Nuclear Security Summit, The Hague, March 2014

Statement on Nuclear Information Security: Progress update

35 States[1] have supported the Multinational Statement on Nuclear Information Security.

The initiative recognised the fundamental need to protect the sensitive nuclear information, technology and expertise necessary to acquire or use nuclear materials for malicious purposes, or to disrupt information technology based control systems at nuclear facilities.

Ahead of the 2014 Nuclear Security Summit, the supporting States have reaffirmed the importance of comprehensive action to ensure the effective protection of sensitive nuclear information, and their commitments to:

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

b) Enhancing their related national security culture;

c) Engaging with 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.

In this context, the supporting States note:

- the IAEA's recognition that information security measures are a fundamental element of a State's nuclear security regime (*Nuclear Security Series 20*) and its forthcoming publication *Protection and Confidentiality of Sensitive Information in Nuclear Security*.
- the European Union Council's Conclusions on *The challenges presented by the proliferation of weapons of mass destruction and their delivery systems* recognising the need to protect sensitive knowledge and know-how.
- the Global Partnership Against the Spread of Materials and Weapons of Mass Destruction's inclusion in its 2013 work programme discussion of good practices in securing sensitive information.

The supporting States also note:

[1] Algeria, Australia, Belgium, Canada, Chile, Czech Republic, Finland, France, Georgia, Germany, Hungary, Indonesia, Israel, Italy, Japan, Kazakhstan, Malaysia, Mexico, Morocco, Netherlands, New Zealand, Norway, Philippines, Poland, Republic of Korea, Romania, Spain, Sweden, Switzerland, Turkey, Ukraine, United Arab Emirates, United Kingdom, United States of America and Viet Nam.

- the role of the nuclear Industry in ensuring effective and comprehensive protection of sensitive information, and the holding of the 2014 Nuclear Industry Summit.
- the World Institute for Nuclear Security's publication *Best Practice Guide on Information Security for Nuclear Operators*.

Responsibility for nuclear security within a State rests entirely with that State, and action to strengthen national nuclear security regimes further needs to take place in a manner appropriate to the national context.

The supporting States encourage further and ongoing action by all States to ensure the effective protection of sensitive information, technologies and associated facilities.

As sponsor of the 2012 Multinational Statement, the UK is pleased to provide an update on some of the voluntary measures taken by supporting States in line with their commitments (Annex A).

Annex A

Australia: The Australian Government Protective Security Policy Framework sets out comprehensive security measures to protect sensitive information from unauthorised use, accidental modification, loss or release. Australia has focused on strengthening national arrangements for information security. This included the introduction of legislation for nuclear technology export controls, development of a facility-level insider threat strategy and the inclusion of a cyber-security component to the national design basis threat. Australia has also started to develop detailed guidance for the classification of nuclear security-related information. Australia's recent IPPAS mission included a review of arrangements for information security and cyber security at nuclear facilities.

Belgium: Belgium recently strengthened and updated its nuclear security legal and regulatory framework, notably with regards to the protection of sensitive nuclear information. The Cyber Security Centre for Belgium, under the authority of the Prime Minister, will be established during the course of 2014. Belgium already took the issue of information security into account by extending the scope of the "stress-tests" set up by the EU after the Fukushima accident to cyber-attacks. Steps will be undertaken with a view to a Design Basis Threat addressing the cyber security threat.

Canada: Through its regulatory body, the Canadian Nuclear Safety Commission (CNSC), Canada has established practices for information security. Among other ongoing steps Canada: is establishing national standards for the protection of electronic data and data systems that will align with the IAEA guidance and best practices; controls the export of nuclear technology under the Nuclear Safety and Control Act (NSCA); collaborates with industry in advancing best practices including to foster an enhanced nuclear security culture; is developing a national standard for cyber protection; and has established regulations and procedures for the vetting and supervision of all nuclear industry staff.

Czech Republic: The Czech Republic recognises the importance of the issue of nuclear information security and UNSC Resolution 1540. The Czech Republic participates in the IAEA initiatives on the issue of sensitive information relating to dual-use exports and the Czech Chamber of Commerce organize educative events. The National Security Authority is the authority for issues of cyber security. The State Office for Nuclear Safety is responsible for Computer Security at Nuclear Facilities and is preparing new legislation in accordance with IAEA recommendations. A governmental coordination agency has been established to respond to computer incidents, namely the Computer Emergency Response Team which operates under the National Cyber Security Centre.

