledges on information security within the nuclear scientific and academic communities, including those working in dual-use areas;

- Development of government processes to monitor and control the export of nuclear information, knowledge and expertise from academic institutions, in line with international obligations as appropriate;

- Encouragement of the formation of professional communities of interest to facilitate further outreach, discussion, promotion and research of best practice in information security.

Nuclear Security Summit, Seoul, March 2012

Multinational statement on Nuclear Information Security

Parties to the Statement

Algeria
Australia
Canada
Chile
Czech Republic
Finland
France
Georgia
Germany
Hungary
Indonesia
Italy
Japan
Kazakhstan
Malaysia
Mexico
Netherlands
New Zealand
Norway
Philippines
Poland
Republic of Korea
Spain
Sweden
Switzerland
Thailand
Turkey
United Arab Emirates
United Kingdom
United States of America
Viet Nam

31 in total