Finland: Finland's gift included developing national requirements and raising awareness of nuclear information security issues both nationally and internationally. Activities in 2013 included: setting up new requirements for operators to enhance nuclear information security posture in Finland as part of new regulatory guide, conducting national joint information security exercises, hosting an IAEA international nuclear security culture workshop, publishing Finland's Cyber Security Strategy, participating in the development and conduct of IAEA training courses in nuclear security and in the development of academic educational programs in nuclear security in cooperation with the IAEA, promoting the EU CBRN action plan related to vetting procedures.

France: Since the NSS 2012, France has initiated a revision of its legislation and guidance on the protection of sensitive information, to update them. A law on cyber-security was adopted in December 2013 as well as new regulation on the protection and control of nuclear materials. The National Agency for Information System Security (ANSSI) is elaborating guidance defining precise requirements for cyber security in vital infrastructures. A review of the implementation of confidentiality rules by operators is to be carried out, with regards to IAEA guidance and French provisions. France encourages its operators to get involved in the IAEA's working groups on the security of information: 2 of them made presentations during the 2013 Conference on Nuclear Security.

Georgia: Georgia has taken a range of measures to strengthen nuclear security culture and nuclear information security practices. Activities have included participating in the EU CBNR Centres of Excellence initiative and hosting a regional secretariat for South East Europe, South Caucasus, Moldova and Ukraine. Georgia together with US partners implemented RIS (Radiation Information System) for taking proper control over all sources of ionizing radiation. Georgia's Integrated Nuclear Security Support Plan continued to be developed. Georgia fully recognises the need to fully implement UNSCRS 1540 and 1887 and taking relevant measures toward.

Hungary: Hungary has developed a comprehensive, systematic and graded approach for the classification and management of sensitive national information in line with the consequences of the disclosure thereof. Based on the IAEA recommendations and guidance, Hungary has prepared a national guideline, entitled „Protection of programmable systems and components in nuclear facilities", which was identified as a good practice by the IPPAS mission hosted by Hungary in 2013. For further enhancing the IT and ITC security, Hungary requested the IAEA to provide a "National Cyber Security Workshop" in June, 2014 for 20-30 participants from competent authorities, licensees and support organizations.

Italy: In January 2013, within the framework of actions to protect sensitive nuclear information, technology and expertise, Italy enacted legislation defining the institutional architecture for managing national security and protecting critical infrastructure, in particular reinforcing protection against the threat of cyber attacks. The architecture foresees three different levels of responsibility and intervention: policy-making and strategic coordination for the development of the national plan; coordination activities to facilitate decision-making and promote the general aims of the legislation; crisis management to define and coordinate response and restoration activities involving all stakeholders.

Japan: Japan's Nuclear Regulation Authority established in 2012 gives operators' guidance on setting clear standards regarding the rigidness of information management and checks operators' procedures at annual physical protection inspections. As a member of all the international export control regimes and a responsible country that implements the UNSCR 1540 and 1887, Japan has been implementing export control of information-security-related items and technologies. The Integrated Support Center for Nuclear Nonproliferation and Nuclear Security of the Japan Atomic Energy Agency provides training programmes and seminars domestically and internationally. Introducing a legal system to check trustworthiness of personnel is now being considered.

Morocco: Under the GICNT, Morocco, in its capacity as chair of RMWG is supportive of sharing information as a GICNT fundamental principle between and among GICNT partner states, the IAEA and relevant international organisations particularly with regard to safety and security incidents involving the use of nuclear and radioactive materials. Any voluntary initiative aimed at building capacity in the field of securing sensitive information particularly in the instance of a cyber attack is welcomed, bearing in mind that the effective protection of sensitive nuclear information fall under the responsibility of relevant state institutions.

Netherlands: In 2011, the Dutch government installed a National Cyber Council. In this Cyber Council public and private parties work together to provide information on relevant developments in the field of digital security. Following this Cyber Council the National Cyber Security Center was established in 2012. This Cyber Center provides advice on how cyber incidents can be avoided and can be detected. An updated version of the National Cyber Strategy was also published last year (2013). In 2013, a Design Basis Threat (DBT) has been approved for the nuclear sector. This DBT will be implemented by the nuclear industry by the end of March 2014.

New Zealand: The New Zealand gift included raising the profile of nuclear information security issues among domestic stakeholders and improving the national implementation of best practices. Ongoing activities have included revision of national Codes of Safe Practice relating to nuclear information security, identification of relevant training opportunities for practitioners and preparations for a future mission to New Zealand by the IAEA International Physical Protection Advisory Service.

Norway: Since the Seoul Nuclear Security Summit 2012, Norway has made progress on nuclear information security. The Norwegian Radiation protection Authority performed in 2012 an audit on nuclear information security measures taken by the operator of the two research reactors. The audit showed that information security procedures were in place and that several measures were taken to prevent such information to be compromised. However there is need for improvements. In this regard Norway is looking closely to the NSS guidelines being issued by the IAEA on information security. At present the whole system of nuclear security is under revision. All regulations and guidelines will be revised in the coming years, well aided by the IPPAS mission that will be conducted in 2015.

Republic of Korea: The Republic of Korea has the up-to-date national system for the effective management of sensitive information. In December 2013, Korea reflected IAEA guidelines on computer security in its national regulations. Korea has been implementing information security-related measures within the framework of export control regimes. In August 2012, Korea launched the Nuclear Export Promotion Service (NEPS), a one-stop online portal which facilitates effective controls on nuclear technology and sensitive information as well as nuclear related items. Korea has also contributed to strengthening discussions on the protection of critical information infrastructure (CII) by producing Seoul Framework and Commitments at the Cyberspace Conference in October 2013.

Romania: In 2013, Romania continued to stress the importance of comprehensive action to ensure the effective protection of sensitive nuclear information. Therefore, a national training course in Computer and Information Security for Nuclear Facilities was organized in Romania, in July 2013, and a national workshop on nuclear security culture has been planned for March 2014, under the Practical Arrangements between the IAEA and the National Commission for Nuclear Activities Control on cooperation in the area of nuclear security.

Switzerland: The Swiss gift basket included a pledge to identify strengths and areas for development in information security. Activities in 2013 included: a National Strategic Leadership Exercise 2013,

testing crisis management of the Swiss Government, which resulted in a report. A professional development training activity organised between the Information Security Officer and the Safety Officer of the Nuclear Power Plants and improving the information exchange and application of best practice between the operators of Swiss nuclear power plants and regulators.

United Arab Emirates: The Critical Infrastructure and Coastal Protection Authority (CICPA) established an Information Protection Program Operating Manual (IPPOM). This defines how relevant entities in the nuclear sector should manage sensitive information. Regulations issued by the Federal Authority for Nuclear Regulation (FANR) for the physical protection of nuclear materials and facilities require that operators develop and implement a Cyber Security Plan to protect against cyber-attack. The nuclear industry is developing these based on international guidance. National regulations for the security of high-activity radioactive sources require the effective management of sensitive information as well as personnel background checks. The UAE will host an IAEA national workshop on cyber security in 2014.

United Kingdom: The UK gift included raising awareness of nuclear information security issues, and promulgating good practices. Activities in 2013 included: hosting discussion meetings in partnership with the Royal United Services Institute, Dutch Embassy and Kings College London, presenting at a meeting of the Global Partnership Against the Spread of Materials and Weapons of Mass Destruction, delivering a conference paper at the 2013 IAEA International Nuclear Security Conference, contributing to IAEA nuclear security guidance with experts from other States, and the UK 2013 UNSCR1540 National Action Implementation Plan highlighting measures to protect sensitive information effectively.

United States of America: Creating a cyber-security directorate and issuing industry regulations to enhance computer security at nuclear facilities; participated in WINS workshop on information security; conducting bilateral exchanges and seminars on best practices in information and personnel security; developing and implementing nuclear security culture training materials; developing guidance, with others, on the Protection and Confidentiality of Nuclear Information; and chairing the IAEA Technical Meeting on the development of “Protection and Confidentiality of Sensitive Information in Nuclear Security.” Also steps taken to develop an insider threat program for classified information and security background checks for licensees handling non-classified information related to sensitive nuclear information.

Viet Nam In Viet Nam, the awareness of nuclear information security was raised through national workshops. Activities in 2013 included: holding a national workshop, in collaboration with the US

DOE on the IAEA Security Series INFCIRC 225/Rev.5, in which Fundamental Principle L – Confidentiality was highlighted; holding, in cooperation with the IAEA a workshop on DBT development methodology, in which protection of information of nuclear security related was emphasised.

EU: The EU encourages member States to ensure that nuclear operators are informed on a need-to-know basis about potential threats. In the absence of a process to quickly transfer security related information, States should consider establishing one. Under the EU CBRN Risk Mitigation Centres of Excellences Initiative, an international project is currently being implemented aiming to develop procedures and guidelines for the creation and improvement of CBRN related information management and exchange systems and to facilitate exchange of best practice. The EU supports the IAEA and contributes to enhancing national responses to cyber-crime. The last CD VI has a budget of approximately 8M Euros.